
Contribuições no Documento Opine - Aqui

Número: OP-944113

Data: 02/06/2025 - 18:36

Resumo: :".", "940688": "a custódia da identidade é obrigação do estado, ninguém mais que o estado teria que ter esses dados, sei lá se esses dados são mesmo criptografados, ou se vão terminar sendo vendidos e por conseguinte minha identidade será suplantado", "940690": "idem anterior", "940693": "não pode ser obrigatório numa sociedade democrática a biométrica como é agora, e só uma tecnologia pública pode fornecer para as empresas esse serviço", "940695": "para situações e trâmites importantes teria que haver uma sala especial de biometria nos poupatempo que sirva como segurança extra onde um funcionário público possa conferir também que essa pessoa que está por fazer a biometria é a mesma pessoa", "940697": "", "940699": "", "940700": "", "940701": "tecnologias mistas, descentralizadas, com centralizadas, etc", "940702": "", "940704": "", "940707": "NÃO SE PODE RESTRINGIR NENHUMA FUNCIONALIDADE, a pessoa tem que ter direito no último caso de ir a um estabelecimento físico a fazer esse trâmite importante e ponto, não podemos ser reféns do mundo digital, e dos hackers", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": "

Contribuinte: LISANDRO VALENTINO BAREMBERG

Número: OP-945269

Data: 04/06/2025 - 17:05

Resumo: : "Devem ser consideradas a coleta de características físicas e/ou comportamentais da pessoa natural que sejam capazes de identificá-las em relação às outras. Por exemplo: voz, íris, impressões digitais, reconhecimento facial, medidas físicas, odores e demais movimentos corporais.", "940688": "Informar os titulares sobre a necessidade de coleta e armazenamento dos dados biométricos a serem coletados e como esses dados serão utilizados e onde estarão armazenados, além de quem poderá ter acesso a esses dados. Inclusive sobre a possibilidade de exclusão dos dados após o uso, se for o caso.", "940690": "A biometria comportamental deve ter uma finalidade específica para que seja justificado sua coleta e que seja declarada a necessidade desse tipo de dado devido ao fato de serem dados extremamente sensíveis por serem capazes de identificar os indivíduos de uma maneira inequívoca.", "940693": "É necessário que a informação seja disponibilizada de maneira adequada aos direitos fundamentais previstos na Constituição Federal. Deve-se priorizar uma linguagem acessível com palavras de uso corrente no português brasileiro. O consentimento pode não ser adequado em contextos de segurança pública.", "940695": "É preciso garantir a segurança do armazenamento e tratamento dos dados biométricos por meio da utilização de servidores

seguros e uso de criptografia. Além da responsabilização proporcional ao dano pessoal ou coletivo em caso de incidentes de segurança.", "940697": "Os controladores devem assegurar o respeito aos direitos fundamentais previstos no ordenamento jurídico brasileiro e a utilização desses dados de forma restrita aos casos estritamente necessários conforme a legislação nacional acerca da proteção aos dados pessoais.", "940699": "Deve-se limitar o tratamento de dados biométricos quando esses dados sejam oriundos de titulares menores de 18 anos e/ou oriundos de indivíduos pertencentes a grupos sociais em situação de vulnerabilidade socioeconômica e socioambiental, como comunidades indígenas ou quilombolas, por exemplo.", "940700": "Deve-se utilizar servidores nacionais para o tratamento de dados a fim de evitar enriquecimento ilícito do setor privado com os dados biométricos coletados por tecnologias de reconhecimento facial. Deve-se seguir as regulamentações definidas por lei e cumprir a ética profissional institucional.", "940701": "Os sistemas de reconhecimento facial devem ser projetados conforme os princípios legais previstos no ordenamento jurídico nacional de forma a garantir a diversidade regional e étnica na criação do banco de dados e a participação multissetorial na criação e implementação desses sistemas.", "940702": "Em contextos educacionais e de saúde, os usos de tecnologia de reconhecimento facial não devem ser utilizados em nenhuma hipótese devido à ameaça à liberdade de expressão e à dignidade da pessoa humana. Nestes casos deve-se utilizar a identificação por senhas pessoais.", "940704": "Deve-se realizar verificações periódicas sobre a segurança do processo completo de coleta, armazenamento e tratamento de dados. Incluindo testes de segurança e correção de vulnerabilidades identificadas. Garantir que os dados sejam anônimos e não seja possível o acesso externo sem autorização legal.", "940707": "Não há qualquer hipótese que justifique a restrição a determinadas funcionalidades em caso de negativa do titular em fornecer seus dados biométricos. Essa opção deve estar disponível sempre ao titular e o poder público deve ter alternativas de acesso nestes casos.", "940708": "As boas práticas são a disponibilização de informações objetivas e inequívocas sobre a necessidade, finalidade, adequação e todos os riscos inerentes ao tratamento dos dados biométricos. Deve-se facultar ao titular dos dados a escolha de disponibilizar ou não seus dados sem prejuízos.", "940709": "Deve ser possível que os titulares tenham acesso a canais de informação em que requeiram informações sobre quais dos seus dados estão disponíveis nos bancos de dados e que eles possam requerer, inclusive, a exclusão dos seus dados.", "940710": "Deve-se criar canais de atendimento aos cidadãos e cidadãs brasileiros e brasileiras em que existam seres humanos no atendimento para que os indivíduos possam revogar o consentimento, corrigir os dados, ter acesso aos dados e as informações necessárias para garantir a autodeterminação informativa.", "940711": "Os pais e responsáveis de crianças e adolescentes devem receber informações precisas em canais digitais e presenciais de fácil acesso e compreensão para que possam ser informados e ter os seus direitos explicados de forma objetiva a fim de que sejam capazes de tomar decisões livres e esclarecidas.", "940712": "O tratamento de dados biométricos de crianças e adolescentes deve ser uma exceção quando não tiver outra possibilidade. Quando for o caso, esses dados devem ser excluídos quando essas crianças e adolescentes atingirem a maioridade a fim de evitar abusos.", "940714": "Não deve ser utilizado método de fornecimento de dados biométricos nesse caso. Mas, se for estritamente necessário, esses dados devem ser armazenados de forma

temporária, sendo excluídos automaticamente ou a pedido do titular e/ou de seu responsável a qualquer tempo.

Contribuinte: GLAUCIA BRIGLIA CANUTO

Número: OP-948454

Data: 09/06/2025 - 12:42

Resumo:

:"", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Contribuinte: MAURICIO ANTONIO TAMER

Número: OP-950124

Data: 10/06/2025 - 21:27

Resumo: "A necessidade do tratamento e maior nível de segurança em todo ciclo de vida do tratamento (da coleta até a exclusão do dado).", "940688": "Identificar ao titular no momento da coleta, com algum pop-up ou ponto de atenção quais são os dados sensíveis que serão coletados, afim, de atender a devida finalidade.", "940690": "A ANPD poderia dispor de dispositivo autorizando ou não o tratamento de dados biométricos comportamentais, ainda mais no momento atual onde a IA consegue replicar facilmente este tipo de dado. O risco é o aumento de fraudes e tratamentos realizados por terceiros.", "940693": "Transparencia prévia ao tratamento, com comunicacao clara e objetiva. No mais, é necessário levar em consideração que um principio do consentimento é a revogação, sendo assim, deve-se avaliar o tratamento em específico, para ter a hipótese legal correta para estes dados.", "940695": "Uma forma seria incluir dados financeiros no rol de dados sensíveis, assim, ficaria mais clara a aplicabilidade para total identificação do titular, afim, de proteger o titular e a própria instituição controladora.", "940697": "Aprimorar o texto para identificar quais dados são necessários para cada tipo de tratamento que vise cumprimento de obrigação legal, e o controlador deve fornecer meios complexos de guarda dos dados.", "940699": "Assegurar a anonimizacao correta dos dados, a ANPD poderia aprimorar o texto com medidas técnicas necessárias uma vez que for utilizada essa base legal.", "940700": "Duplo fator de autenticação, juntamente com a biometria. Deixar o texto claro para utilização da prática via hipótese legal de Prevenção a Fraude.", "940701": "Controlador deve ter evidencias das praticas de Privacy by Design desde a etapa de projeto da solução. E deve haver um canal possível de solicitação de revisao humana para possíveis falhas nos tratamentos.", "940702": "Compra de produtos em supermercados e farmácias, adoção de programas de pontos, identificação para descontos, essas sao atividades simples do dia-dia, que não justificam a utilização de dados sensíveis.", "940704": "As organizações devem

manter RIPD's ou PIA's para os tratamentos envolvendo dados pessoais sensíveis, essa medida visa a identificação de riscos envolvidos no tratamento.", "940707": "Para serviços não essenciais, a ideia é manter o reconhecimento facial apenas para prevenção a fraude e segurança do titular, os demais tratamentos conseguimos identificar outras possibilidades no Art.7 ou Art.11.", "940708": "Um mapeamento correto sobre os tratamentos existentes e quais as suas finalidades. Acredito que será melhor se a ANPD exemplificar os cenários aceitos para este tipo de tratamento.", "940709": "Ampla divulgação dos tratamentos, direitos dos titulares, e bases legais para os tratamentos em questão. Além de abordar os benefícios para os titulares, referente a este procedimento. Aqui a ideia é muita conscientização.", "940710": "Canal de fácil acesso do titular com seu DPO, e que mantenha a política/termo/aviso de privacidade sempre atualizado, mas principalmente com foco objetivo para dados sensíveis.", "940711": "Manter o consentimento claro e atualizado dos pais ou responsáveis legais, com as informações claras e objetivas para eles e a criança/adolescente.", "940712": "Via aplicativo ou email, manter essa conexão direta e constante com os pais, ajudará na observância por parte do titular, e criar conscientizações na linguagem das crianças, para educar nos tratamentos necessários de dados pessoais comuns e sensíveis.", "940714": "Aqui invocamos a Prevenção a Fraude e Segurança do titular. O controlador deverá garantir que todo ciclo de vida deste dado, tenha uma camada de segurança diferenciadas de outros dados tratados.

Contribuinte: Sylvio Sobreira Vieira

Número: OP-952302

Data: 12/06/2025 - 13:25

Resumo:

:"", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Contribuinte: LEONARDO PEIXOTO BARBOSA

Número: OP-961043

Data: 22/06/2025 - 14:32

Resumo:

:"", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Contribuinte: FABIO TETSUO TOLEDO NASSU

Número: OP-963578

Data: 25/06/2025 - 08:07

Resumo: "Embora a Lei Geral de Proteção de Dados Pessoais não traga um conceito específico para dados biométricos, a referida norma os classifica como dados pessoais sensíveis (artigo 5º, II, LGPD). ", "940688": "As boas práticas de transparência devem balizar todo e qualquer tratamento de dados, independentemente do dado ser caracterizado como dado pessoal sensível, como é o caso do dado biométrico. Dessa forma, medidas que garantam aos titulares, o acesso a informações claras e precisas acerca da realizaç", "940690": "A biometria comportamental deve ser tratada à luz dos mesmos princípios e requisitos legais previstos na LGPD e aplicáveis ao tratamento de dados pessoais sensíveis, tal como já ocorre com a biometria tradicional. Isso inclui a observância dos princípios da finalidade, necessidade, qualidade de dado", "940693": "O tratamento de dados pessoais biométricos, à luz da LGPD, fundamenta-se nas bases legais previstas pela LGPD para dados pessoais sensíveis, no âmbito do art. 11 da LGPD. Contudo, deve-se considerar que o consentimento nem sempre será a hipótese autorizativa mais adequada nesse cenário, razão pel", "940695": "A adequada aplicação da hipótese legal da garantia da prevenção à fraude pressupõe o atingimento de requisitos de segurança e da aplicação de princípios balizadores do tratamento de dados pessoais de forma geral, não apenas ao tratamento de dados sensíveis. ", "940697": "No mesmo sentido do item anterior, entende-se que a adequada aplicação da hipótese legal do cumprimento de obrigação legal ou regulatória pressupõe o atingimento de requisitos de segurança e da aplicação de princípios balizadores do tratamento de dados pessoais de forma geral, não apenas ao tratamen", "940699": "Nesse sentido, importante esclarecer que o dado anonimizado se caracteriza pelo dado que não é capaz de permitir a reidentificação posterior, ainda que aplicadas técnicas de cruzamento de bases de dados. Corroborar esse entendimento o conceito de dado anonimizado previsto no art. 5º, III da LGPD. ", "940700": "No que tange ao atingimento do princípio da necessidade e da proporcionalidade, tem-se como alternativa a análise da indispensabilidade do reconhecimento facial. Ou seja, avaliação se o reconhecimento facial é a forma mais adequada e, caso seja, medidas minimizem o uso irrestrito do reconhecimento.", "940701": "Os sistemas de reconhecimento facial devem ser projetados com base nos princípios de privacy by design e privacy by default, incorporando, desde a fase de concepção, medidas técnicas e organizacionais voltadas à precisão, segurança e mitigação de riscos.", "940702": "Não se recomenda o uso de tecnologia de reconhecimento facial quando o tratamento de dados biométricos implicar riscos elevados à privacidade dos titulares sem justificativa proporcional ou base legal adequada. ", "940704": "É de suma importância que os controladores do tratamento dos dados biométricos adotem medidas técnicas e administrativas robustas, entre as quais destacam-se: 1. Programa de Segurança da Informação, Gestão de Acesso, Relatório de Tratamento dos Dados Pessoais, Inviolabilidade dos Dados Pessoais, ", "940707": "Para evitar que a exigência de autenticação biométrica em serviços não essenciais configure discriminação ilícita ou prática abusiva, é fundamental que o tratamento desses dados observe os princípios da LGPD bem como esteja devidamente enquadramento em uma das bases legais autorizativas", "940708": "A proteção eficaz no

tratamento de dados biométricos exige adoção de boas práticas voltadas à transparência, necessidade e mitigação de riscos discriminatórios. Entre essas práticas, destacam-se: 7

Treinamento e Capacitação: oferecer treinamento específico quanto ao tema; 7

Políticas e Procedimentos", "940709": "A proteção eficaz no tratamento de dados biométricos, especialmente no contexto do tratamento contínuo e massivo de dados biométricos, exige adoção de boas práticas voltadas à transparência, necessidade e mitigação de riscos discriminatórios", "940710": "Cumprir destacar que o direito à informação clara, o direito de acesso e à correção dos dados são direitos dos titulares que pressupõem todo e qualquer tratamento de dados pessoais, independentemente de o referido tratamento de dados pessoais estar ou não inserido no contexto de uma decisão tomada ", "940711": "Quando a hipótese legal é o consentimento, este deve ser inequívoco e contemplar as finalidades para a qual o representante do titular concorda com o tratamento. O tratamento dos dados biométricos de crianças e adolescentes também pode ser amparado em outras bases legais que não o consentimento. ", "940712": "A hipótese de Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (Art. 11, II, "g", LGPD). Quando a hipótese legal é o consentimento, este deve ser inequívoco e contemplar as finalidades para a qual o representa", "940714": "Para compatibilizar a prática de verificação de idade com o princípio da necessidade, é essencial que a coleta de dados biométricos seja limitada ao mínimo necessário para atingir a finalidade pretendida, evitando excessos ou tratamentos desproporcionais.

Contribuinte: Patrícia Leal Ferraz bove

Número: OP-965486

Data: 26/06/2025 - 09:30

Resumo: "Considerando que o âmago da tecnologia é a estatística, banco de dados e linguagem de programação, sem prejuízo de outras qualificações, os critérios objetivos a serem observados são: Toda métrica, psicológica e comportamental da pessoa natural humana", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "Transparência da black boss e informação ao titular sem prejuízo de questionamento no judiciário", "940700": "", "940701": "O algoritmo desses sistemas devem passar por auditoria Polícia Federal. Empresas devem ser responsabilizadas pelos falsos positivos e negativos, uma vez que o sistema é alimentado pela programação da própria empresa, ela detém a expertise. Multa de ordem crescente e /ou aplicação C.de Budapeste", "940702": "", "940704": "Acesso restrito de controladores, sala, máquinas diferenciadas, criptografia de ponta, auditorias, corregedorias. Identidade deve ter o mesmo rigor do tratamento dos dados biométricos. Manter a integralidade, confidencialidade, autenticidade dos dados", "940707": "", "940708": "", "940709": "Prejudicado e/ou criação de sistema para que a população denuncie. Utilização do mesmo sistema de alertas sobre a pandemia e alertas meteorológicos nos celulares da população.", "940710": "", "940711": "Educação, palestras, reuniões e todo empenho da comunidade civil. Assunto deve ser tratado como calamidade pública. PREJUDICADO, não

há melhor interesse da criança e adolescente em exposição a cada segundo, em cliks e compartilhamento em redes.", "940712": "", "940714": "O acesso a jogos com dados biométricos devem ser banidos. Prejudicado. Dados biométricos de crianças e adolescentes é moeda extremamente cara para troca de acesso a quaisquer serviços e plataformas

Contribuinte: VALERIA MARIA RAMOS

Número: OP-966029

Data: 27/06/2025 - 08:31

Resumo: "Dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a identificação única dessa pessoa singular, como imagens faciais ou dados dactiloscópicos. (art. 4º, §14 do GDPR).", "940688": "Realizar a distinção entre o que é dado de uso primário (aqui o titular está na ponta, fornecendo seu dado dele e com ciência disso, ex.: dados para acessar condomínio) e o que é dado de uso secundário (usado para uma finalidade diferente daquela para a qual foi originalmente coletado).", "940690": "A biometria comportamental deve ser alvo de uma regulação mais setorial, que leve em consideração os específicos benefícios e riscos envolvidos em cada contexto. A probabilidade de erro em seu uso é muito maior. Logo, defende-se que haja um juízo de necessidade mais delimitado.", "940693": "Deve-se identificar a base legal mais adequada para o tipo de tratamento, sendo o consentimento uma das opções. O consentimento deve ser facultativo, no contexto em que ele é válido e aplicável, deve ser fornecida ao titular uma alternativa clara para seguir na operação sem tratar o dado biométrico.", "940695": "Enviado por Lays Gomes Martins (lays.martins@fgv.br) no e-mail: Assunto: Contribuição - Equipe DPO/FGV - Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos.", "940697": "Deve-se especificar a norma e o respectivo artigo que fundamenta a obrigação legal ou regulatória. Ex.: Lei Geral do Esporte (Lei nº 14.597/2023, arts. 148 e 158, XII) estabelece a obrigatoriedade do tratamento de dados biométricos em estádios com capacidade superior a 20 mil pessoas.", "940699": "A LGPD menciona a anonimização “sempre que possível”, logo, ela não é obrigatória e dependerá do tipo de metodologia de pesquisa adotado e, também, da base de dados sobre análise. É impossível traçar limites genéricos sob pena de violação ao direito constitucional da ciência, tecnologia e inovação.", "940700": "Deve-se evitar a banalização da tecnologia, com análise de impacto, critérios claros de uso, transparência com os titulares, garantindo necessidade, proporcionalidade e não discriminação. Também é importante garantir protocolos para conter situações de falso positivo ou falso negativo.", "940701": "É necessário e imprescindível que esses sistemas possuam treinamento prévio com bases de dados capazes de representar a diversidade da população do local em que essas aplicações irão funcionar. Ainda, é necessário que existam estudos capazes de detectar o índice de confiabilidade da tecnologia.", "940702": "Reconhecimento facial não deve ser usado de forma banal, como acesso às academias ou controle de visitantes. Deve-se priorizar, sempre que possíveis, métodos menos invasivos, como cartões de acesso, tags, aplicativos de celular, chaves ou outros, garantindo menor impacto aos titulares.", "940704": "O relatório de impacto

com avaliação de riscos é indispensável. Nele, devem ser elencadas medidas como: políticas claras para backup dos dados, sua criptografia, o controle de acesso à base de informações e, ainda, a atualização do sistema operacional e aplicações envolvidas.", "940707": "O consentimento só é válido quando for opcional (deve ser livre, informado, inequívoco, específico e revogável). Negar o serviço por falta de consentimento pode ser um ato abusivo. Exemplo aceitável de consentimento: desbloqueio facial opcional em smartphones onde existem outras opções, como senha.", "940708": "Identificar e analisar riscos com mitigadores via relatório de impacto. Sobre transparência, distinguir coleta primária da secundária e, especialmente no primeiro caso, deixar claro ao titular que haverá tratamento de dados biométricos. Preocupação: portarias fazem reconhecimento facial sem avisar.", "940709": "É preciso garantir um aviso de privacidade visível e acessível, com identificação do controlador, base legal, finalidade e canal para que os titulares apresentem requerimentos, pois eles devem ser informados de forma clara e transparente sobre o tratamento.", "940710": "Precisamos de um regulamento sobre direitos dos titulares. Os agentes de tratamento procurarão se ajustar em seguida.", "940711": "O ideal é evitar o tratamento de biometria de crianças, com alternativas que sejam menos invasivas. Deve-se realizar um teste de balanceamento que pondere de um lado os benefícios do tratamento e de outro, os riscos associados sem este exame, fica inviável a defesa irrestrita desse tratamento.", "940712": "Quando os benefícios à criança ficarem claramente destacados em relação aos riscos no teste de balanceamento.", "940714": "Não é razoável coletar a biometria para estimar idade, considerando o princípio da necessidade e o melhor interesse da criança. Devem-se buscar métodos menos invasivos e sempre garantir transparência, consentimento dos responsáveis e mínima exposição.

Contribuinte: LAYS GOMES MARTINS

Número: OP-966032

Data: 27/06/2025 - 08:36

Resumo: "Impressão digital, reconhecimento facial, íris, geometria da mão, voz, padrão de digitação, padrão de marcha, movimento ocular. O dado biométrico precisa ser capaz de identificar de forma única um titular.", "940688": "Explicitar quais dados biométricos serão coletados. Informar base legal e finalidade exata do tratamento. Deixar claro se a coleta é obrigatória ou facultativa, e as consequências da recusa. Informar o contato do DPO no momento da coleta para opt-out.", "940690": "O uso deve ser precedido de RIPD, com atenção a riscos como discriminação, profiling e violações à privacidade. O titular deve ser informado claramente sobre a coleta e uso e seus dados comportamentais, inclusive quando imperceptível. Recomendável oferecer alternativas ao uso das biometrias.", "940693": "Para ser válido, o consentimento para dados biométricos deve ser livre, específico, informado, destacado e inequívoco. Não é adequado quando há desequilíbrio de poder ou quando o titular não pode recusar sem prejuízo.", "940695": "A prevenção à fraude exige prova da real necessidade do uso de biometria, finalidade legítima e mínima coleta. Devem ser adotadas salvaguardas como criptografia, anonimização, RIPD e transparência, para equilibrar

segurança com proteção de direitos.", "940697": "Quando baseado em obrigação legal, o uso de biometria deve ser proporcional, com base clara na norma, mínima coleta e uso restrito à finalidade. Órgãos públicos devem garantir transparência, segurança, RIPD e canais para exercício dos direitos dos titulares.", "940699": "Dados biométricos devem ser anonimizados e usados só para finalidade específica. O cruzamento de bases exige cuidado para evitar reidentificação. Salvaguardas incluem anonimização robusta, controles de acesso, RIPD e transparência para proteger direitos e interesses dos titulares.", "940700": "O uso de reconhecimento facial deve ser limitado ao estritamente necessário, com base clara, transparência e avaliação prévia dos riscos. Salvaguardas incluem teste de viés algorítmico, RIPD, supervisão independente, controles de acesso e mecanismos de responsabilização.", "940701": "Sistemas de reconhecimento facial devem ser projetados com bases diversas, testes rigorosos e validações contínuas. Devem prever correção de falhas, auditorias, feedback em tempo real, RIPD, transparência e supervisão para garantir eficácia, confiabilidade e proteção de direitos.", "940702": "O reconhecimento facial não é recomendado em locais públicos, escolas ou relações de consumo sem real necessidade, por risco à privacidade e discriminação. Alternativas como autenticação por senha, token, QR code, OTP e MFA oferecem segurança com menor impacto aos titulares.", "940704": "É fundamental adotar criptografia, controle de acesso, anonimização e testes de vulnerabilidade. Avaliações de risco periódicas, RIPD, monitoramento contínuo e plano de resposta a incidentes são mínimos para garantir conformidade e proteger dados biométricos.", "940707": "Deve-se oferecer alternativa viável à biometria e informar claramente sua necessidade. A recusa pode limitar funções, desde que de forma proporcional, transparente e sem discriminação. A funcionalidade deve ser justificada tecnicamente e o consentimento, livre e informado.", "940708": "Minimização de dados, criptografia, RIPD, controle de acesso, transparência sobre finalidades, auditorias e testes contra viés algorítmico. Garantir uso ético e proporcional evita discriminação e assegura tratamento responsável dos dados biométricos.", "940709": "Controladores devem garantir transparência com sinalização visível, políticas públicas acessíveis, minimização de dados e bases legais adequadas. Devem oferecer canais eficazes para exercício de direitos, realizar RIPD e garantir supervisão independente e proporcionalidade no uso da biometria.", "940710": "Agentes devem fornecer canais acessíveis para pedidos dos titulares, garantir informações claras sobre o tratamento, permitir correção de dados e facilitar a revogação do consentimento. Sistemas devem ser auditáveis, com intervenção humana e medidas que assegurem o exercício efetivo desses direitos.", "940711": "O tratamento de dados biométricos de crianças exige consentimento dos pais, informação clara e adequada, e uso limitado à finalidade legítima. Deve-se respeitar o melhor interesse da criança, com segurança reforçada, minimização e transparência, conforme art. 14 da LGPD.", "940712": "O tratamento é admissível com consentimento dos pais ou obrigação legal/regulatória. Garantir transparência, canais para dúvidas e revogação, além de medidas como criptografia, controle de acesso e RIPD para prevenir abusos, vazamentos e acessos indevidos, protegendo dados de crianças e adolescentes", "940714": "O tratamento deve ser limitado ao mínimo necessário para verificar a idade, com consentimento dos pais, transparência clara e uso seguro dos dados. Deve garantir o melhor interesse da

criança, evitando coleta excessiva e riscos, alinhado à LGPD e princípios de proteção integral e necessidade.

Contribuinte: MARIANA CASTRO SCAPIN

Número: OP-966760

Data: 29/06/2025 - 08:02

Resumo: "A biometria é um dos instrumentos mais sensíveis da sociedade de vigilância, pois utiliza as características físicas, biológicas e comportamentais, que são intransferíveis e não podem ser alteradas como as senhas, assim entendemos sempre como dados sensíveis e o seu uso somente pode ocorrer com o consentimento, mas só isso não basta, falta um nível de segurança da informação bem alto que não suporte a sua cópia, ou seja, as capturas dessas bases não podem ser duplicadas ou compartilhadas com terceiros sem sua anonimização. ", "940688": "Apresentar o nível de segurança de criptografia dos dados, sua anonimização, não ter opções de compartilhamento das mesmas, adotar a Biometria descentralizada. ", "940690": "A biometria comportamental deve se ater a um público específico, ou seja, local e não se utilizar bases estrangeiras para definir esses parâmetros, para não gerar falhas maiores que o mínimo aceitável.", "940693": "O consentimento dos dados biométricos devem ter um tempo de validade como acontece nos certificados digitais, como acontece na ICP-Brasil, sendo necessário o expurgo das informações se esse consentimento expirar. O uso da Biometria fora do consentimento somente deve ocorrer em questão de vida do titular, em hospitais ou por equipes em eventos extremos. ", "940695": "A biometria não deve ser a única chave num registro de dados de um titular, junto com o dado biométrico deve ter uma chave privada de criptografia criada pelo titular e essa informação não deve ser permanente, ou seja, deve ser revalidada, assim a informação deve ter a data de captura e validade de uso. ", "940697": "A base desta informação não pode ser compartilhada com terceiros, deve estar armazenada no local do dispositivo e não na nuvem. ", "940699": "No caso de pesquisas, devemos ter uma validação externa por órgãos de controle, com a ANPD através de fiscalização e relatórios de controles anuais com a evolução da pesquisa e expurgo destes dados ao final da pesquisa. ", "940700": "O titular poderá a qualquer momento contestar um registro de reconhecimento facial seja numa abordagem policial ou em outro momento, sem ser preso sem uma avaliação por outra tecnologia de validação com acompanhamento de uma testemunha, advogado ou defensor. Somente a informação automatizada não deve ser critério decisório nesse processo. ", "940701": "A utilização de bases nacionais de dados biométricos e voluntárias, sem a utilização de bases estrangeiras de comparação. A valiação por mais de um método e a utilização de pesquisadores que fiscalizem a evolução destas tecnologias. ", "940702": "O reconhecimento facial não deve ser utilizado sem um segundo fator de autenticidade do titular. ", "940704": "Bases biométricas descentralizadas, armazenadas em locais seguros e fiscalizados pela ANPD ou órgão indicado, nunca armazenar em nuvem no país ou no estrangeiro. A evolução das tecnologias deve ser critério para descarte de dados biométricos que estejam vulneráveis. ", "940707": "Sempre deve existir uma contingência ao uso da biometria, nada pode gerar a obrigatoriedade deste tipo de autenticação.

","940708": "A avaliação do ambiente de dados biométricos com testes periódicos de sua eficácia por órgãos de pesquisa e fiscalização de sua capacidade de segurança máxima contra vazamentos e seu nível de criptografia de dados anonimizados. ","940709": "As bases de dados biométricos devem ter registros na ANPD com relatórios do seu nível de criptografia, anonimização e eficácia. ","940710": "Todo e qualquer titular têm direito a uma avaliação por humanos quando divergir de um dado biométrico seu armazenado. Deve acontecer fiscalizações regulares para garantir o nível de segurança das bases de dados biométricos. ","940711": "Os pais e responsáveis deve autorizar por tempo determinado esse armazenamento, até a maioridade, ou plena capacidade da pessoa, após esse prazo, o dado deve ser capturado novamente, ou seja, um dado biométrico de um menor não deve ser utilizado para identifica o mesmo na idade adulta. ","940712": "somente em situações de risco de vida do menor. ","940714": "Na dúvida deve se buscar outro método de identificação além da biometria.

Contribuinte: JOSE GERALDO LEITE COURA

Número: OP-967368

Data: 30/06/2025 - 07:35

Resumo: "Para que um dado seja classificado como biométrico nos termos da LGPD, deve-se observar cumulativamente: (i) caracterizar-se como informação pessoal sensível que reflete traços físicos, fisiológicos ou comportamentais singulares do titular, capazes de diferenciá-lo de forma inequívoca (e.g. impressões digitais, íris, face, voz, padrão de digitação ou marcha); (ii) resultar de tratamento técnico especializado, ou seja, captado por sensores, câmeras ou softwares que extraem, analisam e geram “templates” digitais mediante algoritmos estatísticos ou de aprendizado de máquina; e (iii) permitir ou confirmar a identificação única do indivíduo, ainda que com grau de probabilidade, o que distingue simples fotografias ou gravações sem análise técnica de dados biométricos propriamente ditos. ","940688": "Para assegurar transparência ativa no tratamento de dados biométricos, os controladores devem implementar, antes da coleta, iniciativas como: (i) publicação destacada de avisos de privacidade específicos para biometria em local visível no site ou aplicativo, contendo finalidade exata, base legal, categorias de dados, tempo de retenção e riscos potenciais; (ii) envio de comunicações proativas por e-mail ou SMS com síntese dos termos de uso e link direto para política completa; (iii) disponibilização de painéis interativos em espaços digitais que permitam ao titular consultar, em tempo real, quais dados biométricos foram coletados, para quais finalidades, e por quem; (iv) uso de infográficos e vídeos curtos que expliquem o fluxo de tratamento, medidas de segurança adotadas e direitos do titular; (v) relatórios periódicos por meio de newsletter ou portal dedicado que informem atualizações sobre novos usos, avaliações de impacto à proteção de dados e eventuais incidentes de segurança. ","940690": "A biometria comportamental exige tratamento tão rigoroso quanto a biometria tradicional, porém com atenção reforçada aos princípios da qualidade dos dados e da segurança: (i) exatidão e atualização constantes dos algoritmos de análise comportamental, para reduzir vieses e falsas detecções; (ii) minimização de dados, coletando apenas os

parâmetros estritamente necessários ao propósito legítimo; (iii) segregação de sistemas, isolando os repositórios comportamentais dos demais bancos de dados; (iv) testes e auditorias independentes que avaliem acurácia e viés algorítmico; (v) transparência técnica sobre os métodos de captura e análise, incluindo métricas de erro e protocolos de correção; (vi) controle de acesso, com autenticação multifator e logs detalhados de operações; (vii) adoção de critérios de validade e consentimento contínuo; e (viii) criptografia de template em repouso e em trânsito, garantindo inviabilidade de retroconstrução dos dados brutos.

","940693": "Para que o consentimento ao tratamento de dados biométricos seja válido nos termos da LGPD, ele deve ser apresentado de forma clara e destacada, sem pré-seleção de caixas, descrevendo a finalidade exata, as categorias de dados e a base legal aplicável. O titular deve receber informação prévia sobre riscos, prazo de retenção e direitos, e manifestar sua concordância por meio de ação afirmativa, como clique ou assinatura digital. Além disso, é necessário registrar data, hora e escopo do consentimento para fins de auditoria, oferecer meio simples e gratuito de revogação a qualquer momento e informar eventuais consequências da negativa. O consentimento não é adequado quando há desequilíbrio entre as partes, como em relações de emprego, em casos de tratamento em massa que comprometam a voluntariedade, no cumprimento de obrigação legal ou regulatória, ou em prevenção à fraude, situações em que devem ser adotadas hipóteses legais específicas previstas na

LGPD." , "940695": "A hipótese legal de prevenção à fraude, prevista no art. 11, II, “g” da LGPD, para o tratamento de dados biométricos requer que a coleta se limite aos elementos necessários à detecção de fraudes específicas, evitando propósitos genéricos, e seja formalmente documentada em políticas e processos internos. Antes do início do tratamento, deve-se realizar avaliação de impacto à proteção de dados (DPIA) para identificar riscos a direitos fundamentais e possíveis vieses discriminatórios. É imprescindível adotar salvaguardas técnicas, como criptografia de templates, isolamento de ambientes analíticos e autenticação multifator, e organizacionais, incluindo políticas de governança, treinamentos e auditorias com foco em vieses algorítmicos. A retenção deve obedecer ao princípio da limitação temporal, mantendo-se apenas pelo período estritamente necessário, seguido de anonimização ou exclusão, e o controlador deve assegurar processos de revisão, canais de comunicação com titulares e transparência " , "940697": "Quando o tratamento de dados

biométricos se baseia em “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD), controladores devem adotar critérios claros e salvaguardas robustas. Primeiramente, deve haver norma ou regulação que imponha explicitamente a coleta biométrica, com escopo, finalidade e prazo definidos. Em seguida, é essencial realizar avaliação de impacto à proteção de dados (DPIA) prévia para mapear riscos e propor medidas de mitigação. As salvaguardas técnicas envolvem criptografia de templates em repouso e em trânsito, segregação de redes e autenticação multifator no acesso aos sistemas. Entre as organizacionais, destacam-se políticas internas documentadas, treinamentos obrigatórios para operadores com ênfase em privacidade, auditorias periódicas e nomeação de responsável técnico pela conformidade.

Deve haver ainda canal formal para reclamações e solicitações de titulares, assegurando acesso, correção e exclusão de dados. " , "940699": "Para tratamento de dados biométricos em estudos de pesquisa (art. 11, II, “c”, LGPD), mesmo que haja anonimização, o cruzamento de bases e o risco de reidentificação demandam limites e salvaguardas adicionais. Em primeiro

lugar, deve-se garantir que o grau de anonimização seja irreversível, avaliando tecnicamente a probabilidade de reidentificação a partir de técnicas como k-anonymity e differential privacy. É fundamental estabelecer políticas que restrinjam o compartilhamento de dados a equipes autorizadas e ambientes controlados, com lógica de “need to know”. Recomenda-se a adoção de acordo de confidencialidade e cláusulas que proíbam tentativas de reidentificação. Além disso, o protocolo de pesquisa deve ser submetido a comitê de ética, que analisará a metodologia, riscos e salvaguardas. Para casos de dados pseudonimizados, impõe-se a separação física de chaves de reidentificação, sob guarda de pessoa jurídica distinta ou autoridade independente.

","940700": "O uso de tecnologias de reconhecimento facial, mesmo amparado por hipótese legal, deve respeitar estritamente os princípios da necessidade, proporcionalidade e transparência para evitar discriminação ilícita ou abusiva. Deve-se limitar o escopo ao mínimo indispensável: definir casos de uso claros, documentar justificativas e avaliar alternativas menos invasivas. No aspecto técnico, é imprescindível empregar algoritmos testados quanto a vieses demográficos, com métricas públicas de falso positivo e negativo, e realizar auditorias independentes periódicas. A transparência implica informar titulares de forma acessível sobre quando, onde e por que a identificação ocorrerá, bem como disponibilizar relatórios de impacto e indicadores de desempenho. Juridicamente, recomenda-se instituir política interna que regulamente uso, responsabilidades e penalidades para descumprimento, além de cláusulas contratuais rígidas com fornecedores e proibição de uso em contextos de vigilância indiscriminada."

","940701": "Para garantir eficácia e confiabilidade de sistemas de reconhecimento facial e minimizar erros, devem ser adotadas práticas de Privacy and Security by Design e Teste by Design. Na fase de concepção, é crucial definir métricas-alvo de precisão, sensibilidade e especificidade, além de colecionar bases de treinamento representativas de diferentes perfis étnicos, de gênero e faixa etária. Durante o desenvolvimento, aplicar validação cruzada e testes “in the wild” para avaliar o desempenho em condições reais, mapeando cenários de baixa iluminação ou ângulos diversos. Para corrigir falhas, estabelecer pipeline de revisão humana nos casos de baixa confiança estatística, com registro de logs detalhados para auditoria de decisões. Deve haver mecanismo ágil de reaprendizado contínuo, liberando atualizações de modelo mediante supervisão técnica. Em produção, implementar monitoramento em tempo real de indicadores de erro, alertas automáticos e relatórios periódicos que permitam identificar padrões"

","940702": "Existem situações em que o uso de reconhecimento facial não é recomendado, como em espaços públicos de alta circulação (estações de transporte, eventos de massa) sem consentimento explícito, devido ao alto potencial de vigilância indiscriminada e violação de privacidade coletiva. Também não se aconselha em contextos sensíveis, como locais de tratamento médico, centros de educação infantil e ambientes de protesto, onde há riscos de estigmatização e repressão. Nesses cenários, tecnologias alternativas podem substituir o reconhecimento facial de forma eficaz e menos intrusiva, tais como autenticação por tokens físicos (smartcards, crachás com RFID) ou biometria comportamental restrita (padrões de digitação de credenciais) em ambientes controlados. Para acesso temporário, pode-se optar por QR codes dinâmicos enviados via app seguro, com validade curta e criptografia de ponta a ponta. Essas soluções mantêm níveis adequados de segurança operacional sem expor dados pessoais sensíveis."

","940704": "Dada a gravidade de uma

violação de dados biométricos, controladores devem adotar medidas técnicas e organizacionais robustas, como criptografia de ponta a ponta dos templates tanto em repouso quanto em trânsito, uso de hardware seguro para armazenamento (HSM), autenticação multifator para acesso a sistemas e segmentação de redes com firewalls e sistemas de detecção de intrusão. No plano administrativo, é essencial estabelecer políticas claras de segurança da informação, treinamentos periódicos para todos os colaboradores, revisão contratual rigorosa com fornecedores e planos de resposta a incidentes que definam papéis, procedimentos de contenção e comunicação. Quanto aos parâmetros de avaliação de riscos, recomenda-se implementar avaliações de risco contínuas, com indicadores de risco residual e alertas automáticos para comportamentos anômalos, além de auditorias internas e externas regulares para verificar conformidade com a LGPD. Também é crucial definir métricas de monitoramento."

"940707": "Em serviços não essenciais cujas funcionalidades dependam tecnicamente de autenticação biométrica, controladores devem adotar práticas que evitem discriminação indevida. É recomendável avaliar alternativas menos invasivas que atendam ao mesmo propósito, como códigos de uso único ou autenticação via aplicativo, oferecendo ao titular opção de escolher o método que julgar adequado. Deve-se informar de forma clara e antecipada, por meio de notificações e layouts destacados, que a recusa em fornecer dados biométricos poderá limitar o acesso a determinadas funcionalidades, mas sem comprometer direitos básicos de fruição do serviço principal. A limitação só será proporcional se o controlador demonstrar, em avaliação documentada, que a biometria é indispensável para a função específica, e deve garantir que não haja prejuízo desproporcional ao titular. Em caso de negativa, o usuário deve ter canal de suporte eficiente para discutir alternativas e solicitação de revisão da restrição."

"940708": "Para conferir proteção eficaz no tratamento de dados biométricos, controladores devem adotar medidas alinhadas a “Privacy by Design” e “Privacy by Default”. Isso inclui mapear fluxos de dados e realizar avaliação de impacto (DPIA) antes de implantar qualquer solução biométrica, definindo escopo claro e limitando coleta ao mínimo necessário. No aspecto técnico, recomenda-se criptografar templates com algoritmos modernos, isolar ambientes de processamento e implementar controles de acesso baseados em perfis, além de manter logs imutáveis de operações. Organizacionalmente, é vital instituir políticas de retenção e descarte seguro, capacitar equipes sobre privacidade e segurança e supervisionar fornecedores por meio de cláusulas contratuais rígidas. A transparência deve ser garantida com comunicação contínua ao titular, via painéis ou relatórios, informando uso e eventuais atualizações de risco. Também é fundamental testar regularmente a solução para identificar e corrigir vieses."

"940709": "Em contextos de tratamento contínuo e massivo de dados biométricos, como cidades inteligentes e monitoramento de multidões, controladores devem assegurar a autodeterminação informativa por meio de canais claros e acessíveis. Isso inclui informar previamente, por sinalização digital ou aplicativos, sobre a captação e uso de biometria, disponibilizando detalhes de finalidade, base legal e riscos de forma concisa. Devem existir mecanismos para que titulares exerçam seus direitos de acesso, correção e oposição, por exemplo por totens de autoatendimento ou interfaces móveis que permitam consultar registros biométricos e solicitar exclusão ou limitação de uso. É essencial implementar medidas como geofencing para ativar ou desativar captura em determinadas áreas, além de limitar o período de retenção

e realizar anonimização quando possível. Para garantir transparência real, recomenda-se relatórios públicos periódicos sobre volumes de captação, resultados de auditorias independentes.", "940710": "Agentes de tratamento que utilizam automação em dados biométricos devem assegurar o respeito integral aos direitos dos titulares, especialmente informação clara, acesso, correção e revogação do consentimento. Antes de iniciar o processamento automatizado, o controlador deve fornecer explicação sobre lógica envolvida e possíveis consequências, em linguagem simples e destacada. Deve existir canal dedicado – online ou presencial – para que o titular consulte quais dados biométricos foram processados, obtenha cópia de registros e solicite correções de forma ágil. A revogação do consentimento deve ser permitida com um clique ou solicitação verbal, interrompendo imediatamente qualquer uso futuro dos dados com efeitos prospectivos. Para operações de alto risco, recomenda-se processo de revisão humana antes da tomada de decisão automatizada, garantindo direito ao contraditório e à revisão. Todas essas etapas devem ser registradas em logs auditáveis, disponíveis para autoridades e titulares.", "940711": "Dada a sensibilidade dos dados biométricos de crianças e adolescentes, seu tratamento só será admissível com o consentimento inequívoco de pais ou responsáveis, nos termos do art. 14 da LGPD. Deve-se apresentar informação clara e destacada sobre finalidade, riscos, prazo de retenção e direitos, em linguagem acessível. Pais ou responsáveis devem manifestar consentimento por ato afirmativo, registrado com data, hora e escopo, e ter canal facilitado para revogação. Adicionalmente, recomenda-se avaliação de impacto (DPIA) focada em menores, criptografia forte de templates, segregação de dados em ambientes isolados e controles de acesso rigorosos. Políticas internas e treinamentos específicos devem orientar equipes sobre tratamento de dados de menores, prevendo anonimização ou exclusão automática ao atingir maioria, e relatórios de conformidade periódicos para demonstrar respeito ao princípio do melhor interesse da criança. ", "940712": "O tratamento de biometria de crianças e adolescentes é legalmente admitido quando: (i) há consentimento específico de pais ou responsáveis; (ii) for necessário ao cumprimento de obrigação legal ou regulatória; ou (iii) for destinado a pesquisa por órgão de saúde ou educação, desde que autorizada por conselho de ética. Em todos os casos, deve-se garantir a participação informada dos responsáveis, com avisos prévios detalhando finalidade e riscos, e oferecer meio simples de revogação. Salvaguardas técnicas incluem criptografia de ponta a ponta, pseudonimização de templates, armazenamento em hardware seguro (HSM) e controle de acesso por autenticação multifator. Organizacionais, destacam-se políticas de retenção e descarte seguro, auditorias regulares, cláusulas contratuais rígidas com fornecedores e capacitação contínua de colaboradores. Essas medidas evitam abusos, vazamentos e acessos indevidos, assegurando proteção integral dos menores. ", "940714": "Para verificação ou estimação de idade via dados biométricos, como em plataformas digitais ou jogos, deve-se observar: (i) necessidade e proporcionalidade: coletar apenas parâmetros mínimos que permitam distinguir faixas etárias relevantes; (ii) consentimento informado de pais ou responsáveis para menores; (iii) anonimização ou pseudonimização imediata após a checagem; (iv) avaliação de impacto específica para inferência de idade, prevista na LGPD; (v) transparência: informar claramente ao usuário sobre o uso da biometria para estimativa etária, riscos e direitos; (vi) retenção mínima: descartar templates ou resultados imediatamente após a validação da idade; (vii)

salvaguardas técnicas: criptografia de dados em repouso e trânsito, isolamento de sistemas e autenticação multifator; e (viii) processo de contestação: possibilitar solicitação de revisão da estimativa de idade por método alternativo. Assim, alinha-se o procedimento aos princípios da LGPD e ao melhor interesse de crianças.

Contribuinte: JOAO PEDRO FERRAZ TEIXEIRA

Número: OP-967732

Data: 30/06/2025 - 12:23

Resumo: "A Business Software Alliance (BSA) agradece a oportunidade de fornecer feedback à Autoridade Nacional de Proteção de Dados (ANPD) sobre a consulta pública sobre o tratamento de dados biométricos. A BSA aprecia a importância de garantir que as empresas que processam dados biométricos cumpram a LGPD. Respondemos a todas as três perguntas da ANPD sobre a aplicação da LGPD a esse processamento. Os dados biométricos só devem ser tratados como confidenciais se forem usados para identificar exclusivamente um indivíduo. Isso cria um padrão claro e se alinha com o GDPR da UE, que a ANPD reconhece que inspirou a LGPD. O artigo 9.º do GDPR proíbe o tratamento de dados biométricos sem consentimento se estes forem utilizados para identificar de forma inequívoca uma pessoa singular.", "940688": "Os controladores devem adotar medidas alinhadas ao princípio de transparência da LGPD, que visa garantir que os titulares dos dados tenham informações claras sobre como os dados pessoais são tratados. Os controladores também estão sujeitos à obrigação do Artigo 9 de fornecer informações sobre seu processamento, incluindo as finalidades para as quais os dados pessoais são processados. ", "940690": "A ANPD deve se concentrar na biometria usada para identificar exclusivamente um indivíduo – e reconhecer que os dados biométricos podem apoiar atividades importantes sem identificar indivíduos. Por exemplo, os dados biométricos podem apoiar a segurança, distinguindo uma pessoa de um objeto em um armazém ou contando os passageiros no transporte público. Esses não devem ser usos sensíveis.", "940693": "A LGPD fornece uma série de bases legais para o processamento de dados biométricos. Respondemos a todas as quatro perguntas da ANPD sobre como essas bases legais se aplicam aos dados biométricos. De acordo com a LGPD, os controladores devem obter consentimento ou confiar em outra base legal nos termos do Artigo 11 para processar dados pessoais confidenciais. A orientação sobre dados biométricos deve ser consistente com o reconhecimento da LGPD de que tais dados podem ser tratados com consentimento ou em outras bases reconhecidas na lei. ", "940695": "Os dados biométricos podem ser usados para evitar atividades fraudulentas, em benefício de consumidores e empresas. O artigo 11 permite expressamente o processamento para esse fim, a menos que o interesse em tal processamento seja anulado pelos direitos dos indivíduos. As empresas devem avaliar os benefícios e riscos de tal processamento, para apoiar o uso dessa base legal. ", "940697": "Os controladores devem identificar e avaliar suas obrigações legais e regulatórias de processar dados pessoais sensíveis, incluindo dados biométricos. Para empresas do setor privado, essas obrigações podem vir de estatutos e regulamentos ou ordens específicas de agências governamentais. A orientação deve reconhecer claramente a

importância de tal processamento.", "940699": "As entidades de pesquisa devem realizar estudos alinhados às proteções da LGPD. Isso inclui anonimizar dados pessoais confidenciais sempre que possível. De forma mais ampla, a orientação deve aplicar a LGPD com base na função pretendida e no risco real do uso de uma tecnologia, e não nas características gerais ou capacidades potenciais de uma tecnologia.", "940700": "É importante garantir que as proteções legais existentes, incluindo a LGPD, continuem a ser aplicadas a tecnologias novas e emergentes. Respondemos a uma das perguntas da ANPD sobre essas tecnologias. É importante reconhecer que as tecnologias que tratam dados pessoais estão sujeitas não apenas à LGPD, mas também a outras leis existentes. Pode ser necessário examinar como as leis que proíbem a discriminação ilegal se aplicam ao uso de novas tecnologias. Essas leis devem continuar a proteger contra a discriminação à medida que novas tecnologias são adotadas.", "940701": "", "940702": "", "940704": "A LGPD apoia uma série de boas práticas e governança que podem proteger os direitos dos titulares dos dados e permitir a conformidade. Respondemos a três perguntas sobre como essas práticas e medidas de governança podem ser aplicadas ao processamento de dados biométricos. Reconhecemos que a ANPD está considerando emitir orientações sobre avaliações de impacto à proteção de dados (DPIAs) para tratamentos que apresentem certos riscos. Apoiamos a exigência de que os controladores conduzam DPIAs ao processar dados pessoais confidenciais, incluindo dados biométricos, o que é consistente com o GDPR da UE e outras leis globais de proteção de dados.", "940707": "", "940708": "Os controladores devem adotar práticas alinhadas à LGPD, incluindo limites ao tratamento de dados sensíveis. Além disso, a LGPD exige que os controladores que processam quaisquer dados pessoais sejam transparentes sobre suas atividades e adotem medidas de segurança adequadas. Leis além da LGPD também podem proibir a discriminação e outros atos ilegais.", "940709": "É importante entender se os dados nesses cenários estão sendo processados com a finalidade de identificar exclusivamente os indivíduos. Nesse caso, deve ser protegido como dados biométricos. No entanto, o processamento de dados que revelam o número de pessoas em uma multidão ou apenas fornecem informações agregadas sobre padrões de tráfego não cria as mesmas sensibilidades.", "940710": "A LGPD cria uma série de direitos importantes para os indivíduos em seus dados pessoais. Respondemos a uma pergunta sobre como esses direitos se aplicam ao processamento de dados biométricos. Os direitos criados pela LGPD se aplicam a todos os dados pessoais, incluindo dados biométricos. É altamente recomendável tratar os dados apenas como dados biométricos se forem usados para identificar exclusivamente um indivíduo. Isso também esclarecerá como os novos direitos do titular dos dados se aplicam, porque esses direitos serão atribuídos ao indivíduo que é identificado de forma exclusiva.", "940711": "", "940712": "", "940714": "

Contribuinte: Emily Sayuri Arnaud Yamaguti

Número: OP-967752

Data: 30/06/2025 - 12:39

Resumo: "Devem ser observados os seguintes critérios objetivos para caracterizar os dados como biométricos: • Os dados devem resultar de um processamento técnico das características físicas ou comportamentais de um indivíduo (por exemplo, imagem facial, impressão digital, íris, voz, marcha, ritmo de digitação). • A finalidade do processamento deve ser identificar ou autenticar um indivíduo. • Os dados devem ser suficientemente distintos e estáveis para estabelecer uma ligação verificável com uma pessoa específica. •

A mera recolha de imagens ou sinais em bruto não é admissível, a menos que sejam tratados especificamente para efeitos de reconhecimento de identidade. ", "940688": "Os controladores devem implementar mecanismos de transparência ativos, incluindo: •

Avisos de privacidade em camadas com explicações claras e concisas sobre: o

Quais dados biométricos são coletados (por exemplo, modelo de rosto, impressão digital), o Para quais finalidades (por exemplo, verificação de identidade, prevenção de fraudes), o A base legal (por exemplo, consentimento, obrigação legal), o Períodos de retenção e direitos de exclusão, o Se os dados são compartilhados com terceiros ou armazenados localmente/descentralmente. • Auxílios visuais ou símbolos (ícones que indicam uso biométrico, identificação, etc.). • Uso de linguagem simples e acessível, especialmente para grupos vulneráveis. • Alertas automatizados para alterações no uso de dados ou atualizações do sistema. ", "940690": "A biometria comportamental, embora difiram na modalidade, deve ser tratada com a mesma cautela que os identificadores biométricos tradicionais se usados para identificação ou autenticação. ", "940693": "O consentimento para o tratamento de dados biométricos é livre, específico, destacado, informado e inequívoco quando: • Opções granulares são fornecidas: o consentimento deve ser específico para o propósito (por exemplo, facilitação de viagens versus marketing). • É necessária uma ação afirmativa explícita - sem caixas pré-marcadas ou consentimento implícito. • As informações são facilmente compreensíveis e exibidas com destaque, idealmente antes do ponto de captura de dados biométricos. • Um mecanismo de retirada está disponível a qualquer momento, sem prejuízo para o usuário (a menos que seja essencial para um serviço legal). É importante permitir que os indivíduos consentam com o processamento biométrico, mesmo quando um processamento tradicional é a opção alternativa. ", "940695": "A prevenção da fraude como base legal deve atender ao princípio da necessidade e da proporcionalidade, ou seja: • O processamento biométrico deve ser comprovadamente mais seguro ou preciso do que alternativas menos intrusivas. • O sistema deve operar sob uma estrutura baseada em risco (por exemplo, verificações mais fortes apenas quando um comportamento anormal é detectado). • A finalidade deve ser claramente definida: por exemplo, detecção de fraude durante o autoembarque ou check-in no quiosque. As salvaguardas incluem: • Hash e criptografia de modelo biométrico unidirecional, •

Políticas de revogação ou expiração de modelos, • Carteiras de identidade descentralizadas para reduzir o risco sistêmico de violações, • Logs de auditoria e controles de acesso, • Separação de tarefas para processamento biométrico e verificação de identidade. ", "940697": "Os principais critérios e salvaguardas a serem observados pelos controladores incluem: • A obrigação deve resultar de um mandato legal ou regulamentar claro, tais como: o Requisitos de controle de imigração, o Disposições de segurança pública, o Regulamentos internacionais de aviação (por exemplo, conformidade com

API/PNR). Salvaguardas para garantir a proporcionalidade e a responsabilização: •

Minimização de dados: colete apenas o estritamente necessário (por exemplo, modelo facial vs. imagem facial completa). • Controle de retenção: exclusão automática assim que o objetivo regulatório for cumprido. • Acesso baseado em funções, mesmo em autoridades públicas. • Comunicação clara sobre a natureza obrigatória do processamento, com referência aos instrumentos legais aplicáveis. • Revisão periódica da necessidade

contínua do processamento de dados. ", "940699": "Mesmo os dados biométricos anônimos usados para pesquisa devem ser tratados com extrema cautela devido a: • O risco de reidentificação quando cruzado com outros conjuntos de dados (por exemplo, imagens de vigilância, mídia social). • A natureza sensível dos identificadores biométricos, que são imutáveis e altamente pessoais. Principais limites e salvaguardas: • Adesão estrita às técnicas de minimização e anonimização de dados, incluindo: o Cegamento do modelo, o

Algoritmos de privacidade diferenciais, o Injeção ou agregação de ruído. •

Proibição de uso secundário ou comercialização de conjuntos de dados biométricos. •

Conselhos de revisão de ética independentes ou avaliações de impacto de proteção de dados (DPIAs) antes do início do projeto. • Nenhuma ligação com informações de identificação pessoal (PII) ou identificadores, a menos que legalmente autorizado e justificado. • Direito de recusar, sempre que possível, mesmo após a anonimização. Os controladores devem ser incentivados a us", "940700": "O uso de tecnologias de

reconhecimento facial pode evitar resultados discriminatórios: • Avaliações de risco e viés pré-implantação (por exemplo, testes de desempenho demográfico para detectar preconceito racial/de gênero). • Auditoria independente e avaliação periódica da justiça algorítmica. •

Limpe os caminhos de exclusão quando o FRT for usado em serviços não essenciais. •

Treinamento inclusivo de conjuntos de dados para minimizar o baixo desempenho em grupos minoritários. • Uso de limites diferenciais ou validação human-in-the-loop para populações sensíveis. • Transparência desde a concepção: forneça aos titulares dos dados: o Finalidades e consequências do uso do reconhecimento facial, o Informações

sobre a precisão e os riscos do sistema, o Pontos de contato para reclamações ou dúvidas. ", "940701": "Para minimizar erros de FRT: • Use algoritmos testados pelo NIST

comparados sob condições demográficas variadas. • Implemente controles ambientais (por exemplo, iluminação, ângulos de câmera) e detecção de vivacidade anti-spoofing. •

Calibre para os modos de identificação e verificação, adaptando os limites com base no caso de uso (por exemplo, controle de fronteira versus embarque). • Integre mecanismos de fallback: documentos de viagem tradicionais, revisão manual ou identificação digital móvel. ", "940702": "O reconhecimento facial pode não ser adequado quando: • O

anonimato público é esperado, por exemplo, nas ruas ou protestos públicos. • Não existe

necessidade ou consentimento claro (por exemplo, vigilância de marketing em shopping centers). • Grupos altamente vulneráveis estão envolvidos (por exemplo, crianças nas

escolas). • Pode surgir um desequilíbrio ou coerção significativa de poder. As alternativas devem incluir: • Carteiras de identidade digital descentralizadas com correspondência biométrica no lado do dispositivo (por exemplo, integração no estilo Apple Face ID). •

Verificação baseada em token (por exemplo, códigos QR, cartões de embarque digitais). • Autenticação multifator (MFA) combinando sinais comportamentais,

dispositivos e dados contextuais. ", "940704": "Medidas de segurança essenciais: •

Criptografia no nível do modelo usando hash seguro específico da biometria (por exemplo, biometria cancelável). • Controle de acesso com segregação estrita de funções e logs de auditoria. • Arquitetura de confiança zero para fluxo de dados entre as camadas de coleta, correspondência e armazenamento. • Avaliações de impacto da proteção de dados específicas para dados biométricos. • Monitoramento contínuo de ameaças e detecção de anomalias em tempo real (por exemplo, para ataques de injeção ou repetição). •

Procedimentos imediatos de notificação de violação. ", "940707": "As boas práticas devem incluir: • Garantir a disponibilidade de modalidades alternativas (• Comunique de forma clara e acessível que o uso biométrico é opcional. • A restrição de acesso deve ser: o Proporcional ao risco, o Transparente quanto à justificação, o Não conduza à exclusão de facto dos serviços públicos. ", "940708": "Práticas recomendadas: • Vinculação de finalidade: restrinja o uso de dados biométricos estritamente à finalidade para a qual foram coletados. • Desempenho algorítmico justo: monitore o desempenho do sistema em idade, sexo e etnia. • Fornecer treinamento para os operadores identificarem e reduzirem os casos de exclusão injusta. • Garantir a aceitação explícita quando a base legal for o consentimento. • Auditorias independentes e medidas de mitigação de vieses no projeto do sistema.

", "940709": "Os controladores devem: • Garanta aviso visível e sinalização sobre o uso de dados biométricos em espaços públicos. • Forneça pontos de acesso móveis ou baseados na Web para informações, consentimento e recusa. • Use processamento anônimo ou pseudonimizado sempre que possível. • Nomeie um DPO dedicado ou um canal voltado para o público para solicitações de direitos. • Implemente painéis de privacidade que permitam que os titulares dos dados gerenciem preferências e revoguem a participação.

", "940710": "Os direitos dos titulares dos dados devem ser respeitados como em qualquer outro processamento de dados. Não deve haver requisitos específicos para o tratamento de dados biométricos. Apenas a retirada do consentimento deve produzir efeitos mais rapidamente do que o normal, a fim de garantir que as informações biométricas são

eliminadas das bases de dados num período mais curto, a fim de evitar riscos.", "940711": "A admissibilidade legal deve ser: • Vinculado a uma necessidade clara, como proteção infantil, controle de acesso nas escolas ou segurança no transporte. • Com base no consentimento explícito e informado dos pais ou responsáveis legais. • Acompanhado por explicações adequadas para crianças sobre como seus dados são usados. As salvaguardas incluem: • Minimização de dados apropriada à idade (por exemplo, limitar a retenção ou a riqueza de recursos de modelos biométricos). • Restrições de acesso: apenas pessoal qualificado e com verificação de antecedentes pode lidar com os dados. • Isolamento de dados: sem uso além da configuração específica (por exemplo, sem compartilhamento com terceiros). ", "940712": "", "940714": "Os requisitos incluem: • Uso de estimativa única e não invasiva somente quando estritamente necessário (por exemplo, serviços on-line com restrição de idade). • Evite armazenar modelos biométricos, opte por retenção zero ou processamento sem servidor. • Incorporar avaliações de proporcionalidade e avaliações de impacto infantil. • Forneça uma opção de substituição manual com verificação de identidade pelos pais/responsáveis.

Contribuinte: GUSTAVO RIBEIRO MURAD

Número: OP-968529

Data: 01/07/2025 - 08:27

Resumo: "De acordo com a LGPD, dados biométricos são considerados dados pessoais sensíveis quando se destinam a identificar uma pessoa natural. Para tanto, devem reunir critérios objetivos como: (i) relação com características físicas, fisiológicas ou comportamentais da pessoa; (ii) possibilidade de medição, registro e comparação técnica; (iii) estabilidade relativa ao longo do tempo; e (iv) capacidade de permitir a identificação única ou autenticação do titular. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, voz e padrões comportamentais. Quando não utilizados para identificar ou autenticar, esses dados podem não se enquadrar como sensíveis, exigindo análise do contexto do tratamento.", "940688": "Controladores que tratam dados biométricos devem adotar práticas de transparência ativa que garantam o fornecimento prévio de informações claras e acessíveis aos titulares. Isso inclui: (i) avisos visíveis e compreensíveis nos locais de coleta; (ii) políticas de privacidade específicas, detalhando a finalidade, base legal, tempo de retenção, medidas de segurança, eventual compartilhamento e os direitos dos titulares; (iii) linguagem acessível, especialmente quando o público inclui grupos vulneráveis; (iv) disponibilização de canais de atendimento para dúvidas e solicitações; e (v) divulgação, quando cabível, de versão simplificada do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), promovendo maior confiança e controle por parte dos titulares.", "940690": "A biometria comportamental, por sua natureza dinâmica e dependente de variáveis contextuais (como humor, ambiente e estado físico), demanda maior rigor quanto à qualidade dos dados e à segurança. Deve ser tratada com protocolos específicos de calibração contínua, validação periódica de acurácia e teste de vieses entre diferentes grupos populacionais. Também é essencial garantir que a coleta seja limitada ao mínimo necessário, com registro de logs de acesso e uso, uso de técnicas de anonimização sempre que possível, e consentimento reforçado, dada a dificuldade de antecipação dos usos futuros. Além disso, a segurança deve considerar ataques por engenharia social e spoofing, com métodos atualizados de detecção de fraudes. Por fim, projetos com uso dessa tecnologia devem ser submetidos a RIPD e avaliação prévia de riscos éticos e jurídicos.", "940693": "Considerando que o consentimento, no âmbito jurídico, pressupõe uma decisão livre e consciente, isto é, não viciada por erro, ignorância, entre outros vícios, a maneira de se aferir a validade dessa manifestação de vontade seria por meio de documento denominado "termo de consentimento", no qual o tratamento de dados biométricos seja descrito de forma clara, indicando sua finalidade, a forma de uso e o prazo de armazenamento, exigindo a assinatura com firma reconhecida ou mediante assinatura digital via ICP-Brasil, prevendo sanção pela ausência do documento. Não pode ser considerada uma hipótese mediante consentimento a hipótese "c" quando se tratar de órgão de pesquisa privada.", "940695": "Deve ser elaborado um modelo de formulário que justifique os meios adotados para garantir a segurança e prevenir fraudes, do mesmo modo que, mediante a comprovação das medidas efetivamente implementadas, sendo obrigatória a assinatura do Encarregado (DPO) no referido documento.", "940697": "Igualmente por meio de formulário pelo qual seja possível aferir a

Adequação à finalidade legal, Necessidade e proporcionalidade, Finalidade específica e Transparência", "940699": "Embora a LGPD preveja a possibilidade de tratamento de dados biométricos por órgãos de pesquisa com base no art. 11, II, "c", mesmo sem consentimento, o avanço das tecnologias de análise e cruzamento de bases de dados eleva significativamente o risco de reidentificação, mesmo em cenários de anonimização. Nesse contexto, a legislação poderia evoluir para definir critérios técnicos mínimos de anonimização e exigir avaliações periódicas de risco de reidentificação, com metodologias auditáveis. Além disso, seria desejável que a LGPD incorporasse obrigações específicas de governança para projetos de pesquisa, como a submissão obrigatória de projetos a comitês de ética independentes e a elaboração de RIPD. Por fim, uma possível melhoria normativa seria a previsão expressa de responsabilização objetiva em casos de reidentificação indevida, como forma de reforçar a confiança social na utilização de dados biométricos em pesquisas e proteger efetivamente os direitos fundamentais dos titulares.", "940700": "Mesmo quando amparado por uma hipótese legal, o uso de reconhecimento facial deve observar os princípios da LGPD. Para isso, recomenda-se: (i) realização de Relatório de Impacto à Proteção de Dados (RIPD); (ii) auditorias externas periódicas para revisar código-fonte, bases de dados e logs de uso; (iii) transparência algorítmica, com divulgação das variáveis utilizadas, lógica decisória e taxas de erro; (iv) testes de viés com métricas desagregadas por grupo (raça, gênero, idade etc.) e planos de mitigação quando necessário; (v) treinamento de IA com base em dados representativos e diversos; (vi) adoção de medidas técnicas de segurança, como anonimização sempre que possível; e (vii) estruturação de governança robusta com políticas internas claras e canal para atendimento de titulares. Essas medidas reduzem riscos de discriminação e reforçam a conformidade ética e jurídica do tratamento.", "940701": "Sistemas de reconhecimento facial devem ser projetados com base no princípio do privacy by design, com uso de bases auditadas, testes de acurácia por grupo populacional (raça, gênero, faixa etária) e validação contínua. É essencial prever mecanismos para mitigar falhas, como canal de contestação acessível e multicanal, com registro de protocolo, revisão humana obrigatória e resposta em até 15 dias, com possibilidade de recurso. As ocorrências de erro devem retroalimentar o sistema, promovendo revisão do algoritmo e atualização contínua. Devem ser adotados controle de versões, coleta mínima de dados, revisão periódica do Relatório de Impacto à Proteção de Dados (RIPD) e atuação do DPO na supervisão das correções, garantindo a eficácia, confiabilidade e conformidade do tratamento automatizado.", "940702": "O uso de reconhecimento facial não é recomendado em contextos como vigilância massiva em espaços públicos, escolas, processos de recrutamento, análise de crédito e marketing, devido ao alto risco de discriminação, invasão de privacidade e desproporcionalidade no tratamento dos dados pessoais. Como alternativas eficazes e menos invasivas, os controladores podem adotar tecnologias como crachás com NFC, QR codes, autenticação por senha combinada com token, chaves de segurança FIDO, sensores anônimos para detecção e biometria local que não expõe dados sensíveis, garantindo maior segurança e proteção aos titulares.", "940704": "Para mitigar riscos de violação de dados biométricos, são indispensáveis medidas técnicas e administrativas como a realização de Avaliação de Impacto à Proteção de Dados (DPIA) e auditorias periódicas que verifiquem a conformidade com a LGPD e políticas internas. É essencial implementar criptografia robusta,

anonimização, controle rigoroso de acesso, autenticação multifator e monitoramento contínuo dos sistemas. As organizações devem estabelecer parâmetros mínimos para avaliação constante dos riscos, revisar regularmente as bases legais que legitimam o tratamento e manter um plano estruturado de resposta a incidentes para proteção integral dos dados sensíveis.", "940707": "É fundamental oferecer alternativas à autenticação biométrica, garantindo transparência quanto ao uso dos dados. A recusa do titular não deve impedir o acesso ao serviço, apenas limitar funcionalidades que dependam tecnicamente da biometria, sempre de forma proporcional, justificada e sem discriminação ilícita ou abusiva. Essa limitação deve ser comunicada claramente, respeitando o princípio da transparência e assegurando que o titular tenha escolhas informadas, evitando qualquer forma de tratamento desigual.", "940708": "Boas práticas para o tratamento de dados biométricos incluem a realização de Avaliação de Impacto à Proteção de Dados (DPIA), uso de criptografia forte, anonimização e controle rigoroso de acesso. É fundamental estabelecer política clara de retenção e descarte dos dados. A transparência deve ser garantida por meio de comunicação clara sobre a finalidade e o uso responsável dos dados, incluindo a oferta de alternativas em serviços não essenciais, respeitando o direito de recusa. Além disso, é importante revisar regularmente algoritmos para evitar vieses e discriminação ilícita ou abusiva contra os usuários.", "940709": "Para assegurar a autodeterminação informativa em tratamentos contínuos e massivos de dados biométricos, como em smart cities e monitoramento público, o controlador deve equilibrar a necessidade do tratamento com os direitos dos titulares. É essencial realizar Avaliação de Impacto à Proteção de Dados (DPIA), comunicar de forma acessível e transparente, disponibilizar canais eficazes de atendimento para o exercício dos direitos, minimizar a coleta e retenção de dados e demonstrar proativamente medidas de transparência, controle e prestação de contas, mesmo diante das limitações naturais desses contextos. ", "940710": "Os agentes de tratamento devem garantir o respeito aos direitos dos titulares por meio de transparência ativa e comunicação em linguagem acessível. Devem disponibilizar canais eficazes para solicitações de acesso, correção e revogação do consentimento. Em contextos de tratamento automatizado de dados biométricos, é fundamental assegurar a possibilidade de revisão humana das decisões, além de fornecer explicações claras sobre os critérios adotados, conforme os princípios da LGPD, garantindo a proteção dos direitos e a confiança dos titulares.", "940711": "O tratamento de dados biométricos de crianças e adolescentes deve ocorrer somente com consentimento específico dos pais ou responsáveis, conforme art. 14, §1º da LGPD. Para garantir participação informada, os agentes devem fornecer informações claras e acessíveis, disponibilizar canais para consulta e revogação do consentimento. Medidas técnicas indispensáveis incluem criptografia, controle rigoroso de acesso, monitoramento e registro de logs, além de políticas de retenção e auditoria contínua, assegurando proteção contra vazamentos e uso indevido, em estrito alinhamento com o princípio do melhor interesse do menor. ", "940712": "O tratamento de dados biométricos de crianças e adolescentes é admissível mediante consentimento específico e em destaque dos pais ou responsáveis (art. 14, §1º da LGPD), devendo respeitar o princípio do melhor interesse. É essencial garantir participação informada por meio de linguagem acessível, transparência sobre a finalidade e canais de comunicação eficazes. O tratamento deve ser proporcional, utilizar apenas os dados estritamente necessários e

considerar alternativas menos invasivas. Devem ser adotadas salvaguardas técnicas e organizacionais robustas, como criptografia, controle de acesso e auditorias regulares, para evitar abusos ou vazamentos.", "940714": "A verificação ou estimação de idade por dados biométricos deve observar o princípio do melhor interesse da criança e o da necessidade, conforme a LGPD. O tratamento deve ser proporcional, limitado à finalidade específica e adotar a coleta mínima de dados. Sempre que possível, deve-se priorizar métodos menos invasivos. É indispensável obter consentimento específico dos responsáveis, com informações claras sobre o uso dos dados. Devem ser aplicadas medidas técnicas e organizacionais robustas para evitar riscos, incluindo criptografia, anonimização, retenção limitada e mecanismos de supervisão e auditoria contínua.

Contribuinte: THAIS DE LIMA FERNANDES

Número: OP-968689

Data: 01/07/2025 - 11:46

Resumo: "Critérios objetivos a serem observados: (i) natureza do dado (dados físicos, fisiológicos ou comportamentais); (ii) uso de tecnologia específica para o tratamento; e (iii) finalidade específica (dado coletado com a intenção de identificação ou autenticação única do titular). 1. Relação com características físicas, fisiológicas ou comportamentais O dado deve se referir a elementos únicos do corpo ou do comportamento de uma pessoa natural — como impressão digital, íris, rosto, voz, forma de andar ou digitar. Isso é destacado pelo Art. 4(14) da GDPR e pela orientação do ICO (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/key-data-protection-concepts/#whatisbiometric>). 2. Processamento técnico específico Não basta o dado bruto: é necessário que haja tratamento técnico específico (como algoritmos de reconhecimento facial ou análise de voz), que extraia vetores ou padrões biométricos a partir desses dados. Por ex", "940688": "Devem ser informados, de forma clara e prévia: origem do dado, finalidades específicas, prazo de retenção, compartilhamento, medidas de segurança, direitos e canais de contato. Avisos internos e externos devem ser destacados, com sinalização em coletas automatizadas. As medidas de transparência devem ser alinhadas às exigências já previstas na legislação de proteção de dados pessoais e em recomendações emitidas pela ANPD.", "940690": "A biometria comportamental é menos precisa, mas também menos intrusiva e pode servir como apoio seguro à identificação. Por isso, não exige mais restrições que a biometria tradicional, mas sim tratamento proporcional ao risco, com foco em qualidade dos dados e prevenção de erros.", "940693": "Deve ser ofertada opção real de aceite ou de recusa, sem condicionamento ou coerção imposta ao titular. Não deve ser usado se houver base legal mais adequada ao caso concreto, especialmente quando houver desequilíbrio de poder ou impossibilidade de fornecimento de consentimento válido pelo titular. O consentimento para o tratamento de dados biométricos deve ser livre, informado, específico, destacado e inequívoco, com opção real de recusa e alternativa viável. No entanto, o consentimento não deve prevalecer sobre outras bases legais. Quando outra base legal for mais adequada ao caso concreto, ela deve ser priorizada, garantindo maior proteção ao titular

e mais segurança jurídica ao controlador. O uso do consentimento é inadequado em contextos com desequilíbrio de poder, ausência de transparência ou quando não for possível assegurar sua real voluntariedade.", "940695": "É necessário prezar pela proporcionalidade ao bem jurídico tutelado, como a segurança e a integridade dos titulares. Para avaliar a adequação, considerar a legalidade e o benefício gerado com o tratamento. É possível a combinação com outros métodos, como análise de documentos, como salvaguarda. A aplicação da hipótese legal de prevenção à fraude exige que o uso da biometria seja proporcional ao risco envolvido e ao bem jurídico tutelado, como a segurança patrimonial e a integridade do titular. Deve-se observar a legalidade da atividade, a adequação da medida e a estrita necessidade da coleta do dado biométrico. Para compatibilizar o princípio da necessidade, recomenda-se adotar abordagens graduais, como o uso combinado de biometria com outros métodos (ex.: análise documental ou autenticação multifator), evitando a coleta excessiva. Salvaguardas como avaliação de impacto, medidas de segurança, revisão periódica da eficácia do método e garantia de alternativas viáveis ao titular são fund", "940697": "O critério deve ser se restringir à finalidade específica abrangida pela determinação legal ou regulatória. Salvaguardas a serem observadas: transparência ativa, medidas técnicas como controle de acesso e criptografia, e políticas de governança que assegurem a proteção dos direitos dos titulares.", "940699": "O tratamento deve ocorrer dentro do órgão, com finalidade legítima, em ambiente seguro e mediante anonimização ou pseudonimização. Devem ser adotados controles de acesso, segregação de bases e rastreabilidade das operações, bem como restrições contratuais quanto ao uso e compartilhamento dos dados.", "940700": "Para garantir o uso ético do reconhecimento facial, é preciso diversidade no banco de dados, testes de viés, validação do algoritmo, opções acessíveis, informação clara ao titular, avaliação de riscos, treinamento de equipes e orientações da ANPD dos padrões de segurança e transparência aplicáveis.", "940701": "Devem usar algoritmos precisos sob padrões técnicos adequados (ex: ISO), treinados com bases diversas e atualizadas, garantir segurança no processamento, boa qualidade de imagem e controle ambiental. Devem prever revisão humana, canais de correção e medidas para reduzir erros e proteger titulares.", "940702": "Não é recomendado em identificação remota em tempo real, com crianças ou idosos, para marketing ou para tomadas de decisão automatizadas, por poder ser intrusivo ou discriminatório. Alternativas de identificação com menor impacto à privacidade são crachás, vídeo comum ou autenticação multifator.", "940704": "Verificações de acurácia e vulnerabilidades (auditorias, testes de intrusão e risco), revisão contínua das medidas de segurança, uso de criptografia, controle de acesso, intervenção humana qualificada e monitoramento de aspectos legais e éticos no uso da tecnologia.", "940707": "Boas práticas são: proporcionalidade ao risco, especialmente quanto à proteção contra fraudes e acesso a dados sensíveis; com transparência na justificativa sobre a finalidade de uso e a necessidade da biometria; medidas testadas para evitar discriminação ou exclusão indevida.", "940708": "Boas práticas incluem uso de bases diversas e atualizadas, testes regulares de acurácia e viés, criptografia, controle de acesso, transparência sobre finalidades e riscos, limitação do uso ao necessário, revisão ética (humana) contínua e canais acessíveis para contestação e correção de erros.", "940709": "Controladores podem garantir transparência com placas informando o uso de câmeras com reconhecimento facial e QR Code para acesso a informações adicionais,

como finalidade do tratamento (ex.: segurança pública), identidade do controlador, canal de contato e direitos dos titulares", "940710": "Por meio de medidas de transparência como aviso de privacidade acessível no ponto de coleta, por opções facilitadas de cadastramento com duplo fator de autenticação em comunicações e por canal claro para revogação do consentimento ou oposição no próprio ponto de controle de acesso e comunicações.", "940711": "A participação dos pais deve ser garantida por comunicado específico em linguagem clara sobre a finalidade da biometria. Deve-se avaliar meios menos invasivos e assegurar o melhor interesse do menor, prevalecendo os casos de uso benéficos ao titular para a identificação precisa (ex: segurança).", "940712": "O tratamento é admissível quando alinhado ao melhor interesse da criança. Deve haver participação informada dos responsáveis por meio de avisos de privacidade e comunicações claras. É essencial adotar criptografia, controle de acesso, logs, auditorias contínuas, RIPD e treinamentos.", "940714": "Medidas de verificação de idade não devem ser excessivas, demandando análise de proporcionalidade. Para compatibilizar com o melhor interesse do menor, é preciso minimizar os dados coletados, limitar o prazo de retenção com sua eliminação após verificação, e conduzir RIPD para avaliar impactos.

Contribuinte: Patrícia Carneiro Rodrigues PEREZ

Número: OP-968762

Data: 01/07/2025 - 12:44

Resumo: "Não existem razões para não seguir os critérios presentes na definição do art.º 4º, 14 do RGPD e reiterada no art. 3º, 34 do Regulamento da IA da União Europeia, essencial será a "associação, direta ou indireta, a um indivíduo", em termos tecnicamente inequívocos, como consta no art. 5º, XI da LGPD. (Resposta: Prof. Manuel David Masseno)", "940688": "A transparência ativa exige linguagem clara e acessível, com aviso de privacidade e, se aplicável, consentimento prévio e informado, garantindo que o titular compreenda o tratamento antes de fornecer seus dados. (Resposta: Mariana Ganem)", "940690": "A biometria comportamental deve ter tratamento equivalente à tradicional, com ênfase em controles técnicos e organizacionais que garantam qualidade, segurança e integridade dos dados, mitigando riscos de reidentificação e falhas. (Resposta: Zaira Sardinha)", "940693": "Em especial, deverão ser facultadas as informações sobre as tecnologias empregues para um tratamento automatizado e suas consequências. Em qualquer caso, pois o consentimento será a base crucial comum, devido a assimetria entre o titular e o agente, deverá ser sempre exigido um relatório de impacto. (Resposta: Prof. Manuel David Masseno e Prof. Catarina Sarmento e Castro)", "940695": "A coleta de dados deve ter um propósito documentado, proporcional ao risco de fraude com aviso de privacidade e medidas de segurança de proteção das informações, definição de período de retenção, descarte seguro e autenticação em múltiplos fatores. Essencial RIPD e LIA antes do tratamento de dados. (Resposta: Maria Claudia Gouveia e Cristiane Manzueto)", "940697": "Mesmo com base legal, o tratamento de dados biométricos deve seguir os princípios da LGPD, como: necessidade, segurança e transparência. Órgãos públicos devem justificar a coleta, informar os titulares e

elaborar RIPD, quando aplicável. (Resposta: Luís Antônio Baraúna Lopes)

", "940699": "Mesmo com anonimização, o uso de dados biométricos para pesquisa exige finalidade legítima, minimização, e proteção contra reidentificação. Devem-se aplicar salvaguardas como RIPD, controles de acesso, anonimização robusta e ética na pesquisa para proteger os titulares. (Resposta: Luís Antônio Baraúna Lopes) ", "940700": "É preciso justificar a adoção da FRT e limitar o uso ao mínimo necessário, com base clara e legítima, informar os titulares, garantir revisão humana, auditar algoritmos contra vieses, aplicar segurança reforçada, controle de acesso, RIPD e supervisão por comitês éticos e órgãos independentes. (Resposta: Beatriz Haikal)

", "940701": "Sistemas de reconhecimento facial devem ser projetados com diversidade de dados, testes rigorosos, validação contínua e revisão humana, com auditorias, canais de correção, registros de decisão e mecanismos de contestação e responsabilização. (Resposta: Natane Santos e Gustavo Oliveira)", "940702": "A TRF não é indicada para reconhecer

emoção, vigilância pública em massa, categorizar com IA biometria de dados sensíveis de indivíduos, dados de crianças/adolescentes para evitar discriminação, vigilância abusiva, risco à privacidade. Recomenda-se métodos menos intrusivos: cartões, senhas ou token. (Resposta: Carla de Campos Rebello)", "940704": "Medidas como teste de intrusão (pentest) comprovando aplicação de fraude, controle de acesso, políticas rigorosas e aplicação de treinamentos. Utilizar RIPD, LIA e avaliação/homologação da ferramenta. Auditoria e revisões de segurança (rastreadabilidade/vulnerabilidades) como parâmetros mínimos. (Resposta: Cristiane Manzueto)", "940707": "Em serviços não essenciais com biometria,

ofereça alternativas para garantir o acesso. Restrinja o acesso por recusa de consentimento APENAS se a biometria for tecnicamente essencial à funcionalidade. Seja proporcional, transparente e informe o titular previamente sobre qualquer restrição. (Resposta: William Rocha)", "940708": "Visando proteger esses dados o controlador deve adotar boas práticas, como a realização de uma Avaliação de Impacto e reduzir a coleta. Além disso, é preciso deixar claro ao titular como os dados serão tratados e por quanto tempo, de forma transparente e responsável, como prevê o art. 9º da LGPD. (Resposta: Larissa Carneiro)", "940709": "As medidas devem ter justificativa clara, fim definido, base legal robusta, impacto avaliado e ser não-discriminatórias. Recomenda-se transparência ativa (QR Code), acesso online à informação e direitos via formulário eletrônico, com dados criptografados. (Resposta: Prof. Catarina Sarmiento e Castro)", "940710": "Eles devem ter avisos de privacidade claros, que informem a forma de coleta, finalidade, hipótese legal, direitos dos titulares, segurança, compartilhamento, transferências, retenção, descarte, RIPD, como reclamar à ANPD, contato do encarregado, assegurando transparência e boas práticas utilizadas. (Resposta: Carla de Campos Rebello)", "940711": "A Coleta deve ser mínima, com consentimento claro, específico e destacado de ao menos um responsável. É necessário aviso de privacidade com finalidade, prazo de guarda e exercício de direitos. Deve-se adotar medidas seguras e menos invasivas, com RIPD. (Resposta: Andrea Goes)", "940712": "O tratamento deverá ser excepcional, proporcional e pautado no melhor interesse da criança, conforme o art. 11 da LGPD. Prioriza-se o inciso I e, na ausência de capacidade civil, aplica-se o inciso II, alínea “d”, mediante representação legal. (Resposta: Renato Santa Rita)", "940714": "A coleta biométrica deve ter consentimento dos responsáveis, parceria com

órgãos públicos e seguir a LGPD, considerando riscos (conteúdo, contato, conduta e contrato), garantindo o melhor interesse de crianças e adolescentes com abordagem mínima, segura e transparente. (Resposta: Shirley Figueiredo)

Contribuinte: CARLA DE CAMPOS REBELLO

Número: OP-969104

Data: 02/07/2025 - 07:42

Resumo: "Devem ser considerados dados biométricos todos aqueles derivados de características físicas, fisiológicas ou comportamentais de uma pessoa natural que, por meio de tratamento técnico específico, permitam ou confirmem sua identificação única, como imagens faciais ou dados dactiloscópicos. Essa definição está alinhada ao GDPR (art. 4º, item 14), ao ICO do Reino Unido e às orientações da ANPD na Nota Técnica nº 17/2025. Essa caracterização é essencial para garantir o tratamento diferenciado que os dados biométricos demandam, dada sua natureza sensível e seu potencial lesivo à privacidade e à autodeterminação informativa. ", "940688": "A transparência ativa, prevista nos arts. 6º, VI e 9º da LGPD, é obrigação legal. Porém, dados mostram seu descumprimento sistemático. Apenas 29% dos contratos de reconhecimento facial analisados estavam disponíveis; 64% não indicavam base legal e 84% não tinham cláusulas sobre proteção de dados. Em 70% dos projetos, não havia informação sobre fornecedores; em 80%, faltavam relatórios de impacto. No esporte, nenhum estádio analisado publicava dados sobre sistemas biométricos. Recomenda-se à ANPD: regulamentar a publicação de DPIAs, bases legais, objetivos, tempo de retenção, fornecedores, critérios técnicos, métricas de erro e cláusulas contratuais; garantir canais acessíveis para exercício de direitos; nomeação e visibilidade de DPOs; e publicação ativa de dados consolidados. Também se sugere a criação de selos públicos de boas práticas, inspirados no GDPR. ", "940690": "A biometria comportamental (como digitação, entonação, modo de andar) exige cautela. É classificada como de alto risco pelo Ato Europeu de IA (art. 6.2 e Anexo III), com exigência de gestão de riscos. Por ser coletada de forma contínua e invisível, eleva o risco de vigilância permanente e amplia a assimetria entre agentes e titulares. Pode ser usada para fins invasivos como inferência emocional e controle de produtividade. Devem ser exigidas: proibição de coleta sem consentimento, avaliações de impacto, minimização e limitação de finalidade. Diretrizes da CNIL e do EDPB recomendam proibir esses usos em contextos sensíveis como educação, saúde, trabalho e segurança. Estudo de Kalvaityte mostra que impactos sociais da IA, como manipulação e violação de direitos de trabalhadores e crianças, seguem sem regulação. Dallasta propõe chamá-los de impactos tecnossociais, demandando proteção específica. ", "940693": "O consentimento só é válido se for livre e informado, ou seja, não pode ser condicionado ao acesso a serviços essenciais, nem dado sob linguagem técnica ou opaca. Em contextos como segurança pública, escolas, saúde, transporte e estádios, não há margem real de escolha, o que torna o consentimento presumivelmente inválido. Essa posição é respaldada pelo EDPB (2020) e por decisões da CNIL (França). Na Suécia, escolas foram multadas por uso de reconhecimento facial com base no vício de consentimento diante da autoridade escolar. Diante disso, a

ANPD deve declarar a inadequação do consentimento nesses contextos e exigir avaliação de impacto e alternativas menos invasivas, assegurando que o acesso a serviços não dependa da biometria. O reconhecimento facial não pode ser critério para exercer direitos básicos. A proteção de dados exige que a escolha seja efetiva e nunca imposta pela estrutura de poder.

","940695": "A base legal da “prevenção à fraude” só é legítima quando o risco for iminente, documentado e proporcional à intrusão. A ANPD deve exigir: Relatório de Impacto (DPIA); demonstração de que a biometria é a única alternativa; garantia de contestação humana; retenção limitada; e exclusão automática após verificação. O uso amplo e genérico dessa base viola o princípio da necessidade (art. 6º, III, LGPD) e pode gerar discriminação algorítmica. Não há estudos que comprovem que o reconhecimento facial previne fraudes. Pelo contrário: por ser coletado de forma passiva, esse dado pode ampliar o risco de acesso indevido. Reportagens apontam o uso fraudulento da biometria em sistemas federais, como no caso das 3.000 contas do Gov.br investigadas pela Polícia Federal (COUTINHO, 2024). O uso indiscriminado da biometria, sob o pretexto de prevenção, enfraquece direitos e não garante segurança.

","940697": "Quando o tratamento de dados biométricos se baseia no art. 11, II, “a” da LGPD, a obrigação legal deve estar prevista em norma específica, acessível, relacionada à finalidade do tratamento e dentro da competência do órgão público. A generalidade normativa não pode justificar o uso massivo de dados sensíveis. Relatório do CEsEC e da DPU mostra que, em diversos projetos de TRF no Brasil, essa base tem sido usada de forma genérica, sem fundamento jurídico claro, DPIA ou controle externo. Isso fere os princípios da legalidade, finalidade e autodeterminação informativa, além de contrariar a Convenção 108+ do Conselho da Europa. A ANPD deve exigir: norma pública e específica; realização e revisão periódica de DPIAs; supervisão institucional e auditorias independentes; canais acessíveis de exercício de direitos; e regras claras de retenção e descarte. A invocação genérica da “obrigação legal” não pode isentar o Estado de justificar o uso de tecnologias invasivas como a TRF.

","940699": "Mesmo em pesquisas, dados biométricos exigem salvaguardas específicas, pois sua singularidade aumenta o risco de reidentificação, especialmente em cruzamentos de bases. A anonimização deve seguir padrões técnicos robustos (ISO/IEC 20889:2018), com cláusulas de irreversibilidade, auditorias de risco e proibição contratual de reidentificação. A ANPD deve exigir: documentação clara dos métodos usados; submissão aos comitês de ética independentes; controles técnicos e operacionais de segurança; e critérios para compartilhamento institucional. Também se recomenda proibir o uso de dados biométricos para pesquisa com grupos vulneráveis (como crianças, pessoas em situação de rua ou privadas de liberdade) sem marco legal específico e garantias excepcionais. A base legal da pesquisa não pode ser usada como atalho para legitimar práticas opacas de treinamento algorítmico, como nos escândalos envolvendo bancos biométricos usados sem consentimento.

","940700": "A conformidade do reconhecimento facial com a LGPD exige padrões técnicos auditáveis desde o projeto até a operação. Segundo o EDPB, a ICO e a Convenção 108+, é obrigatório realizar avaliações de impacto que considerem base legal, finalidade, arquitetura do sistema, algoritmo, base de treinamento e qualidade dos dados. Estudos como o Gender Shades revelam erros superiores a 30% em mulheres negras, fruto de vieses nos dados e na modelagem. É necessário exigir métricas como FMR, FNMR e EER segmentadas por raça, gênero e idade, revisão humana

qualificada, criptografia robusta, limitação da retenção e vedação ao uso em vigilância generalizada. Também se impõe o registro de logs, auditorias independentes e transparência pública. Sem essas salvaguardas, o uso da TRF viola princípios da LGPD e reforça discriminações sob a aparência de neutralidade, gerando falsos positivos, abordagens ilegais e exclusões sociais injustificadas. ",940701": "A eficácia e confiabilidade das TRFs exigem: (i) testes rigorosos em contextos reais e diversos antes da implementação; (ii) publicação de métricas de erro como FMR e FNMR; (iii) auditorias externas independentes; e (iv) mecanismos acessíveis de contestação pelos titulares. Como mostram os relatórios do CESeC, o Brasil carece de padrões técnicos mínimos e de qualquer certificação prévia dos algoritmos utilizados. Em estádios e vias públicas, há altos índices de falsos positivos, com constrangimentos ilegais e detenções indevidas. O erro técnico não é uma “falha tolerável”: é um dano real à liberdade, à reputação e à dignidade dos cidadãos. Sem controles rigorosos, o uso da TRF viola princípios fundamentais da LGPD, como necessidade, não discriminação e responsabilização, e transforma tecnologias de segurança em instrumentos de violência algorítmica. ",940702": "O uso de reconhecimento facial não é recomendado em contextos de vigilância massiva (como eventos, transportes, escolas, shoppings e estádios) conforme alertam a ONU, o EDPS e a Recomendação 5/2021 da ANPD. Nesses ambientes, a coleta é, em geral, indiscriminada, desproporcional e opaca, gerando alto risco de abusos e reforço de estigmas sociais. Alternativas menos intrusivas, como QR Codes temporários, cartões magnéticos, tokens criptografados e senhas, devem ser priorizadas. A escolha por tecnologias que minimizem a coleta de dados sensíveis é uma obrigação ética e legal. O reconhecimento facial deve ser restrito a situações excepcionais, com justificativa detalhada, proporcionalidade comprovada e salvaguardas técnicas e jurídicas. Usá-lo como padrão em espaços públicos compromete direitos fundamentais, viola o princípio da minimização e aprofunda desigualdades já existentes. ",940704": "Dados biométricos, por serem permanentes e não substituíveis, exigem proteção reforçada. Medidas técnicas mínimas incluem: criptografia forte dos templates, anonimização ou pseudonimização, retenção limitada, controle de acesso e logging com auditoria. No plano administrativo, devem ser exigidos: avaliações de impacto (DPIA), planos de resposta a incidentes, auditorias periódicas, DPOs nomeados e políticas claras de governança. Esses requisitos são condições mínimas de conformidade com a LGPD. Segundo relatório do CESeC e da DPU, a maioria dos projetos públicos com reconhecimento facial no Brasil carece dessas salvaguardas. A ANPD deve estabelecer parâmetros obrigatórios de avaliação de riscos, incluindo análise de viés, possibilidade de reidentificação e impactos sobre grupos vulneráveis. Proteger dados biométricos é proteger direitos fundamentais, e isso exige rigor técnico, jurídico e institucional. ",940707": "Nos casos em que funcionalidades específicas de um serviço dependem de autenticação biométrica, os controladores devem garantir alternativas tecnológicas viáveis, como autenticação por token ou senha, para evitar discriminação indireta. Essa prática deve ser acompanhada de avaliações de impacto e consulta pública, principalmente em serviços digitais amplamente utilizados. A recusa do titular em fornecer seus dados biométricos, quando o consentimento for a base legal, não pode acarretar exclusão ou desvantagem desproporcional, a não ser em situações em que o uso da biometria seja tecnicamente indispensável, devidamente justificado e documentado. ",940708": "Entre as

boas práticas esperadas estão: publicação de relatórios periódicos de impacto à proteção de dados; disponibilização pública das bases legais e finalidades do tratamento; detalhamento das métricas de erro (FMR, FNMR) por grupo demográfico; canais acessíveis para que titulares possam questionar o uso de seus dados; e mecanismos automatizados de revogação de consentimento. Os projetos de implementação de TRFs devem ser concebidos segundo os princípios de privacy by design e accountability, com documentação pública das decisões técnicas e legais. ", "940709": "Em iniciativas de cidades inteligentes, vigilância urbana ou controle de multidões, como mostrado no relatório Vigilância por lentes opacas, a coleta contínua e opaca de dados biométricos ocorre com baixa ou nenhuma transparência. Para garantir autodeterminação informativa, é essencial que o uso dessas tecnologias esteja submetido a notificações visíveis e acessíveis no local, campanhas de informação pública, mecanismos de exclusão de dados (quando possível), e consulta pública prévia às comunidades afetadas. A coleta massiva sem consentimento informado, sobretudo em espaços com presença de grupos vulneráveis, como crianças, configura violação dos direitos previstos nos artigos 6º e 18 da LGPD. ", "940710": "A garantia desses direitos exige mecanismos acessíveis e contínuos de informação clara sobre o tratamento, incluindo linguagem simples e multicanal (digital e físico), direito à revisão humana em decisões automatizadas (art. 20 da LGPD), possibilidade real de exclusão de dados e transparência sobre a base legal utilizada. Sistemas implementados em locais públicos, como escolas ou estádios, devem ser informados com antecedência, inclusive com sinalização visual e acessível no local. ", "940711": "O tratamento de dados biométricos de crianças e adolescentes deve respeitar simultaneamente a LGPD e o ECA, que garantem a proteção integral e o melhor interesse do menor (art. 227 da CF e art. 1º do ECA). Isso exige consentimento específico, livre e destacado dos responsáveis, com canais de comunicação claros e contínuos. A base legal será, em regra, o consentimento; exceções só se aplicam se houver obrigação legal e estrita necessidade comprovada. O relatório Esportes, Dados e Direitos mostra o uso de reconhecimento facial em estádios sem qualquer consentimento prévio, expondo crianças à vigilância estatal indevida e violando a LGPD e o ECA. Essas práticas devem ser proibidas. A coleta biométrica só pode ocorrer mediante avaliação de impacto, salvaguardas técnicas e organizacionais robustas, e garantia de alternativas não discriminatórias caso o consentimento não seja concedido. Crianças não podem ser sujeitas a riscos invisíveis em nome da segurança. ", "940712": "Mesmo quando há base legal, como consentimento ou obrigação legal, o uso de reconhecimento facial em escolas deve ser fortemente desencorajado. A LGPD exige o cumprimento do princípio da necessidade, e o ECA impõe a proteção integral e o melhor interesse da criança e do adolescente. Por seu caráter invasivo e riscos de discriminação e reidentificação, o reconhecimento facial não se justifica em ambientes educacionais, onde há alternativas menos intrusivas para controle de frequência e segurança. Além disso, o consentimento pode não ser livre ou informado em contextos com forte assimetria de poder, como entre escolas públicas e famílias vulneráveis. O mais coerente com a LGPD, o ECA e as boas práticas internacionais é proibir esse tipo de tratamento nessas instituições, garantindo soluções que respeitem a privacidade, o desenvolvimento e a autonomia dos estudantes. Segurança não pode ser pretexto para vigilância indevida. ", "940714": "Essa prática deve ser precedida de avaliação de

impacto que demonstre a inexistência de alternativa menos intrusiva. Sempre que possível, deve-se optar por meios não biométricos ou sistemas que não retenham dados. O tratamento deve ser limitado à finalidade específica, com exclusão clara após o uso, e jamais utilizado para finalidades secundárias, como publicidade. A coleta de biometria apenas para acesso a entretenimento digital, sem garantias, viola os princípios da necessidade e do melhor interesse da criança e do adolescente previstos na LGPD. Com esta contribuição, buscamos colaborar de forma construtiva com o processo regulatório da ANPD, oferecendo subsídios baseados em evidências, experiências de campo e boas práticas. Reforçamos a necessidade de uma regulação robusta, transparente e centrada na proteção de direitos fundamentais. Colocamo-nos à disposição para aprofundar o diálogo e fortalecer a atuação da Autoridade.

Contribuinte: PABLO DE MOURA NUNES DE OLIVEIRA

Número: OP-969154

Data: 02/07/2025 - 08:50

Resumo: "Faz-se referência à definição contida no GDPR, o que nos parece adequado. No entanto, em nossa opinião, essa definição não é suficiente para que os dados biométricos sejam automaticamente incluídos na categoria de dados sensíveis. Originalmente, as diversas regulamentações consideraram que os dados biométricos exigiam proteção especial com base nas características de privacidade e segurança da tecnologia biométrica à época (na União Europeia, por exemplo, isso se baseou em relatórios de 2003 e 2012). Contudo, a segurança e a privacidade dos dados biométricos evoluíram graças à inovação tecnológica, com normas como a ISO/IEC 24745 – Biometric information protection. Por isso, é importante diferenciar os tipos de dados biométricos conforme sejam templates tradicionais ou Referências Biométricas Renováveis. Anexa-se documento nº1 como referência.", "940688": "É uma boa prática fornecer informações em formato de perguntas frequentes (FAQs) no momento do cadastro para que, além dos termos jurídicos próprios de uma política de privacidade conforme a LGPD, o usuário possa entender de forma simples e até gráfica o que é essa tecnologia, se certos dados serão armazenados, quem terá acesso a eles, quais direitos possui etc. Também devem ser promovidas campanhas de informação sobre a tecnologia e, especialmente, adaptadas ao caso de uso (ex.: não é o mesmo um tratamento que permita ao controlador identificar pessoas indiscriminadamente em espaços públicos sem o conhecimento do usuário, do que quando o próprio usuário decide voluntariamente usar esse método para comprovar sua identidade). Essa distinção foi claramente reconhecida no Regulamento de Inteligência Artificial da União Europeia (AI Act), com grande acerto, por meio do conceito de “remoto”, ou seja, conforme haja ou não participação ativa do usuário no uso. Ver pergunta 14.", "940690": "Não é conveniente fazer esse tipo de distinção com base no tipo ou origem da biometria, pois, por exemplo, no reconhecimento de voz há debate sobre ser ou não “biometria comportamental” (já que a voz é amplamente determinada por características fisiológicas do indivíduo, como pregas vocais, laringe...), e está amplamente difundida há anos, permitindo inclusive superar barreiras geracionais por não exigir conhecimentos digitais para seu uso. Pelo contrário, deve-se focar na existência de

avaliações internacionais sobre precisão, ausência de vieses etc. (como as do NIST dos EUA, principal autoridade internacional em avaliação de tecnologias biométricas), ou sobre resistência a ataques de apresentação (como as avaliações da ISO/IEC 30107-3). A tecnologia avança diariamente, por isso não é recomendável incluir nas instruções da ANPD dados específicos de precisão, mas pode-se exigir que os sistemas sejam avaliados.", "940693": "Se os 5 requisitos forem cumpridos, o consentimento é válido. Por isso, é útil oferecer orientações às empresas sobre como atender a cada um deles. Por exemplo, deve-se oferecer uma alternativa ao usuário, ele deve saber o que será feito com seus dados... e o mencionado na pergunta 2 sobre FAQs explicativas é uma boa prática. Ao tratar do requisito de “liberdade” ou “voluntariedade” do consentimento, não se deve levar a exigência a um ponto que a restrinja. Ou seja, desde que sejam oferecidas alternativas ao usuário e ele conheça as características de cada uma, deve ser livre para escolher entre elas ou a opção biométrica. As autoridades de proteção de dados não devem fazer um juízo prévio e genérico de necessidade ou proporcionalidade, pois isso nega a autonomia dos indivíduos e ignora as especificidades de cada caso de uso. Pelo contrário, devem fornecer ferramentas que indiquem o que o controlador deve fazer para garantir que o usuário possa escolher.", "940695": "Este é um conceito em que o ICO já avançou bastante e que agora vem sendo reivindicado por alguns setores (ex., instituições financeiras) em outros países europeus. Está comprovado que o uso de tecnologia biométrica oferece mais certeza na verificação da identidade do que outros elementos de posse (ex.: documento de identidade) ou de conhecimento (ex.: senhas), que apenas geram uma presunção, pois podem ser roubados ou compartilhados. A prevenção a fraudes exige o uso das soluções mais seguras possíveis, e seu uso não pode depender do consentimento do indivíduo (já que quem pretende fraudar não consentirá). Por exemplo, a identificação biométrica pode ser usada para combater o golpe das “laranja”, típico do branqueamento de capitais. Em todo caso, devem ser realizadas avaliações de impacto à proteção de dados antes de adotar essas soluções sem consentimento do usuário, e pode-se considerar também a comunicação prévia à autoridade competente.", "940697": "Os controladores devem elaborar a devida avaliação de impacto em proteção de dados e assegurar o cumprimento de todos os requisitos específicos previstos na norma que exige ou permite a implementação da solução biométrica.", "940699": "Novamente, o ICO avançou na análise dessa questão. Deve-se considerar que, quanto mais precisa é a solução tecnológica, mais segura é para os usuários e melhor protege seus direitos fundamentais. Ou seja, traduz-se em mais confiança quanto à sua confiabilidade, menos vieses etc. Portanto, o treinamento e o avanço tecnológico são altamente desejáveis também sob a ótica da proteção de dados. Para isso, é essencial ter acesso a dados que possam ser usados no treinamento e na avaliação dos sistemas. Assim, a previsão do art. 11, II, “c” é altamente positiva. Como esse inciso se refere a órgãos de pesquisa, seria conveniente esclarecer o que se entende por tais órgãos: por exemplo, universidades e órgãos de pesquisa, e não empresas privadas com interesses comerciais. Isso pode fomentar alianças entre empresas desenvolvedoras desses sistemas e órgãos de pesquisa, ao mesmo tempo em que evita dúvidas sobre possíveis usos secundários dos dados, interesses ocultos, etc.", "940700": "O uso de Referências Biométricas Renováveis (RBRs), conforme a ISO/IEC 24745, permite por padrão (ex.: com sistemas biométricos baseados em Inteligência Artificial) e/ou por design (ex.: com técnicas avançadas de

criptografia) alcançar características de privacidade e segurança que eliminam os riscos tradicionalmente apontados pelas autoridades de proteção de dados. As RBRs, em contraste com os templates biométricos tradicionais, são privadas, irreversíveis, não interoperáveis, revogáveis e múltiplas. Isso elimina o temor tradicional de que os dados biométricos não poderiam ser alterados nem substituídos. É preciso distinguir entre a característica biométrica (o rosto) e o dado biométrico (que resulta do tratamento técnico aplicado a esse rosto). Com as RBRs, pode-se afirmar que, embora a característica biométrica seja única e imutável, o dado biométrico (RBR) é múltiplo e revogável — ou seja, não é único e pode ser modificado. Anexos os docs. nº1 e nº2 como suporte a essa questão.", "940701": "A introdução da inteligência artificial na tecnologia biométrica trouxe avanços significativos em termos de eficiência, confiabilidade, privacidade e segurança. Focando, por exemplo, no reconhecimento facial, a tecnologia biométrica tradicional baseada em landmarks havia atingido um limite de precisão em torno de 95%. Atualmente, com modelos baseados em IA, a precisão supera amplamente os 99%. Essa confiabilidade pode ser observada, por exemplo, nos relatórios das avaliações do NIST. Também no aspecto da segurança, a biometria moderna baseada em Referências Biométricas Renováveis (RBRs), conforme a ISO/IEC 24745 — o que pode ser alcançado por padrão com o uso de sistemas baseados em IA —, garante que os templates biométricos RBRs tenham características como irreversibilidade, não interoperabilidade, revogabilidade, multiplicidade... Anexos os documentos nº1 e nº2 como suporte a essa questão.", "940702": "Existem alternativas ao reconhecimento facial, como o reconhecimento de voz. Essa tecnologia vem sendo utilizada em casos de uso de contact centers, por exemplo, e permite que os usuários comprovem sua identidade com alta confiabilidade sem sair do canal habitual (telefônico). Além disso, a biometria de voz tem grande aceitação entre pessoas idosas, pois não exige habilidades digitais nem o uso de dispositivos móveis ou computadores. A biometria de voz também é avaliada pelo NIST em termos de confiabilidade e precisão, e pode ser analisada com base na ISO/IEC 30107-3 quanto à resistência contra ataques de falsificação (spoof). Em alguns casos, é recomendável combinar dois tipos de biometria (biometria multimodal) ou combinar biometria (fator de inerência) com outro dado em posse do usuário (por exemplo, seu documento de identidade – fator de posse – ou uma senha – fator de conhecimento). Isso permite uma autenticação reforçada em situações de maior criticidade.", "940704": "Conforme explicado, o uso de RBRs (especialmente difundidas na biometria facial) garante privacidade por padrão e desde a concepção. Se o sistema biométrico for baseado em modelos de IA, isso já representa uma garantia de privacidade por padrão nesse sentido. Portanto, devem ser exigidas medidas que assegurem que os dados biométricos estejam devidamente protegidos e que cumpram os requisitos de irreversibilidade (não permitir o retorno à característica biométrica original), não interoperabilidade (não poder ser utilizado em outros sistemas), revogabilidade (possibilidade de torná-lo inválido sem alterar a característica biométrica) e multiplicidade (possibilidade de atualizá-lo sem alterar a característica biométrica) Como indicado na pergunta 1, a ANPD deve avaliar se um dado biométrico que atenda a essas características deve ou não ser considerado como dado sensível. Em nossa opinião, não deveria, pois essas características eliminam os riscos que antes exigiam uma proteção especial", "940707": "Se o tratamento se basear no consentimento, para que este seja válido é necessário que seja livre,

e, portanto, que exista uma alternativa para quem não quiser consentir. Isso deve ser garantido pelo controlador. Caso o tratamento se baseie em obrigação legal, deverá ser realizada a devida análise de impacto antes da aprovação da norma, de forma a comprovar a existência de um interesse superior que, potencialmente, justifique a limitação da capacidade de decisão do usuário sobre o tratamento de seus dados. A limitação da capacidade de decisão do usuário sobre o tratamento de seus dados biométricos implica uma restrição ao seu poder de disposição sobre esses dados. Assim, da mesma forma que, se o tratamento for baseado em uma norma, esta deve ser devidamente justificada, as autoridades de proteção de dados não podem proibir o usuário de prestar seu consentimento se ele tiver sido devidamente informado, pois estariam limitando seus direitos.", "940708": "Deve-se demonstrar que estão sendo utilizadas soluções avaliadas com base em testes internacionais do NIST quanto à precisão, e certificadas conforme a ISO/IEC 30107-3 quanto à robustez contra ataques de falsificação (spoof). Pode-se deixar aberta a possibilidade de aplicação futura de outras avaliações ou certificações equivalentes reconhecidas internacionalmente. A menção constante ao âmbito internacional se justifica por ser a melhor (ou única) forma de obter evidências do real estado da arte da indústria e do que é tecnicamente possível em cada momento.", "940709": "O Regulamento Europeu de Inteligência Artificial é central neste ponto. Para classificar os sistemas de reconhecimento biométrico conforme seu risco potencial, o regulamento adota um conceito-chave: “remoto” = sem participação ativa do indivíduo e geralmente à distância. Assim, os sistemas de identificação biométrica remotos (1:N) são considerados de risco inaceitável (e, portanto, proibidos) ou alto, pois operam sem a participação ativa do usuário. Por isso, não se pode garantir que o indivíduo tenha ciência do tratamento ou que concorde com ele. Por outro lado, os sistemas de identificação biométrica (1:N) não remotos (ou seja, com participação ativa do usuário) são equiparados aos sistemas de verificação biométrica (1:1) e considerados de baixo ou nenhum risco. Nesses casos, o usuário conhece e busca ativamente o tratamento. Esse conceito —remoto ou não remoto— está diretamente ligado aos conceitos de informação e consentimento no contexto da proteção de dados. Veja doc. nº3.", "940710": "Esse cumprimento se refere, basicamente, ao atendimento dos requisitos da LGPD. Nesse sentido, seriam úteis guias e orientações da ANPD sobre como fornecer informações aos usuários de forma mais clara e acessível. Além disso, quando houver tratamento automatizado, deve-se oferecer ao usuário a opção de entrar em contato com um humano, caso necessário, para evitar uma situação de desproteção. Esse contato pode ser disponibilizado por e-mail, call center, atendimento presencial (por exemplo, em agências bancárias) etc. Ou seja, se o processo automatizado com biometria não funcionar corretamente por qualquer motivo, deve-se oferecer uma alternativa, garantindo que o usuário não fique desprotegido em nenhuma hipótese.", "940711": "A primeira questão que deve ser abordada é a afirmação de que os dados biométricos são sensíveis. Conforme já explicado anteriormente, essa sensibilidade pode ser superada (evitada ou mitigada) com a adoção de soluções biométricas baseadas em RBRs, como as fundamentadas em Inteligência Artificial. Partindo dessa premissa, deve-se retomar o que foi mencionado na pergunta 15 sobre a importância de cumprir os requisitos estabelecidos pela LGPD, incluindo a oferta de informações completas e claras, bem como a possibilidade de solicitar revisão humana.", "940712": "Devem ser garantidos processos de registro que, no momento da

solicitação do consentimento, permitam comprovar que o pai, mãe ou responsável legal recebeu todas as informações e concedeu o consentimento em nome de seus filhos, filhas ou tutelados, quando for o caso. Quanto às medidas técnicas e organizacionais eficazes, remetemo-nos ao que já foi mencionado anteriormente sobre a privacidade e segurança oferecidas por padrão e por design pelas tecnologias biométricas modernas.", "940714": "No âmbito da proteção de dados, devem ser observados os mesmos requisitos mencionados anteriormente. No entanto, é fundamental diferenciar os tipos de tecnologia biométrica, como fez o AI Act na Europa: (1) sistemas de reconhecimento biométrico, que incluem sistemas de identificação e verificação biométrica; (2) sistemas de categorização biométrica; e (3) sistemas de inferência de emoções. Cada um desses sistemas, dependendo do ambiente e das condições de uso, é considerado de risco distinto. Assim, um sistema de estimativa de idade é um sistema de categorização, mas como não classifica com base em atributos sensíveis (já que a idade não é um dado sensível segundo a legislação de proteção de dados), seu nível de risco é baixo. Um sistema de verificação biométrica (1:1) é sempre considerado de baixo ou nenhum risco pelo AI Act. Anexamos os documentos nº 3 e nº4 com mais informações sobre sistemas de estimação de idade.

Contribuinte: Leire

Número: OP-969282

Data: 02/07/2025 - 12:58

Resumo: "Para fins de segurança jurídica e operacional dos agentes de tratamento, a definição de dados como biométricos deve ser guiada por critérios objetivos, evitando generalizações que levem à ampliação desnecessária do conceito. Por exemplo, imagens faciais armazenadas sem tratamento técnico para reconhecimento não deveriam ser enquadradas como biometria, sob pena de comprometer atividades lícitas e legítimas que não envolvam autenticação de identidade. Desse modo, sugerimos a adoção dos seguintes critérios: - Tratamento técnico específico: o dado deve resultar de um processo técnico específico, não apenas coleta bruta; - Finalidade de identificação: a mera presença do dado físico não o torna biométrico, a intenção de identificar é essencial; - Sistemas automatizados: o uso de software ou algoritmo automatizado é o que caracteriza o dado como biométrico; e - Irreversibilidade prática: por serem imutáveis, os dados biométricos demandam mais proteção, justificando o tratamento sensível.", "940688": "Para garantir transparência ativa sem gerar obrigações excessivas, sugerimos que a ANPD reconheça como práticas proporcionais: a inclusão, em Política de Privacidade, de seção específica sobre dados biométricos com linguagem clara; indicação do tempo de retenção e critérios de descarte; e, quando aplicável, registro de consentimento com interface clara — esclarecendo a obrigatoriedade legal quando for o caso. Recomendamos que a própria Política de Privacidade seja reconhecida como instrumento suficiente de transparência, o que traria segurança jurídica e evitaria exigências documentais redundantes, especialmente em ambientes digitais automatizados", "940690": "", "940693": "", "940695": "Para garantir os direitos dos titulares no tratamento automatizado de dados biométricos, os controladores devem adotar medidas

como: fornecer informações claras sobre a finalidade, base legal e tempo de retenção; disponibilizar canais acessíveis para confirmação, acesso e correção de dados; e, quando aplicável, permitir a revogação do consentimento com esclarecimento sobre as consequências. Nos casos de decisões automatizadas, deve-se assegurar o direito à revisão humana. Para grupos vulneráveis, recomenda-se linguagem adaptada, consentimento qualificado (quando exigido) e proteção reforçada contra discriminações. A Política de Privacidade pode consolidar essas informações de forma clara e acessível, promovendo transparência sem onerar os agentes regulados", "940697": "O tratamento de dados biométricos com base na obrigação legal (art. 11, II, "a", LGPD) é essencial em setores regulados, como o de apostas, onde a biometria facial é exigida por lei (Lei nº 14.790/2023, art. 23). Nesses casos, o titular não pode se opor, o que reforça a necessidade de transparência, responsabilidade e governança. Sugerem-se três critérios: (i) existência de norma legal clara e vigente; (ii) uso limitado à finalidade legal, sem desvio de finalidade; e (iii) documentação interna da base legal. Mesmo havendo obrigação, devem ser adotadas salvaguardas como: transparência ativa sobre a obrigatoriedade legal; coleta mínima (ex: apenas template facial); e medidas robustas de segurança da informação. Recomenda-se que a ANPD publique guias orientativos por setor, considerando riscos específicos.", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "O respeito aos direitos dos titulares exige práticas de governança e transparência compatíveis com a proteção de dados sensíveis. É essencial garantir: (i) informação clara no momento da coleta, com base legal, finalidade e tempo de retenção; (ii) acesso e correção de dados pessoais vinculados à biometria (ex: nome, CPF); (iii) possibilidade de revogação do consentimento, quando essa for a base legal, com esclarecimento das consequências e exclusão dos dados, salvo obrigação legal; (iv) em decisões automatizadas, direito à revisão humana e processos auditáveis; e (v) proteção reforçada para crianças, adolescentes e idosos, com linguagem adaptada, consentimento qualificado e restrição do uso da biometria ao estritamente necessário", "940711": "", "940712": "", "940714": "

Contribuinte: HELOISA DE MEDEIROS DINIZ

Número: OP-969488

Data: 03/07/2025 - 05:06

Resumo: "informação pessoal obtida através de características físicas ou comportamentais únicas de um indivíduo, utilizada para identificação ou autenticação. Isso inclui impressões digitais, reconhecimento facial, padrões de íris, voz, entre outros.", "940688": "Para garantir a transparência ativa no tratamento de dados biométricos, os controladores devem fornecer informações claras e detalhadas sobre o processo antes da coleta, incluindo a finalidade do uso, a base legal, a forma de armazenamento, os direitos do titular e os riscos envolvidos.", "940690": "A biometria comportamental, como reconhecimento de voz e padrões de digitação, deve ser tratada com rigor semelhante à biometria tradicional (digital, íris, face) em termos de segurança e qualidade dos dados. Ambas as categorias apresentam

desafios específicos e requerem atenção a princípios como privacidade, consentimento e proteção contra fraudes. ", "940693": "Para garantir um consentimento livre, específico, destacado, informado e inequívoco para tratamento de dados biométricos, conforme a LGPD, é crucial que o titular seja claramente informado sobre a finalidade, duração e forma de uso desses dados, além de ter a liberdade de recusar ou revogar o consentimento sem prejuízos. O consentimento não é adequado quando há desequilíbrio de poder entre o titular e o controlador, ou quando o tratamento é obrigatório por lei, exceto em casos específicos. ", "940695": "A aplicação da hipótese legal de "garantia da prevenção à fraude" (art. 11, II, "g", LGPD) com dados biométricos exige critérios rigorosos de necessidade, proporcionalidade e finalidade. É crucial garantir que o tratamento seja realmente necessário para a prevenção de fraudes, que os dados coletados sejam adequados e suficientes para essa finalidade, e que a coleta e uso sejam transparentes e respeitem os direitos dos titulares. ", "940697": "Em situações onde o tratamento de dados biométricos é realizado para o cumprimento de obrigações legais ou regulatórias, conforme o art. 11, II, "a" da LGPD, os controladores, especialmente órgãos e entidades públicas, devem observar critérios e salvaguardas para mitigar riscos e garantir os direitos dos titulares. Isso inclui a necessidade de fundamentação objetiva e verificável do tratamento, como a existência de uma obrigação legal específica, e a observância de princípios como finalidade, necessidade, adequação, segurança e prevenção à fraude. ", "940699": "A LGPD permite o tratamento de dados biométricos por órgãos de pesquisa, mesmo sem consentimento, quando necessário para estudos e pesquisas, conforme o artigo 11, inciso II, alínea "c". No entanto, a anonimização dos dados não garante imunidade contra reidentificação, especialmente com o cruzamento de bases de dados. Salientando, a anonimização eficaz requer medidas robustas e contínuas para evitar a identificação, e órgãos de pesquisa devem implementar salvaguardas adicionais, como o uso de dados agregados, a limitação do acesso e a análise do risco de reidentificação. ", "940700": "Para garantir um uso ético e legal de tecnologias de reconhecimento facial, mesmo amparado pela LGPD, é crucial adotar uma abordagem que priorize a necessidade, proporcionalidade, transparência e a prevenção de discriminação. Isso implica em implementar salvaguardas técnicas, jurídicas e institucionais robustas para mitigar riscos. ", "940701": "Os sistemas de reconhecimento facial devem ser projetados com base em princípios de privacidade desde a concepção (privacy by design) e segurança desde o projeto (security by design). Isso significa que a eficácia e a confiabilidade devem ser equilibradas com mecanismos robustos de proteção de dados e de mitigação de riscos. Para garantir alta performance e minimizar erros como falsos positivos (identificação incorreta de alguém como outra pessoa) e falsos negativos (falha em reconhecer um indivíduo corretamente)", "940702": "Sim, é possível e necessário identificar contextos em que o uso de tecnologias de reconhecimento facial não é recomendado, especialmente quando os riscos à privacidade e à liberdade individual superam os benefícios esperados. A avaliação deve considerar o princípio da necessidade, previsto na Lei Geral de Proteção de Dados (LGPD), segundo o qual o tratamento de dados deve ser limitado ao mínimo necessário para a finalidade legítima pretendida.", "940704": "Dado o impacto potencialmente irreversível de uma violação de dados biométricos — como o roubo de identidade facial ou digital, que não pode ser "trocado" como uma senha —, é imprescindível que organizações adotem medidas

de segurança robustas, contínuas e auditáveis, tanto técnicas quanto administrativas, em consonância com os princípios da Lei Geral de Proteção de Dados (LGPD).", "940707": "Quando serviços não essenciais condicionam parte de suas funcionalidades à autenticação biométrica, é fundamental que essa exigência seja implementada com proporcionalidade, transparência e respeito à autodeterminação informativa. Caso contrário, o tratamento pode configurar discriminação ilícita ou prática abusiva, nos termos da Lei Geral de Proteção de Dados (LGPD) e do Código de Defesa do Consumidor (CDC).", "940708": "A proteção eficaz no tratamento de dados biométricos, que são classificados como dados pessoais sensíveis pela Lei Geral de Proteção de Dados (LGPD), exige a adoção de boas práticas específicas e rigorosas por parte dos controladores. Tais práticas devem assegurar não apenas a segurança técnica, mas também a responsabilidade ética e jurídica, promovendo o uso transparente, proporcional e não discriminatório desses dados.", "940709": "Para assegurar o respeito à autodeterminação informativa dos titulares no tratamento contínuo e massivo de dados biométricos, como em iniciativas de cidades inteligentes, monitoramento de multidões ou espaços públicos, os controladores devem adotar medidas concretas de transparência, controle e responsabilização, mesmo diante da complexidade e escala dessas operações. A autodeterminação informativa — isto é, o direito de o indivíduo controlar seus próprios dados pessoais — é um pilar central da LGPD e deve ser garantido mesmo em cenários de difícil comunicação direta.", "940710": "Para garantir o respeito efetivo aos direitos dos titulares, especialmente em contextos de tratamento automatizado de dados biométricos, os agentes de tratamento (controladores e operadores) devem adotar práticas que assegurem a transparência, acessibilidade e efetividade no exercício desses direitos, conforme previsto na Lei Geral de Proteção de Dados (LGPD).", "940711": "O tratamento de dados biométricos de crianças e adolescentes — especialmente em contextos como escolas, creches e espaços recreativos — exige atenção redobrada por parte dos controladores, uma vez que envolve dados pessoais sensíveis de pessoas em condição especial de proteção. A Lei Geral de Proteção de Dados (LGPD), em seu artigo 14, estabelece que esse tipo de tratamento só é permitido com o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal, e deve estar claramente alinhado ao princípio do melhor interesse da criança e do adolescente.", "940712": "O tratamento de dados biométricos de crianças e adolescentes, por sua natureza sensível e de alto risco, só é admissível em hipóteses estritamente previstas pela Lei Geral de Proteção de Dados (LGPD) e requer cuidados redobrados para garantir o respeito aos direitos dos titulares e à sua segurança. A legislação brasileira impõe regras específicas (art. 14 da LGPD), com base na doutrina da proteção integral da infância e juventude, exigindo autorização expressa dos responsáveis e o atendimento ao princípio do melhor interesse da criança e do adolescente.", "940714": "Em casos de verificação ou estimação de idade por meio de dados biométricos — como no acesso a plataformas digitais, jogos eletrônicos ou redes sociais — o tratamento de dados de crianças e adolescentes exige critérios rigorosos para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), especialmente os princípios da necessidade e do melhor interesse da criança e do adolescente (art. 14).

Contribuinte: ULISSES CARDOSO VIDAL

Número: OP-977469

Data: 10/07/2025 - 14:22

Resumo: "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, a LGPD classifica dados biométricos como sensíveis, mas não define critérios objetivos para essa caracterização. Parâmetros internacionais, como o GDPR e o ICO do Reino Unido, podem orientar a ANPD, ao indicarem três critérios principais: natureza do dado (físico, fisiológico ou comportamental), aplicação de tratamento técnico específico e finalidade de identificação única. Além disso, outros elementos podem reforçar a segurança jurídica, como o grau de estabilidade do dado, seu potencial de reidentificação, o uso para reconhecimento automático e o nível de exclusividade na identificação de indivíduos. A adoção de critérios claros pela ANPD traria mais previsibilidade e coerência à aplicação da LGPD no tratamento de dados biométricos. ", "940688": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, para cumprir o princípio da transparência, controladores que tratam dados biométricos devem fornecer informações claras e acessíveis antes ou no momento da coleta. O ICO recomenda comunicar, no mínimo: canais de contato, finalidades do tratamento, base legal (inclusive o interesse legítimo, se aplicável), dados coletados, destinatários, existência de transferências internacionais, prazos de retenção (ou critérios) e direitos dos titulares, incluindo revogação do consentimento e reclamações à autoridade. As informações devem ser concisas, claras e adequadas ao público-alvo. A forma de apresentação deve considerar o contexto: em ambientes físicos, recomenda-se o uso de folhetos, QR codes, orientações de funcionários e recursos acessíveis; em meios digitais, destacam-se avisos em camadas, dashboards explicativos e notificações no momento da coleta. ", "940690": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, a biometria comportamental, como reconhecimento de voz e padrões de digitação, traz riscos específicos à privacidade, por permitir inferências sobre sentimentos e pensamentos dos titulares, muitas vezes sem seu conhecimento. Diferente da biometria tradicional, exige monitoramento contínuo e pode violar direitos fundamentais. Apesar disso, ainda não há diferenciação regulatória entre as duas. Assim, seu tratamento deve observar rigorosamente os princípios da LGPD, como qualidade e segurança dos dados. Recomenda-se maior transparência, revisão das finalidades e, em certos casos, elaboração de RIPD. A ANPD deve acompanhar o tema e avaliar a necessidade de normativos específicos. ", "940693": "Em razão da limitação de caracteres, o complemento desta, elaborado pela ABA, resposta será encaminhado ao e-mail informado. Em síntese, para ser válido sob a LGPD, o consentimento para tratamento de dados biométricos deve ser livre, específico, informado, destacado e inequívoco. No entanto, contextos de assimetria ou ausência de alternativas podem comprometer essa validade. O ICO recomenda boas práticas como transparência total, possibilidade real de recusa sem prejuízo e alternativas funcionais ao não consentimento. O consentimento deve ser atrelado a finalidades específicas e manifestado por ação afirmativa clara. Ofertas financeiras, como no caso Tools for Humanity, podem viciar a vontade do

titular. A ANPD pode detalhar diretrizes para garantir o uso legítimo do consentimento e proteger os direitos dos titulares. ", "940695": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o uso da base legal do art. 11, II, "g" da LGPD — prevenção à fraude e à segurança — para tratamento de dados biométricos exige rigor quanto aos princípios da necessidade, proporcionalidade e finalidade. O controlador deve demonstrar que a biometria é indispensável frente a alternativas menos intrusivas, e que sua aplicação é proporcional ao risco. Os dados só podem ser usados para fins estritos de segurança, vedada a reutilização para outros propósitos. Recomenda-se adoção de salvaguardas como: RIPD, tecnologias de privacidade (PETs), criptografia e transparência ativa. A ANPD pode consolidar esses critérios para garantir proteção de direitos fundamentais. ", "940697": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o tratamento de dados biométricos com base no art. 11, II, "a" da LGPD — para cumprimento de obrigação legal — deve ser legítimo, proporcional e respeitar os direitos dos titulares. Segundo o ICO, a obrigação legal deve ser clara, prevista em norma interna, previsível aos titulares e a aplicação do dado biométrico necessária e proporcional. Devem ser adotadas salvaguardas como minimização e limitação da coleta e finalidade, retenção temporária, segurança desde a concepção (privacy by design), transparência ativa e responsabilidade reforçada, incluindo Relatórios de Impacto à Proteção de Dados, especialmente para tecnologias invasivas como reconhecimento facial. ", "940699": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o art. 11, II, "c" da LGPD autoriza o tratamento de dados sensíveis, como biométricos, para pesquisa, desde que respeitados os princípios legais e preferencialmente com dados anonimizados. A anonimização deve ser robusta e irreversível para excluir a aplicabilidade da LGPD, evitando reidentificação por cruzamento de bases. O EDPB e o GDPR reforçam salvaguardas como minimização de dados e pseudonimização, especialmente quando anonimização plena não é possível. Jurisdições europeias exigem consentimento, autorização ou avaliações de impacto específicas. No Reino Unido, normas técnicas indicam irreversibilidade, desvinculação e renovação dos dados biométricos. Assim, pesquisas devem garantir alta governança, segurança e responsabilidade. ", "940700": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o uso de reconhecimento facial, mesmo amparado pela LGPD, requer cautela, transparência e responsabilidade, observando os princípios da necessidade, proporcionalidade, transparência e não discriminação. Sem consentimento válido, deve-se provar que não há alternativa menos intrusiva. O consentimento deve ser livre, informado e oferecer alternativas. É fundamental informar titulares sobre a tecnologia, finalidade, base legal, acesso, armazenamento e exclusão dos dados, além de possibilitar revisão humana. Há riscos de vieses e discriminação contra grupos vulneráveis, exigindo salvaguardas como avaliações de impacto (RIPD), auditorias independentes, proibição em usos de alto risco, governança reforçada, supervisão externa e medidas técnicas para mitigar impactos. ", "940701": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, para garantir eficácia e

confiabilidade, sistemas de reconhecimento facial devem seguir o princípio *privacy by design*, incorporando salvaguardas técnicas desde o início. O EDPB destaca três técnicas para mitigar vieses: pré-processamento dos dados, ajustes no treinamento do modelo e pós-processamento dos resultados. Essas medidas reduzem falsos positivos/negativos, essenciais em segurança e controle de acesso. É vital garantir ao titular revisão humana das decisões automatizadas, que seja tempestiva, real e acessível. Sistemas devem incluir monitoramento contínuo, documentação demográfica e auditorias independentes. A ANPD pode estabelecer requisitos mínimos para assegurar confiabilidade e auditabilidade, especialmente em uso público.

","940702": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, embora não haja restrições absolutas ao uso de reconhecimento facial no Brasil, tendências internacionais indicam cautela. Na Europa, por exemplo, o uso dessa tecnologia para vigilância em massa pela segurança pública é cada vez menos recomendado e até proibido em vários países, devido aos riscos de discriminação e dilemas éticos, como a dificuldade de informar ou obter consentimento dos titulares. Em respeito aos princípios da necessidade e proporcionalidade, alternativas menos invasivas, como autenticação em dois fatores, tokens e senhas, são preferíveis, dependendo do contexto, como em operações bancárias ou acesso a áreas restritas.

","940704": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, devido à natureza sensível e imutável dos dados biométricos, seu vazamento ou uso indevido pode causar danos graves e irreversíveis, como roubo de identidade. Por isso, são necessárias medidas técnicas e administrativas robustas, baseadas em análise de risco detalhada. O ICO recomenda testes contínuos, criptografia forte, controle físico de acesso e avaliação de vulnerabilidades. A norma ISO/IEC 24745 destaca três atributos essenciais: irreversibilidade, desvinculação e revogabilidade dos dados biométricos. Boas práticas incluem verificação local (on-device) e adoção dos princípios de minimização e limitação de armazenamento. A ANPD pode exigir testes periódicos, revisões e Relatórios de Impacto para garantir a conformidade e proteger dados em setores sensíveis.

","940707": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o uso de dados biométricos em serviços não essenciais, especialmente baseado em consentimento, deve respeitar os princípios de proporcionalidade, não discriminação e autonomia do titular. Os usuários devem poder recusar sem sofrer prejuízos, com alternativas equivalentes, como senhas ou tokens, garantindo acessibilidade. O tratamento biométrico deve ser proporcional e nunca condição obrigatória para acesso, salvo se indispensável para execução contratual, com comprovação objetiva. Segundo o ICO, consentimento condicionado à biometria não é válido sem liberdade real de escolha, sendo a execução do contrato base legal mais adequada nesses casos. O tratamento deve ser opcional, informado e não discriminatório, respeitando a autodeterminação informativa.

","940708": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, para proteger dados biométricos, controladores devem seguir princípios da LGPD e padrões internacionais, adotando cautela, responsabilidade e transparência. O tratamento deve ser necessário, proporcional e com finalidade específica, vedando usos secundários. Tecnicamente, recomenda-se *privacy by*

design, uso de B-PETs (templates irreversíveis, desvinculados e revogáveis), criptografia forte, controle de acesso rigoroso e verificação local. Organizações devem garantir transparência ativa, auditorias regulares para mitigar vieses, revisão humana de decisões automatizadas e treinamento de equipes. Dados devem ser armazenados pelo tempo mínimo, com descarte seguro ao fim da finalidade. ", "940709": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o tratamento massivo de dados biométricos em espaços públicos desafia a autodeterminação informativa, exigindo transparência ativa com sinalização clara, materiais informativos, colaboradores capacitados e plataformas digitais acessíveis. As informações devem incluir finalidade, dados coletados, base legal e direitos dos titulares. A coleta deve ser necessária, proporcional e justificada, evitando meios mais intrusivos. No uso público, especialmente para segurança, o reconhecimento facial enfrenta críticas por riscos de discriminação e violação de privacidade, demandando base legal adequada, avaliações de impacto (RIPD), limitação de retenção, segurança robusta e supervisão independente com transparência e auditorias. ", "940710": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o tratamento automatizado de dados biométricos requer transparência ativa, controle e responsabilização para garantir os direitos dos titulares. Avisos claros, acessíveis e em camadas devem ser apresentados antes da coleta, informando dados coletados, finalidade, base legal, tempo de retenção e direitos, com acesso fácil para exercê-los. O titular deve poder acessar e corrigir dados, como solicitar nova captura biométrica. A revogação do consentimento precisa ser tão simples quanto a concessão, com comandos visíveis para desativar o uso. Decisões automatizadas que afetem o titular exigem informação prévia e direito à revisão humana qualificada em prazo razoável. ", "940711": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o tratamento de dados biométricos de crianças e adolescentes requer proteção reforçada, respeitando o princípio do melhor interesse previsto no art. 14 da LGPD. Embora hipóteses legais como consentimento dos responsáveis e cumprimento de obrigação legal sejam aplicáveis, é essencial observar necessidade, proporcionalidade, transparência, minimização e segurança. Precedentes, como o da autoridade polonesa, mostram que consentimento formal não justifica tratamento desnecessário ou invasivo, especialmente se houver alternativas menos intrusivas. É crucial garantir igualdade de acesso, consentimento expresso dos responsáveis, medidas de segurança, exclusão após a finalidade e transparência ativa. A ANPD pode definir diretrizes específicas para proteção em ambientes com menores. ", "940712": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, destaca-se o princípio do melhor interesse do menor e os princípios de necessidade, proporcionalidade, finalidade, minimização, transparência e segurança. Deve-se obter consentimento expresso dos responsáveis, com informações claras sobre o tratamento e garantia de não prejuízo caso optem por recusar. São necessárias medidas técnicas como criptografia ponta a ponta, armazenamento local ou descentralizado, controle rigoroso de acesso, rastreabilidade, Relatório de Impacto (RIPD) e treinamento de pessoal. A governança contínua e a prestação de contas são essenciais, especialmente ao envolver terceiros em

ambientes infantis. ", "940714": "Em razão da limitação de caracteres, o complemento desta resposta, elaborado pela ABA, será encaminhado ao e-mail informado. Em síntese, o uso de dados biométricos para verificação de idade em plataformas digitais acessadas por crianças exige atenção aos princípios da LGPD, especialmente o melhor interesse do menor. O EDPB recomenda avaliar a real necessidade e proporcionalidade do uso, aplicando Avaliação de Impacto (CRIA ou DPIA) em serviços de risco. Devem ser oferecidos métodos alternativos para evitar discriminação e garantir revisão humana em decisões automatizadas. A transparência deve informar finalidade, dados usados, tempo de retenção e direitos dos titulares. O ICO reforça legalidade, minimização, segurança e accountability, exigindo justificativa clara e medidas menos intrusivas. A ANPD pode criar diretrizes específicas para essa verificação.

Contribuinte: RAQUEL VASCONCELOS DE CASTRO

Número: OP-979836

Data: 11/07/2025 - 22:24

Resumo: :"" , "940688": "Para essa finalidade, recomendo que se exija dos controladores a apresentação de avisos de privacidade simplificados e em camadas, contendo, no mínimo: -A finalidade específica e detalhada do tratamento (ex: "Controle de acesso físico à portaria do edifício" em vez de um termo genérico como "Para sua segurança"). -Informações claras sobre o desempenho da tecnologia, incluindo taxas de erro conhecidas (falsos positivos e negativos) e uma declaração sobre os riscos de vieses algorítmicos que podem impactar desproporcionalmente grupos vulneráveis. Pesquisas demonstram que representações internas de modelos de IA podem ser sistematicamente enviesadas por fatores extrínsecos ao seu treinamento, sendo a transparência sobre este risco um dever de lealdade para com o titular. - Um link acessível para uma versão pública e simplificada do Relatório de Impacto à Proteção de Dados (RIPD), permitindo que a sociedade civil e os titulares compreendam a análise de riscos realizada pelo controlador. ", "940690": "A biometria comportamental deve ser objeto de obrigações de segurança, transparência e governança ainda mais rigorosas que a biometria tradicional. A justificativa reside no que a pesquisa em IA denomina "paradoxo da capacidade-interpretabilidade": à medida que os sistemas de IA se tornam mais capazes e complexos, seus processos internos frequentemente se tornam mais opacos e difíceis de entender por um ser humano. Sistemas de biometria comportamental são, por natureza, "caixas-pretas" (black boxes). Enquanto uma correspondência de impressão digital é um processo relativamente intuitivo, a decisão de um algoritmo que nega acesso a um serviço porque o "padrão de digitação do usuário foi anômalo" é opaca para o titular. Isso cria uma "ilusão de entendimento", tornando extremamente difícil para o titular exercer seu direito de correção ou oposição, pois ele não consegue compreender ou contestar a lógica da decisão. ", "940693": "" , "940695": "A hipótese legal é legítima e de grande aplicação prática. Contudo, não pode ser interpretada como um "cheque em branco" que autoriza o uso indiscriminado e desproporcional de dados biométricos. Inspirando-se no AI-Act Europeu, que posiciona a regulação como uma estratégia para construir um mercado de IA confiável e centrada no ser

humano, recomendamos que a ANPD estabeleça que a invocação desta hipótese legal exija do controlador a demonstração cumulativa, por meio do RIPD, dos seguintes critérios: -

Necessidade Estrita: A comprovação de que não existem meios alternativos e menos intrusivos que possam atingir o mesmo nível de eficácia na prevenção da fraude específica em questão. -**Proporcionalidade:** Uma análise que demonstre que os benefícios de segurança para o titular e para a coletividade superam manifestamente os riscos aos direitos e liberdades fundamentais. -**Salvaguardas Robustas:** A implementação de medidas técnicas e administrativas rigorosas para proteger os dados."

"940697": "", "940699": "", "940700": "O uso de FRTs, especialmente em espaços públicos, levanta riscos de vigilância em massa e pode erodir a confiança pública. Para mitigar tais riscos, recomendo que uma abordagem baseada em risco, similar àquela do Regulamento de IA da União Europeia. Sugiro que qualquer tratamento de dados biométricos por meio de FRT em espaços de acesso público seja, por padrão, classificado como de "Alto Risco", obrigando: -**Auditorias de Acurácia e Viés Algorítmico:** Realização de auditorias prévias e periódicas, conduzidas por entidades independentes, para avaliar o desempenho do sistema em diferentes grupos demográficos (gênero, etnia, idade). Pesquisas demonstram que os modelos de aprendizado de máquina são sistematicamente suscetíveis a vieses oriundos de seus dados e arquitetura, tornando a auditoria de viés indispensável para evitar a discriminação ilícita ou abusiva. -**RIPD Mandatório e Público:** A elaboração e publicização de um RIPD detalhado antes do início de qualquer operação."

"940701": "", "940702": "", "940704": "Dado que dados biométricos são imutáveis — uma impressão digital não pode ser "alterada" como senhas —, as medidas de segurança devem ser excepcionalmente rigorosas. Recomendo que se estabeleça como boa prática obrigatória a adoção dos princípios de Privacidade desde a Concepção e por Padrão (Privacy by Design and by Default). Tecnicamente, isso deve incluir, no mínimo, o armazenamento dos dados biométricos na forma de templates criptografados (representações matemáticas), e nunca como imagens ou dados brutos. Como referência para o nível de robustez esperado, a ANPD pode se basear nos extensos requisitos de segurança detalhados em editais de contratação de tecnologia do próprio Governo Federal, como a Consulta Pública nº 09/2025 para NGFW. Tal documento exige, por exemplo, processos formais para gestão de incidentes, análise periódica de vulnerabilidades e controles de acesso rigorosos, que devem ser considerados um baseline mínimo para qualquer controlador que trate dados biométricos"

"940707": "", "940708": "", "940709": "Para garantir a autodeterminação informativa dos titulares em contextos de tratamento massivo de dados biométricos, como em smart cities, proponho uma abordagem de implementação gradual e controlada. A implementação de regulações na Europa mostra que a implementação escalonada de leis como AI-Act e o DSA permitem o estudo de seus impactos e a realização de ajustes. Sugiro que a ANPD recomende um modelo similar para grandes projetos: -**Implementação em Fases (Phased Rollout):** Mandatar que projetos de cidades inteligentes ou de monitoramento de grandes multidões que utilizem biometria sejam implementados em fases, começando com projetos-piloto em áreas geográficas ou funcionais restritas. -**Avaliação Contínua:** Cada fase deve ser acompanhada de avaliações de impacto contínuas e transparentes sobre os direitos dos cidadãos, permitindo que a ANPD, a sociedade civil e os próprios controladores ajustem as tecnologias e as regras de governança antes de uma expansão irreversível.

","940710":"","940711":"O tratamento de dados biométricos de crianças e adolescentes exige a mais alta cautela. Para finalidades que não sejam estritamente necessárias ao cumprimento de obrigação legal ou à proteção da vida, a única hipótese legal admissível para o tratamento de dados biométricos de crianças deve ser o consentimento específico, em destaque, livre, informado e inequívoco, fornecido por, pelo menos, um dos pais ou pelo responsável legal, conforme Art. 14 da LGPD. O princípio do "melhor interesse da criança e do adolescente" deve ser o critério preponderante. Isso impõe ao controlador o ônus de comprovar que o tratamento gera um benefício direto, tangível e significativo para a criança, que suplante os enormes riscos de longo prazo à sua privacidade e autonomia. Esse princípio de proteção à dignidade humana deve ser aplicado com força motriz para resguardar o futuro e a autonomia de indivíduos vulneráveis, como as crianças."","940712":"","940714":

Contribuinte: MARIA ALICE CABRAL MAIA

Número: OP-980224

Data: 12/07/2025 - 15:54

Resumo: "A natureza do dado (corpo do indivíduo); serem dados irreproduzíveis por terceiros; e sua finalidade voltada à segurança."","940688":"Emissão de relatórios periódicos sobre atualizações de protocolos de segurança; relatórios sobre tentativas de acesso irregular ou vazamentos detectados, com notificação imediata ao proprietário; mais de uma opção de modo de acesso além do uso dos dados biométricos."","940690":"Acredito que a biometria comportamental deveria ser usada como um segundo mecanismo de checagem da identidade e para acesso a dados de maior relevância, sendo assim mais restrito a certos setores; órgãos e cargos que tenham acesso a dados sensíveis de pessoas físicas e jurídicas."","940693":"A existência de mais de uma opção de mecanismos de acesso, disponibilizando outras formas de acesso que não impliquem o uso de dados biométricos. O uso do consentimento não pode ser bastante como hipótese legal para o tratamento irrestrito dos dados quando não houver outras opções dadas claramente ao usuário, titular do dado, posto haver nesse momento um contexto de coação no sentido em que se não autorizar o uso, ficará sem acesso ao serviço, moradia, conta, cerceando um direito."","940695":"Uma possibilidade seria não juntar mais de dois dados sensíveis no mesmo banco de dados para acesso. Por exemplo, não arquivar CPF juntamente com reconhecimento facial. Uma vez que um vier a ser acessado irregularmente, não comprometa a segurança das contas bancárias, acessos a prédios. Empresas de segurança predial não deveriam exigir reconhecimento facial e CPF para cadastro, uma vez que ambos são necessários para movimentações financeiras. O nome bastaria. O CPF se tornou banalizado."","940697":"Uso de bancos de dados separados para armazenamento e utilização de mais de um fator de confirmação de identidade no momento do acesso."","940699":"Utilizar o menor número de dados possível, bem como o uso de dados que não possibilitem a identificação por cruzamento de dados, mas que viabilizem a contagem das amostras coletadas, por exemplo, uso de idade com região em que foi feita a coleta das informações."","940700":"As empresas devem adotar mais de uma opção de acesso, sendo que ao menos uma delas não inclua o uso de dados biométricos."","940701":"O uso de

mecanismos de acesso analógicos juntamente ao uso de dados biométricos. Nem todo avanço tecnológico se aplica adequadamente e seguramente ao meio real e social.", "940702": "O Uso indiscriminado em acesso a edifícios residenciais é um abuso da apropriação e do uso de dados sensíveis. Não há necessidade de um morador entregar seu CPF para uma empresa autorizar sua entrada em sua residência. É cercear o direito de ir e vir. O uso da biometria deveria ser uma das formas de acesso aos ambientes internos, não as únicas.", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Contribuinte: FELIPE RODRIGUES DE OLIVEIRA

Número: OP-994148

Data: 21/07/2025 - 15:06

Resumo: : "TozziniFreire: Para caracterizar um dado como biométrico, é necessário que haja o tratamento técnico de características físicas, fisiológicas ou comportamentais específicas (como impressões digitais, reconhecimento facial, voz, leitura de íris, geometria da mão), para fins de identificação ou autenticação única e inequívoca de pessoa natural.

", "940688": "TozziniFreire: Controladores de dados biométricos devem seguir práticas de transparência ativa, conforme o art. 9º da LGPD, informando claramente aos titulares: (i) finalidade do tratamento; (ii) uso e tempo de armazenamento; (iii) direitos dos titulares (acesso, correção, exclusão); e (iv) medidas de segurança. Isso constrói confiança e assegura compreensão sobre o uso dos dados. Recomenda-se: informar sobre a finalidade e compartilhamento; indicar base legal e riscos do tratamento; criar canal de comunicação; usar avisos visuais; realizar avaliação de impacto para tratamentos de alto risco e manter informações atualizadas. As práticas de transparência podem ser diferentes a depender da base legal do tratamento e do caso concreto.", "940690": "", "940693": "TozziniFreire: Consentimento deve incluir: informações claras; consequência da recusa; finalidade destacada e específica; possibilidade de revogação. Contextos inadequados: o consentimento não é adequado nos casos em que não há, de fato, uma possibilidade de livre escolha para o titular ou então em casos onde haja vício de consentimento. A fim de ilustrar as hipóteses de vício de consentimento, observa-se que, nos termos do Código Civil, é anulável o negócio jurídico por vício resultante de erro, dolo, coação, estado de perigo, lesão ou fraude das partes.", "940695": "TozziniFreire: O uso dessa base legal exige proporcionalidade e finalidade específica e legítima, e métodos menos invasivos devem ser priorizados. Deve haver limitação a dados estritamente necessários e garantia de direitos do titular. Salvaguardas incluem RIPD, criptografia, pseudonimização, controle de acesso e prazos definidos de retenção.", "940697": "TozziniFreire: Norma legal/regulatória específica e válida; limitação da coleta à finalidade prevista. Salvaguardas incluem RIPDs e controle de acesso. Órgãos públicos: atendimento a normas de conduta (regras específicas) ou normas de organização (atribuições legais); publicidade e transparência (Art. 23 LGPD).", "940699": "TozziniFreire: Limites: finalidade específica; proibição à divulgação e transferência de dados pessoais; normas éticas; escopo do estudo e anonimização.

Salvaguardas: minimização dos dados; DPIA; técnicas robustas de anonimização; gestão do risco de reidentificação, considerando as bases de dados utilizadas para cruzamento das informações; controle estrito de acesso; pseudonimização/anonimização; segregação de bases de dados.", "940700": "", "940701": "TozziniFreire: Registros sobre avaliação técnica prévia de acurácia algorítmica mínima e do SLA (taxa aceitável de erro, tempo de resposta) e ciclos de feedback técnico; correção tempestiva de falhas: planos de resposta a falhas críticas (protocolos para suspensão da IA); direito do titular de contestar e corrigir dados pessoais; direito de revisão de decisão automatizada, e revisores humanos podem ser incluídos, quando necessário. ", "940702": "", "940704": "TozziniFreire: Criptografia; autenticação multifator; controle de acesso via autenticação de dois fatores; anonimização quando possível; auditorias periódicas, avaliações de impacto (produção de RIPDs), perguntas registradas e monitoramento contínuo. Os agentes devem garantir a transparência sobre uso e compartilhamento de dados, com relatórios e auditorias periódicas. Medidas de segurança devem ser aprimoradas conforme a evolução das ameaças tecnológicas. Considerar distinção entre grupos vulneráveis e tipos de serviços para sopesar o risco e o benefício da coleta.", "940707": "TozziniFreire: Métodos alternativos de autenticação; justificar tecnicamente eventual exigência biométrica e racional para possível restrição de acesso na recusa, se for o caso; proibir discriminação ilícita ou abusiva; informar as consequências da recusa e garantir igualdade de acesso aos serviços como regra; oferecer alternativas seguras, como senhas ou autenticação multifatorial; avaliar a necessidade do uso da biometria com revisões periódicas.", "940708": "TozziniFreire: Minimização de dados; realização de RIPDs; restrição de acesso interno; adoção de políticas de coleta, retenção e eliminação seguras, com avaliações de risco regulares; adoção de medidas contra viés algorítmico; adequação a princípios de ética estabelecidos internacionalmente; transparência com os titulares sobre uso e finalidade; relatórios de prestação de contas; adoção de medidas robustas, como criptografia, monitoramento contínuo e anonimização; garantir transparência sobre o tratamento, informando os titulares sobre finalidades e direitos; definir responsabilidades e processos de resposta a incidentes; vetar o uso de dados biométricos para finalidades não autorizadas ou de discriminação ilícita.", "940709": "TozziniFreire: Recomendamos implementar políticas de transparência proativa, usando canais como sinalizações, websites e aplicativos para informar sobre a coleta e uso de dados biométricos. Mecanismos acessíveis devem permitir que os titulares exerçam seus direitos, como acesso e revogação de consentimento, por meio de canais digitais e analógicos. O controlador deve considerar tecnologias que minimizem a identificação, realizar avaliações de impacto à proteção de dados e garantir governança com responsabilidades claras. Ademais, sugere-se adotar privacy by design, realizar RIPDs periódicos e manter registros de decisão sobre tratamento biométrico. O tratamento biométrico em espaços públicos deve respeitar a LGPD, assegurando um equilíbrio entre inovação e proteção dos direitos dos titulares.", "940710": "TozziniFreire: Transparência sobre dados biométricos utilizados (ainda que não inteligíveis, e acompanhado de respectiva explicação), finalidade e direitos dos titulares; acesso a dados e métricas utilizadas no tratamento automatizado; implementação de revisão de decisões automatizadas; disponibilização de canais para acesso, correção e opção de revogar consentimento; adoção de medidas de segurança dos dados biométricos; adoção

de tecnologia que consiga excluir os dados biométricos e; realização de treinamentos para promover a conformidade com a LGPD.", "940711": "TozziniFreire: Coleta de consentimento explícito dos pais, com informações claras sobre riscos e finalidades, por meio de termo separado e linguagem simples, em reuniões ou assinatura em e-mails ou o tratamento com base em outra base legal, desde que observado e prevalecente o melhor interesse da criança/adolescente. O tratamento deve oferecer benefícios à criança, como segurança; elaboração de relatório de impacto; retenção mínima; canal direto para dúvidas e relatórios de transparência periódicos. Caso seja utilizada a base legal do consentimento, os responsáveis devem ter a opção de revogar o consentimento a qualquer momento.", "940712": "TozziniFreire: O tratamento é admissível com consentimento dos responsáveis ou para proteção da criança ou com base em outra base legal, desde que observado e prevalecente o melhor interesse da criança/adolescente. É essencial informar claramente os responsáveis, adotar controles de acesso, criptografia e políticas rígidas para evitar abusos, vazamentos e acessos não autorizados. Sugere-se a implementação de (a) ferramentas para segurança da informação, como criptografia, controle de acesso e autenticação multifatorial; (b) avaliações de impacto sempre que ocorrer o tratamento dos dados, a fim de mitigar possíveis riscos e danos aos titulares; e (c) minimização da coleta, para que sejam tratados apenas os dados efetivamente essenciais ao melhor interesse das crianças e adolescentes.", "940714": "TozziniFreire: A prática se justifica dependendo do contexto e se o menor estiver exposto a maior risco sem o tratamento, priorizando melhor interesse; exclusão de dados após verificação da idade; consentimento de responsáveis, informando sobre riscos e finalidades (sendo possível a aplicação de outra base legal, desde que observado e prevalecente o melhor interesse da criança/adolescente); RIPD e testes de balanceamento; coleta mínima de informações imprescindíveis para a realização da atividade oferecida, evitando o risco de vazamentos, uso indevido ou assédio. A LGPD proíbe que o controlador condicione a participação de crianças (nos termos do Estatuto da Criança e do Adolescente, menores de até 12 anos incompletos) em jogos, aplicações de internet ou outras atividades ao fornecimento de seus dados pessoais, além daqueles estritamente necessários para a sua execução.

Contribuinte: MARIA EUGENIA GEVE DE MORAES LACERDA

Número: OP-995585

Data: 22/07/2025 - 14:47

Resumo:

:"", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "dsds", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Contribuinte: LUISA ALBUQUERQUE XAVIER MALUFE RIBEIRO

Número: OP-996562

Data: 23/07/2025 - 09:04

Resumo: "Qualquer dado que não possa ser modificado pelo indivíduo: face, digital, sangue, dna", "940688": "A ANPD deve exigir que os controladores pratiquem transparência ativa: Consentimento Específico para Treinamento: Exigir que a permissão para usar dados para treinar algoritmos seja uma escolha separada e clara, e não embutida em termos de serviço genéricos, dadas as limitações técnicas do "Machine Unlearning". Transparência sobre Limitações: Obrigar a informação prévia ao cidadão caso seus dados, uma vez usados no treinamento de uma IA, não possam ser 100% eliminados (tanto por Remoção de Informação Observada quanto por Supressão de Saída) Interfaces Padronizadas: Criar normas para as interfaces de consentimento para combater "dark patterns" e garantir que a escolha do usuário seja livre. Divulgação de Riscos: Obrigar a divulgação prévia e clara das taxas de erro e dos riscos de viés discriminatório dos sistemas biométricos. Acesso ao Relatório de Impacto (RIPD): Exigir que o link público para o Relatório de Impacto à Proteção de Dados seja de fácil acesso para o titular.", "940690": "A biometria comportamental (voz, digitação) deve ter regras de transparência e segurança mais rigorosas que a tradicional (digital, face). Justificativa: Por operar como uma "caixa-preta" (black box), ela cria uma assimetria de poder que impede o cidadão de entender ou contestar uma decisão, ferindo a autodeterminação informativa. A regulação deve compensar essa opacidade.", "940693": "Para garantir que o consentimento seja livre e inequívoco, conforme a LGPD, a ANPD deve normatizar que: Consentimento Granular: Proibir o "consentimento embutido". A permissão para compartilhar dados com terceiros deve ser uma escolha granular, separada dos termos de uso principais, e não uma condição para usar o serviço. O "Opt-in Ativo" é obrigatório: A opção de compartilhar dados deve vir sempre desmarcada por padrão. O silêncio do usuário não pode ser interpretado como consentimento. As Interfaces devem ser justas: Os botões "Aceito" e "Recuso" devem ter o mesmo destaque visual, para evitar o uso de "dark patterns" que induzam o usuário à opção menos privada.", "940695": "A base legal de "prevenção à fraude" (Art. 11, II, "g") não pode ser um "cheque em branco" para o uso de biometria. Recomendação: Seu uso deve ser condicionado a um teste de necessidade e proporcionalidade, exigindo que o controlador demonstre formalmente que não existem alternativas menos intrusivas e igualmente eficazes para atingir o mesmo objetivo de segurança. ", "940697": "Jamais divulgar com terceiros e só solicitar caso não exista nenhuma outra forma de segurança que possa substituir", "940699": "Jamais utilizar sem consentimento, e nunca incluir como padrão na hora de cadastros", "940700": "O uso de Tecnologias de Reconhecimento Facial (FRTs) em espaços de acesso público deve ser classificado pela ANPD como uma atividade de "Alto Risco". Consequência: Isso deve acionar a obrigatoriedade de auditorias prévias e independentes para avaliar o viés e a acurácia do sistema antes de sua implementação. O ônus da prova deve ser do implementador, não da vítima. Para sistemas de alto risco, os controladores devem também ser obrigados a manter e disponibilizar Relatórios de Proveniência de Dados (Data Provenance Reports), detalhando as fontes e os vieses conhecidos em seus dados de treinamento. Para sistemas proativos, pode-se exigir a capacidade de gerar um "Gráfico de Crenças" (Belief Graph), um

relatório legível que mostre o caminho que a Inteligência Artificial percorreu para chegar a uma conclusão. Isso torna funcional o direito à revisão.

","940701":"","940702":"","940704": "Dada a imutabilidade dos dados biométricos, deve ser mandatória a aplicação da "Privacidade desde a Concepção e por Padrão" e de padrões de segurança mínimos: · 1. Proibição do Armazenamento de Dados Brutos e Exigência de "Salt" no Hashing e de Criptografia Robusta: Proibição do armazenamento do dado biométrico bruto, permitindo armazenamento apenas de sua representação matemática (template hash). Processamento dos templates via hash criptográfico forte (SHA-256 ou +), com a adição obrigatória de um "salt" (dado aleatório único) para cada usuário. Assim, em caso de vazamento, os dados não permitem ataques de comparação em massa. A base de dados deve ser protegida com criptografia forte e de padrão industrial (AES-256 ou +). As chaves criptográficas devem ser gerenciadas em ambientes seguros e isolados, como HSMs (Hardware Security Modules). · 2. Detecção de Vivacidade (Liveness Detection): O uso da tecnologia deve ser obrigatório, garantindo a presença do titular na auten","940707":"","940708":"","940709":"","940710": "Para garantir os direitos dos titulares em sistemas de IA, especialmente o direito à eliminação de dados (Art. 18, VI), a ANPD deve: Regular o "Direito ao Esquecimento" como "Supressão de Saída": O controlador deve ser obrigado a provar que seu sistema de IA não gera mais a informação pessoal de quem solicitou a eliminação. Esta é uma solução tecnicamente viável. Priorizar a Prevenção: Se a eliminação completa é um desafio técnico, a minimização de dados se torna ainda mais crucial. A coleta de dados deve se ater estritamente ao necessário para a finalidade informada. Exigir Transparência sobre a Permanência: O cidadão tem o direito de ser informado, no momento da coleta, que a influência de seus dados no treinamento de um modelo de IA pode não ser permanentemente reversível.", "940711": "O tratamento de dados biométricos de crianças para fins não essenciais (e.g., cantina escolar) exige o mais alto padrão de proteção, baseado no "melhor interesse da criança" (Art. 14). Regra Proposta: O consentimento dos pais é necessário, mas não suficiente. O controlador deve ser obrigado a provar que o tratamento gera um benefício direto, tangível e superior para a criança, que supere o risco vitalício de ter sua identidade imutável registrada. Conveniência administrativa para a instituição não é uma justificativa válida. ","940712":"","940714": "

Contribuinte: LARISSA DE FRANCA SOBRINHO

Número: OP-997897

Data: 24/07/2025 - 08:59

Resumo: : "Informações únicas que identifiquem um ser humano a partir de marcações biológicas próprios (DNA, íris, voz, face, digitais, arcadas dentárias, etc) ", "940688": "A ANPD deve exigir que os controladores pratiquem transparência ativa: · Consentimento Específico para Treinamento: Exigir que a permissão para usar dados para treinar algoritmos seja uma escolha separada e clara, e não embutida em termos de serviço genéricos, dadas as limitações técnicas do "Machine Unlearning". Transparência sobre Limitações: Obrigar a informação prévia ao cidadão caso seus dados, uma vez usados no treinamento de uma IA,

não possam ser 100% eliminados (tanto por Remoção de Informação Observada quanto por Supressão de Saída) Interfaces Padronizadas: Criar normas para as interfaces de consentimento para combater "dark patterns" e garantir que a escolha do usuário seja livre. Divulgação de Riscos: Obrigar a divulgação prévia e clara das taxas de erro e dos riscos de viés discriminatório dos sistemas biométricos. Acesso ao Relatório de Impacto (RIPD): Exigir que o link público para o Relatório de Impacto à Proteção de Dados seja de fácil acesso para o titular.", "940690": "A biometria comportamental (voz, digitação) deve ter regras de transparência e segurança mais rigorosas que a tradicional (digital, face). Justificativa: Por operar como uma "caixa-preta" (black box), ela cria uma assimetria de poder que impede o cidadão de entender ou contestar uma decisão, ferindo a autodeterminação informativa. A regulação deve compensar essa opacidade.", "940693": "Para garantir que o consentimento seja livre e inequívoco, conforme a LGPD, a ANPD deve normatizar que: Consentimento Granular: Proibir o "consentimento embutido". A permissão para compartilhar dados com terceiros deve ser uma escolha granular, separada dos termos de uso principais, e não uma condição para usar o serviço. O "Opt-in Ativo" é obrigatório: A opção de compartilhar dados deve vir sempre desmarcada por padrão. O silêncio do usuário não pode ser interpretado como consentimento. As Interfaces devem ser justas: Os botões "Aceito" e "Recuso" devem ter o mesmo destaque visual, para evitar o uso de "dark patterns" que induzam o usuário à opção menos privada.", "940695": "A base legal de "prevenção à fraude" (Art. 11, II, "g") não pode ser um "cheque em branco" para o uso de biometria. Recomendação: Seu uso deve ser condicionado a um teste de necessidade e proporcionalidade, exigindo que o controlador demonstre formalmente que não existem alternativas menos intrusivas e igualmente eficazes para atingir o mesmo objetivo de segurança. A base legal de "prevenção à fraude" (Art. 11, II, "g") não pode ser um "cheque em branco" para o uso de biometria. Recomendação: Seu uso deve ser condicionado a um teste de necessidade e proporcionalidade, exigindo que o controlador demonstre formalmente que não existem alternativas menos intrusivas e igualmente eficazes para atingir o mesmo objetivo de segurança.", "940697": "", "940699": "", "940700": "O uso de Tecnologias de Reconhecimento Facial (FRTs) em espaços de acesso público deve ser classificado pela ANPD como uma atividade de "Alto Risco". Consequência: Isso deve acionar a obrigatoriedade de auditorias prévias e independentes para avaliar o viés e a acurácia do sistema antes de sua implementação. O ônus da prova deve ser do implementador, não da vítima. · Para sistemas de alto risco, os controladores devem também ser obrigados a manter e disponibilizar Relatórios de Proveniência de Dados (Data Provenance Reports), detalhando as fontes e os vieses conhecidos em seus dados de treinamento. Para sistemas proativos, pode-se exigir a capacidade de gerar um "Gráfico de Crenças" (Belief Graph), um relatório legível que mostre o caminho que a Inteligência Artificial percorreu para chegar a uma conclusão. Isso torna funcional o direito à revisão.", "940701": "", "940702": "", "940704": "Dada a imutabilidade dos dados biométricos, deve ser mandatória a aplicação da "Privacidade desde a Concepção e por Padrão" e de padrões de segurança mínimos: · 1. Proibição do Armazenamento de Dados Brutos e Exigência de "Salt" no Hashing e de Criptografia Robusta: Proibição do armazenamento do dado biométrico bruto, permitindo armazenamento apenas de sua representação matemática (template hash). Processamento dos templates via hash

criptográfico forte (SHA-256 ou +), com a adição obrigatória de um "salt" (dado aleatório único) para cada usuário. Assim, em caso de vazamento, os dados não permitem ataques de comparação em massa. A base de dados deve ser protegida com criptografia forte e de padrão industrial (AES-256 ou +). As chaves criptográficas devem ser gerenciadas em ambientes seguros e isolados, como HSMs (Hardware Security Modules).

· 2. Detecção de Vivacidade (Liveness Detection): O uso da tecnologia deve ser obrigatório, garantindo a presença do titular na autenticação.

"940707": "", "940708": "", "940709": "", "940710": "Para garantir os direitos dos titulares em sistemas de IA, especialmente o direito à eliminação de dados (Art. 18, VI), a ANPD deve: Regular o "Direito ao Esquecimento" como "Supressão de Saída": O controlador deve ser obrigado a provar que seu sistema de IA não gera mais a informação pessoal de quem solicitou a eliminação. Esta é uma solução tecnicamente viável. Priorizar a Prevenção: Se a eliminação completa é um desafio técnico, a minimização de dados se torna ainda mais crucial. A coleta de dados deve se ater estritamente ao necessário para a finalidade informada. Exigir Transparência sobre a Permanência: O cidadão tem o direito de ser informado, no momento da coleta, que a influência de seus dados no treinamento de um modelo de IA pode não ser permanentemente reversível."

"940711": "O tratamento de dados biométricos de crianças para fins não essenciais (e.g., cantina escolar) exige o mais alto padrão de proteção, baseado no "melhor interesse da criança" (Art. 14). Regra Proposta: O consentimento dos pais é necessário, mas não suficiente. O controlador deve ser obrigado a provar que o tratamento gera um benefício direto, tangível e superior para a criança, que supere o risco vitalício de ter sua identidade imutável registrada. Conveniência administrativa para a instituição não é uma justificativa válida."

"940712": "", "940714": "

Contribuinte: LUCIANE CORREIA AVELAR

Número: OP-999971

Data: 27/07/2025 - 14:15

Resumo: "[Contribuição Petrobras] Um dado biométrico deve ser caracterizado por qualquer característica física ou comportamental de uma pessoa que seja mensurável e permita a identificação direta da pessoa."

"940688": "[Contribuição Petrobras] A depender da criticidade da utilização do caso concreto, algumas práticas podem ser utilizadas. A utilização destas práticas deverá considerar o contexto da utilização, categoria e tipo de titulares envolvidos.

1. Elaboração de Aviso de Privacidade Específico;
2. Consentimento Informado e Granular, quando esta for a hipótese legal;
3. Informação Prévia ao Tratamento, por meios físicos e/ou digitais, contendo:
 - Categorias de dados biométricos;
 - Utilização e compartilhamento, inclusive com terceiros
 - Direitos dos titulares e como podem exercê-los
4. Comunicação sobre Decisões Automatizadas, quando aplicável
5. Canais para exercício de Direitos dos Titulares
6. Realização de Análise de Impacto à Proteção de Dados, em casos de maior criticidade
7. Análise e acompanhamento de algoritmos biométricos verificando vieses, precisão e proteção dos dados
8. Análises internas para avaliar tanto os aspectos técnicos quanto os processuais.
9. Educação e Sensibilização"

"940690": "[Contribuição Petrobras] A biometria comportamental exige maior rigor que a tradicional devido à sua

natureza dinâmica e riscos de reidentificação e perfilamento. Controladores devem garantir qualidade dos dados, segurança (criptografia, anonimização), avaliação de impacto, consentimento granular e proibir reutilização indevida para fins não declarados. Deve haver controles adicionais para garantir a não discriminação e prevenção de práticas intrusivas

","940693": "[Contribuição Petrobras] O consentimento para dados biométricos deve ser rigorosamente controlado para atender os requisitos da LGPD e evitar uso abusivo. Em contextos de obrigações legais ou proteção coletiva, outras hipóteses legais parecem ser mais adequadas para garantir um tratamento ético. O consentimento deve ser livre, específico, destacado, informado e inequívoco.

","940695": "", "940697": "", "940699": "", "940700": "[Contribuição Petrobras] O reconhecimento facial, por sua natureza intrusiva, exige salvaguardas rigorosas para evitar abusos e discriminação. A adoção de medidas técnicas, jurídicas e institucionais, aliada à observância dos princípios da LGPD, é essencial para equilibrar inovação e proteção aos direitos fundamentais. O uso de reconhecimento facial deve observar necessidade, proporcionalidade e transparência, evitando discriminação. Salvaguardas incluem avaliação de impacto em casos de maior criticidade, dados minimizados, treinamento de algoritmos para evitar vieses, criptografia, análises e acompanhamento sobre viés, anonimização, governança de dados e canais para exercício de direitos.", "940701": "[Contribuição Petrobras] Sistemas de reconhecimento facial devem usar bases de dados diversas, algoritmos treinados para evitar vieses, testes rigorosos e auditorias contínuas. Mecanismos de correção podem incluir monitoramento em tempo real, revisão humana em decisões críticas e atualizações regulares. Avaliação de impacto à privacidade em casos de maior criticidade e governança de dados são essenciais. Utilização de frameworks de Privacidade seria visto como boa prática para garantir esses cuidados desde a concepção.", "940702": "[Contribuição Petrobras] Monitoramento em larga escala “não justificado”: Uso de reconhecimento facial em espaços públicos para vigilância indiscriminada, sem base legal clara, pode violar direitos de privacidade e gerar discriminação. Serviços Não Essenciais: Solicitar biometria em ações de marketing ou programas de fidelidade pode ser visto como desproporcional Alternativas: Cartões de Proximidade (RFID) - Senhas ou PINs: em serviços não críticos - Autenticação Multifatorial (MFA) - QR Codes ou Códigos Temporários: Para acessar serviços, podem ser gerados dinamicamente, evitando coleta de dados biométricos. - Reconhecimento de Dispositivos: Identificação baseada no hardware ou navegador usado pelo titular, limitando o processamento de dados pessoais sensíveis.", "940704": "[Contribuição Petrobras] A depender da criticidade do caso concreto, algumas práticas podem ser utilizadas. Essas práticas deverão considerar o contexto da utilização, categoria e tipo de titulares. 1. Medidas Técnicas: • Criptografia Avançada, Anonimização/Pseudonimização, • Controle de Acessos, Monitoramento e Log • Armazenamento Seguro: templates biométricos em vez de dados brutos. 2. Medidas Administrativas: • Políticas internas de Segurança e/ou Privacidade • Capacitação das equipes envolvidas na adoção e operação dos dados biométricos • Auditorias internas: Avaliar continuamente riscos e conformidade com a LGPD. • Contratos: Exigir cláusulas de proteção em relação a terceiros. Essas medidas, combinadas, reduzem o impacto de violações e reforçam a confiança no uso da biometria 1. Avaliação de Riscos 2. Monitoramento Contínuo, a depender da criticidade da solução •

Sistemas de Detecção e Resposta • Indicadores de Risco • Testes de Penetração e Gestão de Vulnerabilidades", "940707": "", "940708": "[Contribuição Petrobras] - Minimização e Finalidade: Coletar apenas os dados indispensáveis para finalidades claras e legítimas, evitando usos secundários não autorizados. - Criptografia e Armazenamento Seguro: armazenar templates em vez de dados brutos. - Anonimização: Quando possível, anonimizar dados para reduzir riscos de reidentificação. - Análise/acompanhamento de algoritmos biométricos - Avaliação de riscos nos operadores, quando aplicável; - Base Diversificada: Treinar algoritmos com dados representativos para evitar vieses. + Garantia de Transparência e Responsabilidade: - Informar claramente os titulares sobre finalidades, riscos e direitos. 1. Informar claramente os titulares sobre finalidades, riscos e direitos. 2. Implementar canais para exercício de direitos (ex.: contestação de decisões). Revisão humana em decisões automatizadas para evitar discriminação", "940709": "", "940710": "", "940711": "", "940712": "", "940714": "

Contribuinte: ELTON LUIS MITIDIERI ARNAUD

Número: OP-1000400

Data: 28/07/2025 - 08:03

Resumo: "[Binance por Opice Blum] Critérios objetivos a serem observados: (i) natureza do dado (dados físicos, fisiológicos ou comportamentais); (ii) uso de tecnologia específica para o tratamento; e (iii) finalidade específica (dado coletado com a intenção de identificação ou autenticação única do titular).", "940688": "[Binance por Opice Blum] Devem ser informados, de forma clara e prévia: forma do tratamento, finalidades específicas, prazo de retenção, compartilhamento, medidas de segurança, direitos e canais de contato. Avisos internos e externos devem ser destacados, com sinalização em coletas automatizadas.", "940690": "[Binance por Opice Blum] A biometria comportamental é menos intrusiva e pode servir como apoio seguro à identificação, principalmente para prevenção à fraude (ex: detectar movimentação e presença). Assim, não exige mais restrições que a biometria tradicional, mas proporcionalidade ao risco, focado em qualidade dos dados.", "940693": "[Binance por Opice Blum] Deve ser ofertada opção real de aceite ou de recusa, sem condicionamento ou coerção imposta ao titular. Não deve ser usado se houver base legal mais adequada ao caso concreto, especialmente quando houver desequilíbrio de poder ou impossibilidade de fornecimento de consentimento válido pelo titular.", "940695": "[Binance por Opice Blum] Critério principal: aderência aos objetivos de validação, autenticação, segurança e prevenção à fraude. Compatibilidade ao setor financeiro, bancário e de ativos virtuais: necessidade de controles eficientes contra fraudes e de verificação de identidade, segurança das transações, validação dos dados.", "940697": "[Binance por Opice Blum] Critério orientado ao disposto na determinação legal ou regulatória, vinculante e/ou recomendada como prática necessária do setor (ex: instituições de ativos virtuais orientadas por normas do setor financeiro). Salvaguardas: minimização de dados e registro sobre as obrigações e sua aplicação.", "940699": "[Binance por Opice Blum] O tratamento deve ocorrer dentro do órgão, com finalidade legítima, em

ambiente seguro e mediante anonimização ou pseudonimização. Devem ser adotados controles de acesso, segregação de bases e rastreabilidade das operações, bem como restrições contratuais quanto ao uso e compartilhamento dos dados.", "940700": "[Binance por Opice Blum] Técnicas contra vieses: diversidade no banco de dados, testes de viés, validação e monitoramento contínuo do algoritmo, opções acessíveis, minimização de dados.

Governança: avaliação de riscos, treinamento de equipes multidisciplinares sobre segurança e transparência aplicáveis.", "940701": "[Binance por Opice Blum] Usar algoritmos precisos sob padrões técnicos (ex: ISO), treinados com bases diversas e atualizadas. Garantir boa qualidade de imagem e controle ambiental. Contemplar supervisão humana, transparência sobre tomada de decisão, canais de correção. Adotar medidas robustas de segurança e detecção de erros.", "940702": "[Binance por Opice Blum] Contextos de vigilância pública ou identificação remota em tempo real, com grupos vulneráveis ou ambientes sensíveis (ex: saúde, educação e religião), por poder ser intrusivo ou discriminatório. Alternativas com menor impacto: credenciais tradicionais, detecção de anomalias, autenticação multifator.", "940704": "[Binance por Opice Blum] Verificações de acurácia e vulnerabilidades (auditorias, testes de intrusão), revisão contínua das medidas de segurança, uso de criptografia, controle de acesso, intervenção humana qualificada, segregação das bases de dados, avaliação de riscos e diligências de conformidade de terceiros envolvidos.", "940707": "[Binance por Opice Blum] Boas práticas são: proporcionalidade ao risco, especialmente quanto à proteção contra fraudes e acesso a dados sensíveis; com transparência na justificativa sobre a finalidade de uso e a necessidade da biometria; medidas testadas para evitar discriminação ou exclusão indevida.", "940708": "[Binance por Opice Blum] Boas práticas incluem uso de bases diversas e atualizadas, testes regulares de acurácia e viés, criptografia, controle de acesso, transparência sobre finalidades e riscos, limitação do uso ao necessário, revisão ética (humana) contínua e canais acessíveis para contestação e correção de erros.", "940709": "[Binance por Opice Blum] Controladores podem garantir transparência com placas informando o uso de câmeras com reconhecimento facial e QR Code para acesso a informações adicionais, como finalidade do tratamento (ex.: segurança pública), identidade do controlador, canal de contato e direitos dos titulares.", "940710": "[Binance por Opice Blum] Por meio de medidas de transparência como aviso de privacidade acessível no ponto de coleta, por opções facilitadas de cadastramento com duplo fator de autenticação em comunicações e por canal claro para revogação do consentimento ou oposição no próprio ponto de controle de acesso e comunicações.", "940711": "[Binance por Opice Blum] A participação dos pais deve ser garantida por comunicado específico em linguagem clara sobre a finalidade da biometria. Deve-se avaliar meios menos invasivos e assegurar o melhor interesse do menor, prevalecendo os casos de uso benéficos ao titular para a identificação precisa (ex: segurança).", "940712": "[Binance por Opice Blum] O tratamento é admissível quando alinhado ao melhor interesse da criança. Deve haver participação informada dos responsáveis por meio de avisos de privacidade e comunicações claras. É essencial adotar criptografia, controle de acesso, logs, auditorias contínuas, RIPD e treinamentos.", "940714": "[Binance por Opice Blum] Medidas de verificação de idade não devem ser excessivas, demandando análise de proporcionalidade. Para compatibilizar com o melhor interesse do menor, é preciso

minimizar os dados coletados, limitar o prazo de retenção com sua eliminação após verificação, e conduzir RIPD para avaliar impactos.

Contribuinte: Maria Eduarda Annarumma Guedes

Número: OP-1002117

Data: 29/07/2025 - 13:44

Resumo: "A LGPD (Art. 5º, II) define dado biométrico como aquele relacionado a características físicas, comportamentais ou fisiológicas que possibilitem a identificação de uma pessoa natural. Embora o Brasil não esteja juridicamente subordinado ao GDPR (Art. 4(14)) ou às diretrizes do EDPB (Guidelines 05/2022), tais normativas estrangeiras oferecem parâmetros técnicos consolidados que auxiliam na interpretação da LGPD, dado seu grau de maturidade regulatória. Nessa perspectiva, para que uma informação seja qualificada como dado biométrico, deve resultar de tratamento técnico específico (template, hash, vetorização), ser vinculada a características únicas e permanentes da pessoa, e possibilitar sua identificação ou autenticação. Doutrinadores como Bruno Bioni e Patrícia Peck destacam a sensibilidade e a irreversibilidade como critérios fundamentais para enquadramento jurídico da biometria como dado pessoal sensível." "940688": "Embora o Brasil não esteja juridicamente vinculado ao GDPR ou às diretrizes do European Data Protection Board (EDPB), suas boas práticas oferecem referência relevante para a interpretação da LGPD, especialmente em temas sensíveis como o tratamento de dados biométricos. Controladores devem adotar medidas de transparência ativa, conforme os arts. 6º, 9º e 18 da LGPD, tais como: (i) avisos prévios em linguagem clara antes da coleta; (ii) dashboards ou portais de privacidade com informações sobre finalidades, base legal, riscos, retenção e direitos dos titulares; (iii) QR Codes ou avisos visuais nos pontos de coleta; (iv) logs acessíveis de uso dos sistemas; e (v) atualização contínua das informações. A doutrina nacional, como Peck Pinheiro, destaca a importância da accountability por meio de mecanismos visíveis e auditáveis. Ainda que não obrigatórios, modelos europeus como os da CNIL, ICO e EDPB reforçam parâmetros úteis de consentimento informado e governança transparente." "940690": "Tanto a biometria tradicional (digitais, íris, face) quanto a comportamental (voz, digitação, olhar) são consideradas dados pessoais sensíveis, nos termos do art. 5º, II da LGPD, quando utilizadas para identificação ou autenticação. A biometria comportamental, no entanto, exige cuidados adicionais devido à sua alta variabilidade e maior suscetibilidade a falsos positivos e vieses, impactando diretamente os princípios da qualidade dos dados (art. 6º, V) e da segurança (art. 6º, VII). Mesmo que o Brasil não esteja vinculado ao GDPR ou ao EDPB, boas práticas internacionais sugerem: (i) RIPD obrigatório (LGPD, art. 38), (ii) validação contínua dos modelos, (iii) logs acessíveis e auditáveis, (iv) descarte seguro e ciclo de vida bem definido, (v) governança técnica estruturada. Bioni e Peck enfatizam que a eficácia dos direitos dos titulares." "940693": "Para que o consentimento seja válido segundo a LGPD (arts. 7º, I e 8º; art. 11, I), ele deve ser livre, informado, específico, destacado e inequívoco. Isso exige clareza na comunicação, apresentação prévia de informações sobre a finalidade, riscos, retenção e compartilhamento dos dados, além de linguagem acessível, preferencialmente com

suporte de funcionários treinados. O titular deve poder negar ou revogar o consentimento sem prejuízo. Contudo, em contextos de risco elevado ou desequilíbrio de poder, o consentimento não deve ser utilizado como base legal - como em eventos com grandes aglomerações, instituições financeiras, ou no contexto de segurança pública, nos quais a base legal adequada seria o cumprimento de obrigação legal, proteção da vida ou tutela da incolumidade física (art. 11, II da LGPD). O uso do consentimento nesses casos pode comprometer a autodeterminação informativa do titular.", "940695": "Para aplicar a hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) no tratamento de dados biométricos, é essencial observar os princípios da necessidade (uso mínimo e proporcional), segurança (adoção de controles técnicos e organizacionais, como criptografia e plano de gestão de crise), e responsabilização (demonstrar a eficácia técnica e a justificativa da solução biométrica escolhida). A utilização deve ser precedida de avaliação de impacto (RIPD) e limitada a contextos em que se comprove a efetividade superior da biometria na mitigação de fraudes. A compatibilização com o princípio da necessidade exige prova de que não há meio menos invasivo disponível. Devem ser previstas salvaguardas como logs auditáveis, canal ao titular, mecanismos de contestação e plano de resposta à ANPD, assegurando equilíbrio entre prevenção à fraude e proteção às liberdades individuais.", "940697": "Quando o tratamento de dados biométricos for fundamentado no cumprimento de obrigação legal ou regulatória (art. 11, II, “a”, LGPD), o controlador - especialmente entes públicos - deve garantir que a base legal esteja expressamente indicada no aviso de privacidade, em meio acessível, como portais institucionais ou aplicativos. É essencial assegurar a finalidade específica do tratamento, a proporcionalidade da medida, bem como a limitação ao mínimo necessário. Devem ser disponibilizados: formulário claro para exercício dos direitos do titular (art. 18), canal efetivo com o encarregado de dados (art. 41) e mecanismos de segurança e prestação de contas (art. 6º, X). Também é recomendável a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) nos casos que envolvam risco relevante, conforme o art. 38 da LGPD, visando à mitigação de riscos e à preservação dos direitos fundamentais do titular.", "940699": "Muito embora a hipótese legal de estudos por órgão de pesquisa (art. 11, II, “c”, LGPD) preveja a anonimização de dados, não há como garantir a impossibilidade de reidentificar os dados posteriormente. Por conta disso, sua restrição deve ser mais rígida e, portanto, esses dados não devem ser compartilhados ou transferidos internacionalmente sem o consentimento do titular com outros atores do mercado que não tenham relação com o tratamento de dados realizado; não devem ser comercializados; não devem ser usados para finalidades diversas senão para a específica do tratamento informado. Nesse sentido a o princípio da transparência sobre o que será realizado com aquele dado deve ser o fundamento para aquele tratamento, assim como a boa-fé e a disponibilização aos titulares do código de conduta, de ética do controlador, de avisos de privacidade e do atendimento aos direitos dos titulares. Todas essas medidas são fundamentais para mitigar riscos e garantir a proteção aos direitos fundamentais.", "940700": "A utilização de tecnologias de reconhecimento facial deve seguir estritamente os ditames legais, sendo legitimada apenas quando proporcional e relevante frente às normas constitucionais. Sua aplicação precisa ser justificada e revisada constantemente, com foco na dignidade da pessoa humana. Não deve ser automática nem irrestrita. A transparência no tratamento deve ser assegurada por meio de informações claras

e acessíveis aos titulares. O consentimento deve ser livre, informado, específico, destacado e voltado a finalidades determinadas. Salvaguardas técnicas como criptografia, anonimização, avaliação de riscos, controle de acesso, auditorias em algoritmos e mitigação de vieses, somadas as jurídicas como base legal adequada, regulamentação específica, respeito à não discriminação, além de medidas institucionais como comitês de ética digital e autonomia dos encarregados pelo tratamento dos dados, são essenciais para a mitigação de riscos frente ao uso das tecnologias neste tratamento.", "940701": "Deve ser implementado o que se chama de privacy by design e privacy by default. Além disso, os sistemas devem adotar práticas de desenvolvimento ético e responsável, com datasets diversos e representativos para minimizar vieses raciais, étnicos e de gênero, visando maior equidade entre grupos populacionais. É essencial, ainda, realização de testes contínuos para aferir métricas como taxas de falsos positivos/negativos e acurácia por grupo demográfico. Em ambientes automatizados, é fundamental contar com revisões humanas qualificadas, bem como mecanismos de ajustes em tempo real, como feedbacks, registros e auditorias automáticas. Recomenda-se ainda o uso de técnicas que promovam justiça nos algoritmos e tornem suas decisões mais explicáveis (XAI). Por fim, é essencial seguir boas práticas de governança em inteligência artificial e a realização de monitoramento contínuo após a implementação.", "940702": "Em contextos de risco elevado de discriminação, como espaços públicos, escolas e transportes, recomenda-se cautela na adoção da tecnologia de reconhecimento facial. É necessário, antes, regulamentar sua aplicação, como forma de ponderar os direitos sensíveis envolvidos. Deve-se observar os princípios de privacidade desde a concepção (privacy by design), com política específica de uso que oriente a implantação e assegure conformidade com a LGPD. Diante do tratamento de dados sensíveis em larga escala, inclusive de vulneráveis, recomenda-se a elaboração de Relatório de Impacto à Proteção de Dados, avaliando riscos e medidas mitigadoras. O uso deve ser justificado pelo critério da necessidade. Quando o impacto à privacidade supera os benefícios, alternativas menos invasivas, como autenticação multifator (MFA), reconhecimento comportamental, QR Codes ou tokens físicos, reduzem a exposição de dados e fortalecem o controle do titular.", "940704": "A biometria facial, por ser dado pessoal sensível, exige base legal específica e alto nível de proteção. Como medidas técnicas recomendadas temos criptografia robusta, autenticação multifator, anonimização ou pseudonimização, minimização de dados, auditorias e testes constantes, além de monitoramento em tempo real para identificar acessos indevidos. Administrativamente, são indispensáveis políticas claras sobre coleta e uso, treinamentos periódicos, gestão formal de riscos, avaliações de impacto à proteção de dados (RIPD) e planos de resposta a incidentes. Parâmetros mínimos incluem avaliação prévia de proporcionalidade e necessidade, revisões periódicas das práticas, monitoramento contínuo e auditorias independentes para garantir conformidade. A banalização do uso da biometria, sobretudo em contextos não essenciais, deve ser evitada, exigindo justificativas sólidas de finalidade e medidas que respeitem os direitos fundamentais dos titulares.", "940707": "Os controladores devem adotar boas práticas que evitem discriminação, oferecendo meios alternativos de acesso, como senhas, tokens ou cartões. A negativa do titular em fornecer dados biométricos deve ser respeitada, e eventuais restrições precisam ser proporcionais, justificadas e comunicadas com clareza. É fundamental avaliar se a biometria é estritamente necessária para a funcionalidade, garantindo a aplicação

dos princípios de necessidade, adequação, garantindo a minimização de dados. Nos casos em que a biometria seja indispensável, o controlador deve documentar a justificativa técnica e jurídica, garantindo transparência sobre os riscos e os direitos do titular. Auditorias e avaliações de impacto à proteção de dados devem ser realizadas periodicamente para assegurar que restrições impostas não violem direitos fundamentais nem resultem em tratamento discriminatório.", "940708": "Para proteger dados biométricos, controladores devem adotar governança em privacidade alinhada à LGPD, com diretrizes claras de segurança, gestão de riscos e direitos dos titulares. Políticas internas devem regular coleta, armazenamento e uso, com avaliações frequentes de proporcionalidade, necessidade e impacto. É essencial garantir transparência sobre finalidade, base legal, período de retenção e formas de exercício dos direitos. Profissionais dos agentes de tratamento precisam de capacitação contínua e auditorias periódicas devem ser realizadas. Para uso responsável, os titulares devem ser informados de forma clara sobre riscos e garantias, com canais para acesso, correção, exclusão ou oposição. Monitorar vieses algorítmicos e impedir decisões automatizadas discriminatórias ou finalidades não previstas são medidas indispensáveis para assegurar proporcionalidade e legalidade.", "940709": "Respeitar os princípios da necessidade e finalidade, coletando apenas dados estritamente necessários e com finalidades legítimas e específicas. Garantir que os titulares sejam informados de forma prévia e clara, inclusive em ambientes complexos, por meio de sinalizações, políticas acessíveis e canais de comunicação eficazes. Sempre que possível, oferecer mecanismos de controle e consentimento, além de alternativas para quem não quiser participar. Realizar avaliações de impacto à proteção de dados (RIPD) completas, com envolvimento da sociedade e órgãos reguladores. Implementar governança transparente e responsável, com supervisão independente e prestação de contas pública.", "940710": "É fundamental que os agentes de tratamento disponibilizem avisos de privacidade claros e acessíveis, para que os titulares possam compreender, de forma objetiva e transparente, como ocorre a coleta dos dados pessoais, inclusive os biométricos, informando a finalidade do tratamento, a hipótese legal que o justifica, os direitos assegurados aos titulares, as medidas de segurança adotadas, eventuais compartilhamentos com terceiros, inclusive em transferências internacionais, além do período de retenção e os critérios para o descarte dos dados ao final de sua necessidade. Também devem constar informações sobre a realização do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), os canais apropriados para que os titulares possam apresentar reclamações junto à Autoridade Nacional de Proteção de Dados (ANPD), bem como os meios de contato do encarregado pelo tratamento de dados, promovendo a transparência e evidenciando o compromisso com as boas práticas de governança em privacidade.", "940711": "A coleta de dados pessoais deve ser sempre minimizada, utilizando-se meios menos invasivos e adotando, quando necessário, a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). O tratamento desses dados deve respeitar o artigo 14 da LGPD, sendo indispensável o consentimento livre, informado, específico, destacado e fornecido por pelo menos um dos responsáveis legais. É essencial a disponibilização de aviso de privacidade contendo, de forma clara e acessível, informações sobre os dados coletados, a finalidade do tratamento, os direitos assegurados aos titulares, o tempo de retenção dos dados, as medidas de segurança implementadas, os canais de comunicação com o encarregado pelo tratamento e

demais informações pertinentes. As práticas adotadas devem priorizar a segurança e a não exposição excessiva do titular, garantindo sempre o uso proporcional e responsável dos dados pessoais tratados.", "940712": "O tratamento de dados pessoais sensíveis de crianças e adolescentes deve ocorrer de forma excepcional, proporcional e fundamentado no melhor interesse do menor, nos termos do artigo 11 da Lei Geral de Proteção de Dados (LGPD). Deve-se priorizar a aplicação do inciso I do art. 11, e, quando isso não for possível, adotar o inciso II, especialmente a alínea “d”, que permite o tratamento para o exercício regular de direitos. É imprescindível garantir que a representação legal seja adequada e legítima, tendo em vista a incapacidade civil das crianças e adolescentes para firmar contratos. Assim, a atuação dos agentes de tratamento deve ser cautelosa, garantindo que a coleta e o uso de dados ocorram de forma justificada, segura, limitada ao estritamente necessário e em conformidade com as normas protetivas específicas voltadas a esse público vulnerável, respeitando sempre os princípios da boa-fé, necessidade e transparência.", "940714": "A coleta de dados pessoais, especialmente biométricos, de crianças e adolescentes deve ser realizada com extrema cautela, observando os princípios da minimização, segurança e transparência, sempre em conformidade com o artigo 14 da LGPD e com foco no melhor interesse do menor. É essencial obter o consentimento claro, específico e destacado de ao menos um responsável legal, além de estabelecer parcerias com órgãos públicos para reforçar a legitimidade e segurança do tratamento. Deve-se avaliar cuidadosamente os riscos envolvidos, considerando as categorias de conteúdo acessado, contatos estabelecidos, condutas observadas e a eventual formação de contratos. A abordagem deve ser sempre a menos invasiva possível, pautada em boas práticas e medidas técnicas e organizacionais adequadas, assegurando que os dados coletados sejam estritamente necessários à finalidade proposta e que os direitos dos menores sejam devidamente resguardados em todo o processo.

Contribuinte: ERIKA MOTA TOCANTINS

Número: OP-1002202

Data: 29/07/2025 - 15:06

Resumo: "O primeiro critério deve ser a natureza do dado: aquele que diz respeito às características físicas, fisiológicas ou comportamentais de uma pessoa, seguindo a definição adotada, por exemplo, pela GDPR. Cabe destacar que o objeto a ser regulado são os dados biométricos - não as “características biométricas”, que existem de forma independente ao processo de extração da informação. O segundo critério objetivo deve ser a identificabilidade: Seguindo o artigo 5º da LGPD, considera-se que um dado biométrico é um dado pessoal sensível, necessariamente vinculado a uma pessoa natural. A identificação (direta ou indireta) dos indivíduos vinculados aos dados é o que os circunscreve dentro do contexto da proteção de dados pessoais. Não se deve estabelecer dentre os critérios o formato do dado biométrico. Isso limitaria a aplicação da proteção de dados a tais formatos, que poderiam se tornar defasados a depender da evolução do estado da técnica. O critério da unicidade não deve ser considerado", "940688": "Divulgação obrigatória de documentos essenciais envolvendo o tratamento de dados, nos moldes do artigo 9 da LGPD, em que constem: (I) Finalidade do

tratamento; (II) Forma e duração do tratamento; (III) identificação do controlador; (IV) informações de contato do controlador. No contexto da execução de políticas públicas, deverá haver divulgação obrigatória e periódica de relatórios de impacto, que descreva de forma clara, simples e compreensível os riscos associados ao tratamento para o titular. O relatório deve conter informações específicas sobre riscos discriminatórios. Divulgação obrigatória de políticas de proteção de dados e segurança da informação referentes ao tratamento. Em locais com coleta automatizada de dados biométricos, deve haver avisos visuais nos locais de coleta."

"940690": "A biometria comportamental pode ser capaz de identificar uma pessoa, portanto ela deve ser tratada da mesma forma que a biometria tradicional. Há um agravante, entretanto: o aumento do risco à privacidade, já que frequentemente é coletado sem o conhecimento do titular, o que exige transparência reforçada por parte dos controladores. Isso está alinhado com o princípio da prestação de contas e o dever de informação clara e acessível ao titular. Além disso, a biometria comportamental é altamente sensível a variações contextuais – humor, fadiga, ambiente, estresse. Isso impacta diretamente o princípio da qualidade dos dados. Esse risco é particularmente crítico em sistemas de autenticação contínua, onde falsos positivos/negativos podem levar à exclusão injusta de usuários ou ao acesso indevido por terceiros. Em relação à segurança, a biometria comportamental é vulnerável à interceptação e reutilização maliciosa, pois os padrões de digitação ou movimento podem ser capturados com facilidade."

"940693": "O titular deve ter liberdade real de escolha quanto ao consentimento, sem coação, intimidação ou prejuízo em caso de recusa; deve-se oferecer alternativas equivalentes não biométricas, especialmente em serviços públicos ou essenciais e garantir que a recusa em consentir não resulte em perda de acesso ou discriminação; apresentar as finalidades específicas do uso dos dados biométricos, como "autenticação em acesso ao sistema", "monitoramento de presença"; Inserir caixas de seleção claras e separadas para consentimento com dados biométricos; usar linguagem simples e direta, informando sobre a tecnologia, base legal, direitos do titular, consequências da negativa; evitar consentimento implícito por uso continuado da plataforma; permitir a revogação simples do consentimento. O consentimento não deve ser utilizado quando há desequilíbrio de poder, falta de alternativas ou vulnerabilidade. Quando a negativa de consentimento impede o acesso a um serviço, ele não é considerado livre."

"940695": "A base legal da prevenção à fraude não pode ser tratada como salvo-conduto para a biometrização da vida cotidiana. O tratamento de dados biométricos, sobretudo faciais, só é legítimo se tecnicamente necessário e juridicamente proporcional. Assim, exigível avaliação de impacto, demonstração clara de adequação frente a meios menos intrusivos (como MFA, autenticação local ou chaves criptográficas), e respeito ao princípio da minimização. O uso massivo e difuso desses dados, inclusive em contextos tecnicamente frágeis (portarias, apps bancários), amplia o vetor de risco em vez de reduzi-lo, ainda mais diante de ataques por deepfake e da irreversibilidade da biometria. Salvaguardas robustas, como hash local, não reidentificação e alternativa não biométrica, são inegociáveis. A ANPD deve coibir práticas pseudotécnicas que transformam a “fraude” em justificativa genérica para vigilância. Prevenir riscos, aqui, exige mais do que palavras: exige arquitetura institucional e técnica à altura."

"940697": "A invocação da obrigação legal para justificar o uso de biometria por órgãos públicos demanda base normativa específica, com finalidade clara, escopo limitado e controles efetivos. Num

cenário de baixa maturidade institucional e terceirização técnica generalizada, esse tratamento só se sustenta se precedido por avaliação de impacto à proteção de dados, com consulta pública e consideração real dos riscos a grupos vulnerabilizados. A ANPD deve exigir salvaguardas como separação de finalidades, limitação temporal, controle de acesso, e vedação de reuso não autorizado. A transparência ativa e a intervenção humana qualificada são fundamentais para limitar a automatização opaca do acesso a direitos. Dados biométricos não são infraestrutura neutra. O uso público desses dados, sem o devido anteparo democrático e técnico, pode ampliar desigualdades e comprometer a liberdade informacional dos titulares. ", "940699": "O tratamento de dados biométricos para pesquisa encontra limite na possibilidade de reidentificação, mesmo após anonimização. Dado o alto poder identificador da biometria e o potencial de cruzamento de bases, a anonimização, se reversível ou vulnerável, não descaracteriza o dado como pessoal. Persistindo risco razoável de reidentificação, exige-se base legal adicional. A “exceção científica” não pode justificar usos extrativistas de dados sensíveis, sobretudo sobre populações vulnerabilizadas. A autodeterminação informativa, a minimização e a não ocorrência da reidentificação são balizas intransponíveis. Como salvaguardas, recomendam-se: anonimização robusta ou pseudonimização com chaves segregadas; coleta mínima; avaliações de impacto; criptografia ponta-a-ponta; vedação expressa ao perfilamento; governança ética e transparente; revisão independente; canais de denúncia; comunicação acessível com os titulares; transparência e consentimento específico.", "940700": "TRFs devem passar por RIPD robustos, demonstrando necessidade, adequação e inexistência de alternativa menos intrusiva. A proporcionalidade impõe limitação de escopo, minimização da coleta e descarte imediato de dados não pertinentes. Transparência demanda avisos claros, mecanismos de contestação, auditoria externa, além de acesso público aos contratos, fins do uso, software e hardware utilizados. A acurácia deve ser, no mínimo, acompanhada de métricas de sensibilidade, especificidade e erro diferencial por raça, idade e gênero. Salvaguardas técnicas incluem: logs imutáveis, revisão humana, datasets auditáveis, código aberto e vedação a perfilamento. Juridicamente: base legal clara, finalidade específica, proibição de decisões exclusivamente automatizadas, autorização judicial prévia para usos invasivos e responsabilização. Institucionalmente: auditoria externa, controle público sobre fornecedores, padronização nacional, participação social qualificada, e supervisão da ANPD.", "940701": "Sistemas de reconhecimento facial devem ser projetados com bases de dados de qualidade (diversas, representativas, precisas, atualizadas e legalmente coletadas), com alta resolução, anotação correta e documentação transparente sobre sua origem e limitações. Para garantir eficácia e confiabilidade, é fundamental monitorar continuamente métricas como False Acceptance Rate (FAR) e False Rejection Rate (FRR), realizar testes cruzados, auditorias externas e reavaliações periódicas. Devem aplicar princípios de privacy by design, assegurar a explicabilidade das decisões automatizadas e ter validação humana. O tratamento de dados deve respeitar a LGPD, incluindo consentimento livre e informado, minimização de dados e relatórios de impacto (RIPD). Falhas devem ser corrigidas de forma tempestiva por meio de mecanismos de supervisão, revisão automatizada e canais acessíveis de contestação ao titular dos dados.", "940702": "Sim, há contextos em que o uso de TRFs não é recomendado, especialmente quando há alto risco de erro, discriminação ou violação de direitos

fundamentais. Situações como controle de presença em escolas (expondo dados de crianças), monitoramento em locais públicos sem consentimento, triagem automatizada em processos seletivos, policiamento preditivo e uso em ambientes hospitalares são exemplos em que o impacto sobre os titulares pode ser desproporcional, impreciso e incontrolável. Nesses casos, o uso de tecnologias mais proporcionais é indicado. Alternativas eficazes incluem: autenticação multifator (MFA), que reforça a segurança com menor exposição de dados; biometria por impressão digital, quando estritamente necessária e bem regulada; e bases de dados integradas com informações tradicionais, como registros civis ou dados forenses, estes apenas quando autorizado por lei. Essas soluções reduzem riscos e respeitam os princípios da LGPD."

"940704": "O tratamento de dados biométricos exige armazenamento seguro, como por meio de TEEs (Trusted Execution Environment, enclaves de hardware isolados, onde os mesmos permanecem criptografados e inacessíveis mesmo para administradores), e medidas que neutralizem sua utilidade em caso de vazamento, como a autenticação multifatorial adaptativa (MFA). Combinando biometria com análise comportamental em tempo real, a MFA visa invalidar tentativas de fraude mesmo que um ator malicioso obtenha cópia do template biométrico, pois não depende apenas do dado estático, mas de características dinâmicas ligadas ao usuário, como padrões de interação com dispositivos, tornando dados vazados inúteis sem o comportamento associado. É crucial observar se a coleta não reforça estruturas de monitoramento intrusivo, considerando se: (1) o uso da biometria é estritamente necessário (minimização); (2) há transparência algorítmica; e (3) existem salvaguardas contra usos secundários voltados à vigilância. "

"940707": "Boas práticas incluem oferecer alternativas claras e não biométricas para acesso às funcionalidades dos serviços não essenciais, e realizar RIPDs focados em vieses discriminatórios. É vital o treinamento do sistema com dados diversos e a auditoria contínua para correção de vieses, dado que a tecnologia possui taxas de erro desproporcionais para grupos vulneráveis como pessoas negras, indígenas e trans. A recusa do titular ao consentimento pode justificar, de forma proporcional e transparente, a limitação de funcionalidades apenas quando a biometria for tecnicamente indispensável para a operação específica - e desde que não inviabilize o acesso ao serviço principal. A limitação ao consentimento só é legítima se houver demonstração da necessidade, ausência de alternativa viável e comunicação clara sobre os impactos da escolha, sem coerção nem efeito inibitório. Negativas devem ser justificadas ao titular e registradas de forma auditável, garantindo transparência sem expor dados pessoais."

"940708": "A proteção eficaz no tratamento de dados biométricos exige medidas técnicas robustas, e demanda responsabilização concreta sobre todo o ciclo de uso. Controladores devem garantir armazenamento seguro, controle rigoroso de acesso, coleta restrita ao necessário (minimização) e eliminação imediata de dados de pessoas não envolvidas no tratamento, além de consentimento informado e finalidade legítima, claramente definida. A participação de fornecedores terceirizados requer supervisão independente e transparência ativa sobre sua atuação no ciclo de tratamento. Para evitar discriminações, é fundamental que sistemas sejam treinados com dados diversos, auditados continuamente e acompanhados por RIPDs com foco em vieses contra grupos vulnerabilizados. A transparência deve alcançar não só o titular, mas também o debate público, por meio de relatórios que permitam aferir o impacto social das decisões automatizadas, inclusive sobre negativas de acesso. "

"940709": "Não há

observância efetiva da autodeterminação informativa em contextos de tratamento contínuo e massivo de dados biométricos, como em smart cities e monitoramento de multidões. Pela LGPD, o titular tem direito a controle, informação clara e consentimento livre, o que é inviável em espaços públicos, onde a coleta é indiscriminada e constante. A complexidade tecnológica e o grau de opacidade impedem que titulares compreendam, controlem ou exerçam seus direitos efetivamente, especialmente grupos vulneráveis. Além disso, a ausência de transparência real, a dificuldade de acesso a informações e a impossibilidade de recusar o tratamento tornam esse modelo incompatível com a proteção de dados pessoais. Assim, recomenda-se que a legislação vigente, em consonância com a Constituição Federal, não permita acomodar como legítima prática que fere prerrogativas de autodeterminação informativa, direito à imagem, à liberdade e à dignidade da pessoa humana.", "940710": "Os agentes de tratamento devem adotar medidas proativas para garantir os direitos dos titulares, especialmente diante do uso de dados biométricos e decisões automatizadas. No caso de crianças e adolescentes, a LGPD, em seu art. 14, impõe salvaguardas adicionais com base no princípio do superior interesse da criança, exigindo informações claras, acessíveis e compatíveis com sua compreensão. É essencial assegurar os direitos de acesso, correção e revogação do consentimento. Diante das limitações técnicas da IA, como a opacidade e as inferências não consentidas, o consentimento por si se mostra insuficiente. Assim, é necessário fortalecer o arcabouço regulatório para garantir transparência, explicabilidade e limites a práticas abusivas, sobretudo no tratamento de dados de grupos vulneráveis.", "940711": "Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em ambientes como escolas e espaços recreativos, a participação informada dos pais ou responsáveis deve ser assegurada por meio de consentimento específico, destacado e com informações claras e acessíveis, nos termos do art. 14, §6º da LGPD. O tratamento só é admissível quando estritamente necessário para atender ao melhor interesse da criança, conforme o caput do art. 14, e deve respeitar os princípios da necessidade, adequação e minimização. Devem ser adotadas salvaguardas técnicas e organizacionais, como a anonimização, sempre que possível, e a criptografia dos dados biométricos, a fim de mitigar riscos à privacidade. Além disso, é essencial garantir o exercício dos direitos dos titulares, incluindo acesso, correção e revogação do consentimento. O uso de dados biométricos não pode ser excessivo nem condicionar o acesso a direitos fundamentais, como educação ou lazer.", "940712": "Idealmente, o tratamento de dados biométricos de crianças e adolescentes deve se restringir a hipóteses excepcionais, como identificação de desaparecidos ou em situações de urgência em que não haja alternativa eficaz. Fora desses casos, somente se admite o uso vinculado a necessidades essenciais (saúde, educação, segurança, etc.), observando sempre o princípio do melhor interesse da criança e oferecendo meios alternativos de identificação. É imprescindível o consentimento específico e destacado dos pais ou responsáveis (art. 14, §1º), com atenção à sua alfabetização digital e à clareza das informações prestadas. O tratamento deve observar medidas técnicas e organizacionais rigorosas: criptografia forte, registros de acesso imutáveis, uso exclusivo para finalidade determinada, vedação de compartilhamento indevido e exclusão imediata dos dados. Também é necessário mitigar riscos de reidentificação e falhas, especialmente diante de elevadas taxas de erro em sistemas biométricos

infantis.", "940714": "A compatibilização entre verificação de idade via biometria e os princípios da necessidade e do melhor interesse exige avaliação rigorosa de proporcionalidade: o tratamento deve ser imprescindível à finalidade, considerando o risco do serviço, e não pode haver meio menos invasivo. Métodos biométricos são altamente sensíveis, com margem de erro significativa entre crianças racializadas e mais novas, e podem gerar exclusão e discriminação. Seu uso só se justifica quando há risco concreto à integridade da criança e deve ser precedido de avaliação de impacto aos direitos fundamentais. O melhor interesse demanda, ainda, transparência, consentimento dos responsáveis com linguagem acessível e garantias técnicas robustas. Sempre que possível, deve-se aplicar design universal com proteção por padrão (privacy by design), evitando o uso excessivo de dados e promovendo ambiente digital seguro a todas as idades.

Contribuinte: ANDRE LUCAS FERNANDES

Número: OP-1003688

Data: 30/07/2025 - 10:29

Resumo: : "Origem biológica e pessoal do dado: O dado biométrico deve estar relacionado a características físicas, comportamentais ou fisiológicas de uma pessoa natural, como digitais, íris, voz, reconhecimento facial, entre outros. Capacidade de identificação ou autenticação individual: O dado deve ser suficiente para identificar de forma única ou autenticar a identidade de uma pessoa. A identificação deve ser possível de forma direta ou indireta. Tratamento automatizado para identificação: Os dados biométricos geralmente são processados por meios eletrônicos, com fins de controle de acesso ou segurança, o que envolve tratamento automatizado (ex.: sistemas de reconhecimento facial ou leitores de digitais). Finalidade específica no tratamento: A LGPD exige que a finalidade do uso do dado biométrico esteja claramente definida (ex: controle de acesso de moradores ou prestadores de serviço) e seja necessária e proporcional ao risco que se pretende mitigar, como proteção de pessoas e patrimônio.", "940688": "Aviso de Privacidade visível e acessível: Instalar placas, avisos físicos ou digitais nas áreas de coleta (portarias com biometria facial ou digital), contendo: Finalidade da coleta (segurança, controle de acesso); Base legal do tratamento (interesse legítimo); Dados coletados (impressão digital, imagem facial); Tempo de retenção dos dados; Direitos dos titulares; Contato do encarregado (DPO) ou responsável. Disponibilização da Política de Privacidade: Tornar a política de tratamento de dados disponível: Em locais de uso comum (muais); Por meio digital (site do condomínio, aplicativo, e-mail); Em formato simplificado e, quando necessário, com linguagem acessível a idosos e crianças. Consentimento esclarecido quando exigido: Embora o consentimento não seja sempre obrigatório, nos casos em que for necessário, Precedido de informações claras sobre riscos, direitos e finalidade. Canal de atendimento ao titular: direto com o síndico, administradora ou administração. ", "940690": "A biometria comportamental (como padrões de digitação, voz ou movimento ocular) exige tratamento mais rigoroso que a biometria tradicional (digital, facial, íris), pois envolve dados dinâmicos e inferenciais, com maior risco de erro e invasividade. Assim, impõe-se atenção especial aos princípios da qualidade dos

dados (exatidão, atualização e relevância) e da segurança (criptografia, controle de acesso e auditoria dos sistemas), além da necessidade de transparência adicional aos titulares. Devido à complexidade e aos riscos envolvidos, recomenda-se a realização de avaliação de impacto (DPIA) e a disponibilização de alternativas ao uso desse tipo de dado, sobretudo em ambientes condominiais residenciais, nos quais a adoção dessa tecnologia ainda é, em regra, desproporcional frente aos seus benefícios."

"940693": "Para garantir que o consentimento para o tratamento de dados biométricos seja válido nos termos da LGPD, é essencial que ele seja obtido de forma livre, específica, destacada, informada e inequívoca (art. 8º), por meio de documento claro, separado de outras cláusulas contratuais, com a indicação da finalidade, base legal, prazo de retenção e os direitos do titular. Além disso, o titular deve poder revogar o consentimento a qualquer momento, sem prejuízo. No entanto, o consentimento não é a base legal mais adequada em contextos como controle de acesso em áreas comuns de condomínio, pois há desbalanceamento de poder entre o controlador (condomínio) e o titular (morador ou visitante), além da dificuldade prática de gerenciar a revogação. Nestes casos, recomenda-se utilizar bases legais mais apropriadas, como o interesse legítimo (art. 7º, IX) ou a proteção à vida e à segurança (art. 11, II, e), desde que respeitados os princípios da necessidade e proporcionalidade."

"940695": "Para aplicar corretamente a hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, da LGPD) no tratamento de dados biométricos, é necessário demonstrar que o uso desses dados é estritamente necessário, proporcional ao risco de fraude, e que não existem meios menos intrusivos para atingir a mesma finalidade. No caso de acesso a soluções bancárias ou financeiras, por exemplo, o uso de biometria (como reconhecimento facial ou digital) pode ser considerado legítimo desde que limitado à finalidade de autenticação e segurança, evitando qualquer reutilização indevida ou compartilhamento para outras finalidades. Para compatibilizar o uso com o princípio da necessidade, o controlador deve restringir a coleta ao mínimo necessário, manter política de retenção clara, e garantir medidas técnicas e organizacionais robustas (como criptografia, segregação de bases, e autenticação multifator). Além disso, devem ser implementadas salvaguardas como: avaliação de impacto à proteção de dados"

"940697": "Quando o tratamento de dados biométricos se fundamenta na hipótese legal de “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, da LGPD), os controladores — especialmente entidades e órgãos públicos — devem observar que: (i) a obrigação esteja expressamente prevista em norma legal ou regulatória válida; (ii) o uso da biometria seja necessário, proporcional e adequado à finalidade legal; e (iii) sejam implementadas salvaguardas compatíveis com a natureza sensível dos dados, como minimização da coleta, definição clara de prazos de retenção, controles de acesso rigorosos, e documentação do fluxo de tratamento. Além disso, o princípio da transparência exige que os titulares sejam informados, de forma clara, sobre os fundamentos legais, os direitos garantidos e os canais para exercício desses direitos. Para mitigar riscos e garantir conformidade, recomenda-se a realização de avaliações de impacto à proteção de dados (DPIA), bem como a implementação de governança contínua sobre"

"940699": "O tratamento de dados biométricos para fins de pesquisa, mesmo c/ base na hipótese legal do art. 11, II, “c”, da LGPD, está sujeito a limites estritos, espec devido ao alto risco de reidentificação quando há cruzamento de bases de dados. Ainda que os dados estejam anonimizados, a

biometria possui traços únicos e persistentes, o que eleva o risco de reversão da anonimização. Por isso, os controladores e órgãos de pesquisa devem aplicar técnicas robustas de anonimização, evitar o acoplamento de dados que possam gerar perfis individualizáveis e realizar testes periódicos de risco de reidentificação. Além disso, exige-se a implementação de salvaguardas adicionais, como: restrição de acesso aos dados a equipes qualificadas e sujeitas a confidencialidade; publicação de resultados apenas em formato agregado; proibição de compartilhamento com terceiros não autorizados; e realização de avaliação de impacto (DPIA) antes do início da pesquisa. O princípio da deve ser rigidamente observado.", "940700": "Para garantir que o uso de reconhecimento facial respeite os princípios da necessidade, proporcionalidade e transparência, o controlador deve demonstrar que não há meio menos intrusivo para atingir a finalidade, limitar a coleta ao mínimo necessário e informar claramente os titulares sobre o tratamento. Para evitar discriminação, é essencial auditar algoritmos quanto a vieses, aplicar testes de acurácia por grupo social e proibir decisões automatizadas com efeitos discriminatórios. Devem ser adotadas salvaguardas como: DPIA prévia, registro de logs, controle rigoroso de acesso, anonimização quando possível, e políticas públicas claras e acessíveis, especialmente em ambientes públicos ou de vigilância.", "940701": "Sistemas de reconhecimento facial devem ser projetados com base no princípio de privacy by design, priorizando acurácia e não discriminação desde a concepção. Isso inclui o uso de bases de dados diversas e auditadas, treinamento constante dos algoritmos e testes de desempenho segmentados por idade, raça e gênero. Para reduzir falsos positivos/negativos, recomenda-se autenticação multifator, calibração contínua e limiares de confiança ajustáveis. Devem ser previstos mecanismos de correção imediata, como canal direto de contestação, revisão humana obrigatória em decisões sensíveis e logs de falhas analisáveis. Tecnologias automatizadas devem prever auditoria periódica, supervisão humana significativa e medidas corretivas com base em métricas claras de erro.", "940702": "Sim, o uso de reconhecimento facial não é recomendado em contextos de acesso a serviços essenciais, espaços públicos amplos, populações vulneráveis (crianças, idosos, pessoas com deficiência) e em ambientes com pouca transparência ou sem supervisão adequada. Nesses casos, há alto risco de discriminação, vigilância massiva e violação de direitos fundamentais, além de maior margem para erros de identificação. Como alternativas, podem ser utilizadas tecnologias como QR Codes temporários, chaves digitais criptografadas, cartões RFID, ou biometria por impressão digital com consentimento e controle local. Essas opções, quando bem implementadas, oferecem segurança operacional com menor impacto sobre a privacidade, respeitando melhor os princípios da proporcionalidade, necessidade e minimização da LGPD.", "940704": "Diante do alto impacto de violações de dados biométricos, é indispensável adotar medidas técnicas como criptografia forte, armazenamento segregado, controle de acesso baseado em função (RBAC), logs de auditoria, testes de intrusão e autenticação multifator. No plano administrativo, devem existir políticas internas claras, treinamentos contínuos, resposta a incidentes e avaliação prévia de impacto (DPIA). Como parâmetros mínimos, exige-se análise periódica de riscos, monitoramento contínuo dos sistemas, revisão anual das medidas de segurança e auditorias independentes, garantindo conformidade com os princípios da LGPD e a proteção integral dos direitos dos titulares.", "940707": "Em serviços não essenciais, a biometria só deve ser exigida quando for

tecnicamente indispensável para a funcionalidade ofertada. Para evitar discriminação ilícita, é fundamental oferecer métodos alternativos de autenticação, como senhas, tokens ou PINs. A restrição de funcionalidades em caso de recusa do titular só será legítima se for proporcional, transparente e previamente informada, com base no consentimento válido e livre. É aceitável limitar o acesso quando a biometria for necessária para segurança reforçada (ex: transações financeiras de alto valor), desde que haja justificativa técnica clara e que o titular tenha sido informado previamente, com possibilidade real de escolha.", "940708": "Boas práticas incluem: minimização da coleta, uso de criptografia robusta, armazenamento em bases segregadas, controle estrito de acesso, auditorias regulares e realização de DPIA antes do tratamento. Para garantir uso transparente e responsável, o controlador deve informar claramente a finalidade, base legal, riscos e direitos dos titulares, além de prever mecanismos de contestação e supervisão humana em decisões automatizadas. É essencial auditar algoritmos quanto a viés discriminatório, treinar equipes e documentar todo o ciclo de vida dos dados. A adoção de códigos de conduta e governança ajuda a reforçar a confiança e a conformidade com a LGPD.", "940709": "Controladores devem garantir autodeterminação informativa por meio de transparência ativa, com sinalização clara em áreas monitoradas, avisos públicos acessíveis, e divulgação em sites e apps sobre o tratamento biométrico. Devem disponibilizar canais acessíveis para exercício de direitos (acesso, oposição, eliminação), mesmo em contextos massivos. É essencial realizar DPIA público, limitar a coleta ao estritamente necessário, adotar anonimização sempre que possível e prever revisão humana em decisões automatizadas. A criação de comitês de ética, auditorias externas e relatórios de impacto acessíveis ao público reforça a legitimidade e o controle social sobre o uso da biometria em larga escala.", "940710": "Agentes de tratamento devem garantir os direitos dos titulares com interfaces acessíveis e funcionais, como portais digitais ou canais físicos, que permitam: (i) consulta clara sobre quais dados biométricos são tratados, com que finalidade e por qual base legal; (ii) solicitação de acesso, correção e eliminação; e (iii) revogação facilitada do consentimento, sem prejuízo ao titular. Em tratamentos automatizados, é essencial assegurar transparência algorítmica, com explicação simples das decisões tomadas, além de revisão humana significativa e mecanismos para contestação. Tudo deve ser registrado e auditável, conforme os princípios da LGPD e os direitos previstos nos arts. 9º, 18 e 20 da lei.", "940711": "O tratamento de dados biométricos de crianças e adolescentes exige consentimento específico e em destaque dos pais ou responsáveis legais, precedido de informação clara, acessível e adequada à compreensão. Só é admissível quando necessário para proteger a criança, garantir segurança ou controle de acesso em escolas e espaços recreativos, com base no melhor interesse do menor (art. 14, LGPD). Devem ser observadas as condições de: (i) coleta mínima necessária; (ii) transparência ativa sobre finalidade e riscos; (iii) possibilidade de revogação do consentimento sem prejuízo ao menor; e (iv) salvaguardas técnicas e administrativas robustas para evitar uso indevido ou exposição indevida dos dados sensíveis.", "940712": "O tratamento de dados biométricos de crianças e adolescentes é admissível, segundo a LGPD, com consentimento específico e destacado dos pais ou responsáveis (art. 14, §1º), e desde que em atenção ao melhor interesse do menor. Hipóteses legais incluem: (i) proteção da vida e da segurança (art. 11, II, "e"), como no controle de acesso a escolas; ou (ii) execução de políticas públicas, quando realizado por

órgãos públicos. A participação informada se dá por meio de avisos claros, linguagem acessível, canais de esclarecimento e opção real de escolha. Devem ser adotadas medidas como: criptografia dos dados, controle de acesso restrito, auditoria periódica, limitação da retenção e treinamento de pessoal, garantindo um ambiente seguro e ético no tratamento dessas informações sensíveis.", "940714": "Na verificação de idade por biometria em plataformas digitais e jogos, o tratamento de dados de crianças e adolescentes deve observar: (i) finalidade clara e legítima, como restringir conteúdos inadequados; (ii) consentimento dos pais ou responsáveis, quando houver identificação direta; e (iii) uso da biometria apenas se estritamente necessário, conforme o princípio da necessidade (art. 6º, III, LGPD). A compatibilização com o princípio do melhor interesse da criança exige que a tecnologia empregada seja proporcional ao risco e não exponha o menor a coleta excessiva ou discriminação. Sempre que possível, devem ser adotadas alternativas menos invasivas, como estimativas por autodeclaração com validação progressiva, além de políticas de privacidade acessíveis e canais de contato com os responsáveis.

Contribuinte: EVELISE SOUZA WAGNER

Número: OP-1003891

Data: 30/07/2025 - 12:08

Resumo: "Para que um dado seja caracterizado como biométrico nos termos da LGPD, é necessário que ele derive de características físicas, fisiológicas ou comportamentais de uma pessoa natural, seja submetido a tratamento técnico específico — como uso de sensores, algoritmos ou softwares — e tenha como finalidade a identificação ou autenticação individual. A simples existência da característica física não configura dado biométrico; é o tratamento com objetivo de identificar que o torna sensível. Assim, impressões digitais, reconhecimento facial, íris, voz e até padrões de comportamento, quando tratados tecnicamente para identificar alguém, são considerados dados biométricos sensíveis, exigindo maior rigor no seu tratamento, conforme os princípios da LGPD.", "940688": "Controladores que tratam dados biométricos devem adotar práticas de transparência ativa, garantindo que os titulares recebam informações claras, acessíveis e prévias sobre o tratamento. Isso inclui a disponibilização de políticas de privacidade com linguagem simples, explicando a finalidade do uso dos dados biométricos, a base legal aplicada, os direitos dos titulares, o tempo de retenção dos dados, possíveis compartilhamentos e medidas de segurança adotadas. Também é recomendável o uso de avisos visuais em locais de coleta (como totens ou catracas), além de canais de atendimento para dúvidas. A transparência deve ser contínua, permitindo que o titular exerça seus direitos de forma plena, conforme os artigos 6º, 9º e 18 da LGPD.", "940690": "A biometria comportamental deve receber o mesmo nível de proteção que a biometria tradicional, pois também permite a identificação única do titular, sendo, portanto, dado pessoal sensível nos termos da LGPD. No entanto, por envolver dados dinâmicos, frequentemente coletados de forma contínua e automatizada, ela exige atenção especial aos princípios da qualidade dos dados — garantindo que sejam exatos, atualizados e relevantes — e da segurança, com medidas técnicas robustas para evitar acessos indevidos ou

inferências abusivas. Além disso, o uso dessas tecnologias pode demandar avaliações de impacto à proteção de dados (DPIA), dada sua complexidade e potencial invasivo, conforme o art. 38 da LGPD, reforçando a necessidade de documentação e mitigação de riscos específicos.", "940693": "Para garantir que o consentimento para o tratamento de dados biométricos seja válido nos termos da LGPD, ele deve ser obtido de forma livre, ou seja, sem coação ou condicionamento ao acesso a serviços; específico, indicando claramente a finalidade do tratamento; destacado, separado de outros termos contratuais; informado, com linguagem clara sobre riscos, direitos e usos; e inequívoco, mediante manifestação expressa do titular. Contudo, o consentimento não é adequado quando houver assimetria de poder, como em relações trabalhistas ou contratuais obrigatórias, em que o titular possa se sentir compelido a consentir. Nesses casos, é preferível recorrer a outras hipóteses legais do art. 11, como prevenção à fraude, obrigação legal ou proteção da vida, sempre com avaliação de proporcionalidade e necessidade.", "940695": "A aplicação da hipótese legal de “prevenção à fraude” exige a demonstração de que o uso de dados biométricos é estritamente necessário para mitigar riscos reais e relevantes de fraude, especialmente em setores como o financeiro. O controlador deve comprovar que não existem meios menos invasivos para atingir a mesma finalidade, em conformidade com o princípio da necessidade. Para compatibilizar segurança e proteção de dados, é essencial realizar avaliação de impacto (DPIA), implementar autenticação multifatorial, limitar o acesso aos dados biométricos, aplicar anonimização sempre que possível e garantir a retenção mínima. Transparência, revisão periódica das bases legais e governança robusta são salvaguardas fundamentais para equilibrar a proteção contra fraudes com a preservação das liberdades e direitos dos titulares.", "940697": "Quando o tratamento de dados biométricos se baseia no cumprimento de obrigação legal ou regulatória, o controlador deve demonstrar que a coleta está expressamente prevista em norma jurídica válida, com finalidade legítima e específica. Órgãos públicos e entidades devem limitar o tratamento ao estritamente necessário, adotando medidas de segurança compatíveis com o nível de sensibilidade dos dados. Devem ainda garantir transparência ativa, informar claramente os titulares sobre a base legal utilizada e permitir o exercício de seus direitos. Avaliações de impacto (DPIA), controles de acesso, registro das operações e políticas de governança são salvaguardas essenciais para mitigar riscos e evitar tratamentos excessivos ou desproporcionais, assegurando a autodeterminação informativa do cidadão.", "940699": "Mesmo quando os dados biométricos são utilizados para fins de pesquisa e passam por anonimização, o tratamento deve observar limites rigorosos, pois há risco real de reidentificação, especialmente em cruzamentos de grandes bases. A anonimização deve ser tecnicamente robusta, seguindo padrões atualizados e auditáveis. Os órgãos de pesquisa devem aplicar salvaguardas como o uso de ambientes controlados, acesso restrito, segregação de dados, e cláusulas éticas em protocolos de pesquisa. Além disso, devem prever mecanismos de auditoria, revisão por comitês de ética e transparência quanto às metodologias empregadas. A finalidade deve ser legítima, sem fins comerciais, e os resultados não podem permitir a identificação direta ou indireta dos titulares, conforme os princípios da LGPD e a autodeterminação informativa.", "940700": "Para que o uso de reconhecimento facial esteja em conformidade com os princípios da LGPD, é essencial justificar sua adoção com base na necessidade real e proporcionalidade, avaliando se existem meios menos invasivos para

alcançar os mesmos fins. Deve-se garantir transparência ativa, com informações claras aos titulares, e adotar medidas que evitem viés algorítmico, especialmente contra grupos vulneráveis. Salvaguardas incluem avaliações de impacto (DPIA), auditorias independentes, supervisão institucional, treinamento contínuo de operadores e políticas claras de não discriminação, além de governança algorítmica com critérios éticos e técnicos bem definidos.

","940701": "Sistemas de reconhecimento facial devem ser projetados com base no conceito de privacy by design, utilizando bancos de dados diversos e representativos para treinamento, a fim de minimizar viés e reduzir falsos positivos/negativos. Devem incluir validação contínua de acurácia, mecanismos de correção e possibilidade de revisão humana de decisões automatizadas, conforme art. 20 da LGPD. A rastreabilidade das decisões, o direito à contestação e o registro de logs são mecanismos essenciais para mitigar falhas e responsabilizar os agentes envolvidos no tratamento automatizado de dados."

","940702": "", "940704": "Para mitigar riscos em caso de violação de dados biométricos, as organizações devem adotar criptografia forte, segregação de dados, autenticação multifator, controle de acesso baseado em função, monitoramento contínuo e testes regulares de segurança. Devem implementar planos de resposta a incidentes e realizar avaliações de impacto (DPIA), especialmente quando o tratamento envolver alto risco aos direitos dos titulares. Os parâmetros mínimos incluem revisão periódica de vulnerabilidades, gestão de ciclo de vida dos dados e auditorias independentes. Como os dados biométricos são imutáveis, é essencial minimizar sua exposição e adotar tecnologias que evitem seu armazenamento centralizado, sempre que possível."

","940707": "Em serviços não essenciais, a exigência de autenticação biométrica só deve ocorrer quando estritamente necessária para garantir segurança ou prevenir fraudes, e sua recusa não pode resultar em exclusão ou discriminação indevida. É boa prática oferecer meios alternativos de autenticação, garantindo a livre escolha do titular. Quando o tratamento for baseado em consentimento, a negativa do titular pode justificar, de forma proporcional e transparente, a restrição ao uso de certas funcionalidades, desde que isso seja informado previamente e claramente, com respeito aos princípios da transparência, necessidade e não discriminação da LGPD."

","940708": "Boas práticas incluem a adoção do “privacy by design”, com minimização de dados, coleta limitada à finalidade e uso de tecnologias que armazenem dados localmente ou de forma descentralizada. Os controladores devem manter registros detalhados das operações, políticas internas de privacidade específicas para dados biométricos e realizar treinamentos contínuos com suas equipes. Devem garantir transparência sobre o uso desses dados, inclusive algoritmos envolvidos, e oferecer canais acessíveis para o exercício dos direitos dos titulares. A prevenção à discriminação deve ser reforçada com testes de viés algorítmico, avaliações éticas e revisão periódica dos impactos sociais."

","940709": "Em contextos de tratamento contínuo e massivo, como cidades inteligentes e monitoramento de multidões, os controladores devem garantir comunicação clara, visível e prévia sobre a coleta de dados biométricos, inclusive por meio de sinalização em áreas públicas. Devem disponibilizar portais de transparência, canais de atendimento e mecanismos simples para acesso, correção ou oposição ao tratamento dos dados. Além disso, devem aplicar avaliações de impacto e políticas de governança que respeitem a autodeterminação informativa, incluindo anonimização ou pseudonimização sempre que possível. A supervisão por órgãos

independentes e a revisão ética dessas iniciativas são medidas essenciais para garantir legitimidade e controle social. ", "940710": "Para garantir os direitos dos titulares, os agentes de tratamento devem adotar canais acessíveis e eficazes para solicitação de informações, acesso, correção e revogação do consentimento. Isso inclui interfaces claras, suporte contínuo e procedimentos simplificados, inclusive em sistemas automatizados. No tratamento de dados biométricos, deve haver transparência sobre os algoritmos utilizados, direito à revisão humana em decisões automatizadas (art. 20) e registros de atividades. A revogação do consentimento deve ser tão simples quanto sua concessão, com garantia de eliminação ou anonimização dos dados, conforme o art. 18 da LGPD. ", "940711": "Deve haver linguagem clara, adaptada à compreensão do público-alvo e dos responsáveis, com explicação dos riscos e finalidades. A base legal só é válida se o tratamento estiver alinhado ao melhor interesse da criança, como controle de acesso escolar ou segurança, e mesmo assim, deve ser avaliado se há meios menos invasivos. É essencial manter registros da base legal aplicada e garantir proteção técnica reforçada. ", "940712": "O tratamento de dados biométricos de crianças e adolescentes pode se fundamentar no consentimento dos responsáveis ou em obrigação legal, quando houver previsão específica. Em ambos os casos, os controladores devem garantir a participação informada dos responsáveis com comunicação transparente, linguagem acessível e consentimento verificável. Devem ainda adotar medidas como criptografia, controle rigoroso de acesso, segregação de dados e anonimização sempre que possível. Auditorias internas, treinamentos e avaliações de impacto (DPIA) são práticas recomendadas para prevenir abusos e garantir a segurança e legalidade do tratamento. ", "940714": "Na verificação de idade por biometria em plataformas digitais, é necessário observar os princípios da necessidade e do melhor interesse, limitando a coleta ao estritamente necessário para a finalidade. A prática deve ser tecnicamente proporcional, evitando coleta excessiva ou retenção desnecessária. O uso de dados deve priorizar soluções menos invasivas, como estimativas sem identificação plena, e garantir o envolvimento dos responsáveis legais. Também devem ser adotadas salvaguardas como anonimização, transparência sobre os métodos utilizados, e opção de contestação, sempre assegurando a proteção da criança contra riscos e discriminação.

Contribuinte: CLOVIS FERREIRA DE ARAUJO

Número: OP-1004090

Data: 30/07/2025 - 14:34

Resumo:

:"", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Contribuinte: LUCAS GALVAGNA

Número: OP-1004215

Data: 30/07/2025 - 16:08

Resumo: : "Nos termos da LGPD, um dado é considerado biométrico quando é uma característica física ou comportamental e deve atender aos critérios de universalidade, distintividade, permanência e mensurabilidade, sendo utilizado para identificar ou autenticar de forma individual o titular.", "940688": "Controladores devem adotar: política de privacidade clara, avisos no ponto de coleta, consentimento informado, canal de atendimento ao titular e divulgar relatórios de impacto (DPIA). Essas medidas garantem transparência no uso de dados biométricos, conforme LGPD e GDPR.", "940690": "A biometria comportamental exige cuidados específicos, como consentimento reforçado, limitação da coleta, anonimização e auditoria algorítmica. Obriga a garantir qualidade (dados exatos, atualizados) e segurança (criptografia, controle de acesso, DPIA), conforme a LGPD.", "940693": "", "940695": "Para aplicar a base legal da LGPD para prevenção à fraude com biometria, é preciso demonstrar necessidade real, realizar DPIA, adotar medidas de segurança (criptografia, descentralização), minimizar dados e garantir transparência. O uso deve ser proporcional, seguro e com alternativas, se viáveis.", "940697": "", "940699": "", "940700": "Para mitigar riscos no uso de reconhecimento facial, devem-se adotar salvaguardas técnicas (criptografia, anonimização, privacy by design), jurídicas (DPIA, base legal clara, respeito à LGPD) e institucionais (auditorias, governança de dados e capacitação contínua das equipes).", "940701": "Os sistemas devem usar bases de dados significativas e representativas estatisticamente, auditorias algorítmicas, avaliações de impacto e correção de falhas em tempo real. É essencial prever mecanismos de revisão humana (ou automatizada) e governança ética desde a concepção do sistema (by design).", "940702": "", "940704": "Medidas essenciais incluem criptografia, controle rigoroso de acesso, anonimização, auditorias regulares e planos de resposta a incidentes. Avaliações contínuas de risco (DPIA) e monitoramento ativo são obrigatórios para garantir conformidade com a LGPD e proteger dados biométricos contra vazamentos e fraudes.", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "Recomenda-se: realizar DPIA focado em crianças/adolescentes; criar canais de comunicação claros com famílias; adotar “Privacy by Design” para minimizar dados sensíveis; formar comissões escolares para conscientização e fiscalização; respeitar a autonomia da criança/adolescente.", "940712": "O referido tratamento exige consentimento conforme art. 14. Interesse legítimo não é base válida, mesmo em serviços públicos. Campanhas e materiais educativos sobre biometria, visando debate e conscientização. RIPD, ISO 24745, controle de acesso e auditorias, anonimização de dados.", "940714": ""

Contribuinte: IZABELA LEHN

Número: OP-1004793

Data: 31/07/2025 - 08:32

Resumo: "Conforme o Information Commissioner's Office, dado biométrico é aquele que: (i) se refere a característica física, fisiológica ou comportamental; (ii) é processado por técnica específica; e (iii) permite identificar unicamente a pessoa.", "940688": "Controladores devem adotar transparência ativa com linguagem clara e aviso prévio, por meio de folhetos, QR codes, vídeos explicativos, FAQs, ícones, sinalização, equipe treinada, design visual acessível, mídias digitais, avisos sonoros, demonstrações, pesquisas com usuários e canais de dúvida.", "940690": "A biometria comportamental exige salvaguardas reforçadas, por ser coletada de forma contínua e pouco perceptível. Deve ter controles mais rigorosos de contexto, acurácia e limitação de escopo, reforço da transparência, além de revisões frequentes de qualidade e segurança algorítmica.", "940693": "Para ser válido, o consentimento deve ser expresso, destacado, com linguagem clara, finalidade específica e opção real de recusa sem prejuízo. É inadequado quando há desequilíbrio de poder, como em relações laborais, serviços essenciais ou vigilância ampla, por ausência de liberdade decisória.", "940695": "É preciso demonstrar risco concreto de fraude, eficácia da biometria para mitigá-lo e ausência de meio menos intrusivo. A coleta deve ser proporcional, com segurança reforçada, acesso restrito, revisão periódica da eficácia, transparência sobre o uso, elaboração de RIPD e retenção dos dados.", "940697": "O tratamento deve restringir-se ao necessário para cumprir obrigação legal expressa, com base normativa clara, segurança robusta, controle de acessos, revisão periódica, transparência ativa, canais acessíveis ao titular, elaboração de RIPD que avalie impactos e proponha salvaguardas específicas.", "940699": "Mesmo com anonimização, o cruzamento de bases pode permitir reidentificação. É necessário demonstrar a necessidade do uso biométrico, aplicar técnicas robustas de anonimização, limitar acessos, proibir reidentificação, realizar avaliação de riscos e garantir supervisão ética contínua.", "940700": "É preciso justificar a adoção da FRT frente a alternativas menos intrusivas, limitar a coleta ao estritamente necessário, assegurar transparência, testes regulares de viés e acurácia, auditorias independentes, revisão humana e governança institucional clara com a elaboração de RIPD.", "940701": "É preciso justificar a adoção da FRT frente a alternativas menos intrusivas, limitar a coleta ao estritamente necessário, assegurar transparência, testes regulares de viés e acurácia, auditorias independentes, revisão humana e governança institucional clara com a elaboração de RIPD.", "940702": "O uso de FRTs não é recomendado em contextos de alto risco, como vigilância massiva em espaços públicos ou decisões automatizadas sensíveis. Alternativas menos intrusivas incluem câmeras tradicionais sem identificação automática, cartões de acesso em áreas controladas e autenticação multifator.", "940704": "Criptografia forte, armazenamento seguro, segmentação da base, controle de acesso e logs auditáveis são indispensáveis. Além disso, elaborar RIPD para identificar os riscos e implementar das medidas adequadas, plano de resposta a incidentes e monitoramento contínuo da operação.", "940707": "É essencial garantir alternativas à biometria, garantindo acesso às funcionalidades principais. A recusa do titular só pode afetar o uso da funcionalidade em que a biometria seja comprovadamente indispensável. A medida deve ser proporcional, não discriminatória e devidamente justificada.", "940708": "Coleta mínima e finalística, base legal adequada, RIPD, armazenamento seguro, auditorias, revisão humana em decisões automatizadas e governança clara sobre o ciclo de vida dos dados. Para evitar discriminação,

aplicar testes de viés, corrigir falhas e oferecer alternativas como senha ou token.", "940709": "Em contextos com pouca possibilidade de escolha, deve-se garantir transparência ativa com sinalização visível, campanha informativa, QR code, folheto, política de privacidade e canais acessíveis. É preciso assegurar que os titulares compreendam o tratamento e exerçam seus direitos de forma efetiva.", "940710": "Agentes devem assegurar linguagem clara sobre o uso da biometria, facilitar o acesso aos dados tratados, permitir correções e oferecer canais simples para revogação do consentimento. Em decisões automatizadas, devem garantir revisão humana e informar os critérios usados no tratamento.", "940711": "É preciso informar os responsáveis com aviso claro, linguagem acessível e canal de contato. Só é lícito com base no art. 11 da LGPD (ex.: consentimento, obrigação legal, saúde ou prevenção à fraude) e alinhado ao melhor interesse, sendo necessário, seguro e transparente.", "940712": "O tratamento é lícito nas hipóteses do art. 11 da LGPD. É preciso garantir participação informada dos responsáveis e adotar medidas como controle de acesso, segregação de dados, logs, políticas de descarte e anonimização quando possível, prevenindo abusos, vazamentos e acessos indevidos.", "940714": "A verificação etária por biometria deve ser proporcional, usar dados minimamente necessários e, sempre que possível, técnicas menos intrusivas. É essencial garantir transparência, segurança, descarte após a verificação e alinhamento ao melhor interesse, com participação informada dos responsáveis.

Contribuinte: GABRIELA RIBEIRO GOMES SOTOMAYOR

Número: OP-1004811

Data: 31/07/2025 - 08:57

Resumo: "As respostas, aqui inseridas, refletem o posicionamento da ANCORD – Associação Nacional das Corretoras e Distribuidoras de Títulos, Valores Mobiliários, Câmbio e Mercadorias. Para a caracterização de um dado como biométrico nos termos da LGPD, o critério objetivo fundamental é que ele se refira a uma característica física, fisiológica ou comportamental de uma pessoa natural identificada ou identificável, conforme disposto no art. 5º, inciso II da LGPD, de forma que seja possível tecnicamente identificar o titular associado a tais características a partir do tratamento realizado com a informação biométrica. A resposta completa foi enviada por e-mail", "940688": "As práticas de transparência ativa destacadas pelas Associadas são: (i) Apresentação clara da finalidade específica do tratamento, especialmente em hipóteses que não se baseiam no consentimento, como o uso da biometria para autenticação em sistemas eletrônicos; (ii) Indicação dos dados biométricos que serão coletados e sua respectiva finalidade; Além da definição em Políticas quanto a Informação sobre o período de retenção dos dados, bem como sobre eventuais compartilhamentos com terceiros; Identificação do controlador e disponibilização de canal de contato com o encarregado pelo tratamento de dados pessoais; Publicação de Política de Privacidade atualizada, contendo as informações acima de forma compreensível ao titular; Esclarecimento quanto às consequências da recusa do titular em fornecer o dado biométrico; Garantia de que todas essas informações estejam acessíveis antes da coleta, de forma

destacada, transparente e gratuita. A resposta completa foi enviada por e-mail. ", "940690": "É importante que tanto a biometria comportamental, quanto a tradicional, estejam submetidas aos mesmos princípios e diretrizes gerais da LGPD, assegurando previsibilidade regulatória e igualdade de tratamento no que se refere à proteção de dados pessoais. Também devem ser implementados algoritmos de aprendizado adaptativo para maior precisão dos dados coletados; medidas técnicas capazes de assegurar a integridade e evitar vieses, bem como implantação de medidas de segurança robustas para minimizar falsificação ou simulação de características biométricas “spoofing”.", "940693": "As Associadas entendem que para garantir que o consentimento seja livre, específico, destacado, informado e inequívoco, é importante que sejam adotadas medidas de forma a garantir que (i) o titular obteve de forma transparente as informações necessárias em relação ao tratamento de dado biométrico que será realizado, em especial a sua finalidade específica de tratamento (a qual deverá ser bem delimitada, evitando tratamento posterior para finalidades incompatíveis com a finalidade original); (ii) que este aceite foi de fato dado de forma inequívoca pelo titular – como através do uso de check-box para opt-in, ou por meio de Termo de Consentimento; e (iii) que tal aceite seja apresentado como opção efetiva do titular (isto é, não constitua condição singular do titular para acesso a determinado produto, serviço, ambiente ou benefício, sem efetiva necessidade para tal. A resposta completa foi enviada por e-mail. ", "940695": "A aplicação da hipótese legal de “garantia da prevenção à fraude” para o tratamento de dados biométricos exige a observância rigorosa dos princípios da necessidade, proporcionalidade e finalidade. O uso da biometria deve ser indispensável para a segurança do processo, especialmente em sistemas eletrônicos, e ineficazmente substituível por métodos menos invasivos. No contexto do setor financeiro, existe uma demanda adicional de segurança (a exemplo, combate de lavagem de dinheiro, prevenção à fraude, anticorrupção entre outros), e as instituições financeiras possuem regulamentações específicas para subsídio de prevenção a fraude. A biometria tem papel fundamental na autenticação de usuários e na mitigação de fraudes, sendo crucial para proteger tanto os titulares quanto as próprias instituições. A resposta completa foi enviada por e-mail. ", "940697": "O tratamento de dados biométricos deve estar expressamente previsto em norma legal ou regulatória vigente. Mesmo quando realizado por órgãos públicos, esse tratamento deve observar os princípios da LGPD, especialmente os da necessidade, minimização e segurança. Devem ser adotadas medidas de transparência, segurança da informação, informação clara ao titular e, quando cabível, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais. Os órgãos públicos devem manter padrões de segurança equivalentes aos do setor privado, para mitigar riscos e evitar danos em caso de incidentes de segurança. Nos casos em que a transparência total não seja possível, como em investigações criminais ou situações com restrição de sigilo, é essencial que a regulamentação assegure a legitimidade da operação e o equilíbrio com os direitos dos titulares. ", "940699": "Deve-se observar a finalidade específica do estudo, tratando apenas os dados estritamente necessários, evitando coletas excessivas. É fundamental segregar os dados de pesquisa em relação a outros bancos de dados e restringir o acesso apenas a pessoas autorizadas, adotando técnicas robustas de anonimização sempre que possível. Além disso, é imprescindível vedação expressa a reidentificação e o cruzamento de bases sem controle prévio e justificado, e sem a necessidade de um novo consentimento, exceto para uma

finalidade distinta, garantindo que os dados permaneçam em ambiente seguro e com acesso controlado, conforme previsto no art. 13 da LGPD, e sob supervisão ética e científica das atividades de pesquisa. A resposta completa foi enviada por e-mail. ", "940700": "É essencial garantir ao titular o acesso a informações claras sobre a real necessidade do uso da tecnologia, bem como a possibilidade de questionamento e correção em caso de falhas ou erros na identificação, evitando privações indevidas de acesso a produtos ou serviços. Para mitigar os riscos de discriminação ilícita ou abusiva, devem ser adotadas salvaguardas técnicas, jurídicas e institucionais, como a avaliação de impacto à proteção de dados pessoais, a adoção de mecanismos de anonimização sempre que possível, e o controle sistemático de viés nos sistemas utilizados. Também se recomenda o uso de algoritmos treinados com dados representativos de diferentes grupos sociais, incluindo diversidade de gênero, raça e etnia, a aplicação de métricas de conformidade contínuas, e a previsão de revisão humana.", "940701": "Os sistemas devem ser desenvolvidos com testes contínuos, base de dados representativa e calibração. É importante incorporar, nos casos em que os interesses e liberdade do titular são afetados pelo reconhecimento facial, mecanismos de correção, como canais acessíveis para contestação por parte dos titulares e a possibilidade de revisão por pessoa humana, especialmente nos casos de decisões automatizadas. Auditorias internas periódicas e processos de correção ágeis também devem ser implementados, a fim de assegurar a integridade do sistema e mitigar os impactos negativos decorrentes de eventuais falhas de identificação.", "940702": "Nestes casos, poderiam ser identificados contextos e situações em que o uso de tecnologias de reconhecimento facial não seja recomendado. Destacam-se alguns casos, como: situações que envolvam crianças e adolescentes; espaços de saúde; ambientes religiosos ou políticos, uma vez que, estes ambientes envolvem outros dados com características de dados sensíveis, os quais podem levar a um cenário de discriminação, conforme os critérios e finalidades específicos e atendimento aos princípios da LGPD. Como alternativa, pode ser considerados o uso de autenticação multifator, biometria por dispositivo (impressões digitais) ou token físico. Ainda, é essencial que o uso da tecnologia observe os princípios da necessidade e adequação, sendo avaliada a real sensibilidade do ambiente e os riscos envolvidos para os titulares, de modo a evitar sua exposição desnecessária e assegurar um tratamento proporcional, transparente e legítimo.", "940704": "Entre as medidas técnicas, destacam-se: a criptografia dos dados, controle rigoroso de acesso, armazenamento seguro, registro e análise de logs, auditorias periódicas, além da implementação de plano de resposta a incidentes. Já do ponto de vista administrativo, é essencial a implantação de uma Política de Segurança da Informação, treinamentos periódicos para colaboradores e terceiros, análise de riscos de prestadores de serviços antes do início das atividades, além da existência de um plano de continuidade de negócios e monitoramento diário das operações. Adicionalmente, devem ser exigidos das organizações parâmetros mínimos de avaliação de riscos contínua, incluindo a realização de Relatório de Impacto (nos termos do art. 38 da LGPD), garantindo a conformidade com os princípios da lei e a proteção integral desses dados sensíveis.", "940707": "É fundamental que a norma traga a definição de serviços não essenciais, para o uso da biometria e funcionalidades específicas de serviços não essenciais seja informado de forma clara ao titular, destacando seu caráter opcional sempre que o tratamento se basear no consentimento. Também é

recomendável que sejam oferecidas alternativas viáveis de autenticação e que se justifique tecnicamente a adoção da biometria, evitando práticas que possam configurar discriminação ilícita ou abusiva. A negativa do titular ao fornecimento de seus dados biométricos somente poderá justificar a restrição ao uso de determinadas funcionalidades quando estiver fundamentada a real necessidade da utilização da biometria para garantir maior segurança, prevenir fraudes ou assegurar a integridade da operação. Nesses casos, é essencial que o controlador informe claramente as finalidades do tratamento, as consequências da recusa e eventuais meios alternativos de acesso. A resposta completa foi enviada por e-mail

","940708": "Os controladores devem adotar boas práticas específicas como a coleta mínima de dados, com uso estritamente justificado, revisão periódica da real necessidade de manutenção dessas informações, e anonimização ou pseudonimização sempre que possível. A transparência é essencial. É igualmente importante a adoção de políticas internas claras, treinamentos regulares para equipes envolvidas no tratamento de dados sensíveis, canal de comunicação com os titulares e esteiras específicas para o atendimento de seus direitos. Além disso, devem ser proibidas práticas de reidentificação indevida e adotados mecanismos robustos de prevenção à discriminação, como a supervisão contínua de vieses algorítmicos e mecanismos que permitam contestar e corrigir eventuais erros de identificação. Dessa forma, assegura-se que o uso de dados biométricos seja feito de maneira responsável, proporcional e respeitosa aos direitos fundamentais dos titulares.", "940709": "Os controladores devem adotar medidas que assegurem transparência, segurança e respeito aos direitos dos titulares. Isso inclui: (i) Informação clara e acessível, com sinalização visível e uso de canais digitais para informar o tratamento realizado e seus objetivos; (ii) Canais para exercício de direitos, como acesso, oposição e contestação de decisões automatizadas; (iii) Revisão humana em decisões automatizadas com impacto relevante, isto é, nos casos em que as decisões tomadas de forma automatizada podem impactar de forma efetiva em liberdades e direitos individuais do titular dos dados; (iv) Limitação da coleta ao mínimo necessário, respeitando os princípios da necessidade e proporcionalidade; e (v) Segurança técnica e administrativa adequada, incluindo anonimização, controle de acesso e políticas internas. A resposta completa foi enviada por e-mail.", "940710": "Os agentes de tratamento devem garantir informações claras sobre o uso de dados biométricos por meio de Políticas de Privacidade acessíveis e canais adequados para o exercício dos direitos dos titulares, como acesso, correção e revogação do consentimento. É importante que haja mecanismos simples e eficazes para esses pedidos, com canais de atendimento de fácil acesso, e que aproveitem mecanismo já existentes como os canais de privacidade ou outros canais já administrados pelo controlador. No tratamento automatizado, deve-se garantir revisão humana, permitir contestação e assegurar a transparência sobre a lógica envolvida na decisão. A revogação do consentimento deve ser viabilizada com clareza quanto às suas consequências, inclusive quanto à necessidade ou não de manter os dados para finalidades legítimas.", "940711": "A participação informada dos pais ou responsáveis deve ser garantida por meio de transparência prévia, com informações claras, acessíveis e adequadas à compreensão do público-alvo. O tratamento de dados biométricos de crianças e adolescentes é admissível quando necessário para finalidades legítimas, como segurança ou acesso a serviços, desde que seja proporcional, justificado e limitado à coleta mínima indispensável. Deve estar alinhado ao princípio do melhor interesse da criança e do

adolescente, o que exige a adoção de salvaguardas robustas, como medidas de segurança reforçadas, restrição de acesso aos dados, avaliação de impacto e revisão periódica da real necessidade do tratamento.", "940712": "O tratamento seria admissível em casos de proteção da criança, conforme previsão na LGPD. A participação informada dos pais ou responsáveis deve ser assegurada por meio de comunicação clara e acessível, com informações transparentes sobre a finalidade do tratamento conforme determinado em Políticas de Privacidade e aos princípios da LGPD. Para evitar abusos, é necessário ter políticas claras, controle de acesso, anonimização, quando possível e auditorias periódicas para prevenir abusos e vazamentos. Essas medidas devem ser orientadas pelo princípio do melhor interesse da criança e do adolescente.", "940714": "A verificação ou estimação de idade por meio de dados biométricos só deve ser adotada quando estritamente necessária, observando o princípio da necessidade e do melhor interesse da criança ou do adolescente. Sempre que possível, devem ser priorizados métodos menos invasivos, como checagem documental, autodeclaração com responsabilização dos pais ou responsáveis, ou validação por terceiros confiáveis. Caso o uso da biometria se justifique, é fundamental assegurar a transparência com os pais ou responsáveis, adotar medidas técnicas robustas de proteção dos dados, garantir a mínima retenção das informações, anonimização quando aplicável, impossibilidade de reutilização dos dados para outras finalidades, bem como supervisão contínua do tratamento.

Contribuinte: AMANDA DE OLIVEIRA DA SILVA

Número: OP-1004895

Data: 31/07/2025 - 10:40

Resumo: "Embora a LGPD não defina expressamente "dado biométrico", sua interpretação deve considerar a definição do GDPR (art. 4.14) e as diretrizes do EDPB. Assim, três critérios cumulativos devem ser observados: (i) o dado deve derivar de características físicas, fisiológicas ou comportamentais de uma pessoa natural; (ii) deve ser gerado por meio de um tratamento técnico específico (ex: algoritmos, sensores); e (iii) deve ter como finalidade permitir ou confirmar a identificação única da pessoa. Esses critérios visam evitar o enquadramento indiscriminado de qualquer dado corporal como biométrico, e orientar a regulação para os tratamentos de maior risco à privacidade e demais direitos fundamentais. Além disso nossa orientação vai no sentido de serem considerados dados sensíveis os dados de crianças e adolescentes.", "940688": "A LGPD exige transparência (art. 6º, VI), mas, no caso de dados biométricos, isso implica ir além de políticas genéricas. É necessário adotar práticas de transparência ativa e contextualizada, como: sinalização visível nos espaços de coleta, uso de avisos em camadas (layered notice), com explicação clara e acessível sobre finalidade, base legal, duração do tratamento e direitos dos titulares. A CNIL recomenda pictogramas visuais com links ou QR Codes para mais informações. O titular deve ser informado antes da coleta, especialmente em ambientes públicos ou de difícil contestação bem como a questão do consentimento deveria ser revista em casos de relações jurídicas assimétricas onde se presume a não

comprovação dos requisitos de validade do consentimento além da fragilidade de tal base legal diante das críticas da doutrina (fadiga e fiação do consentimento) na prática, e mesmo diante das insuficientes medidas de mitigação como minimização de dados e anonimização.", "940690": "A biometria comportamental (voz, digitacão, modo de andar) apresenta riscos acrescidos por ser invisível, contínua e inferencial. Deve receber o mesmo nível de proteção que a biometria física, aplicando-se integralmente o art. 11 da LGPD. Entretanto, devido ao seu caráter preditivo e à imprecisão técnica, é necessário reforçar os princípios da qualidade dos dados (art. 6º, V) e da segurança (art. 6º, VII). Isso inclui avaliação técnica da acurácia, adoção de mecanismos robustos de revisão e contestação de decisões automatizadas e controle rigoroso sobre inferências que possam revelar estado emocional, saúde ou comportamento. Além disso merecem atenção o reconhecimento dos neurodireitos evitando ainda mais acesso e tratamento de dados ainda mais sensíveis falando-se em neurocapitalismo. No mínimo deveria ser exigida a elaboração prévia de avaliação de impacto algorítmico por equipe independente, multietnica e multidisciplinar, que entenda de direitos fundamentais", "940693": "o consentimento nunca na prática alcançaria tais requisitos ou seria muito difícil a começar pelo grau de pensamento crítico, conscientização e educação do país em termos gerais, que influem em tais requisitos. A maior parte há assimetria informacional, ausência de transparência não só quanto ao algoritmo em si e tomada de decisão mas quanto ao compliance com insuficiência apresentação de documentos pelas empresas. Pior ainda em situações de relações assimétricas - o que não ocorre em relações assimétricas (emprego, acesso a serviços públicos, educação). A AEPD e o EDPB rejeitam o consentimento em contextos onde há dependência ou coerção implícita. No Brasil, seu uso deve ser limitado a situações onde exista alternativa viável e equivalente ao titular. Fora disso, o consentimento se torna meramente formal e inválido. Fora isso os data brokers vendem e distribuem os dados para outras finalidades, sem haver informação adequada disso e portanto, sem consentimento novamente", "940695": "A “prevenção à fraude” não pode ser invocada genericamente. É necessário demonstrar que a biometria é indispensável, não existindo meios menos intrusivos ou seja aplicando-se de fato o princípio da proporcionalidade e seus 3 subprincípios o que é desvalorizado e mal feito no Brasil, já que se ignora isso e quem elabora quando elabora não entende de teoria dos direitos fundamentais e de proporcionalidade, muitas vezes considerando como sinônimo de razoabilidade o que é um equívoco. O controlador deve elaborar um Relatório de Impacto à Proteção de Dados (RIPD), e ou AIA demonstrando a avaliação de riscos, proporcionalidade e necessidade do uso e de forma prévia e com requisitos específicos a serem observados e de preferência por equipe independente. Salvaguardas incluem: uso de templates criptografados, armazenamento local (no dispositivo do titular), auditorias periódicas, e opções alternativas para titulares que não possam ou não queiram fornecer dados biométricos. ", "940697": "A mera obrigação genérica (como controle de ponto) não justifica seu uso. Além disso, mesmo nos casos de obrigação legal válida, devem ser implementadas medidas técnicas e organizacionais adequadas, como: minimização da coleta, armazenamento seguro e limitado, RIPD obrigatório, e transparência ativa com a população afetada, incluindo consultas públicas quando em espaços públicos. O mais importante: obrigatoriedade de elaboração prévia de

Avaliação de impacto algorítmico e ou de relatório de impacto de proteção de dados por equipe independente.", "940699": "Mesmo com anonimização, há riscos concretos de reidentificação, especialmente em estudos com grandes bases cruzadas. Por isso, a pesquisa deve seguir os princípios da minimização, segurança e finalidade, com justificativa clara para o uso de dados biométricos. São necessárias medidas como: anonimização forte e irreversível (com testes de reidentificação), uso de dados sintéticos, revisão ética por comitês independentes, e RIPD prévio. A proteção dos titulares deve ser ex ante e contínua, com controle institucional sobre o uso secundário dos dados e vedação de reutilização indevida. Focar na prevenção de danos e na proatividade da empresa, ao não passar os custos ao usuário/titular ", "940700": "Para garantir o respeito aos princípios da LGPD e evitar discriminação, o uso de reconhecimento facial deve ser justificado por uma demanda urgente, ser proporcional e efetivo, e ter uma finalidade específica e determinada. É crucial avaliar se há meios menos invasivos para atingir o objetivo pretendido. As justificativas para o uso em locais públicos devem ser revistas anualmente. As salvaguardas jurídicas e institucionais incluem a criação de estruturas administrativas de supervisão com cadeias de responsabilidade claras sobre o uso e acesso aos dados. A tecnologia deve envolver intervenção humana. É essencial adotar uma abordagem com foco no "fundamental rights by design", realizar Avaliações de Impacto (AIA) com atenção a direitos fundamentais, especialmente de populações vulneráveis (ver revista ethikai.org sobre direitos fundamentais by design e avaliação de impacto algorítmico independente)", "940701": "A documentação indica que os sistemas de reconhecimento facial apresentam altos índices de erros de identificação, como falsos positivos, e vieses que discriminam com base em raça, classe e gênero. Para minimizar essas falhas, os sistemas devem ser projetados sob o paradigma do "fundamental rights by design", que busca garantir a proteção de todos os direitos fundamentais desde a concepção. O documento menciona que a regulamentação na União Europeia exige que as avaliações de conformidade sejam realizadas por organismos notificados independentes, garantindo competência e ausência de conflitos de interesse. Além disso, deve-se considerar o AI ACT, que proíbe o uso em espaço público com exceções rigidamente definidas e reguladas, exigindo autorização judicial prévia, limitando tempo, localização e dados. A intervenção humana é um mecanismo essencial de correção, pois os sistemas devem funcionar sob supervisão e controle de um agente humano.", "940702": "O Tribunal de Apelação de Londres considerou ilegal o uso por falta de supervisão adequada e critérios claros. Na França, foi proibido em escolas por ser possível atingir a mesma finalidade com meios menos invasivos. O parecer sugere que a tecnologia é problemática em áreas como reincidência criminal, desempenho no trabalho e policiamento preditivo devido aos altos riscos de vieses e erros. O uso de reconhecimento facial só deve ocorrer quando a finalidade não puder ser alcançada por outros meios, sugerindo que a busca por soluções menos invasivas é uma alternativa em si. A privacidade é uma das condições para a livre expressão do indivíduo, e a vigilância em massa é um sintoma de desrespeito aos princípios democráticos.", "940704": "As medidas de segurança essenciais para mitigar os riscos de violação de dados biométricos devem ir além das proteções básicas da LGPD. A LGPD não possui uma regulamentação específica sobre o tema, diferente da

norma uruguaia que exige avaliaç,ão de impacto. As organizaç,ões devem adotar uma cultura de direitos e responsabilidade preventiva (accountability). Para^metros mi^nimos de avaliaç,ão de riscos e monitoramento incluem a elaboraç,ão obrigató^ria e pre^via de um Relatório de Impacto a^ Protec,ão de Dados (DPIA) e Avaliaç,ão de Legi^timo Interesse (LIA). A qualidade dos dados, documentaç,ão, rastreabilidade, transpare^ncia e supervisa~o humana sa~o requisitos essenciais.; a avaliaç,ão de impacto deve ser feita por uma estrutura institucional independente, como uma age^ncia governamental, e na~o pelo pro^prio fornecedor.", "940707": "Para evitar discriminac,ão, boas pra^ticas devem incluir a oferta de alternativas para quem na~o quiser utilizar a biometria, tanto no setor pu^blico quanto no privado. O consentimento deve ser livre, ou seja, na~o pode ser uma imposic,ão para o uso de um servic,õ ou acesso. A recusa do titular em fornecer dados biome^tricos pode justificar a restric,ão de funcionalidades apenas se essa limitac,ão for proporcional e transparente, e se for devidamente informada ao titular. ex o caso de um empregador que exige biometria para acesso, onde o trabalhador na~o pode recusar sem consequ^ncias, mostrando a assimetria de poder e a falta de liberdade real de recusa.", "940708": "As boas pra^ticas para uma protec,ão eficaz incluem a adoc,ão de uma lo^gica preventiva e transparente, ale^m de programas de governanc,a que incorporam valores da LGPD. Os controladores devem realizar avaliaç,ões constantes de proporcionalidade e riscos, e elaborar um Relatório de Impacto a^ Protec,ão de Dados (DPIA). Para evitar discriminac,ão, e^ fundamental que a LGPD e a ANPD elaborem diretrizes claras sobre responsabilidades, seguranc,a da informac,ão, gesta~o de riscos e mecanismos de resposta a incidentes. A transpare^ncia pode ser garantida com a obrigatoriedade de informac,ão pre^via em formato de aviso aos consumidores, como no caso da loja Hering, onde uma decisã~o administrativa considerou abusiva a falta de consentimento e informac,ão clara.", "940709": "Para assegurar a autodeterminac,ão informativa em contextos de tratamento massivo, e^ vital a exige^ncia de Avaliaç,ões de Impacto pre^vias, que garantam transpare^ncia siste^mica e reforcem a responsabilidade do operador de dados. Os titulares devem ser informados sobre as finalidades, bases legais e riscos, e ter direitos de acesso, correc,ão e oposic,ão garantidos. Em locais pu^blicos, na~o se pode presumir o consentimento da comunidade. Os indivi^duos devem ser avisados sobre o emprego de qualquer tecnologia de reconhecimento facial. Destaca-se a importa^ncia de um "fundamental rights by design" e de uma arquitetura normativa que mitigue riscos estruturais a^ autodeterminac,ão informacional, a^ na~o discriminac,ão e a outras protec,ões humanas. O monitoramento em massa e^ considerado um desrespeito aos princí^pios democrá^ticos.", "940710": "O respeito aos direitos dos titulares no tratamento biome^trico — notadamente o direito a^ informac,ão clara (art. 6o, VI; art. 9o), ao acesso (art. 18, II), a^ correc,ão (art. 18, III) e a^ revogac,ão do consentimento (art. 18, §5o) — exige, primeiro, uma governanc,a de dados responsiva e centrada no titular. Isso implica a adoc,ão de interfaces acessi^veis para que o titular exerc,a seus direitos de forma descomplicada e eficaz, inclusive nos casos de decisõ~es automatizadas (art. 20). A revogac,ão do consentimento deve ser ta~o simples quanto sua concessã~o, respeitando o princí^pio da autodeterminac,ão informativa. Em sistemas automatizados de reconhecimento facial, deve-se garantir o direito a^ revisã~o humana significativa, com canais de contestac,ão e reversã~o eficaz. Ale^m disso, exige-se auditoria conti^nuada, transpare^ncia algorí^tmica e documentaç,ão do

tratamento via RIPD (Relatório de Impacto à Protecção de Dados), conforme melhores práticas internacionais..", "940711": "Nos termos do art. 14 da LGPD, o tratamento de dados pessoais de crianças e adolescentes deve estar fundamentado no princípio do melhor interesse e condicionado ao consentimento específico e em destaque de pelo menos um dos pais ou responsável legal. A simples obtenção de autorização não basta: ela deve ser precedida por informação compreensível, clara e acessível, considerando o nível de compreensão dos pais e do público infantojuvenil. O uso de avisos visuais simplificados, além de documentos explicativos acessíveis em linguagem adequada, é fundamental. O tratamento biométrico em escolas ou espaços recreativos apenas pode se justificar quando imprescindível (por exemplo, para segurança em transporte escolar), e mesmo nesses casos deve ser precedido de avaliação de impacto, oferecendo meios alternativos de controle de acesso para aqueles que não desejarem consentir. ", "940712": "As hipóteses legais possíveis são: (i) consentimento específico do responsável legal (art. 14); (ii) protecção da vida ou incolumidade física (art. 11, II, e); ou (iii) cumprimento de obrigação legal ou regulatória (art. 11, II, a), desde que a norma autorize explicitamente o uso de biometria. Em qualquer caso, o princípio da necessidade exige que o tratamento seja estritamente indispensável para o fim alegado, e que não existam meios menos invasivos. A protecção contra abusos exige medidas técnicas e organizacionais robustas, como: • Criptografia e segmentação dos templates biométricos; • Controle estrito de acesso e registro de logs; • Auditorias periódicas independentes; • Política de retenção mínima e eliminação automática; • Adoção de Privacy Enhancing Technologies (PETs) e governança por design ("by design and by default") especialmente ajustadas a grupos vulneráveis. Avaliação de impacto algorítmico prévia e com foco em direitos fundamentais", "940714": "A verificação de idade por meio de biometria em plataformas digitais (ex: jogos online, redes sociais, streaming) deve observar o princípio da minimização e da necessidade (art. 6º, III) e o melhor interesse da criança ou adolescente (art. 14, §1º). A biometria não deve ser a solução padrão; deve ser considerada último recurso, após esgotadas outras formas de verificação, como declarações dos responsáveis ou mecanismos técnicos de validação não biométrica. Quando inevitável, o tratamento deve ser precedido de: • Avaliação de impacto (RIPD) com análise específica de riscos à infância; • Consentimento dos responsáveis com explicações detalhadas sobre os riscos da coleta biométrica; • Garantias de que os dados não serão reutilizados para outras finalidades;

Contribuinte: PAOLA CANTARINI QUEIROLO

Número: OP-1005024

Data: 31/07/2025 - 12:22

Resumo:

:"", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "A coleta e o tratamento de dados biométricos de crianças e adolescentes devem ser considerados como último recurso, especialmente quando associados a decisões

automatizadas. Crianças são titulares plenos dos direitos da LGPD (art. 18) e gozam de proteção reforçada (art. 14), que exige transparência ativa, qualificada e acessível, conforme §2ª e §6º. Produtos e sistemas devem adotar o “direito por design”, com interfaces adequadas à autonomia progressiva. Termos genéricos e práticas opacas são incompatíveis com o dever de informação. A experiência internacional mostra que ferramentas como o Playful by Design ajudam a equilibrar metas comerciais e direitos da criança. Por isso, seria importante consolidar diretrizes específicas sobre o tema, conforme previsto na agenda regulatória e o Mapa de Temas Prioritários da ANPD. O detalhamento completo encontra-se no documento enviado por e-mail.", "940711": "O tratamento de dados biométricos de crianças e adolescentes só deve ocorrer em casos excepcionais, com base em avaliação robusta de necessidade, proporcionalidade e no melhor interesse da criança (art. 14 da LGPD). Isso exige a realização de avaliações de impacto específicas (CRIAs) e a priorização de meios menos invasivos. A coleta biométrica em escolas, por exemplo, não pode ser justificada por ganhos operacionais, como controle de frequência, sobretudo diante de alternativas adequadas. A Resolução CONANDA nº 245/2024 reforça que tais práticas devem respeitar a privacidade e garantir o direito à informação e à oposição, conforme o grau de maturidade da criança. O consentimento parental, por si só, não basta. Tecnologias biométricas devem ser vetadas quando os riscos superam os benefícios. O detalhamento completo da resposta está no documento encaminhado por e-mail.", "940712": "O tratamento de dados biométricos de crianças e adolescentes exige mais do que a indicação formal de base legal: deve estar ancorado no melhor interesse do titular, com avaliação prévia de impacto e salvaguardas robustas. A LGPD impõe um padrão mais elevado para dados sensíveis e titulares vulneráveis. Ainda que o consentimento parental (art. 14, §1º) seja juridicamente possível, ele não é suficiente sem transparência, linguagem acessível e real compreensão dos riscos. As hipóteses legais mais viáveis incluem: prevenção à fraude (art. 11, II, “g”) e proteção da vida (art. 11, II, “e”). Todas demandam demonstração de necessidade e proporcionalidade. É essencial garantir participação informada dos responsáveis (art. 14, §6º), escuta ativa da criança (Res. CONANDA nº 245/2024), e revisão contínua da tecnologia. O uso de biometria por conveniência ou utilitarismo é incompatível com a LGPD e a doutrina da proteção integral. O detalhamento completo da resposta está no documento por email", "940714": "A verificação ou estimação de idade por biometria só deve ser adotada como último recurso, após avaliação de impacto nos direitos da criança (CRIA) e demonstração de necessidade e proporcionalidade (art. 14, § 4 LGPD). Métodos como análise facial, digitação ou fala implicam riscos elevados à privacidade, acurácia e dignidade, especialmente para crianças negras, neuroatípicas ou com deficiências. É essencial distinguir verificação (alto grau de certeza) de estimação etária (probabilística), priorizando soluções menos invasivas. Salvaguardas incluem: uso limitado e não retentivo de dados; transparência técnica; auditorias independentes; e participação infantojuvenil no design (Res. CONANDA nº 245/2024). Iniciativas como a EU Age Verification Solution demonstram a viabilidade de sistemas interoperáveis sem biometria. Exigir dados biométricos como condição de acesso viola frontalmente a LGPD. O detalhamento completo da resposta está no documento encaminhado por e-mail.

Contribuinte: Júlia Fernandes de Mendonça

Número: OP-1005080

Data: 31/07/2025 - 13:21

Resumo: "O dado biométrico deve resultar de um tratamento técnico que permita a identificação única e inequívoca de uma pessoa natural. Como por exemplo, impressões digitais, rosto, voz, íris ou qualquer outro elemento capaz de identificar um atributo humano. A identificação deve ser única, confiável e baseada em características físicas, fisiológicas ou comportamentais.", "940688": "Divulgar de forma clara a finalidade, base legal, prazo de retenção, direitos dos titulares, canais de contato e medidas de segurança por meio de avisos de privacidade, sinalização visível e comunicação acessível. Práticas recomendadas incluem avisos de privacidade detalhados, sinalização visível nos ambientes físicos (como QR codes em lojas), comunicação digital acessível e treinamentos para colaboradores. De fato, hoje o arcabouço normativo nacional não fornece elementos suficientes em que possamos nos basear para tratar tais dados em um contexto comercial. Assim, é necessário esclarecer os casos de uso, bem como a base legal que deve ser aplicada a cada um deles. Por exemplo, no caso de lojas, podemos considerar a segurança privada como um interesse legítimo para utilizar uma tecnologia baseada em reconhecimento facial, tendo em vista as ameaças à segurança que enfrentamos diariamente?", "940690": "Devemos ter cuidado com o fato de que, na maioria das vezes, essa análise depende de algoritmos, ou seja, de um sistema de inteligência artificial. Para esses casos, como não dispomos de um marco nacional sobre o uso responsável e justo da IA, devemos esclarecer em quais situações esse tratamento é permitido e em quais não é (ou seja, fornecer diretrizes). Além disso, deve seguir as mesmas salvaguardas da biometria tradicional, com atenção adicional à transparência, qualidade dos dados e ao risco de perfis injustos (exemplo: riscos de discriminação).", "940693": "Hoje, consideramos que o consentimento é inadequado para casos de uso como segurança no varejo. Contudo, o legítimo interesse ou a prevenção à fraude podem oferecer uma base legal proporcional e sustentável, desde que existam diretrizes apropriadas para implementar esse tipo de tecnologia, garantindo o respeito aos direitos dos titulares e a aplicação de todas as salvaguardas necessárias. Em outras palavras, isso significa que deve estar claramente documentado.", "940695": "A prevenção à fraude justifica o uso proporcional de biometria, com limitação de finalidade, avaliação de impacto à proteção de dados (DPIA), forte segurança e governança. No varejo, por exemplo, permite a mitigação de furtos por meio do reconhecimento facial e o engajamento discreto da equipe, sem exposição ou viés. Portanto, os critérios a serem implementados incluem a limitação a casos de uso documentados, diretrizes claras para implementação e a definição da base legal adequada para o tratamento.", "940697": "É fundamental que o controlador defina claramente a obrigação legal ou regulatória que fundamenta o tratamento de dados biométricos, assegurando que o uso seja limitado ao estritamente necessário para o cumprimento dessa obrigação. Devem ser implementadas medidas de segurança reforçadas para proteger os dados, incluindo controles técnicos e administrativos adequados. Além disso, todas as decisões relativas ao tratamento devem ser devidamente documentadas, e avaliações de impacto à proteção de dados (DPIAs) devem ser conduzidas regularmente para identificar e mitigar riscos potenciais. A

transparência em relação ao tratamento e a responsabilização do controlador são essenciais, especialmente no caso de entidades públicas, garantindo o respeito aos direitos dos titulares e a conformidade com a LGPD.", "940699": "O tratamento de dados biométricos para pesquisa deve ser limitado ao estritamente necessário, adotando forte anonimização e garantindo a impossibilidade de reidentificação. É essencial a segregação dos dados e o descarte após o uso. Devem ser realizadas avaliações rigorosas de risco, com controles de acesso efetivos para assegurar a proporcionalidade e a ética na pesquisa, como em estudos médicos. Além disso, o cruzamento de bases de dados exige supervisão ética contínua e protocolos de segurança reforçados. Transparência, consentimento informado (quando aplicável) e bases legais adequadas são fundamentais para proteger os direitos dos titulares e garantir a conformidade com a LGPD.", "940700": "As organizações devem estabelecer procedimentos operacionais claros e promover treinamento abrangente para todos os colaboradores envolvidos. Devem ser realizadas auditorias regulares e revisões periódicas dos sistemas para avaliar desempenho e identificar possíveis vieses ou erros. A transparência deve ser proativa, incluindo comunicação clara aos titulares sobre o uso, finalidades e direitos, com canais acessíveis para o exercício desses direitos. O uso dessas tecnologias deve ser estritamente preventivo e não discriminatório, respaldado por salvaguardas institucionais robustas, como frameworks de governança, mecanismos de responsabilização e controles técnicos para evitar uso indevido, vazamentos de dados e exposição indevida de grupos vulneráveis.", "940701": "Realizar provas de conceito, testes de precisão e manter registros auditáveis e supervisão humana constante. Monitorar continuamente os sistemas para identificar e corrigir rapidamente falhas, minimizando falsos positivos e negativos. Implementar governança robusta e critérios técnicos rigorosos para garantir a confiabilidade do sistema. Além disso, é fundamental informar os titulares dos dados e manter total transparência sobre o uso dessas tecnologias.", "940702": "O uso de tecnologias de reconhecimento facial deve ser evitado em contextos onde não haja propósito claro ou justificativa proporcional, para prevenir vigilância excessiva e proteger a privacidade dos titulares dos dados. Alternativas eficazes incluem autenticação multifatorial, tokens físicos, reconhecimento por voz ou padrões comportamentais, que oferecem segurança com menor impacto sobre a proteção de dados pessoais.", "940704": "É indispensável adotar criptografia robusta, controle de acessos, anonimização, monitoramento contínuo e resposta eficaz a incidentes. Avaliações frequentes de riscos e auditorias também são fundamentais, além de políticas internas específicas e treinamentos regulares para os colaboradores. É essencial estabelecer contratos claros com terceiros, garantindo que esses parceiros estejam submetidos às mesmas obrigações legais e padrões de segurança. O uso de ferramentas automatizadas de detecção de anomalias e registros auditáveis também ajuda na identificação precoce de falhas ou acessos indevidos. Finalmente, deve-se garantir que todos os procedimentos estejam documentados, revistos periodicamente e alinhados à criticidade dos dados biométricos, promovendo uma cultura organizacional voltada à prevenção e à proteção integral dos titulares.", "940707": "Para evitar discriminação, é essencial garantir que a autenticação biométrica em serviços não essenciais seja sempre opcional, oferecendo meios alternativos de acesso, como senhas ou tokens. O consentimento deve ser livre, informado e revogável, sem penalizar ou limitar o titular de forma desproporcional. A negativa ao fornecimento dos dados

biométricos só pode justificar restrição quando a funcionalidade for tecnicamente dependente do dado e houver justificativa clara, documentada e transparente sobre essa dependência. Devem ser realizados testes de proporcionalidade e avaliações de impacto (DPIA), assegurando que o tratamento não seja excessivo e que não afete de forma desigual grupos vulneráveis. Do ponto de vista técnico, é necessário testar antes da implementação para verificar os resultados e garantir que o treinamento do algoritmo de reconhecimento facial tenha sido feito com conjuntos de dados precisos e diversos.", "940708": "Boas práticas para proteção eficaz no tratamento de dados biométricos incluem a implementação de governança robusta com políticas claras e responsabilidades definidas. Devem ser conduzidas avaliações de impacto à proteção de dados (DPIAs) para identificar e mitigar riscos, além de aplicar anonimização sempre que possível para minimizar o uso de dados sensíveis. É fundamental garantir canais acessíveis para que titulares exerçam seus direitos e implementar políticas rigorosas contra discriminação ilícita e abusiva. Controles de acesso restrito aos dados, monitoramento contínuo e auditorias regulares ajudam a prevenir abusos e vazamentos. A transparência com os titulares é vital, fornecendo informações claras sobre finalidades, usos, bases legais e medidas de proteção adotadas. A responsabilização dos agentes de tratamento deve ser contínua, assegurando conformidade com a LGPD e proteção integral dos dados biométricos.", "940709": "Para assegurar o respeito à autodeterminação informativa em contextos de tratamento contínuo e massivo de dados biométricos, como em cidades inteligentes, monitoramento de grandes multidões em estádios e espaços públicos, os controladores devem implementar sinalização visível e clara informando sobre a coleta e uso dos dados. Devem disponibilizar canais acessíveis para que os titulares possam obter informações detalhadas e exercer seus direitos com facilidade. É essencial realizar avaliações de risco contínuas para identificar e mitigar possíveis impactos. A comunicação deve ser proativa e contínua, com campanhas de educação digital que conscientizem os titulares sobre seus direitos e o uso dos dados. Além disso, devem ser implantados mecanismos técnicos e administrativos que garantam o controle efetivo dos titulares sobre seus dados, mesmo em situações de difícil transparência.", "940710": "Os agentes de tratamento devem garantir canais acessíveis e comunicação clara para que os titulares possam exercer seus direitos de acesso, correção e revogação do consentimento. Devem implementar processos eficientes para retificação de dados e revisão humana em decisões automatizadas. É fundamental assegurar controle efetivo dos titulares sobre seus dados, garantindo que o direito de não ser submetido a decisões exclusivamente automatizadas seja respeitado e possa ser exercido plenamente.", "940711": "O tratamento de dados biométricos de crianças e adolescentes deve ser evitado sempre que possível, sendo fundamental que a autoridade defina com precisão os casos muito restritos em que esse tratamento é permitido. Caso a coleta ocorra de forma inadvertida, devem ser implementados mecanismos para identificar e eliminar esses dados rapidamente. É imprescindível utilizar bases legais adequadas, respeitar o princípio do melhor interesse da criança e do adolescente, e aplicar níveis elevados de transparência e segurança para garantir a proteção integral desses titulares.", "940712": "Devem existir mecanismos eficazes para garantir o consentimento dos pais ou responsáveis, ou uma base legal clara para o tratamento. É fundamental assegurar comunicação acessível, segurança técnica robusta, controle de acesso rigoroso, auditorias constantes e prevenção contra

vazamentos ou abusos. No entanto, esse tipo de tratamento deve ser evitado sempre que possível. No contexto de lojas, por exemplo, a coleta de dados biométricos de crianças, mesmo que acompanhadas, deve ser cuidadosamente avaliada quanto à sua necessidade e obrigatoriedade.", "940714": "A regra básica deve ser limitar a coleta ao mínimo necessário, como em contextos médicos, garantindo o consentimento dos pais ou responsáveis e máxima transparência. É fundamental aplicar medidas de segurança rigorosas, permitir a correção e exclusão dos dados, alinhando-se ao princípio do melhor interesse e evitando o tratamento excessivo.

Contribuinte: MARIANA ISABELE DE SOUSA MEDEIRO

Número: OP-1005093

Data: 31/07/2025 - 13:50

Resumo:

: "", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": "

Contribuinte: CARLA CRISTINA VRECHE

Número: OP-1005104

Data: 31/07/2025 - 14:06

Resumo: : "", "940688": "Devem ser adotadas práticas de transparência ativa, como: disponibilizar política de privacidade em linguagem clara e acessível; informar previamente a finalidade da coleta; obter consentimento específico e destacado; oferecer canais para exercício dos direitos dos titulares; divulgar avisos visíveis no ponto de coleta; e garantir fácil acesso às informações sobre o tratamento. No que diz respeito ao uso de tecnologia de reconhecimento facial na segurança pública, por exemplo, é fundamental que a população seja avisada que em determinada área física há uso de TRF em tempo real, podendo o público evitar a região, caso não deseje que seus dados biométricos sejam tratados. Essa sinalização deve permitir que a pessoa possa definir com antecipação sua passagem pela área - portanto, não pode acontecer muito perto do local e nem apenas pelas redes sociais - e conter, expressamente, a finalidade da coleta e os informar os limites de compartilhamento entre setor público e privado.", "940690": "As preocupações com relação à biometria tradicional devem ser estendidas à comportamental, a qual deve ainda demandar obrigações específicas de avaliação de impacto e governança algorítmica, dada sua complexidade e potencial invasivo. Esses dados são, frequentemente, coletados de forma contínua e passiva, o que reforça a demanda por transparência e obtenção de consentimento. Além disso, a análise com base em comportamento, especialmente com uso de inteligência artificial, influi na perfilização de indivíduos, podendo levar a decisões discriminatórias e/ou enviesadas que

impactam negativamente direitos. Cabe destacar, nesse sentido, e na área da segurança, o edital de compra de tecnologia de reconhecimento facial da Prefeitura de São Paulo, que, em 2020, usou o termo “vadiagem” no contexto da análise de comportamento de pessoas em áreas públicas, com o objetivo de identificar “comportamentos suspeitos”, apontando riscos de criminalização de populações historicamente vulneráveis.”, "940693": "Qualquer base legal para o uso da tecnologia de reconhecimento facial por uma autoridade deve incluir um dever intransferível, por sua parte, de executar uma série de avaliações de impacto no que tange a todos os direitos fundamentais, antes da implantação de qualquer nova forma de uso da TRF. Tais avaliações devem incluir, entre outros, o exame do impacto sobre os direitos fundamentais e da necessidade absoluta e da proporcionalidade desse uso. Além disso, devem ser adotadas práticas de transparência ativa, sendo fundamental, por exemplo, que a população seja avisada que em determinada área física há uso de TRF em tempo real, podendo o público evitar a região, caso não deseje que seus dados biométricos sejam tratados. Essa sinalização deve permitir que a pessoa possa definir com antecipação sua passagem pela área - e conter, expressamente, a finalidade da coleta e os informar os limites de compartilhamento entre setor público e privado.”, "940695": "", "940697": "Nenhuma nova forma de uso de tecnologia de reconhecimento facial deve ser implementada se uma avaliação de impacto determinar que o sistema e a demografia do conjunto de dados de treinamento do algoritmo dele produzem, direta ou indiretamente, resultados enviesados contra qualquer característica protegida – incluindo raça, gênero ou idade – em um ambiente operacional. Uma autoridade de aplicação da lei não deve implantar nenhuma nova tecnologia se ela não for estritamente necessária ou proporcional. Essas avaliações devem ser feitas anualmente para cada tecnologia de reconhecimento implementada. Se um sistema de TRF for reprovado por qualquer uma dessas avaliações, ele deve ser desativado. Na área da segurança pública, e considerando a previsão do Art. 4, III, da LGPD, mas também da Nota Técnica nº 175/2023/CGF/ANPD, destaca-se compliance com privacidade, acesso restrito aos dados e registro detalhado de todas as atividades por meio de logs, o que permite a realização de auditorias.”, "940699": "", "940700": "O uso de TRF na segurança pública no Brasil exige atenção rigorosa. O reconhecimento em tempo real deve ser banido e a análise retrospectiva de imagens pode ser uma possibilidade desde que respeitadas as seguintes condições: O tratamento de dados deve estar fundamentado em hipótese prevista em lei, assim como o uso de tais ferramentas deve contar com autorização e base jurídica específica; a avaliação de impacto sobre direitos fundamentais deve ser compulsória e disponibilizada ao público antes da implementação da tecnologia; Os titulares devem ser informados sobre como os seus dados serão utilizados, autoridades devem documentar cada busca feita por meio dessa ferramenta e responsáveis pela apresentação de relatórios anuais sobre casos de identificação incorreta; Devem ser implementadas medidas de controle e registros de acesso, procedimentos de auditoria e previsão de revisão humana de decisão automatizada; Canais de denúncia sobre abusos ou erros devem ser fortalecidos.”, "940701": "Os sistemas de reconhecimento facial devem ser projetados com base em medidas de “privacidade desde a concepção e por padrão”, em atendimento ao previsto no art. 46º, § 2º da LGPD, garantindo que em todo processo sejam consideradas a eficácia, confiabilidade e mitigação de riscos. Por conta dos riscos profundos e estruturais que representam a direitos fundamentais, tecnologias

de reconhecimento facial em tempo real devem ser proibidas, já que envolvem a vigilância constante e indiscriminada de pessoas, violam o princípio da presunção de inocência e representam uma impossibilidade prática de garantir os princípios da proporcionalidade e necessidade. Além disso, o uso de TRF para análise retrospectiva na segurança pública, e com relação a mecanismos de correção, deve considerar a obrigatoriedade de revisão humana em decisões sensíveis e um resultado de reconhecimento, por si só, não deve ser tido como base suficiente para interrogatório, prisão ou detenção.", "940702": "Tecnologias de reconhecimento facial em tempo real, especialmente quando utilizadas em espaços públicos ou semi abertos apresentam riscos profundos e devem ser banidas. Essa ferramenta envolve vigilância constante e indiscriminada de todas as pessoas sem consentimento ou suspeita prévia. Além disso, o monitoramento contínuo é incompatível com o direito à privacidade, protegido constitucionalmente. Um ponto fundamental a considerar é que, essas ferramentas possuem vieses raciais e de gênero que impactam diferentes grupos sociais de forma desproporcional, submetendo-os mais frequentemente aos falsos positivos, conforme casos amplamente noticiados. As TRFs ao vivo produzem efeitos imediatos e, potencialmente, irreversíveis, além de também apresentarem riscos ao direito à manifestação. Uma alternativa viável, mas não sem risco, é o reconhecimento após um evento específico, com análise pontual e mediante autorização judicial.", "940704": "Para a mitigação de riscos deve-se adotar a segmentação da infraestrutura do sistema e controle rigoroso de acessos (quem, quando e sob quais circunstâncias), com autenticação multifator. Além disso, é fundamental o registro de acessos, operações e consultas e, também, a adoção de estratégias para tornar os dados menos identificáveis quando a identidade direta não for necessária. Igualmente importante é o treinamento técnico e ético de pessoal responsável pelo tratamento e segurança desses dados. Quanto à avaliação de risco e monitoramento da TRF na segurança pública, é necessário considerar quantas fotos há no banco de dados; como foram obtidas; por quanto tempo são armazenadas; com que frequência limpezas são feitas; qual processo para uma pessoa ser removida do banco de dados; quem tem acesso a ele; como é mantido e atualizado (evitando-se que pessoas com casos já julgados sejam reconhecidas por desatualização dos dados, por exemplo); e a política de privacidade adotada.", "940707": "", "940708": "No caso do uso de TRF, qualquer que seja seu tipo, em cada uma de suas etapas, há riscos de erro e identificação incorreta, bem como de vigilância discriminatória, desproporcional e desnecessária. Logo, todas essas fases devem ser cuidadosamente analisadas quando houver uma avaliação de como a TRF afeta direitos fundamentais. E, dado que a tecnologia tem exibido vieses raciais e de gênero, tais preconceitos devem ser sempre pautados nessa análise. Para garantir a proteção de direitos no tratamento de dados biométricos, é essencial que controladores adotem medidas de segurança técnica e transparência, com o limite de acesso a informações sensíveis e realização de auditorias regulares, as quais devem avaliar o viés algorítmico e garantir a equidade dos sistemas. Relatórios sobre o uso desses dados e comunicação transparente com os titulares deles para que possam exercer seus direitos também são fundamentais.", "940709": "Conforme exposto na questão 10, as TRF em tempo real, especialmente quando utilizadas em espaços públicos ou semi abertos apresentam riscos profundos por envolverem vigilância constante, indiscriminada e sem consentimento ou suspeita prévia, o que é incompatível com o direito à

privacidade, e, portanto, devem ser banidas. Também cabe reiterar aqui os impactos para grupos historicamente vulnerabilizados, devido aos vieses de raça e gênero da tecnologia, bem como os riscos ao direito à livre manifestação. Uma alternativa viável, mas não sem risco, é o reconhecimento após um evento específico, com análise pontual e mediante autorização judicial. Ainda nessa hipótese, contudo, é necessária a disponibilização de informação visível e acessível no local em que a tecnologia for utilizada sobre quais imagens estão sendo coletadas e para quais fins.", "940710": "Os agentes de tratamento de dados biométricos, especialmente em contextos automatizados, devem garantir o respeito aos direitos dos titulares adotando práticas que sejam transparentes e acessíveis. Para assegurar o direito à informação clara, por exemplo, devem ser fornecidas informações detalhadas sobre o processo de coleta e o uso desses dados, como a finalidade, tempo de retenção e com quem eles serão compartilhados. No que diz respeito ao acesso e à correção, os titulares devem ter meios simples para visualizar, corrigir ou excluir seus dados, por meio de portais de autoatendimento e/ou sistemas automatizados para corrigir eventuais erros. Os titulares também devem exercer o seu direito de retirar o seu consentimento a qualquer momento, sem penalidades, por meio de mecanismos simples, como botões ou links de revogação.", "940711": "", "940712": "", "940714": "Não deve ser utilizado.

Contribuinte: ARQUIAS SOFOCLES GUIMARAES SOARES CRUZ

Número: OP-1005106

Data: 31/07/2025 - 14:09

Resumo: "Reposta Câmara Brasileira da Economia Digital: LGPD e dado biométrico: A Lei Geral de Proteção de Dados (LGPD) não traz definição de “dado biométrico”, limitando-se a enquadrá-lo como espécie de dado pessoal sensível. Aplicação prática e teleológica na LGPD: A LGPD adota uma definição taxativa de dados pessoais sensíveis (art. 5º, II). Para fins de enquadramento, é recomendada uma interpretação finalística, ou seja, na ausência de intenção ou finalidade de inferir informações sensíveis, o dado não deve ser considerado sensível. Por exemplo, o uso de fotos ou vídeos disponíveis publicamente, sem extração ou inferência de dados biométricos ou outras informações sensíveis, não configura tratamento de dados pessoais sensíveis. Ainda, deve-se considerar que, de acordo com a LGPD, para aplicação do artigo 11, é preciso que o tratamento de dados pessoais “revele dados pessoais sensíveis e que possa causar dano ao titular”. (Continuação por e-mail/anexo)", "940688": "Reposta Câmara Brasileira da Economia Digital: Transparência e dados biométricos: As boas práticas de transparência devem orientar todo e qualquer tratamento de dados pessoais, inclusive de dados sensíveis, como os dados biométricos. Medidas que facilitem o acesso dos titulares a informações claras e precisas sobre esse tratamento, especialmente no que se refere à indicação de finalidades legítimas, específicas e explícitas, constituem referência de boas práticas em matéria de transparência. Transparência e proporcionalidade na LGPD: O princípio da transparência deve ser interpretado de forma proporcional e funcional, considerando o contexto e as circunstâncias da operação de tratamento. Por exemplo, quando o controlador não mantém relação direta com os titulares,

entende-se como suficiente a adoção de medidas razoáveis para disponibilizar as informações exigidas pela LGPD em site de acesso público. (Continuação por e-mail/anexo)", "940690": "Reposta Câmara Brasileira da Economia Digital: LGPD e dados biométricos: Lembra-se que a LGPD não define expressamente “dato biométrico”, limitando-se a classificá-lo como dato pessoal sensível. Para fins de enquadramento, é necessária uma interpretação finalística: na ausência de intenção ou finalidade de inferir informações sensíveis, o dato não deve ser considerado sensível. Por exemplo, o uso de fotos ou vídeos disponíveis publicamente, sem extração ou inferência de dados biométricos ou outras informações sensíveis, não configura tratamento de dados pessoais sensível. Além disso, o art. 11 exige que o tratamento revele dato sensível e possa causar dano ao titular. Referências conceituais: Segundo o art. 4.14 do GDPR, dato biométrico é o resultado de tratamento técnico específico de características físicas, fisiológicas ou comportamentais que permita ou confirme a identificação única de uma pessoa natural. (Continuação por e-mail/anexo)", "940693": "Reposta Câmara Brasileira da Economia Digital: Ausência de hierarquia entre as bases legais do art. 11 da LGPD: Qualquer uma das hipóteses previstas no art. 11 da LGPD pode ser utilizada para legitimar o tratamento de dados pessoais sensíveis, inclusive biométricos. O consentimento não possui caráter preferencial ou hierarquicamente superior às demais bases legais e deve ser analisado conforme a finalidade e o contexto do tratamento. Assim, nos casos em que dados biométricos são tratados nos termos da LGPD, incentivamos a ANPD a fornecer orientações práticas e proporcionais sobre outras bases legais apropriadas para tal tratamento. (Continuação por e-mail/anexo)", "940695": "Reposta Câmara Brasileira da Economia Digital: Critérios para o tratamento de dados biométricos com base na garantia da prevenção à fraude e à segurança do titular: O enquadramento do tratamento de dados biométricos na hipótese legal de “garantia da prevenção à fraude e à segurança do titular” deve observar os critérios estabelecidos no art. 11, inciso II, alínea “g”, da LGPD. Nessa hipótese, o tratamento será permitido quando: (i) tiver como finalidade garantir a prevenção à fraude e a segurança do titular; (ii) for realizado por meio de processos de identificação e autenticação de cadastro em sistemas eletrônicos; (iii) forem respeitados os direitos previstos no art. 9º da LGPD; e (iv) não prevalecerem os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (Continuação por e-mail/anexo)", "940697": "Reposta Câmara Brasileira da Economia Digital: Adequação do tratamento de dados biométricos para cumprimento de obrigação legal ou regulatória: A adequada aplicação da hipótese legal de cumprimento de obrigação legal ou regulatória pressupõe o atendimento a requisitos de segurança e a observância dos princípios balizadores do tratamento de dados pessoais de forma geral. O princípio da necessidade, por exemplo, exige que os dados biométricos sejam utilizados apenas na medida estritamente necessária para o alcance da finalidade, assegurando a disponibilização de informações claras, precisas e acessíveis aos titulares sobre o tratamento realizado. O tratamento desses dados deve estar fundamentado na aplicação desse princípio, em conjunto com outros, bem como em boas práticas de governança e segurança da informação, visando garantir controle, rastreabilidade e proteção eficaz dos dados biométricos. (Continuação por e-mail/anexo)", "940699": "Reposta Câmara Brasileira da Economia Digital: Conceito de dato anonimizado: O dato anonimizado caracteriza-se por ser o dato que não é capaz de permitir

a reidentificação posterior, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (conceito de dado anonimizado previsto no art. 5º, III da LGPD). Uma vez realizado o processo de anonimização, os referidos dados não são considerados dados pessoais, tendo em vista que não é possível identificar o titular. Consequentemente, os dados deixam de ser considerados dados sensíveis. (Continuação por e-mail/anexo)", "940700": "Resposta Câmara Brasileira da Economia Digital: Reconhecimento vs. detecção facial: Somente se caracteriza como dado biométrico aquele cujo tratamento tem como finalidade a identificação ou autenticação única de um indivíduo. Assim, cumpre destacar a diferença entre reconhecimento e detecção facial. O reconhecimento facial envolve: (i) o mapeamento de pontos e linhas específicas da face; (ii) a comparação com um banco de dados já existente, o qual envolve dados de pessoas identificáveis e identificadas; e (iii) a identificação de pessoas específicas. Por outro lado, a detecção facial é uma técnica que localiza rostos humanos em uma dada imagem ou vídeo, a partir de pontos de referência da face na boca, no nariz, nos olhos e na sobrancelha, e até o posicionamento da face. (Continuação por e-mail/anexo)", "940701": "Resposta Câmara Brasileira da Economia Digital: Desenvolvimento e mitigação de riscos em sistemas de reconhecimento facial: Recomenda-se que os sistemas de reconhecimento facial sejam concebidos desde a fase inicial com medidas técnicas e organizacionais que assegurem precisão, segurança e mitigação de riscos, alinhadas aos princípios de privacy by design e privacy by default. O engajamento de diferentes partes interessadas (indústria, academia e sociedade civil) pode ser importante para aprimorar o design e a eficácia dessas tecnologias. Porém, é necessário reconhecer que não é possível eliminar totalmente os erros desses sistemas, sendo muitas vezes preciso equilibrar fatores como precisão, recall, equidade, discriminação e necessidade. (Continuação por e-mail/anexo)", "940702": "Resposta Câmara Brasileira da Economia Digital: Limitações no uso do reconhecimento facial: Não é recomendável o uso de tecnologias de reconhecimento facial quando o tratamento de dados biométricos acarreta riscos elevados à privacidade dos titulares e quando não há justificativa proporcional para o tratamento, implementação de medidas mitigação de riscos e/ou indicação de base legal adequada. ", "940704": "Resposta Câmara Brasileira da Economia Digital: Ausência de medidas específicas e determinadas: Não existe um conjunto definido de medidas de segurança, técnicas e administrativas que devam ser consideradas indispensáveis para mitigar riscos de segurança. Assim, diversas salvaguardas podem ser implementadas, isoladas ou conjuntamente, para alcançar uma abordagem proporcional e que considere a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento, bem como seu contexto específico. (Continuação por e-mail/anexo)", "940707": "Resposta Câmara Brasileira da Economia Digital: Abordagem proporcional e observância da LGPD: Não existe um conjunto único de práticas aplicável universalmente. É fundamental adotar uma abordagem proporcional que considere o caso de uso e os riscos ou danos potenciais ao indivíduo, garantindo que o tratamento de dados biométricos esteja enquadrado em uma das bases legais da LGPD e observe os princípios de necessidade, não discriminação e transparência. (Continuação por e-mail/anexo)", "940708": "Resposta Câmara Brasileira da Economia Digital: Boas práticas: Entre boas práticas possíveis, destacam-se a oferta de treinamentos específicos sobre o tema; o reforço, em políticas e procedimentos, de informações detalhadas sobre a forma adequada

de tratamento desse tipo de dado; e a elaboração de relatórios de impacto à proteção de dados pessoais, quando aplicável.", "940709": "", "940710": "Resposta Câmara Brasileira da Economia Digital: Desafios práticos e abordagem proporcional: A ANPD deve reconhecer os desafios práticos na facilitação dos direitos dos titulares de dados quando os dados biométricos foram inseridos em um formato legível por máquina (por exemplo, seguindo o "processamento técnico específico"), de modo que podem não ser legíveis por pessoas e talvez não possam ser fornecidos em outro formato. A orientação da ANPD, portanto, precisa ser: (i) proporcional; (ii) baseada em princípios; e (iii) suficientemente flexível para fornecer uma estrutura relevante para os métodos utilizados para facilitar os direitos de proteção de dados no contexto de dados biométricos, em linha com a orientação do ICO sobre dados biométricos. (Continuação por e-mail/anexo)", "940711": "Resposta Câmara Brasileira da Economia Digital: Hipóteses legais para tratamento de dados biométricos de crianças e adolescentes: O tratamento de dados biométricos de crianças e adolescentes deve seguir as hipóteses legais previstas no artigo 11 da LGPD, aplicando-se também as regras do artigo 14, que exige respeito ao melhor interesse do menor. Segundo o Enunciado nº 1/2023 da ANPD, esses dados podem ser tratados com base nas hipóteses do artigo 7º ou 11 da LGPD, desde que haja observância e prevalência do melhor interesse da criança ou adolescente. Quando a base legal for o consentimento, ele deve ser claro e específico, abrangendo as finalidades do tratamento e, no tratamento de dados de crianças, fornecido pelo representante legal. (Continuação por e-mail/anexo)", "940712": "Resposta Câmara Brasileira da Economia Digital: Hipóteses legais para tratamento de dados biométricos de crianças e adolescentes: O tratamento de dados biométricos de crianças e adolescentes pode ser amparado em qualquer das hipóteses legais previstas no artigo 11, haja visto o disposto no Enunciado ANPD nº 1/2023. Nesse sentido, a hipótese legal de garantia da prevenção à fraude e à segurança do titular ganha especial relevância nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (Art. 11, II, “g”, LGPD). Quando a hipótese legal for o consentimento, deve haver transparência quanto às finalidades do tratamento. (Continuação por e-mail/anexo)", "940714": "Resposta Câmara Brasileira da Economia Digital: Princípio da necessidade: O princípio da necessidade deve ser compreendido não como uma limitação ao tratamento do menor volume possível de dados, mas sim como o uso dos dados essenciais para atingir finalidades legítimas, em consonância com os demais princípios da LGPD e o melhor interesse de crianças e adolescentes. A relação entre a proteção de dados e a segurança deve ser analisada conforme as circunstâncias específicas, permitindo uma ponderação cuidadosa entre valores que possam ser conflitantes. Em certos casos, a coleta de dados adicionais pode ser a medida mais adequada para garantir a proteção do melhor interesse das crianças e adolescentes. (Continuação por e-mail/anexo)

Contribuinte: MAIRA LOBO HAYASHIDA BARRETO

Número: OP-1005260

Data: 31/07/2025 - 17:37

Resumo: "A LGPD exige interpretação restritiva do conceito de dado biométrico: qualquer dado fisiológico ou comportamental que permita identificar ou autenticar um indivíduo de forma única deve ser tratado como sensível, ainda que não seja capturado por tecnologias tradicionais. Essa identificação pode ser direta ou inferida com outros dados. Ampliar essa proteção é essencial para evitar tratamentos abusivos ou reidentificação indevida. A interpretação deve seguir o princípio da precaução, dada a irreversibilidade da exposição biométrica. ", "940688": "A transparência deve ser proativa e radical, dada a natureza sensível e irreversível dos dados biométricos. Apenas informar não basta: é dever do controlador demonstrar compreensibilidade e efetiva compreensão pelo titular. Informações devem ser visuais, acessíveis e com linguagem não técnica, além de expor riscos e não apenas finalidades. O Relatório de Impacto (DPIA) deve ser público nos casos de alto risco. O silêncio do titular nunca pode ser interpretado como anuência, sob risco de nulidade do tratamento. ", "940690": "A biometria comportamental exige proteção ainda mais rigorosa do que a tradicional. Como seus padrões são invisíveis ao titular e muitas vezes captados sem percepção clara (ex: digitação ou entonação), há alto risco de tratamento oculto e opaco. É inaceitável presumir consentimento ou necessidade técnica sem comprovação. A coleta deve ser precedida de análise de impacto e autorização explícita, com bases técnicas auditáveis. A assimetria informacional é maior, o que exige controles adicionais para garantir qualidade e segurança. Por fim, esses dados são projetados para serem gerados em contextos de utilização de ferramentas e plataformas para que o dono do serviço ou controlador do dado utilize essas informações para fins industriais/comerciais, agravando os riscos associados a garantia dos direitos do titular de dados. ", "940693": "Consentimento só é válido quando plenamente livre e informado, o que exclui ambientes com relações assimétricas, como emprego, escola, serviços essenciais, prestação de assistência pelo poder público ou pelo terceiro setor. Nessas situações, tratá-lo como base legítima é mascarar coerção. O consentimento deve ser destacado, granular e revogável a qualquer tempo, sem prejuízo ao titular. Qualquer tentativa de condicionar acesso a funcionalidades básicas, políticas públicas e direitos fundamentais à coleta biométrica deve ser considerada abusiva e ilegal, mesmo com aceite formal. ", "940695": "A cláusula de “prevenção à fraude” (art. 11, II, g) não pode ser usada como pretexto genérico para coleta biométrica. A finalidade deve ser estrita, documentada e proporcional. O princípio da necessidade exige prova de que não há método menos invasivo que atenda ao mesmo fim. A coleta deve ser subsidiada por DPIA, segregação de dados e auditoria independente. O uso abusivo dessa base legal pode legitimar vigilância indevida e criar risco sistêmico de exclusão digital e discriminação algorítmica. Em todos os casos deve-se preservar a transparência desses dados pelo controlador, garantindo que todos os titulares de dados possam acessar em tempo real quais dados pessoais estão nos bancos de dados do controlador, monitorar o tratamento e clareza da finalidade de cada um desses tratamentos, podendo inclusive revogar a permanência desses dados em posse do controlador. ", "940697": "Mesmo em hipóteses de obrigação legal (art. 11, II, “a”), o Estado não pode ser dispensado do dever de necessidade, minimização e transparência. A imposição legal deve ser específica e proporcional, não podendo se apoiar em normas genéricas. O poder público deve adotar salvaguardas reforçadas: anonimização por padrão, ciclo de vida limitado dos dados, publicidade dos relatórios de impacto e possibilidade de auditoria civil. A função

estatal não legitima vigilância em massa nem coleta excessiva. ", "940699": "A anonimização não elimina o risco de reidentificação, especialmente quando se trata de dados biométricos, cuja unicidade os torna mais vulneráveis à reidentificação por meio de cruzamento com outras bases. Mesmo em estudos científicos, o uso desses dados deve ser precedido de avaliação de impacto, controle de acesso rigoroso e plano de descarte. Bases biométricas não devem ser reutilizadas para finalidades não previstas. A transparência deve ser privilegiada para que o titular de dados tenha total ciência de como os dados estão sendo tratados. A ciência não pode ser escudo para diluir direitos fundamentais. ", "940700": "O reconhecimento facial, mesmo com base legal, deve ser tratado como tecnologia de risco extremo, com alto potencial discriminatório, especialmente contra grupos racializados, refugiados, pessoas trans e pessoas com deficiência. O princípio da proporcionalidade exige prova robusta de que o uso é indispensável e que outros meios não alcançam o mesmo resultado. Sistemas devem ser treinados com diversidade de dados, auditados contra viés e submetidos a supervisão humana significativa. Ausência dessas medidas deve ensejar proibição. ", "940701": "Todo sistema de reconhecimento facial deve ser projetado com prioridade à prevenção de falsos positivos e negativos, que têm impacto desproporcional em contextos sensíveis como segurança pública ou acesso a serviços. A LGPD exige que erros sejam corrigidos com urgência, e o sistema, suspenso se houver risco de dano. O controlador deve prever mecanismos de recurso acessível, revisão humana obrigatória e registro de decisões automatizadas. A ausência de transparência algorítmica deve tornar o uso inviável. ", "940702": "O uso de reconhecimento facial deve ser vetado em locais públicos, em tempo real, e sem consentimento claro, como em estádios, escolas, transporte ou manifestações. A mera vigilância não justifica a erosão de liberdades civis. Em tais contextos, há desequilíbrio irremediável entre o controlador e o titular. Tecnologias alternativas, como autenticação via token, senha ou biometria local (armazenada no dispositivo), devem ser priorizadas sempre que possível, pois preservam a autodeterminação informativa. ", "940704": "Dado que dados biométricos são irrevogáveis e irrecuperáveis, qualquer violação representa dano permanente. Por isso, medidas de segurança devem incluir criptografia forte, anonimização sempre que possível, dupla autenticação para acesso à base e log de auditoria obrigatório. A avaliação de impacto deve ser periódica e pública em setores críticos. Organizações devem ser responsabilizadas por danos indiretos, e ausência de proteção mínima deve ensejar sanções exemplares. Tolerância zero com vazamentos biométricos. ", "940707": "A exigência de biometria para funcionalidades secundárias, como login facilitado, fila rápida ou acesso preferencial, pode representar discriminação indireta se não houver alternativa igualmente acessível. O princípio da igualdade material impõe que a recusa do titular em fornecer biometria não pode gerar exclusão ou constrangimento. A função deve ser efetivamente opcional, e sua indisponibilidade não pode comprometer a experiência de uso do serviço. Consentimento, aqui, deve ser tratado como revogável sem ônus. ", "940708": "O mínimo aceitável em boas práticas deve incluir: (i) limitação estrita da finalidade; (ii) coleta sob consentimento específico ou base legal robusta e documentada; (iii) armazenamento descentralizado (preferencialmente no dispositivo do titular); (iv) controles de acesso com autenticação múltipla; (v) auditoria contínua dos algoritmos quanto à acurácia e viés. O dado biométrico não pode ser utilizado para fins secundários sem nova base legal. Qualquer ambiguidade

interpretativa deve ser resolvida em favor da não coleta. ", "940709": "Em ambientes como smart cities ou grandes eventos, onde o titular não pode consentir individualmente, o uso de biometria deve ser presumido incompatível com a LGPD, salvo raras exceções com previsão legal específica. O direito à autodeterminação informativa exige: aviso claro em campo visual, opção real de recusa, anonimização em tempo real e vedação à identificação retroativa. A ausência de transparência nesses ambientes compromete a legalidade e deve inviabilizar o tratamento. ", "940710": "O controlador deve assegurar: (i) interface para acesso facilitado aos dados biométricos tratados; (ii) possibilidade de correção e exclusão sem justificativas excessivas; (iii) mecanismo visível e gratuito de revogação do consentimento, inclusive com exclusão dos dados históricos. Sempre que houver decisão automatizada baseada em biometria, o titular tem direito à revisão humana e explicação clara dos critérios usados. A opacidade algorítmica é incompatível com os direitos previstos na LGPD. ", "940711": "O tratamento só deve ocorrer quando absolutamente necessário e com consentimento expresso e destacado dos pais ou responsáveis. A coleta deve respeitar o princípio do melhor interesse da criança (art. 14, LGPD), o que implica avaliar se há meio menos invasivo. O dado biométrico não pode ser exigido para acesso à educação ou recreação. Sistemas devem prever controles específicos para impedir uso indevido, reidentificação ou perfilamento precoce. Criança não pode ser convertida em perfil digital fixo. ", "940712": "Mesmo quando o tratamento de biometria infantil se basear em consentimento ou obrigação legal (ex: segurança escolar), é indispensável: (i) DPIA específico para o público infantojuvenil; (ii) design de privacidade desde a concepção ("privacy by design"); (iii) acesso restrito por perfil profissional com capacitação técnica e ética. Deve ser proibido o uso para marketing, segmentação ou qualquer finalidade que extrapole o escopo declarado. A responsabilização deve ser objetiva, com inversão do ônus da prova em caso de incidente. ", "940714": "Estimativas de idade via biometria facial ou de voz são altamente falhas e discriminatórias, com taxas de erro superiores a 20% em alguns grupos, além de implicar coleta de dado sensível sem necessidade real. Essas práticas violam o princípio da minimização e não devem ser consideradas válidas, sobretudo quando envolvem crianças. Verificação de idade deve priorizar mecanismos alternativos, como declarações sob responsabilidade dos pais ou token de verificação documental. A conveniência técnica não pode se sobrepor ao direito à proteção integral.

Contribuinte: ALEXANDRE ZAGO BOAVA

Número: OP-1005612

Data: 01/08/2025 - 07:16

Resumo: "Os critérios objetivos são: (i) origem em atributos únicos do indivíduo (ex.: impressão digital, geometria facial, voz, padrões neurais); (ii) uso de tecnologia para coleta e processamento; (iii) finalidade de autenticação ou identificação exclusiva. Essa definição deve abranger dados de neurotecnologias, como interfaces cérebro-computador (BCI) e optogenética. Essas tecnologias coletam dados fisiológicos (frequência cardíaca, SpO2, sono) e neurais (EEG, fMRI), que revelam padrões de atividade cerebral associados a pensamentos

e emoções. Tais dados, especialmente os neurais, ao permitirem a identificação única e revelarem aspectos íntimos da saúde e estado mental, devem ser considerados biométricos e sensíveis, exigindo proteção rigorosa nos termos da LGPD, independentemente de futura classificação legal específica.", "940688": "Podem ser exigidas políticas claras com tipo de dado biométrico, finalidade, base legal, retenção e compartilhamentos; avisos visíveis, linguagem simples, testes de compreensão com os titulares, alternativas ao reconhecimento facial, canais de atendimento e, publicação de relatórios de impacto. Além disso, a usabilidade (usuário como centro do produto serviço) deve ser guiada por acessibilidade, com alternativas de coleta biométrica facial/tátil/voz, para indivíduos com limitação em um modelo predeterminado. Por exemplo, para um titular com impossibilidade de uso da face ou dedos, como as vítimas de AVC ou portadores de paralisia cerebral, ou, para além disso, a biometria tátil ou de voz para pessoas cegas. É fundamental sempre manter uma alternativa de coleta ou uma biometria universal acessível por todos.", "940690": "O tratamento de dados comportamentais desloca de uma simples verificação de identidade para uma avaliação dinâmica e contínua de estado, capacidades e preferências da pessoa humana, agravando os riscos à luz da LGPD. Há uma maior dificuldade na percepção desta coleta e uma maior tendência a falta de transparência. A exemplo, para o princípio de qualidade, a aferição do dado comportamental é mais propensa a falha por se afastar de um cenário objetivo, podendo gerar uma exclusão ou classificação incorreta do dado. Por isso, considerando o princípio da segurança, é necessário que as medidas técnicas sejam mais rigorosas, antecipando problemáticas com falsos positivos para melhor monitorar a precisão do dado, se afastando de erros sistêmicos e de discriminação.", "940693": "A validade do consentimento para dados biométricos é revestida de uma complexidade jurídica, uma vez que não depende apenas da manifestação do titular, mas também de um ecossistema que garanta sua escolha livre, específica, destacada, informada e inequívoca. Para a exigência de um consentimento "livre", é necessário que não haja desequilíbrio de poder entre o titular e o controlador, bem como uma alternativa válida para a coleta. Também deve ser uma solicitação transparente, com informações claras e possibilidade de manifestação afirmativa objetiva, além da necessidade de expressar a finalidade determinada de maneira destacada no termo. Dessa forma, em situações onde há dependência econômica, relação de trabalho, serviços essenciais, não são hipóteses recomendáveis para a base legal do consentimento, uma vez que são contextos provenientes de relações desequilibradas.", "940695": "O tratamento de dados biométricos deve ser acompanhado de uma ponderação de interesses detalhada em RIPD, principalmente com o interesse de garantir que a base legal escolhida foi adequada para o tratamento, uma vez que a fraude que se busca prevenir deve ser aquela que afeta diretamente o titular dos dados.", "940697": "A utilização da base legal de cumprimento de obrigação regulatória perpassa pela necessidade de justificação não só da legalidade, mas também da legitimidade, necessidade e proporcionalidade da medida. Para isso, deve-se considerar que há essencialidade para a coleta daquele dado, visando atingir de forma menos invasiva o objetivo público almejado. Além disso, deve-se publicar o RIPD para garantir maior transparência ao processo, bem como um cuidado especial para prever o desvio de finalidade daqueles dados biométricos coletados, um grande risco envolvendo os órgãos públicos. Em termos gerais, há a necessidade de ter uma segurança de ponta, uma política de retenção

mínima dos dados, transparência, e em alguns casos, legislação específica e restrita.", "940699": "O estudo deve ser informado ao titular (se a coleta for primária) ou definido no escopo da pesquisa (se a base for secundária). A reidentificação nessa hipótese deve ser duramente reprimida (Art. 16, § 2º). Como salvaguarda sugerem-se técnicas de Privacy by Design e Privacy Enhancing Technologies, não deixando de observar a inclusão de práticas de diversidade e inclusão significativa.", "940700": "Para garantir conformidade com a LGPD, o uso de reconhecimento facial deve observar os princípios do art. 6º e o art. 20, § 1º: medidas estritamente necessárias e proporcionais ao atendimento do interesse público, com previsão legal específica e respeito ao devido processo. Devem-se adotar salvaguardas técnicas, jurídicas e organizacionais, como: (i) controles de acesso e autenticação segura; (ii) biometria cancelável e criptografia; (iii) avaliações de impacto (DPIA) para identificar riscos e discriminação algorítmica; (iv) verificação contínua de vieses e auditorias independentes; (v) consentimento informado ou base legal adequada; (vi) políticas claras, canais acessíveis, governança com DPO e capacitação. O uso deve ser limitado, justificado e com mecanismos de accountability para prevenir abusos.", "940701": "Adotar Privacy by Design, testes contínuos de acurácia e viés, datasets auditáveis e representativos, tal como o Banco de Imagens Brasileiro. Estabelecer procedimentos de revisão e auditoria humana e logs automatizados para correção de erros (falsos positivos/negativos). Além disso, importa mencionar que são imprescindíveis a inclusão de ações afirmativas (práticas de diversidade e inclusão) nas ações de Privacy by Design, para evitar vieses nos desenvolvimentos de produtos e serviços que envolvam dados biométricos desde a concepção, tais como: diversidade e inclusão de desenvolvedores como PCDs e pessoas negras; banco de dados de testes que reflitam a mesma diversidade, ações afirmativas nos eventuais outputs.", "940702": "Sim. Contextos inadequados incluem espaços com alta vulnerabilidade ou risco de discriminação, como escolas, serviços públicos, eventos e ambientes com pessoas com deficiência ou características faciais atípicas (paralisia, epidermólise bolhosa, autismo), pois a tecnologia tende a falhar nesses casos. Além disso, estudos do Panóptico mostram que sistemas de reconhecimento facial no Brasil têm altos índices de falsos positivos, atingindo desproporcionalmente pessoas negras, evidenciando viés racial e risco de discriminação ilícita. Alternativas menos invasivas e mais inclusivas incluem cartões com chip, senhas dinâmicas, tokens físicos, chaves criptográficas e autenticação multifator. A escolha deve seguir critérios de proporcionalidade e impacto reduzido sobre dados sensíveis.", "940704": "Deve ser considerada a adoção de medidas de segurança aptas a mitigar o risco de vazamento de dados biométricos, sendo indispensável a adoção de: 1. Ferramenta de detecção de ataques de apresentação, que determinará se a amostra biométrica está sendo coletada do titular em vida; 2. Criptografia de dados em trânsito e em repouso, para proteção do dado quando transacionado e armazenado; 3. Controles de acesso rigorosos, evitando tanto quanto possível o uso e manuseio dessas informações; 4. Plano de resposta a incidentes que determine ação rápida e eficaz diante de qualquer ocorrência; 5. Ferramenta de verificação e auditoria, para monitoração do ambiente; 6. Revisão humana das decisões automatizadas. Para uma avaliação de riscos e monitoramento eficaz, devem ser adotados os seguintes parâmetros mínimos 1. Elaboração de RIPD; 2. Aplicação da matriz de risco de impacto e probabilidade; 3. Análise da escala do

tratamento (volume e abrangência); 4. Presença de titulares vulneráveis.", "940707": "O uso de autenticação biométrica em serviços não essenciais expõe o titular ao risco de discriminação e exclusão caso não possa ou não queira fornecer o dado. As seguintes boas práticas devem ser observadas 1. Em atendimento aos princípios da finalidade e necessidade, a biometria só deve ser exigida quando não houver nenhuma outra forma de autenticação que cumpra com a finalidade pretendida; 2. Deve ser ofertada autenticação alternativa para os titulares que não querem ou não podem fornecer a autenticação biométrica; 3. Transparência e comunicação com o titular sobre a necessidade da coleta biométrica, e sobre os métodos alternativos; 4. Aplicação de testes de equidade de explicabilidade, para garantir a adequação dos resultados. A recusa do fornecimento de biometria pelo titular somente pode implicar em restrição de acesso a determinadas funcionalidades quando a coleta for necessária para garantir a segurança do titular, como no caso de transações bancárias e acesso à dados de saúde.", "940708": "Além das medidas já previstas e reconhecidas como estruturação de uma equipe de governança e ética de dados, implementação de políticas internas e treinamento e medidas de segurança, o controlador deve: aplicar testes de equidade e explicabilidade que sejam aptos a demonstrar a lógica por trás das ações do mecanismo de autenticação, prevenindo o risco de discriminações ilícitas e abusivas e implementar auditoria periódica dos mecanismos de autenticação biométrica. Por fim, limitação e/ou camadas adicionais de segurança e para conformidade com as Leis Berenice Piana (autismo) – Lei 12.764/2012; Lei Brasileira de Inclusão - 13.146/2015; Lei de Diretrizes e Bases da Educação Nacional (LDB), Lei nº 9.394/96 – em especial o Capítulo V, arts. 58 a 60, nos produtos e serviços que utilizem dados biométricos de PCDs; além da Convenção Internacional sobre os Direitos das Pessoas com Deficiência, Decreto 6949/2009, do ECA e do Estatuto do Idoso.", "940709": "Controladores devem assegurar transparência ativa e acessível: sinalização clara em espaços públicos, QR Codes com informações, mensagens sonoras e recursos inclusivos (voz, vídeo, braille). Devem publicar Relatórios de Impacto à Proteção de Dados (DPIA), informando finalidade, riscos e salvaguardas, além de garantir canais simples para exercício de direitos, inclusive por meios não digitais. É essencial prever mecanismos de opt-out quando possível, informar bases legais utilizadas e adotar medidas de minimização e anonimização. A supervisão contínua por autoridades, auditorias independentes e governança com DPO fortalecem a autodeterminação, mesmo em contextos de monitoramento massivo.", "940710": "Os agentes de tratamento devem implementar fluxos eficazes (manuais e automatizados) para atender aos direitos previstos na LGPD (arts. 9º e 18), assegurando respostas em até 15 dias. É fundamental oferecer canais acessíveis, comunicação clara dos prazos e status das solicitações via painel ou dashboard intuitivo. Devem ser disponibilizados mecanismos simples para: (i) acesso e correção de dados; (ii) revogação do consentimento; (iii) oposição ao tratamento. Sempre que possível, utilizar autenticação segura para evitar fraudes. Transparência contínua deve ser garantida por políticas publicadas, relatórios e orientação aos titulares, com suporte multicanal (voz, chat, presencial) para inclusão digital.", "940711": "O tratamento de dados biométricos de crianças e adolescentes, por envolver dados sensíveis (art. 5º, II, LGPD), exige base legal do art. 11. Quando envolver crianças, aplica-se também o art. 14, que impõe consentimento específico e em destaque de ao menos um responsável, salvo hipóteses de proteção ou contato com os pais. A ANPD

admite o uso de outras bases legais, desde que observado o princípio do melhor interesse, o qual requer análise de necessidade, proporcionalidade, minimização de dados e medidas técnicas de segurança. A participação informada dos responsáveis deve incluir informação clara sobre finalidade, riscos, bases legais e direitos, além de controle efetivo sobre o tratamento. O uso da biometria em ambientes escolares e recreativos deve ser justificado por risco, indispensabilidade e ausência de alternativas menos invasivas.", "940712": "", "940714": ""

Contribuinte: JEIEL DE SANTANA BARBOSA

Número: OP-1005625

Data: 01/08/2025 - 07:45

Resumo: "Dados biométricos são informações obtidas por meio de processos técnicos que captam, extraem, analisam ou comparam características físicas, fisiológicas ou comportamentais de uma pessoa. Eles permitem a identificação única do indivíduo, diferindo de dados genéricos ou anonimizados. Por serem sensíveis e irreversíveis — como impressões digitais, íris, voz ou padrões faciais — exigem alto cuidado jurídico. Seu uso em autenticação ou decisões automatizadas pode afetar a privacidade e os direitos dos titulares, demandando salvaguardas, avaliações de impacto e conformidade com a LGPD, especialmente quanto aos princípios da necessidade, finalidade, proporcionalidade e segurança.", "940688": "Os controladores devem adotar práticas de transparência que garantam aos titulares informações claras, acessíveis e compreensíveis sobre o tratamento de dados biométricos. Isso inclui a disponibilização de avisos de privacidade nos pontos de coleta, canais digitais e ambientes físicos, com destaque para a finalidade do tratamento, a base legal utilizada, os direitos dos titulares e os meios de contato com o encarregado de dados.", "940690": "A biometria comportamental é altamente sensível e exige rigor no uso, especialmente em autenticação. Seus dados são voláteis, influenciados por ambiente, saúde e estado emocional, o que afeta sua precisão. A coleta contínua demanda transparência, consentimento e auditoria para evitar discriminação e violações de direitos. É essencial justificar sua necessidade, detalhar o tipo de dado, tratamento, armazenamento e descarte. Devem ser adotadas medidas como validação de algoritmos, controle de falsos positivos/negativos, criptografia, segmentação de dados e controle de acesso. Boas práticas como Privacy by Design/Default e avaliações de impacto são fundamentais, além da adoção de frameworks como NIST SP 800-63B, ISO/IEC 30107-3, 27001 e 27701.", "940693": "Nos termos da LGPD (art. 5º, XII), o consentimento é manifestação livre, informada e inequívoca do titular para tratamento de dados com finalidade específica. Para dados biométricos (art. 5º, II), por serem sensíveis e irreversíveis, exige-se maior rigor. O consentimento deve ser livre, sem coação, específico, granular e destacado em linguagem clara. É vedado condicionar serviços essenciais à sua concessão, salvo necessidade e proporcionalidade. A informação ao titular deve ser completa, incluindo tipo de dado, finalidade, base legal, riscos, segurança e compartilhamentos. A manifestação deve ser afirmativa, como clique ou assinatura, sendo inválido o silêncio. O agente deve manter registros, permitir revogação simples e revisar periodicamente o consentimento,

especialmente em tratamentos contínuos ou automatizados.", "940695": "A aplicação da base legal de prevenção à fraude exige finalidade legítima, necessidade e proporcionalidade, com testes comparativos entre métodos biométricos e não biométricos. Deve haver documentação técnica e jurídica, como relatórios de impacto e registros de riscos. A base legal deve ser clara e comprovada. A coleta deve ser minimizada (ex.: template, não imagem bruta), segmentada por finalidade e com retenção limitada. Auditorias contínuas são essenciais. Medidas de segurança incluem criptografia, anonimização, controle de acesso, explicabilidade e contestabilidade. Mesmo nessa hipótese, recomenda-se obter consentimento. Algoritmos devem ser avaliados quanto a vieses, e a governança deve ser transparente, com políticas claras e uso de frameworks como NIST e ISO.", "940697": "Conforme o art. 11, II, “a” da LGPD, o tratamento de dados sensíveis, como biométricos, pode ser legitimado por obrigação legal ou regulatória. No entanto, isso não isenta o controlador — especialmente órgãos públicos — de seguir os princípios da proteção de dados e adotar salvaguardas. O tratamento deve estar vinculado a obrigação legal específica, documentada e proporcional. Devem ser aplicadas medidas como RIPD, minimização de dados, limitação de finalidade e retenção, transparência e garantia dos direitos dos titulares. A atuação pública deve ser ética, segura e alinhada à legalidade, proporcionalidade e aos valores constitucionais, como dignidade, autodeterminação informativa e intimidade.", "940699": "Conforme o art. 11, II, “c” da LGPD, órgãos de pesquisa podem tratar dados biométricos sem consentimento, desde que para fins científicos e, sempre que possível, com anonimização. No entanto, o risco de reidentificação exige salvaguardas adicionais, como anonimização validada, acesso restrito e cláusulas de confidencialidade. É essencial aplicar o princípio da minimização, garantir transparência sobre os estudos, métodos e governança. Projetos devem ser supervisionados por comitês de ética e privacidade, com parecer do CEP, assegurando o respeito aos direitos dos titulares e mitigando riscos residuais.", "940700": "Projetos de reconhecimento facial devem seguir princípios como privacidade desde a concepção, minimização de dados, finalidade clara e avaliações de impacto. É essencial reduzir erros (FAR, FRR, ERR), evitar vieses, atualizar algoritmos e realizar testes periódicos. Devem existir mecanismos de correção em tempo real, logs, canais de contestação e revisão humana. O uso em contextos como espaços públicos, escolas ou para classificação por características sensíveis deve ser evitado. O tratamento deve ser necessário, proporcional e transparente, com testes de viés, explicabilidade, governança ética e RIPD. Mesmo com base legal, o uso deve respeitar os direitos fundamentais à privacidade, igualdade e não discriminação.", "940701": "A biometria é uma das possibilidades de autenticação e identificação do titular, fazendo parte da tríade da autenticação multifator, que são: o que você sabe(senha), algo que você possui (token) e quem você é (biometria), por este motivo tecnologias alternativas devem e podem ser utilizadas pelos controladores, como por exemplo: - Autenticação multifator (MFA), com combinações entre senhas, tokens e biometria menos invasiva (impressão digital). - Biometria comportamental, como padrões de digitação, uso do mouse, ritmo de fala. - Cartões inteligentes com chip criptográficos, usados em ambiente corporativos com alta segurança. - QR Codes dinâmicos com autenticação por aplicativos, que evitam a exposição de dados biométricos e permite rastreabilidade. - Reconhecimento por dispositivos locais (on-device), sem envio de dados para servidores externos, como o Face ID no smartphone.", "940702": "O

uso de reconhecimento facial, mesmo com base legal, pode ser inadequado em contextos com alto risco à privacidade, ausência de consentimento ou potencial discriminação, como espaços públicos, escolas, locais de trabalho e eventos sem base clara. Nesses casos, o impacto aos direitos supera os benefícios. Alternativas menos invasivas incluem autenticação multifator com senhas, tokens, biometria local, QR Codes, cartões inteligentes e biometria comportamental de baixo impacto. A escolha da tecnologia deve seguir os princípios da necessidade, proporcionalidade e minimização, priorizando segurança com menor impacto à privacidade."

"940704": "A proteção de dados biométricos exige medidas técnicas como criptografia forte (ex.: AES-256), armazenamento em template, pseudonimização, controle de acesso com MFA, monitoramento contínuo (SIEM), testes de viés e robustez, e gestão de vulnerabilidades (DAST, SAST, IAST). Medidas administrativas incluem políticas específicas, RIPD, comitês de ética, treinamentos, planos de resposta a incidentes e gestão de consequências. A avaliação deve considerar indicadores de risco, auditorias, revisão de contratos e algoritmos. Em contextos de monitoramento massivo, exige-se transparência ativa, consentimento contextual, mecanismos de oposição, minimização e supervisão independente."

"940707": "Quando funcionalidades não essenciais dependem de autenticação biométrica, é essencial evitar discriminação. O uso de dados sensíveis deve seguir os princípios da LGPD: necessidade, proporcionalidade e transparência. O consentimento deve ser livre, informado e destacado, sem coação. A recusa do titular só pode limitar funcionalidades se não houver alternativa viável e menos invasiva. O controlador deve informar claramente as consequências, oferecer meios alternativos e garantir que a limitação não afete serviços essenciais. Avaliações de impacto, revisão periódica e canais de contestação são fundamentais para mitigar riscos e proteger os direitos dos titulares."

"940708": "É recomendável que os controladores implementem programas de governança em privacidade que contemplem, dentre outros mecanismos, DPIA (sigla em inglês para Data Protection Impact Assessment) — ou Relatório de Impacto à Proteção de Dados Pessoais (RIPD), segundo a Lei Geral de Proteção de Dados (LGPD) para operações que envolvam biometria. Essas avaliações devem assegurar que o tratamento seja proporcional, justificado e livre de vieses discriminatórios. Além disso, a adoção de mecanismos de revisão periódica, monitoramento de algoritmos e validação de critérios de decisão automatizada são medidas essenciais para garantir o uso ético e responsável dos dados biométricos dos titulares de dados."

"940709": "O tratamento contínuo e massivo de dados biométricos exige salvaguardas que assegurem a autodeterminação informativa dos titulares. É fundamental que os agentes de tratamento ofereçam alternativas ao uso da biometria sempre que possível, informem de forma clara sobre a coleta e o uso dos dados, e mantenham canais acessíveis para o exercício dos direitos previstos na LGPD. A realização de auditorias internas e a adoção de mecanismos de controle e rastreabilidade também contribuem para a transparência e a responsabilização."

"940710": "Os agentes de tratamento devem estruturar processos internos que viabilizem o exercício dos direitos dos titulares de forma eficiente e segura, nos moldes previstos nos arts. 18 e 20 da LGPD. Em operações que envolvam biometria, é essencial garantir que os titulares possam compreender os critérios utilizados no tratamento – como, porque e para que seus dados pessoais estão sendo utilizados, garantindo assim o princípio da transparência. É imprescindível também que os

titulares tenham acesso a canais de atendimento preparados para responder de forma clara e tempestiva. A existência de fluxos padronizados e equipes capacitadas é uma boa prática que fortalece a confiança dos titulares e a conformidade com a LGPD.", "940711": "O tratamento de dados biométricos de crianças e adolescentes deve seguir o princípio do melhor interesse do menor (art. 14 da LGPD). É necessário obter consentimento específico e destacado dos responsáveis, com linguagem clara e acessível. O tratamento só é admissível se estritamente necessário, proporcional e compatível com o contexto educacional ou recreativo, sendo vedado para fins comerciais. Devem ser adotadas salvaguardas como pseudonimização, limitação de acesso, RIPD e revisão periódica. É proibido condicionar a participação em atividades ao fornecimento de dados além dos necessários. A atuação deve ser ética, responsável e alinhada à proteção integral dos direitos da criança e do adolescente.", "940712": "O tratamento de dados biométricos de crianças e adolescentes só é permitido com base legal expressa na LGPD, priorizando o melhor interesse do menor (art. 14). A principal base é o consentimento específico e destacado de ao menos um responsável legal, obtido de forma livre e clara. Excepcionalmente, o tratamento pode ocorrer sem consentimento para contatar responsáveis ou proteger a criança, desde que justificado. É essencial fornecer informações completas e acessíveis, adotar medidas como pseudonimização, controle de acesso, RIPD e revisão periódica. A atuação deve ser ética, transparente e proporcional, conforme a LGPD e o ECA.", "940714": "O tratamento de dados biométricos de crianças e adolescentes deve seguir critérios rigorosos, com consentimento específico e destacado de ao menos um responsável legal, em linguagem clara e acessível. Deve-se demonstrar o melhor interesse do menor, com justificativa documentada da necessidade, como verificação de idade para proteção. É essencial garantir transparência, proibir perfilamento automatizado e assegurar que a biometria seja a única forma viável para cumprir obrigações legais. Medidas adicionais incluem interfaces amigáveis para exercício de direitos, RIPD específicos para menores e política de privacidade infantil separada e acessível.

Contribuinte: CLARA CAROLINE OLIVEIRA DA CRUZ

Número: OP-1005627

Data: 01/08/2025 - 07:46

Resumo: : "Conexis: Com base na LGPD (art. 5º, II), dados biométricos são aqueles ligados a características físicas, fisiológicas ou comportamentais de uma pessoa natural, tratados por meios técnicos com o objetivo de identificá-la de modo único. Imagens, gravações ou registros brutos não são, por si, dados biométricos, apenas se processados por tecnologias específicas (ex: softwares de reconhecimento facial ou de voz). Assim, a fotografia não é biométrica, mas os pontos extraídos dela, sim. O mesmo se aplica à análise de voz por IA para identificação. Essa definição, alinhada a autoridades como o INAI (México), o ICO (Reino Unido) e a legislação chilena, garante segurança jurídica e flexibilidade interpretativa, desde que respeitados os princípios da LGPD e o contexto de uso. Ainda, destaca-se que a caracterização como dado biométrico requer, cumulativamente: origem em característica

singular; tratamento técnico específico; e finalidade de identificação ou autenticação, conforme LGPD e GDPR. ", "940688": "Conexis Brasil Digital: A transparência deve permitir que o titular compreenda, com clareza e antecedência, como seus dados serão tratados. Isso inclui o fornecimento de informações sobre as finalidades, hipóteses legais, responsabilidades dos agentes de tratamento, canais de atendimento, bem como os direitos assegurados pela LGPD. Também devem ser indicadas eventuais consequências da não autorização ou do fornecimento de dados incompletos. O conteúdo deve estar em linguagem acessível e compatível com o perfil do público-alvo, podendo ser adaptado conforme o meio de comunicação utilizado.", "940690": "Conexis Brasil Digital: A LGPD não distingue entre modalidades biométricas, razão pela qual eventual regulamentação não deve criar obrigações distintas sem respaldo legal, sob pena de violação ao princípio da legalidade. Biometrias faciais, vocais e comportamentais devem ser tratadas com o mesmo rigor, considerando riscos e salvaguardas. A biometria comportamental, por sua natureza dinâmica e coleta muitas vezes contínua, exige validação periódica, mitigação de viés e medidas específicas de segurança, como proteção contra replay e segmentação lógica de bases. Defende-se regulamentação uniforme quanto aos princípios, com requisitos proporcionais à complexidade técnica, assegurando governança flexível, avaliação de impacto quando aplicável, canal de contestação e transparência sobre acurácia. O equilíbrio entre proteção de dados e inovação deve guiar a abordagem regulatória, sem criar barreiras indevidas ao uso ético e seguro dessas tecnologias.", "940693": "Conexis Brasil Digital: Embora previsto na LGPD, o consentimento nem sempre será a base legal adequada para o tratamento de dados biométricos. Seu uso exige manifestação livre, informada, destacada, específica e inequívoca — requisitos que não se cumprem quando não há alternativa viável, como em processos de prevenção a fraudes, autenticação cadastral, segurança pública ou serviços essenciais. Nesses casos, a recusa inviabilizaria a atividade ou aumentaria riscos a terceiros, tornando necessário o uso de bases legais alternativas, como obrigação legal/regulatória.", "940695": "Conexis Brasil Digital: No setor de telecomunicações, o uso de biometria para prevenção à fraude encontra respaldo no art. 11, II, “g”, da LGPD, desde que observados critérios de necessidade, proporcionalidade e segurança. Relatórios de impacto e mecanismos de transparência fortalecem a legitimidade da prática. A biometria atua como fator adicional em modelos de autenticação em camadas, sendo essencial para proteger consumidores de fraudes cada vez mais sofisticadas. A documentação de riscos e justificativas técnicas é recomendável para demonstrar conformidade e evitar retrocessos na segurança jurídica e operacional dos serviços.", "940697": "Conexis Brasil Digital: A biometria facial pode ser legitimamente enquadrada na base legal do art. 11, II, “a” da LGPD sempre que for meio razoável e proporcional ao cumprimento de obrigação legal ou regulatória, como previsto na Resolução Anatel 738/2020, que impõe deveres específicos de prevenção a fraudes. A adoção da biometria para validação de identidade em habilitação, portabilidade e troca de titularidade é compatível com esse fim. Para isso, o controlador deve comprovar a base normativa, limitar o uso à finalidade legal, aplicar medidas de segurança adequadas (como por exemplo: criptografia, controle de acesso, retenção mínima) e garantir os direitos dos titulares. Essa abordagem assegura segurança jurídica, protege os titulares e garante harmonia entre a LGPD e a regulação setorial.", "940699": "Conexis Brasil Digital: O uso de dados biométricos em

pesquisas deve respeitar os princípios da LGPD, especialmente diante do risco de reidentificação. Técnicas de anonimização ou pseudonimização devem ser tecnicamente robustas, com barreiras reais à reidentificação e proibição de cruzamentos não controlados. Recomenda-se ainda a adoção de termos de responsabilidade, protocolos éticos quando aplicável, medidas contratuais e segurança da informação proporcional ao risco. As organizações de pesquisa devem ter flexibilidade para definir salvaguardas adequadas ao seu contexto, desde que alinhadas à proteção dos titulares. A regulamentação deve evitar impor exigências que desestimulem a pesquisa científica legítima, preservando a autonomia dos institutos de pesquisa e garantindo, ao mesmo tempo, o tratamento ético e seguro dos dados biométricos.", "940700": "Conexis Brasil Digital: A fim de garantir o uso responsável do reconhecimento facial, é essencial adotar medidas que assegurem transparência, necessidade e não discriminação. A transparência deve ser proporcional ao contexto: quando o uso da biometria é prática consolidada e esperada, como na autenticação de identidade no setor de telecomunicações, é suficiente o fornecimento do Aviso de Privacidade em pontos de contato com o titular. A necessidade e proporcionalidade exigem justificativa técnica de que a biometria é meio adequado frente a alternativas, com uso limitado à finalidade declarada. A adoção dessas salvaguardas garante o uso ético, seguro e juridicamente adequado da tecnologia, respeitando os princípios da LGPD.", "940701": "Conexis Brasil Digital: A promoção da qualidade dos sistemas de reconhecimento facial deve considerar práticas alinhadas ao contexto de uso, aos riscos envolvidos e à capacidade técnica de cada organização. As empresas devem ter autonomia para definir seus próprios parâmetros de desempenho e mecanismos de controle, adotando medidas que permitam acompanhar, revisar e aprimorar continuamente seus sistemas. A regulamentação deve priorizar diretrizes principiológicas que incentivem a melhoria contínua e a mitigação de falhas, evitando a imposição de requisitos técnicos rígidos que possam comprometer a inovação, a proporcionalidade e a efetividade das soluções.", "940702": "Conexis Brasil Digital: O reconhecimento facial é uma ferramenta tecnológica eficaz e legítima para fins de autenticação e segurança, podendo ser adotada pelas organizações conforme a análise de viabilidade técnica, eficácia, riscos e contexto de aplicação. As operadoras devem ter autonomia para avaliar quando essa tecnologia é a mais apropriada, considerando a natureza do serviço, os objetivos da aplicação e os princípios da LGPD, como necessidade, minimização e não discriminação.", "940704": "Conexis Brasil Digital: Entendemos que as organizações devem ter flexibilidade para implementar medidas de segurança proporcionais ao seu porte, volume de dados tratados e riscos específicos de suas operações. A proteção de dados biométricos deve seguir uma abordagem baseada em risco, considerando a sensibilidade da aplicação e a escala do tratamento. Medidas técnicas e organizacionais adequadas devem ser adotadas conforme o contexto, respeitando os princípios da proporcionalidade e da efetividade. A definição dessas medidas deve observar as boas práticas de cibersegurança, sem impor exigências padronizadas e rígidas que possam gerar custos desnecessários, sem ganhos proporcionais em segurança.", "940707": "Conexis Brasil Digital: Além das salvaguardas contra discriminação, é importante que a acessibilidade das soluções tecnológicas seja considerada no desenho de processos de verificação. A decisão sobre oferecer métodos alternativos à biometria deve levar em conta a viabilidade técnica, a

eficácia prática dessas alternativas — que muitas vezes não possuem o mesmo nível de segurança — e os riscos envolvidos. A regulamentação deve preservar a autonomia das empresas para adotar as soluções tecnológicas que melhor equilibrem proteção dos usuários, prevenção a fraudes e continuidade operacional.", "940708": "Conexis Brasil Digital: Retomamos as respostas dos questionamentos 2, 5, 8 e 11, reforçando a importância da avaliação de riscos de cibersegurança e dos controles recomendados por autoridades como ICO e INAI, incluindo governança interna, privacy by design, limitação de finalidade e auditoria contínua. Quanto à transparência, o fornecimento do Aviso de Privacidade, considerando o contexto do setor de telecomunicações e obrigações regulatórias da ANATEL, é suficiente para atender ao art. 9º da LGPD, sem exigir práticas excessivas. Para evitar discriminação, recomenda-se a adoção de mecanismos éticos e técnicos alinhados ao posicionamento do ICO. As organizações devem integrar a governança de dados biométricos às suas políticas gerais de proteção de dados, usando estruturas já existentes, como o DPO, evitando burocracia desnecessária e custos operacionais sem valor agregado.", "940709": "Conexis Brasil Digital: No tratamento de dados biométricos no setor de telecomunicações, recomenda-se que as operadoras adotem práticas de transparência e segurança compatíveis com seu contexto operacional e com os riscos envolvidos. Tais medidas devem estar alinhadas à LGPD, às diretrizes da Anatel e às políticas internas de governança e proteção de dados, buscando assegurar o equilíbrio entre a proteção dos titulares e a viabilidade técnica e econômica da operação. A definição dos mecanismos de transparência, comunicação e descarte de dados deve observar critérios de proporcionalidade e adequação à realidade de cada empresa.", "940710": "Conexis Brasil Digital: Além das práticas de transparência já mencionadas, o atendimento aos direitos dos titulares no tratamento de dados biométricos deve considerar as especificidades desse tipo de dado e ser estruturado de forma proporcional ao porte, volume e contexto das operações de cada empresa. As instituições devem assegurar meios adequados para que os titulares exerçam seus direitos, com informações claras, acessíveis e alinhadas ao nível de maturidade dos seus canais de relacionamento e capacidade operacional.", "940711": "Conexis Brasil Digital: Entendemos que o uso de biometria em ambientes educacionais pode ser justificado quando visa à segurança e proteção das crianças e o vínculo com o melhor interesse da criança, conforme o art. 14 da LGPD. É fundamental aplicar a minimização de dados e realizar avaliação contínua dos riscos e finalidades educacionais ou protetivas. As instituições devem ter flexibilidade para comunicar-se com pais e responsáveis pelos canais já utilizados e avaliar a necessidade do uso da biometria conforme sua realidade específica, implementando medidas de proteção proporcionais ao seu porte e recursos. Ressaltamos a importância de evitar requisitos que inviabilizem o uso legítimo da tecnologia, especialmente para instituições de menor porte.", "940712": "Conexis Brasil Digital: Deve-se permitir flexibilidade para que as instituições escolham a base legal mais adequada ao seu contexto e adotem soluções tecnológicas proporcionais aos riscos envolvidos, considerando sua estrutura e capacidade. A comunicação com os usuários deve ser clara e apropriada ao público-alvo, sempre com foco na proteção de crianças e adolescentes e na adoção de medidas menos intrusivas sempre que possível.", "940714": "Conexis Brasil Digital: Entendemos que o uso de dados biométricos para verificação de idade é uma solução tecnológica importante e eficaz

para proteger crianças e adolescentes no ambiente digital, desde que observados os princípios de proporcionalidade, minimização e anonimização quando possível, com exclusão imediata após verificação. Alternativas técnicas menos invasivas devem ser priorizadas. As empresas devem ter autonomia para implementar soluções adequadas aos riscos específicos de suas plataformas, evitando uma padronização única que pode não ser adequada a todos os serviços. A verificação eficaz da idade é fundamental para proteger menores de conteúdos inadequados, e a biometria pode ser legítima quando usada com as salvaguardas adequadas, sempre alinhada ao princípio do melhor interesse dos menores.

Contribuinte: Jonathan Naves Palhares

Número: OP-1005635

Data: 01/08/2025 - 07:52

Resumo: "As respostas aos quesitos são apresentadas em nome da FecomercioSP e complementadas por relatório encaminhado por e-mail. Com base no entendimento da Autoridade de Proteção de Dados do México (INAI), EDPB e do art. 16 ter da Lei de Proteção de Dados Chilena, consideram-se dados biométricos aqueles que, cumulativamente, atenda aos seguintes requisitos: (a) estejam relacionados a características físicas, fisiológicas, comportamentais ou traços de personalidade de um titular de dados; e (b) resultem de um tratamento específico (em regra, uma forma de medição), cuja finalidade seja identificar, de maneira única, o titular. Dessa forma, imagens captadas em vídeo, fotografias, gravações de voz ou dados semelhantes não devem ser, em si mesmos, considerados dados biométricos. Em outras palavras, dados sobre a fisionomia ou outras características biológicas de alguém somente são dados pessoais sensíveis quando usados para identificação desta pessoa no mundo real. ", "940688": "Conforme a Autoridade de Dados do Reino Unido (ICO), não há método único aplicável a todos os casos para garantir a transparência. A forma mais adequada de ser transparente ao titular quanto ao uso de seus dados biométricos deverá ponderar fatores, como: i) o caso de uso; ii) relação com o titular; e iii) dados envolvidos. Nesse sentido, quanto mais óbvia a atividade de tratamento em análise, considerando as práticas habituais de mercado e a natureza do relacionamento com o titular, menor a exigência de práticas ativas de transparência. Exemplos: (a) se câmeras em espaço acessível ao público coletam dados biométricos, sem relação prévia com o titular, é razoável requerer a adoção de avisos visíveis e acessíveis, como placas informativas antes da entrada, modelo aceito pela ANPD (Nota Técnica nº 29/2024, §6.1.4); (b) Na validação de identidade para abertura de conta, em que a coleta é previsível, o aviso de privacidade durante a jornada do usuário atende ao dever de transparência. ", "940690": "É essencial avaliar cuidadosamente se e quando os dados comportamentais devem ser qualificados como dados biométricos, porque características comportamentais nem sempre apresentam a estabilidade ou a exclusividade necessária para identificação confiável. O escopo da definição deve ser limitado àqueles casos em que o tratamento possui o propósito de identificar alguém de forma exclusiva, de modo a evitar a captura de ampla gama de dados não identificadores. Dito isso, mesmo nessas hipóteses, não existem obrigações legais específicas que distinguem as diferentes

modalidades de biometria facial, não podendo eventual regulamentação sobre a legislação criar uma obrigação distinta, onde a legislação não a traz, o que implicaria em violação do princípio da legalidade. Nesse sentido, apesar de tanto a INAI, quanto o ICO diferenciarem dados biométricos físicos e fisiológicos daqueles comportamentais, nenhuma das autoridades traz obrigações específicas aplicáveis de forma diversa. ", "940693": "Para ser válido, o consentimento deve ser: (a) livre, ou seja, o titular deve poder negar ou revogar sem prejuízo, salvo quando a biometria for essencial e não houver outra base legal. Devem existir alternativas sem uso de biometria, exceto se esta for necessária ao serviço. Incentivos não invalidam o consentimento, desde que se atendam aos requisitos de validade; (b) informado, fornecendo-se ao titular as informações requeridas pelo art. 9º, da LGPD; (c) inequívoco, requerendo manifestação ativa de vontade; (d) específico, com consentimento separado para cada finalidade, salvo se eventuais usos adicionais se enquadrarem em base legal distinta do consentimento; e (e) destacado, com ênfase nas informações sobre o tratamento de dados sensíveis. O consentimento não é adequado quando esses quesitos de validade não forem satisfeitos, como em contextos em que inexistente relação direta com o titular, como no monitoramento de espaços públicos.", "940695": "A hipótese legal de “garantia da prevenção à fraude” deve ser interpretada de forma abrangente, de modo a incluir o uso de dados biométricos de qualquer forma que proteja, previna ou permita a investigação de possíveis ações ilegais que envolvam práticas de roubo de identidade ou assemelhadas que demandem a autenticação do indivíduo. Conforme Guia sobre o Legítimo Interesse, aplicam-se a “prevenção à fraudes” os critérios do Teste de Balanceamento do legítimo interesse, exceto a vedação ao tratamento de dados sensíveis.", "940697": "Em relação às salvaguardas a serem adotadas para mitigação de riscos, entendemos que devem ser as mesmas apontadas no quesito nº 5, sempre que possível no caso concreto. Isso porque as medidas de proteção de dados devem ser proporcionais aos riscos envolvidos, independentemente da base legal utilizada para justificar o tratamento. Quanto aos critérios para o enquadramento do tratamento de dados biométricos na base legal do art. 11, II, “a”, da LGPD, entendemos que este não deve ser limitado às raras hipóteses em que a regulação expressamente comanda o tratamento de dados biométricos, devendo abranger também aquelas situações em que o tratamento de dados biométricos é meio razoável de se conformar com as normas legais. O poder público deve adotar medidas de transparência para garantir os direitos dos titulares, mesmo sem relação direta com estes.", "940699": "A anonimização não é requisito para a realização de estudos por órgãos de pesquisa, conforme posição desta ANPD, em seu guia sobre atividades de tratamento desta natureza. Deste modo, o termo “necessária” empregado no questionamento não é aplicável, pois não sendo a anonimização mandatória, não é obrigatória a adoção de medidas adicionais em razão do risco de reidentificação. Feita essa consideração, o que deve ser avaliado não é a existência do risco de reidentificação afinal, a própria ANPD já reconheceu, em seu Estudo Preliminar sobre Anonimização, que tal risco está sempre presente –, mas o grau desse risco e as medidas técnicas e organizacionais adotadas para reduzi-lo a nível aceitável. As medidas a serem adotadas devem, portanto, ser proporcionais ao risco concreto de reidentificação. Fundamental avaliar a adoção de mecanismos que assegurem a irreversibilidade e a não vinculabilidade (unlinkability) dos templates biométricos.", "940700": "Em relação aos quesitos de transparência, aplicam-se as

considerações já apresentadas no quesito nº 2. Quanto ao princípio da necessidade, ele não se refere a absoluta essencialidade, mas à necessidade de que a atividade de tratamento seja “uma forma direcionada e proporcional” de alcançar a sua finalidade, como leciona o ICO. Com base no guia da INAI, o controlador deve considerar os seguintes cuidados: a) sendo possível, descartar as amostras biométricas, armazenando apenas os templates gerados, que serão utilizados para comparações futuras; b) limitar o volume de amostras coletadas, por meio de amostras de melhor qualidade. Para mitigar vieses discriminatórios, uma série de medidas podem ser implementadas, como garantir diversidade étnica e de gênero nos dados de treino e testar a presença de vieses. Um conjunto abrangente de medidas a serem consideradas foram incluídas no relatório complementar. ", "940701": "As medidas voltadas à garantia da eficácia e confiabilidade de sistemas de reconhecimento facial devem ser proporcionais aos riscos concretos associados à sua utilização, considerando-se as distintas etapas do ciclo de vida da solução — por se tratar de uma tecnologia de inteligência artificial. Para tanto, com base no Guia de IA do ICO, elencamos, no relatório complementar uma série de medidas a serem consideradas para cada etapa do ciclo de vida do sistema, por exemplo, na fase de planejamento, definir um nível mínimo de acuracidade estatística e na fase de seleção de dados, assegurar que os dados sejam adequadamente representativos, completos, exatos e corretamente rotulados. Tais medidas, destacamos, devem ser compreendidas como recomendações a serem consideradas, conforme a avaliação de risco do sistema em questão, e não como exigências obrigatórias ou universais. ", "940702": "O reconhecimento facial não será mecanismo apropriado quando os benefícios, e o bem jurídico, que a aplicação de reconhecimento facial almeja resguardar não for proporcional aos riscos aos direitos e liberdades aos titulares afetados. Em relação às tecnologias alternativas, existem outras informações que podem ser utilizadas como apoio ou em substituição ao reconhecimento facial, sempre de acordo com o caso concreto. Por exemplo, o uso da digital para acesso a instalações. Outro mecanismo útil na prevenção de fraudes é a utilização de dados provenientes do setor de telecomunicações. Para que as organizações possam, quando apropriado e considerando os riscos envolvidos, adotar mecanismos alternativos ao reconhecimento facial, é fundamental que a ANPD promova a construção de um ecossistema regulatório que estimule a pesquisa e o desenvolvimento de soluções seguras e eficazes, o que só é possível pela flexibilidade do controlador de adaptar suas práticas a diferentes casos concretos. ", "940704": "Em relação ao primeiro questionamento (isto é, quais boas práticas devem ser observadas para garantir que a limitação não configure discriminação ilícita ou abusiva), reiteramos os pontos já descritos no quesito nº 8. Em relação as medidas de segurança essenciais, aplicam-se as salvaguardas mais relevantes apontadas no quesito nº 5. Em relação aos parâmetros a serem adotados para a gestão de riscos de segurança, não entendemos existir diferença das práticas adotadas para outros cenários de cibersegurança. Nesse sentido, com base na ISO/27005, os parâmetros básicos são: (a) definir critério de riscos; (b) identificar os riscos; (c) analisar os riscos; (d) tomar decisão sobre os riscos; (e) monitorar os riscos. Descrevemos, no relatório complementar, cada um desses parâmetros e realizamos considerações específicas em relação a dados biométricos. ", "940707": "Em relação ao primeiro ponto, além das medidas indicadas no quesito nº 8, é essencial considerar a acessibilidade da ferramenta utilizada. Quanto ao tratamento baseado no consentimento,

entendemos que a negativa à coleta de dados biométricos pode impedir o uso de funcionalidades que dependam efetivamente desse tratamento. Por outro lado, não é admissível condicionar o acesso a serviços cuja operação não requeira, de fato, biometria. Nas demais situações, a recusa configura exercício de fato do direito de oposição. Assim, o não oferecimento da funcionalidade será lícito se: (a) for tecnicamente inviável sua disponibilização sem o tratamento biométrico, conforme já mencionado; ou (b) os direitos e interesses resguardados pela exigência de biometria forem legítimos e prevalentes sobre a recusa do titular – por exemplo, quando há bem juridicamente relevante a ser protegido.

","940708": "Retomamos as respostas já oferecidas aos quesitos nºs 2, 5, 8 e 11. Sobre os mecanismos de proteção, além da avaliação de riscos de cibersegurança (quesito nº 11), reforçamos os controles indicados no quesito nº 8, com base em guias de autoridades como ICO, INAI e a Autoridade de Dados da Coreia. Quanto à transparência, a obrigação legal limita-se ao fornecimento das informações do art. 9º da LGPD. A forma de disponibilização, conforme o quesito nº 2 e o posicionamento do ICO, dependerá do caso de uso, da relação com o titular e das características do tratamento. Quanto mais evidente a atividade de tratamento, menor será a exigência de práticas ativas de transparência. Por fim, a adoção de privacy-enhancing technologies, ainda que não obrigatória, deve ser incentivada, com destaque para técnicas como privacidade diferencial, SMPC e criptografia homomórfica. Por fim, quanto ao risco de discriminação, reitera-se o previsto no quesito nº 8, com base no posicionamento do ICO.

","940709": "Em relação ao direito de informação, conforme já destacado no quesito nº 2, em contextos nos quais não há expectativa razoável por parte dos titulares quanto à coleta de seus dados biométricos, e nem relação prévia entre os titulares e a empresa controladora, é exigido esforço adicional no cumprimento do dever de transparência. Esse dever pode ser atendido, por exemplo, por meio da instalação de placas em locais de fácil visualização contendo informações gerais sobre a atividade de tratamento, além da indicação dos meios para obtenção de informações mais detalhadas e para o exercício dos direitos dos titulares. Igualmente, podem ser disponibilizados em locais fixos QR Codes, que direcionam para a Política de Privacidade da organização, a qual deve conter as informações elencadas na legislação. Situação semelhante já foi analisada por esta Autoridade, que entendeu como adequadas essas providências de transparência, conforme consta da Nota Técnica nº 29/2024/FIS/CGF/ANPD, §6.1.4.

","940710": "Além das práticas de transparência já tratadas, o atendimento aos direitos dos titulares deve considerar as particularidades da biometria: 1.Quanto ao direito de acesso, conforme o ICO, os dados biométricos geralmente são outputs matemáticos ilegíveis para seres humanos. Assim, o fornecimento pode ser substituído por declaração que: (a) justifique a impossibilidade de entrega direta; (b) descreva a natureza do dado; e (c) esclareça como é armazenado. Isso não impede o acesso a outros dados vinculados, como CPF ou amostras, se houver. 2.O direito de correção não se aplica à correspondência probabilística, mas pode ser exercido se houver erro na associação do template ou alteração física relevante. Para isso, os templates devem ser revogáveis e renováveis. 3.A revogação do consentimento também requer templates revogáveis, mas não implica exclusão de registros pretéritos, que podem ser mantidos para fins legítimos, como obrigação legal, preservação de evidências ou segurança.

","940711": "Nos termos do Enunciado CD/ANPD nº 1/2023, o tratamento de dados pessoais de crianças e adolescentes

pode se basear em qualquer das hipóteses legais do art. 11, da LGPD, desde que observados os requisitos legais e assegurado o melhor interesse do menor. Assim, o uso de biometria pode se apoiar em qualquer base legal do dispositivo, desde que adequadamente enquadrado. Quanto à transparência e participação dos responsáveis, é recomendável se considerar, quando viável: comunicação formal aos responsáveis com informações claras sobre a atividade de tratamento; indicação de canais de contato; e, se aplicável, meios acessíveis para exercício do direito de oposição. A avaliação do melhor interesse deve ser casuística, considerando: a) o bem jurídico protegido; b) a existência de alternativas menos intrusivas; e c) a volatilidade de certas informações biométricas infantojuvenis. ", "940712": "Em relação às hipóteses legais e a participação informada dos pais e responsáveis, aplica-se o já descrito no quesito de nº 16. Isto é: · Em relação às hipóteses legais: conforme reconhecido pela ANPD no Enunciado CD/ANPD nº 1/2023, o tratamento de dados pessoais de crianças e adolescentes pode se basear em qualquer das hipóteses legais do art. 11, da LGPD, desde que respeite, de forma prioritária, o melhor interesse do menor. · Em relação às informações a serem prestadas: além de fornecer informações no aviso de privacidade da organização, é importante que, sendo viável, se avalie realizar a comunicação formal dos pais e responsáveis, oferecendo as informações essenciais da atividade de tratamento e os mecanismos para o exercício de direitos. Por fim, no tocante às medidas de segurança, aplicam-se as diretrizes já estabelecidas nos quesitos nºs 5 e 11. ", "940714": "A adoção de mecanismos de verificação de idade deve considerar: (a) o contexto específico da verificação; (b) a acuracidade da tecnologia empregada; e (c) a existência de meios menos intrusivos com eficácia equivalente. O relatório complementar contém uma exposição desses requisitos. O contexto é essencial para avaliar a proporcionalidade da biometria com base no princípio da necessidade e no melhor interesse do menor. Conforme o ICO, a técnica deve ser proporcional aos riscos envolvidos. Por exemplo, biometria facial pode ser adequada para impedir o acesso de menores a conteúdos sensíveis, mas desnecessária para fins como recebimento de newsletters. A existência de meios menos invasivos, como autodeclaração ou verificação via cartão de crédito, também deve ser considerada. Nesse sentido, a escolha pela biometria deve ser ponderada, considerando riscos, eficácia, escalabilidade e o melhor interesse da criança ou adolescente.

Contribuinte: Jean Michel Duarte Santana

Número: OP-1005673

Data: 01/08/2025 - 08:41

Resumo: : "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940688": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940690": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940693": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940695": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940697": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940699": "Ante a limitação de caracteres, a

resposta foi encaminhada em documento via email. ", "940700": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940701": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940702": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940704": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940707": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940708": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940709": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940710": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940711": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940712": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email. ", "940714": "Ante a limitação de caracteres, a resposta foi encaminhada em documento via email.

Contribuinte: DEBORAH CRISTINA COURI

Número: OP-1005679

Data: 01/08/2025 - 08:49

Resumo: "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) A LGPD carece de uma definição clara de "dados biométricos" (Art. 5, II), sendo crucial alinhar a interpretação a padrões internacionais (GDPR, EDPB, ICO). Sugerimos três critérios cumulativos para tal qualificação: Características inerentes: Dados derivados de traços físicos, fisiológicos ou comportamentais. Processamento técnico específico: Uso de tecnologia para extrair ou converter essas características (medidas/templates). Finalidade de identificação/autenticação: O uso deve visar identificar ou autenticar o titular. A mera captura de características humanas não implica tratamento biométrico sensível sem a finalidade de identificação. Atividades como detecção de presença ou contagem de pedestres, sem identificação, não deveriam ser classificadas como dados biométricos. Adotar essa interpretação garante segurança jurídica e promove o uso responsável de tecnologias, focando a regulação onde o risco é maior. Para uma análise completa", "940688": "", "940690": "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) A biometria comportamental (voz, padrões de digitação, movimento ocular) deve ser tratada com os mesmos três critérios essenciais aplicados à biometria tradicional internacionalmente (explicados na pergunta 1): referência a características inerentes, processamento técnico específico e finalidade de identificação/autenticação. A mera coleta de comportamentos não os torna dados biométricos sensíveis. Um elemento crucial é a imutabilidade relativa da característica. Enquanto voz ou marcha, baseadas em padrões corporais estáveis, podem ser consideradas biométricas, comportamentos voluntários e facilmente modificáveis (ex: hábitos de consumo, preferências de navegação) não se qualificam. Assim, o método de processamento e a finalidade de uso são cruciais para evitar interpretações amplas e desproporcionais, garantindo assim o equilíbrio entre proteção de

dados e inovação tecnológica. Para uma análise completa, por favor, consultem a submissão do", "940693": "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) Para o consentimento biométrico ser conforme a LGPD, o titular deve compreender a finalidade e expressar sua vontade autonomamente, sem coerção. A oferta de serviço por consentimento é válida desde que haja transparência e ausência de desvantagens desproporcionais ou discriminatórias. O dinamismo do ecossistema digital permite ao titular exercer sua autodeterminação, escolhendo serviços que se alinhem às suas preferências. Consentimento pode ser inadequado em desequilíbrios estruturais (ex.: governo-cidadão) ou quando recusas causam prejuízo desproporcional. Nesses casos, outras bases legais devem ser usadas. É vital que a ANPD reconheça as particularidades do consentimento na economia digital, para evitar abordagens restritivas que afetem modelos legítimos, de maneira a equilibrar a proteção de direitos e inovação. Para análise completa, consulte a submissão do ITI enviada via e-mail.", "940695": "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) O uso de biometria para prevenção de fraudes é legítimo e essencial (Art. 11, II, "g" LGPD), especialmente dado o alto índice de golpes no Brasil. Frequentemente, é a forma mais segura e menos invasiva de proteger usuários e o sistema financeiro. Essa base legal da LGPD representa um avanço em relação ao GDPR. O tratamento biométrico, com salvaguardas robustas (minimização, segurança, governança e avaliação de impacto), é socialmente desejável e atua como um mecanismo de inclusão digital ao garantir acesso seguro a serviços essenciais. Considerando a realidade nacional e a proteção contra ameaças sistêmicas, o tratamento de dados biométricos para prevenção de fraudes deve ser reconhecido como legítimo, necessário e proporcional, conciliando direitos individuais com a segurança das relações sociais e econômicas. Para uma análise completa, por favor consultem a submissão do ITI enviada via e-mail.", "940697": "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) Ao processar dados biométricos para cumprimento de obrigação legal ou regulatória, os controladores, especialmente entidades públicas, devem aderir rigorosamente aos princípios da LGPD para mitigar riscos e garantir os direitos dos titulares. Essencialmente, o processamento deve ser guiado pela finalidade, onde o uso da biometria deve estar diretamente vinculado à obrigação legal/regulatória específica, sendo proibido para outros fins. Além disso, a necessidade exige que se comprove que o dado biométrico é estritamente indispensável para a obrigação, e que o objetivo não seria atingido por meios menos invasivos. Complementarmente, a minimização impõe coletar e processar apenas a informação biométrica indispensável, evitando excessos. Adicionalmente, medidas técnicas e administrativas robustas são cruciais para a segurança desses dados sensíveis. Para uma análise completa, por favor consultem a submissão do ITI enviada via e-mail.", "940699": "", "940700": "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) O uso de reconhecimento facial, mesmo legalmente amparado pela LGPD, exige rigorosa observância dos princípios de necessidade, proporcionalidade, transparência e não discriminação. Em cenários como prevenção de fraudes em sistemas financeiros e serviços digitais, a biometria pode ser crucial para segurança e integridade operacional, desde que proporcional ao risco e com salvaguardas adequadas. O princípio da necessidade limita o uso ao indispensável para a finalidade original, sem desvios. A proporcionalidade requer que os benefícios coletivos (ex: segurança, estabilidade econômica) superem os impactos aos

direitos dos titulares. A transparência impõe informação clara sobre coleta e uso, assegurando os direitos da LGPD. Em suma, o reconhecimento facial é legítimo na prevenção de fraudes se pautado por critérios técnicos, legais e éticos que protejam direitos e evitem abusos. Para análise completa, consulte a submissão do ITI via e-mail. ", "940701": "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) Sistemas de reconhecimento facial devem ser concebidos sob o princípio de privacidade desde a concepção (privacy-by-design). Seu treinamento exige bases de dados amplas e diversas, representativas da população, para alta precisão e minimização de erros e vieses. O processamento de dados biométricos não identificáveis (não pessoais sob a LGPD), como dados anonimizados, é crucial para o aprimoramento e a eficácia desses sistemas. A ANPD deve reconhecer expressamente esta premissa, garantindo segurança jurídica ao desenvolvimento tecnológico responsável e à proteção de dados, sem restrições desproporcionais ao uso de informações não pessoais. Para análise completa, consultem a submissão do ITI via e-mail.", "940702": "", "940704": "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) Diante do alto potencial de dano decorrente de vazamentos de dados biométricos, como em casos de roubo de identidade, é crucial que medidas técnicas e administrativas robustas sejam adotadas. O setor de tecnologia já incorpora segurança avançada desde o desenvolvimento, incluindo criptografia, anonimização, controle de acesso e rastreabilidade. Muitas empresas aplicam privacy by design, processando biometria para padrões e calibração, sem reidentificação, o que reduz riscos à privacidade. Para garantir a conformidade com a LGPD, é essencial que organizações adotem parâmetros mínimos para avaliação contínua de riscos via Relatórios de Impacto à Proteção de Dados (RIPDs) e monitoramento de vies e falhas de segurança. Políticas internas claras, treinamento e governança ativa garantem o tratamento responsável. Isso prova que inovação e proteção de dados podem coexistir. Para análise completa, consultem a submissão da ITI enviada via e-mail. ", "940707": "", "940708": "", "940709": "", "940710": "INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI) O setor de tecnologia avançou significativamente na garantia dos direitos dos titulares, mesmo em contextos complexos como no tratamento automatizado de dados biométricos. Empresas de tecnologia adotam medidas técnicas e organizacionais que facilitam o exercício dos direitos da LGPD (informação, acesso, correção, revogação de consentimento) via interfaces amigáveis e canais digitais eficientes. O setor investe em soluções para promover a transparência, que incluem painéis de controle e logs de acesso e outros recursos para que titulares gerenciem dados autonomamente. Na biometria, salvaguardas como privacy-by-design, uso de dados pseudonimizados para treinamento e revisão humana de decisões automatizadas são incorporadas, demonstrando compromisso com o uso ético e seguro da tecnologia, protegendo dados sem comprometer a inovação. Para análise completa, consultem a submissão do ITI enviada via e-mail.", "940711": "", "940712": "", "940714": "

Contribuinte: HUSANI DURANS DE JESUS

Data: 01/08/2025 - 09:30

Resumo: "Recomenda-se utilizar a definição apresentada pela ANPD no Radar tecnológico 02: características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitam confirmar a identificação dessa pessoa, como dados faciais, voz, íris, assinatura, modo de andar ou impressões digitais. ", "940688": "A LGPD (art. 4º, §2º) estabelece que pessoas jurídicas de direito privado não podem realizar a totalidade do tratamento de dados pessoais para fins de segurança pública, persecução penal, defesa nacional e segurança do Estado. Nesses casos, o órgão público responsável deve notificar a ANPD e tutelar o tratamento realizado por entes privados. Essa regra justifica, por exemplo, a emissão de nota técnica pela ANPD no âmbito do projeto Estádio Seguro. A finalidade do tratamento deve ser sempre clara e informada, respeitando o princípio da transparência. Assim, os órgãos públicos devem disponibilizar, por meio de canal unificado, informações sobre a finalidade, agentes envolvidos, custos, bases legais, medidas de segurança e mitigação de riscos. Projetos como Smart Sampa e Câmera Interativa evidenciam fragilidades nesse processo, ao atribuir indevidamente a tutela dos dados a entes privados, ou omitir o papel de co-controladores, o que fere os princípios da LGPD e direitos de titulares.", "940690": "Biometrias comportamentais devem ser tratadas com maior restrição, sobretudo quando aplicadas a políticas de repressão criminal e à gestão educacional. Em ambientes escolares, onde há tratamento de dados sensíveis de crianças e adolescentes, o princípio do melhor interesse deve ser observado de forma rigorosa, conforme alerta a ANPD (Radar nº 2). O uso dessas tecnologias levanta sérias preocupações éticas, pois além de erros técnicos frequentes, há o risco de rotulação indevida, vigilância excessiva e discriminação. Relatório da UFPR e PUC-PR sobre reconhecimento facial e de emoções em escolas destaca que expressões faciais são influenciadas por fatores culturais e biológicos, especialmente em adolescentes em desenvolvimento, o que compromete a precisão e justiça do uso desses dados. Soma-se a isso o risco de vazamento de dados sensíveis, muitas vezes controlados por empresas privadas, sem garantias adequadas de proteção, transparência ou responsabilização.", "940693": "O consentimento para o tratamento de dados biométricos só pode ser considerado válido quando for de fato livre, informado, específico, destacado e inequívoco, conforme determina a LGPD. Não é considerado livre quando há assimetria de poder, como no caso de políticas públicas em que o titular não tem alternativas reais – mesmo que a política traga benefícios aparentes. A ANPD, no Voto nº 1/2025 (Processo nº 00261.006742/2024-53), reforça que consentimentos obtidos sob pressão, compensações financeiras ou falta de informação clara são inválidos. Em contextos de larga escala, como em cidades inteligentes, o consentimento individual pode ser impraticável e inapropriado. Nesses casos, é essencial adotar salvaguardas como software livre, auditorias públicas, avaliação de proporcionalidade, relatórios de impacto com divulgação ampla, transparência em todo o ciclo do projeto, cláusulas contratuais robustas e medidas antidiscriminatórias que garantam o respeito aos direitos de titulares. ", "940695": "", "940697": "", "940699": "No tratamento de dados biométricos para fins de pesquisa (art. 11, II, “c”, da LGPD), mesmo quando se recorre à anonimização, é essencial observar rigorosamente os limites legais, especialmente diante dos riscos de reidentificação por meio do cruzamento de bases de dados. A possibilidade técnica de reidentificação exige que a anonimização seja robusta, contínua e atualizada frente às

novas capacidades analíticas. Além disso, a natureza jurídica da entidade pesquisadora deve ser considerada (art. 5º, XVIII da LGPD), exigindo controle e fiscalização quanto à finalidade e proporcionalidade do tratamento.", "940700": "É imprescindível o cumprimento do art. 4º, §§ 2º e 4º da LGPD quando entes privados participam de projetos que envolvem tratamento de dados para fins de segurança pública e persecução penal. A legislação determina que a atuação de pessoas jurídicas de direito privado nesse contexto seja limitada e tutelada, não podendo exercer o tratamento de forma autônoma. Tais entes devem comunicar a ANPD sobre suas atividades, assegurando transparência e prestação de contas. Exemplo positivo foi o do acordo entre MJSP e CBF, no projeto Estádio Seguro, com notificação à ANPD. Contudo, casos como o Câmera Interativa, na Bahia, e o Projeto Smart Sampa, em São Paulo, evidenciam falhas estruturais, como ausência de salvaguardas, transparência e controle social, além de possíveis ilegalidades em transferências de dados e co-responsabilidade mal definida. A ANPD deve reforçar sua atuação fiscalizatória, exigindo o cumprimento da LGPD como condição para a legalidade do uso dessas tecnologias.", "940701": "Sistemas de reconhecimento facial (TRFs) devem ser projetados desde sua concepção com base no princípio da "privacidade desde a concepção" (privacy by design), utilizando bases de dados diversas e representativas, com documentação transparente sobre a origem e a legalidade dos dados de treinamento. A conformidade com a LGPD exige atenção à base legal, à minimização de dados e à não discriminação. A eficácia e a confiabilidade dos sistemas passam também pela definição clara do seu propósito, com uso restrito a contextos que observem os princípios de necessidade, adequação e proporcionalidade. Devem ser implementados mecanismos robustos de monitoramento contínuo, auditoria independente, avaliação de impacto e correção imediata de falhas, sobretudo em casos de falsos positivos ou negativos. A participação social e o controle público são essenciais para garantir a legitimidade e a accountability desses sistemas, especialmente quando operam de forma automatizada.", "940702": "O uso de tecnologias de reconhecimento facial (TRFs) não deve ser admitido em contextos de segurança pública e persecução penal, devido ao alto índice de falsos positivos, viés discriminatório e riscos à privacidade. Estudos do LAPIN (2021, 2024, 2025) evidenciam que tais tecnologias, quando utilizadas de forma massiva e sem salvaguardas, aprofundam desigualdades e promovem cercamentos digitais sobre populações vulnerabilizadas. A implementação de TRFs em estádios, por exemplo, como previsto na Lei nº 14.597/2023, poderia ser substituída por tecnologias menos invasivas, como a leitura de impressões digitais. Além disso, é fundamental garantir avaliações de necessidade, proporcionalidade e transparência, com publicação de relatórios de impacto e mecanismos alternativos ao reconhecimento facial. Sempre que possível, o titular deve poder optar por outra forma de identificação, resguardando sua liberdade e dignidade informacional.", "940704": "", "940707": " Em regra, a recusa do titular em fornecer seus dados biométricos não deve resultar em limitação ou restrição de funcionalidades em serviços não essenciais. Meios alternativos de acesso devem ser garantidos. ", "940708": " LAPIN (2021) aponta que o fluxo informacional de dados deve ser levado em conta, de modo que todo o processamento de dados seja mapeado, protetivo e seguro, considerando em cada tratamento: finalidade, adequação, período e políticas de eliminação dos dados; além da metodologia privacy by design.", "940709": "Em regra, não é admissível o uso de dados biométricos para

fins de vigilância contínua e massiva, como em iniciativas de cidades inteligentes ou no monitoramento de multidões em espaços públicos. Tais usos violam os princípios da LGPD, especialmente os da finalidade, necessidade, proporcionalidade e da autodeterminação informativa. O tratamento automatizado e indiscriminado de dados sensíveis impõe riscos desproporcionais aos titulares, sem garantir meios efetivos de informação, consentimento ou controle. Nesses contextos, é essencial suspender ou evitar o uso de TRFs, priorizando alternativas menos invasivas. Quando excepcionalmente considerado, deve haver transparência ativa, participação deliberativa da população afetada, mecanismos de responsabilização e garantia de direitos. A autodeterminação só é efetiva se houver possibilidade real de contestação, alternativa de não adesão e controle público contínuo sobre os projetos (ARTIGO 19; INTERNETLAB; LAPIN, 2022). ", "940710": "Para garantir os direitos dos titulares, especialmente em tratamentos automatizados de dados biométricos, os agentes públicos devem implementar mecanismos participativos desde a concepção dos projetos, assegurando que a proteção dos direitos surja dessa interação contínua. A transparência ativa, o acesso facilitado aos dados e a possibilidade de correção e revogação do consentimento devem ser garantidos por meio de canais acessíveis e eficientes. Exemplos como a atuação do Conselho Nacional de Saúde (CNS) demonstram o fortalecimento do controle social e da participação coletiva, essenciais para legitimar e monitorar o uso de dados sensíveis. ", "940711": "Em regra, o tratamento de dados biométricos de crianças e adolescentes só é admissível quando não existirem métodos alternativos menos invasivos para identificação ou autenticação, respeitando sempre o princípio do melhor interesse (art. 14, LGPD). O uso de tecnologias como reconhecimento facial deve ser evitado em escolas e espaços recreativos, dada a vulnerabilidade dos titulares e os riscos éticos e técnicos envolvidos. A participação informada dos pais ou responsáveis é imprescindível, garantindo consentimento livre, informado e inequívoco, além de medidas rigorosas de proteção, transparência e fiscalização. ", "940712": "", "940714": "

Contribuinte: PEDRO DIOGO CARVALHO MONTEIRO

Número: OP-1005713

Data: 01/08/2025 - 09:39

Resumo: : "", "940688": "CAIDP recommends that data controllers should provide adequate and contestable information regarding the technology used (eg, AI), the type of data processed, and the possible risks to the rights and freedoms of data subjects, according to the LGPD and the UNESCO Recommendation on the Ethics of AI.I. ", "940690": "Behavioral biometrics pose unique risks due to continuous collection and context sensitivity. They must be subject to stricter safeguards and limits on retention and profiling. Red lines should ban covert use and application of surveillance, unitary scoring, and secret profiling.", "940693": "Consent must be obtained through clear, separate, and accessible channels, with no coercion or bundling. Consent cannot be considered adequate to justify biometric processing in employment, public access, or essential services, where power imbalance or lack of alternatives undermines voluntariness. ", "940695": "CAIDP urges Brazil

to establish clear requirements for independent impact assessments prior to the deployment of AI systems for fraud prevention. Safeguards should include purpose limitation, human oversight, redress rights, and bans on reuse.", "940697": "Brazil must establish clear red lines prohibiting uses of biometric data by public entities that violate human rights. Independent impact assessments before processing, provision of contestable information, as well as continuous monitoring and oversight are essential. ", "940699": "", "940700": "Real risks over promises. Necessity/Proportionality: FRTs only when essential for a legitimate aim, with minimal data collection Transparency: Clear & contestable information Non-Discrimination: fairness through testing and audits Safeguards: independent assessments, encryption, and ongoing monitoring ", "940701": "Design with diverse, high-quality datasets, regular bias and data quality audits, and testing. Ensure human oversight, error reporting, and rapid correction protocols. Provide contestable information, and continuous monitoring to minimise and address identification errors. ", "940702": "International best practices and regulatory guidance advise prohibitions for FRT use in mass public surveillance, biometric categorization, predictive policing, emotion recognition, social scoring, behavioural analysis, and sensitive environments with power imbalances, to protect fundamental rights and prevent abuse.", "940704": "Privacy Enhancing Technologies (“used to protect sensitive information from unauthorised access and misuse, by minimising or eliminating the need for an organisation training an AI model to collect personal data” – OECD) encryption, access controls, multi-factor authentication, regular audits, and incident response plans. Organizations must enforce strict governance.", "940707": "Provision of accessible alternatives to biometric authentication (e.g., OTPs, smart cards etc.), ensure clear, informed consent, and justify any restriction with necessity and proportionality. Restrictions must be transparent, minimal, and not exclude vulnerable groups. ", "940708": "Impact assessments, data minimisation, security, clear user information, enable alternatives, ensure transparency, regularly audit systems, and implement safeguards to prevent bias and discrimination in biometric processing.", "940709": "CAIDP recommends that data controllers should provide adequate and contestable information regarding the technology used (e.g. AI), they type of data processed and the possible risks to the rights and freedoms of data subjects, according to the LGPD the UNESCO Recommendation on the Ethics of AI. ", "940710": "Provide clear, accessible information on biometric processing, offer simple mechanisms for data access, correction, and consent withdrawal, and ensure these rights are easily exercise, especially for vulnerable groups, through accessible policies and support channels. ", "940711": "CAIDP urges Brazil to uphold the highest standards of data protection, privacy, particularly concerning the collection and use of biometric data and the protection of vulnerable individuals in line with the Resolution No. 245/2024 of the National Council for the Rights of Children and Adolescents. ", "940712": "Processing children's biometric data requires explicit, informed, and revocable parental consent or exceptionally a legal obligation. Clear, accessible information must be provided, ensuring informed participation and the right to refuse or withdraw without harm. ", "940714": "Any processing of children’s biometric data must be subject to rigorous risk and impact assessments, with a focus on the unique risks to children’s privacy, autonomy, and well-being. There should be independent oversight and regular audits to ensure compliance with child protection standards.

Número: OP-1005718

Data: 01/08/2025 - 09:44

Resumo: "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: Na ausência de critérios técnicos definidos pela LGPD, a caracterização de um dado como biométrico deve seguir interpretação sistemática e comparada, sendo considerado assim quando resultar do tratamento técnico específico de características físicas, fisiológicas ou comportamentais, com o objetivo de permitir ou confirmar a identificação inequívoca da pessoa natural. ", "940688": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: Controladores que realizam tratamento de dados biométricos devem adotar práticas de transparência ativa que garantam ao titular, no momento ou antes da coleta, o acesso claro às finalidades, bases legais, critérios de retenção, eventuais compartilhamentos e direitos previstos na LGPD. Essas informações devem ser apresentadas em linguagem acessível, adaptada ao público-alvo, por meio de interfaces físicas ou digitais, e estruturadas preferencialmente em camadas. Sempre que houver uso de biometria em decisões automatizadas ou categorização comportamental, devem ser fornecidas explicações adicionais sobre os critérios envolvidos, seus possíveis efeitos e meios eficazes de contato com o encarregado pelo tratamento. ", "940690": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: A biometria comportamental pode inferir informações sobre o estado emocional, mental ou de saúde do indivíduo. Sempre que for o caso, é recomendada a elaboração de avaliação de impacto com ênfase em discriminação e viés algorítmico e adoção de medidas de segurança compatíveis com a criticidade dos dados tratados, como anonimização, criptografia e governança técnica por design. ", "940693": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: O consentimento para o tratamento de dados biométricos só será válido quando for obtido de forma livre, informada, específica, destacada e inequívoca, o que exige a adoção de medidas como: apresentação clara das finalidades, facilitação da revogação e linguagem acessível ao público-alvo. Contudo, o consentimento não é base legal adequada quando o tratamento se destina à prevenção à fraude e segurança do titular, casos em que se aplicam as hipóteses do art. 11, II da LGPD, e o uso da biometria deve ocorrer com base em deveres do controlador voltados à proteção de dados e mitigação de riscos.", "940695": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: Deve-se considerar que está no âmbito de responsabilidade e, portanto, de atuação do controlador a ponderação sobre a necessidade, proporcionalidade e adequação de uso de biometria para a finalidade de prevenção à fraude. De outra forma, haveria cerceamento do uso de medida de segurança mais robusta em detrimento da responsabilidade do próprio controlador. Além disso, é importante interpretar com a devida cautela o posicionamento de autoridades europeias que exigem a subsidiariedade para o uso de biometria em casos de prevenção à

fraude. O mesmo não ocorre no Brasil, que estabeleceu base legal própria para a prevenção à fraude, de forma compatível com o nosso numeroso cenário de fraudes e universalização de serviços digitais. ", "940697": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: O tratamento de dados pessoais com base em obrigação legal ou regulatória deve ser amparado por norma clara e específica que assegure segurança jurídica e previsibilidade aos titulares. Além disso, é imprescindível que o tratamento observe os princípios da necessidade, idoneidade e proporcionalidade, de modo que o uso dos dados biométricos seja estritamente necessário para atingir a finalidade legítima. Para tanto, o controlador deve comprovar que o sistema adotado é adequado para alcançar o objetivo pretendido, considerando as limitações e riscos inerentes à tecnologia biométrica, como possíveis erros e vieses. A medida deve ainda ser equilibrada, de modo que os benefícios superem os impactos sobre os direitos dos titulares, acompanhada de salvaguardas técnicas e administrativas que garantam transparência, segurança e respeito aos direitos fundamentais.", "940699": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: O tratamento de dados biométricos para fins de pesquisa deve demonstrar a necessidade do uso desses dados biométricos para alcançar seus objetivos de forma proporcional e razoável, não havendo alternativa menos invasiva. Além disso, é imprescindível que o tratamento não cause danos substanciais significativo aos indivíduos, respeitando princípios éticos e legais. Além disso, o tratamento deve estar claramente vinculado ao interesse público, justificando o benefício social da pesquisa. É fundamental implementar salvaguardas adicionais, como garantir a anonimização eficaz para minimizar riscos de reidentificação, adotar medidas técnicas e organizacionais robustas e assegurar transparência e responsabilidade durante todo o processo.", "940700": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: O uso de tecnologias de reconhecimento facial, mesmo quando amparado por base legal, deve observar os princípios da necessidade, proporcionalidade, transparência e não discriminação, exigindo salvaguardas técnicas (como auditorias e explicabilidade), jurídicas (avaliação de impacto e limitação de uso) e institucionais (participação social), a fim de mitigar riscos de discriminação e garantir a proteção efetiva dos direitos fundamentais.", "940701": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: Sistemas de reconhecimento facial podem ser projetados de forma eficaz e confiável por meio da aplicação consistente do Privacy by Design, incluindo o uso de bases de dados representativas, testes regulares de acurácia, calibração contínua de modelos e mecanismos de auditoria algorítmica. Para minimizar falsos positivos e negativos, é essencial garantir diversidade demográfica nos dados, monitoramento técnico permanente e validação independente. A correção tempestiva de falhas em tecnologias de tratamento automatizado exige a implementação de revisão humana obrigatória, comitês de supervisão ética, canais de contestação acessíveis aos titulares e atualização constante dos Relatórios de Impacto. Com esses mecanismos, é possível equilibrar inovação e segurança jurídica, promovendo o uso responsável da tecnologia sem comprometer os direitos dos titulares.", "940702": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: O uso remoto e em tempo real

do reconhecimento facial em espaços públicos impõe riscos desproporcionais à privacidade, liberdade e não discriminação. A vigilância biométrica em larga escala ameaça a autonomia individual, podendo restringir direitos e promover discriminação, especialmente devido a vieses técnicos que afetam minorias e grupos vulneráveis. Assim, o uso da TRF deve ser proibido em espaços públicos e privados sensíveis, salvo exceções legais fundamentadas e controladas previamente pela autoridade de proteção de dados.", "940704": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: Para mitigar os riscos relacionados ao tratamento de dados biométricos, é indispensável que as organizações adotem medidas técnicas como criptografia robusta, autenticação multifator, e testes contínuos de segurança, bem como medidas administrativas como treinamentos, planos de resposta a incidentes, políticas de continuidade de negócios e cláusulas contratuais específicas com operadores. Quanto aos parâmetros mínimos de avaliação de riscos e monitoramento, devem ser exigidos: elaboração e atualização periódica de Relatórios de Impacto (RIPD), uso de indicadores de segurança, auditorias externas regulares e canais internos de reporte de riscos. Esses mecanismos garantem a conformidade com a LGPD e fortalecem a proteção integral de dados biométricos, permitindo que o setor privado atue com responsabilidade e segurança jurídica no desenvolvimento de tecnologias sensíveis.", "940707": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: A exigência de biometria em funcionalidades não essenciais é legítima quando tecnicamente indispensável, desde que acompanhada de justificativa transparente, medidas de minimização e sem excluir o titular do serviço principal. A recusa do consentimento pode justificar a limitação de acesso a funcionalidades específicas, desde que proporcional, comunicada previamente e sem configurar tratamento discriminatório. A oferta de vantagens exclusivas com base no fornecimento de dados biométricos, sem alternativa técnica equivalente, pode representar discriminação indireta, vedada pela LGPD.", "940708": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: A proteção eficaz no tratamento de dados biométricos exige a adoção de medidas técnicas e organizacionais que assegurem sua utilização proporcional, transparente e justificada. Cabe ao controlador garantir a segurança da informação, respeitar os princípios da LGPD e prevenir práticas discriminatórias diretas ou indiretas. O uso responsável da biometria deve se fundamentar em necessidade técnica real, ser informado de forma clara ao titular e estar sujeito a mecanismos de controle, revisão e mitigação de riscos contínuos.", "940709": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: Em tratamentos biométricos contínuos e massivos, a autodeterminação informativa deve ser garantida por um conjunto de medidas proporcionais que combinem transparência acessível, canais eficazes para o exercício de direitos e práticas robustas de governança. A regulação deve considerar a viabilidade técnica e os contextos de aplicação, evitando rigidez normativa que possa prejudicar soluções legítimas e de interesse coletivo.", "940710": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: O respeito aos direitos dos titulares em tratamentos automatizados de dados biométricos exige um compromisso ativo com a transparência, simplicidade nos mecanismos de controle e

atenção à proporcionalidade no uso da tecnologia. A regulação deve valorizar medidas práticas, seguras e tecnicamente viáveis para assegurar o exercício real desses direitos, considerando as particularidades de cada contexto de uso.", "940711": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: O tratamento de dados biométricos de crianças e adolescentes exige transparência e participação informada dos pais ou responsáveis, com informações claras sobre a finalidade e os direitos envolvidos. A escolha da base legal deve considerar o contexto e a necessidade do tratamento: a proteção da vida (art. 11, II, “e”) pode ser usada em situações excepcionais, enquanto a prevenção à fraude e à segurança (art. 11, II, “g”) é adequada para controle de acesso e proteção em ambientes institucionais. Para estar em conformidade com o art. 14 da LGPD, o tratamento deve ser proporcional, necessário e demonstrar claramente que atende ao melhor interesse da criança ou adolescente.", "940712": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: O tratamento de dados biométricos de crianças e adolescentes pode ser admissível quando demonstrada sua real necessidade diante de riscos concretos no ambiente de uso, e desde que fundado em base legal compatível, como a prevenção à fraude e à segurança do titular. A participação informada dos pais ou responsáveis deve ser viabilizada por meio de comunicação clara e acessível, e o tratamento deve estar condicionado à adoção de medidas técnicas e organizacionais robustas que garantam a proteção da privacidade e dos direitos desses grupos vulneráveis.", "940714": "Contribuição enviada por e-mail em razão da extensão dos apontamentos e limitação de caracteres da plataforma. Tese: A verificação ou estimação de idade por biometria só se justifica quando for comprovadamente necessária para proteger crianças e adolescentes em ambientes digitais de risco, sendo imperativo limitar a coleta ao estritamente necessário, adotar salvaguardas técnicas rigorosas e garantir a supervisão dos responsáveis legais. O tratamento deve ser orientado pelos princípios da minimização, transparência e pelo melhor interesse do menor, evitando qualquer uso abusivo ou desproporcional da tecnologia.

Contribuinte: JULIANA DE LOPES DORIA

Número: OP-1005725

Data: 01/08/2025 - 09:52

Resumo: : "Para a ABESE os dados biométricos se traduzem na identificação única do indivíduo, logo, é preciso observar se há captura automatizada de características físicas fisiológicas ou, possivelmente, comportamentais, afinal, diferente dos dados pessoais comuns como uma senha de um banco, por exemplo, os dados biométricos não podem ser modificados sendo este o traço determinante para o maior rigor no seu tratamento.", "940688": "Numa primeira análise, a ABESE entende que os controladores devem adotar e disponibilizar previamente informações visíveis e acessíveis sobre suas políticas de privacidade, devendo constar capítulo específico sobre o tratamento de dados pessoais sensíveis. A forma de acesso pode ser diversa como placas, sites e apps, através de um QR-CODE, visando inclusive evitar dispêndio de elevados recursos desnecessariamente.

", "940690": "Além da elevada importância e complexidade, a pergunta revela em si parte da resposta no sentido de que os dados biométricos demandarão, ao menos em alguns aspectos, tratamentos distintos conforme o tipo de dado biométrico. Em linhas gerais, é preciso obedecer à minimização de dados, bem como observar riscos específicos de reidentificação e monitoramento não autorizado. O refinamento e distinções de tratamento demandará estudo aprofundado das tecnologias e possibilidades de gestão. ", "940693": "Eis providência desafiadora. Para a ABESE, é preciso traçar um roteiro que possa ser padronizado e sistematizado para atender a estes passos ao tempo de evidenciar sua aplicação pela segurança das partes relacionadas, sobretudo dos responsáveis pelo tratamento dos dados (controladores e operadores). Quanto aos contextos que tratam do consentimento, no âmbito da segurança eletrônica, vertical dos serviços de Portaria Remota, há grande controvérsia quanto a exigibilidade ou não destes dados biométricos implementados para fins de segurança de um condomínio. A aplicação normalmente é deliberada em assembleia condominial, e a recusa de um usuário tem potencial de comprometer a segurança de todos. O consentimento nesse contexto vulnerabiliza toda uma operação de segurança, em detrimento da coletividade do condomínio de modo que a ABESE considera que a base legal que autoriza o tratamento dos dados é o legítimo interesse aliado ao cumprimento do contrato, sem prejuízo do titular dos dados", "940695": "Por um lado, a hipótese legal de “prevenção à fraude” está relacionada à análise de risco concreto à segurança do sistema ou do patrimônio, para demonstrar que o uso de dados biométricos é proporcional e necessário frente a alternativas menos invasivas. Por outro, as partes podem desejar se valer do seu uso. A compatibilização com o princípio da necessidade ocorre pela adoção de medidas de minimização dos dados, coleta específica à finalidade, e limitação temporal do armazenamento. Para mitigação dos riscos, a criptografia forte, autenticação multifator, segregação de acesso, registro de logs de auditoria e relatórios de impacto podem ser o caminho. ", "940697": "Nos casos em que o tratamento de dados biométricos se fundamenta no “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD), é prudente que o controlador comprove a existência de norma expressa que exija ou autorize tal tratamento, como boa prática. A finalidade deve ser específica, legítima e documentada, com coleta restrita ao mínimo necessário. Entidades públicas devem observar os princípios da legalidade, proporcionalidade, transparência e eficiência, com publicação de Relatório de Impacto à Proteção de Dados (RIPD) sempre que aplicável. Como salvaguardas adicionais, recomenda-se a adoção de controles de acesso, registros de operações, eventualmente auditorias internas, anonimização sempre que possível, e mecanismos para exercício dos direitos dos titulares. Essas medidas reforçam a segurança jurídica e a proteção à autodeterminação informativa, mas é importante ponderar, ainda, para o fator recursos. Uma preocupação do mercado que a ABESE reputa legítima é u", "940699": "Sabemos que mesmo quando há anonimização, o tratamento de dados biométricos para fins de pesquisa (art. 11, II, “c”, LGPD) exige cautela redobrada devido ao alto risco de reidentificação por cruzamento de bases. O tratamento deve estar limitado a finalidades científicas, estatísticas ou relevantes para interesse público, vedada sua reutilização para fins distintos. Os dados devem ser efetivamente anonimizados com técnicas robustas e atualizadas, e o processo documentado. Como salvaguardas, recomenda-se: comitê de ética, controle de acesso restrito, termos de confidencialidade, segregação de dados,

auditoria independente e avaliação contínua do risco de reidentificação. Sempre que possível, adotar pseudonimização adicional e eliminar os dados ao final da pesquisa. Tais medidas preservam os direitos dos titulares e a integridade da pesquisa.", "940700": "Eis mais um ponto desafiador, e é importante reconhecer que nenhuma tecnologia é infalível. Em linhas gerais, a coleta deve ser limitada à finalidade específica e com base legítima, como segurança ou prevenção à fraude. A transparência deve ser assegurada com informações claras ao titular e canal para exercício de direitos. Como salvaguardas, o desenvolvimento de treinamentos de algoritmos com bases diversas para evitar viés discriminatório, auditoria contínua de desempenho, relatórios de impacto, criptografia, trilhas de auditoria e segregação de acesso, nos parecem ser caminhos para este fim. Políticas internas e códigos de conduta devem regular o uso e corrigir desvios. O uso responsável dessas tecnologias fortalece a segurança e a confiança no setor da segurança eletrônica.", "940701": "Para elevar a eficácia e confiabilidade desde a concepção, os sistemas de reconhecimento facial devem ser desenvolvidos com base em princípios de privacy by design e by default, adotando algoritmos treinados com bases de dados diversas e atualizadas, que evitem viés e aumentem a conformidade. É essencial a realização de testes periódicos de performance, com monitoramento de taxas de falsos positivos e negativos, além da calibração contínua dos sistemas. Mecanismos de correção devem incluir validação humana em decisões críticas, registros detalhados de acesso (logs), e canais de contestação acessíveis aos titulares. No setor de segurança eletrônica, tem havido significativa evolução, inclusive na aplicação dessas tecnologias em locais de aglomeração de pessoas, esta sim área mais sensível para sua aplicação.", "940702": "A ABESE não tem certeza sobre este ponto que merece mais pesquisa e estudo.", "940704": "Diante do alto risco associado aos dados biométricos, é indispensável adotar medidas técnicas como criptografia forte em trânsito e repouso, autenticação multifator, controle segmentado de acessos, logs imutáveis, backups protegidos e testes regulares de intrusão. Administrativamente, a empresa deve implementar política de segurança da informação, plano de resposta a incidentes, avaliação de impacto à proteção de dados (DPIA) e governança com papéis bem definidos. O monitoramento contínuo, auditorias internas e a revisão periódica dos riscos são essenciais para manter a conformidade com a LGPD. No setor de segurança eletrônica, onde o tratamento é constante e sensível, essas práticas devem ser integradas ao ciclo de vida dos sistemas, com foco na prevenção de vazamentos e na responsabilização.", "940707": "Esta é uma questão relativa, porque ainda que não e trate de serviço essencial a opção pode ser pelo uso do dado biométrico em razão de praticidade, ou até maior segurança operacional, como ocorro no mercado da segurança eletrônica. Em todo caso, é possível garantir ao titular dos dados meios alternativos de acesso, como senhas, QR Codes ou cartões. Para evitar discriminação, a recusa ao fornecimento dos dados não pode implicar exclusão total do serviço, salvo se a funcionalidade for tecnicamente inviável sem a biometria — o que deve ser justificado de forma proporcional e documentada. A transparência exige aviso prévio sobre os impactos da negativa, com linguagem acessível. No setor de segurança eletrônica, isso significa respeitar o direito de escolha dos usuários em condomínios ou empresas, sem comprometer a segurança coletiva. A adoção de alternativas e o registro das escolhas do titular são boas práticas indispensáveis.", "940708": "Boas práticas para o tratamento de dados biométricos

exigem medidas como a adoção de política específica de proteção a dados sensíveis, mapeamento de riscos, minimização de dados, definição clara da base legal, criptografia, controle de acesso com autenticação forte, e revisão periódica de segurança. A transparência deve ser garantida com aviso prévio ao titular, linguagem clara, política de privacidade acessível e canal direto com o encarregado de dados. Para evitar discriminação, é essencial validar os algoritmos usados, garantir diversidade nas bases de treinamento e permitir revisão humana nas decisões automatizadas. No setor da segurança eletrônica, essas práticas asseguram a confiança do usuário, a efetividade da tecnologia e o alinhamento com os princípios da LGPD.

","940709": "Eis mais um grande desafio que confronta o interesse coletivo versus direitos individuais. Numa primeira análise, entendemos que para respeitar a autodeterminação informativa em contextos de tratamento massivo e contínuo, como smart cities que, aliás, a ABESE contribui, e monitoramento em locais públicos, os controladores podem adotar medidas como sinalização clara sobre o uso de biometria, disponibilização de políticas de privacidade em locais visíveis (físicos e digitais), criação de portais de informação com canais para exercício de direitos, e uso de tecnologia que permita anonimização ou pseudonimização. O tratamento deve ter base legal adequada, com avaliação de impacto e supervisão de autoridade pública, quando necessário. Em situações de difícil transparência, é fundamental reforçar a governança de dados, garantindo que o titular tenha meios de compreender e questionar o uso de suas informações.

","940710": "Em um cenário ideal, os agentes de tratamento devem garantir os direitos dos titulares com políticas de privacidade claras e acessíveis, canais de atendimento eficazes e mecanismos digitais que permitam consulta, correção e revogação do consentimento de forma simples, quando essa for a base. Em tratamento automatizado de dados biométricos, é essencial oferecer revisão humana de decisões, registros de tratamento, e transparência quanto às finalidades e impactos. A comunicação deve usar linguagem compreensível e estar disponível em múltiplos meios (apps, sites, portarias). Todavia, é fundamental ressaltar as barreiras que existem atualmente para oferecer aos titulares mecanismos digitais para essas consultas atualmente. A exemplo da massa de empresas constituídas no Brasil, o universo da segurança eletrônica é composto predominantemente, por empresas de menor porte, com dificuldades para essa adaptação. Mesmo as grandes carecem de soluções para dar efetividade a tais comandos, daí um",

","940711": "O tratamento de dados biométricos de crianças e adolescentes exige rigor extremo, dado seu caráter sensível. A participação informada dos pais ou responsáveis deve ser garantida por meio de consentimento explícito, livre, informado e inequívoco, preferencialmente por escrito, antes do início do tratamento. Legalmente, o tratamento é admissível quando necessário para cumprir obrigação legal ou regulatória, para a execução de políticas públicas previstas em lei, ou com o consentimento dos responsáveis, conforme art. 14 da LGPD.

","940712": "O tratamento de dados biométricos de crianças e adolescentes é admissível nas hipóteses previstas no art. 14 da LGPD: com consentimento específico dos pais ou responsáveis, para cumprimento de obrigação legal ou regulatória, para proteção da vida ou da incolumidade física do titular ou de terceiros, ou para execução de políticas públicas. Para garantir a participação informada dos responsáveis, deve-se obter consentimento claro, prévio, informado e documentado, com linguagem acessível. Além disso, as empresas devem implementar medidas técnicas (criptografia, controle de acesso,

anonimização) e organizacionais (treinamento, políticas internas, auditorias) para prevenir abusos, vazamentos e acessos não autorizados, assegurando a segurança, a privacidade e o respeito ao princípio do melhor interesse do menor. ", "940714": "Entendemos que o tratamento de dados biométricos para verificação ou estimação de idade de crianças e adolescentes em plataformas digitais deve observar os princípios da necessidade e do melhor interesse, limitando a coleta ao mínimo indispensável para a finalidade específica. Em todo caso, a plataforma deve garantir que o uso dos dados não exponha a criança ou adolescente a riscos ou discriminações, respeitando direitos fundamentais e legislação aplicável, em especial o art. 14 da LGPD, que prioriza a proteção integral do menor. No mercado da segurança eletrônica essa não é uma questão comum, o que impõe maior reflexão junto ao mercado que lida com dados de menores, lembrando que o foco é a segurança.

Contribuinte: JOSE LAZARO DE SA SILVA

Número: OP-1005871

Data: 01/08/2025 - 11:11

Resumo: "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Para apoiar a definição de critérios para caracterizar um dado como biométrico nos termos da LGPD, destacam-se o INAI, o EDPB e a Lei de Proteção de dados chilena, pelos quais é necessário que ele: (i) esteja vinculado a características físicas, fisiológicas ou comportamentais de uma pessoa; (ii) resulte de um tratamento técnico específico (como uma medição); e (iii) tenha como finalidade a identificação ou autenticação única do titular. Assim, imagens, vídeos ou gravações de voz, por si sós, não são dados biométricos, a menos que sejam processados tecnicamente com essa finalidade. O dado biométrico não é o dado bruto em si, mas aquele tratado para extrair padrões únicos (como vetores faciais). Essa distinção, adotada pelo EDPB, é essencial para evitar a ampliação indevida do regime de dados sensíveis e garantir segurança jurídica, especialmente em contextos de baixo risco, como cadastros sem reconhecimento automatizado.", "940688": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Segundo a Autoridade de Proteção de Dados do Reino Unido (ICO), a transparência no uso de dados biométricos deve considerar: (i) o caso de uso; (ii) a relação com o titular; e (iii) os dados envolvidos. Com base nisso, quanto mais claro for o tratamento para o titular, menor a exigência de medidas adicionais. No setor financeiro, por exemplo, o uso de biometria para autenticação em serviços como acesso à conta ou solicitações de crédito ocorre em ambiente autenticado e sob vínculo prévio, com exigências regulatórias específicas (ex.: Resolução CMN nº 4.893/21). Nesses casos, é suficiente indicar a Política de Privacidade ao longo da jornada do cliente ou prestar explicações sobre o tratamento, quando solicitadas (por exemplo, nos casos em que o reconhecimento facial é necessário para ativar um determinado serviço, indicar na tela antes de obter o reconhecimento às finalidades para as quais ocorrerá o tratamento).", "940690": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: A legislação vigente não diferencia biometria comportamental da tradicional, tampouco impõe obrigações distintas entre elas. Assim, eventuais normas infralegais não podem criar exigências diferenciadas sem respaldo legal, sob pena de violar o princípio da legalidade. Embora o

INAI (México) e o ICO (Reino Unido) fazem distinções conceituais, não há deveres legais específicos para cada tipo. Ambas estão sujeitas aos mesmos princípios, como qualidade dos dados e segurança. No setor financeiro, a Resolução CMN nº 4.893/21 e a Resolução Conjunta nº 6/23 reforçam a exigência de mecanismos antifraude com dados íntegros e governança clara. O WP29 relata que a biometria comportamental melhora a detecção de fraudes e a agilidade de resposta. A PDPC de Singapura também reconhece seu valor em estratégias de segurança.", "940693": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: É imperativo que a futura regulamentação reconheça explicitamente que o consentimento não deve ser a única base legal para tratar dados biométricos, especialmente no setor financeiro. A LGPD prevê, no art. 11, II, “g”, a hipótese de tratamento para prevenção à fraude e segurança do titular, aplicável a atividades como abertura de contas, autenticação de acesso e recuperação de senha. Também se aplica o art. 11, II, “a”, que autoriza o tratamento desses dados quando houver obrigação legal, como nas exigências de autoridades do SFN relacionadas à segurança cibernética, KYC e PLD/FT. Mesmo quando o tratamento se baseia em outras hipóteses legais, o controlador deve garantir transparência e os direitos do titular. Quando o consentimento for a base aplicável, deve ser livre, informado, específico, destacado e inequívoco, com camadas de informação claras, como checkbox de opt-in e acesso facilitado à política de privacidade e termo específico.", "940695": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: No caso da garantia da prevenção à fraude e à segurança do titular, os critérios para o tratamento de dados biométricos devem ser (i) finalidade específica e restrita; (ii) proporcionalidade entre segurança e risco à privacidade; (iii) medidas robustas de segurança; e (iv) transparência. No setor financeiro, tais dados são compatíveis com o princípio da necessidade, por viabilizarem segurança, inclusão e boa experiência do usuário. Diante do alto índice de fraudes no Brasil, a biometria é mais eficaz do que senhas ou tokens. Recomenda-se elaborar relatório de impacto e adotar salvaguardas como: acesso controlado, criptografia, pentests, armazenamento segregado e logs. Também se recomenda guardar apenas templates biométricos e seguir normas como a ISO/IEC 24745:2022. Autoridades como ICO, INAI e PIPC reforçam essas práticas para mitigar riscos e proteger os direitos dos titulares.", "940697": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: No contexto do sistema financeiro, diversas normas que fundamentam o tratamento de dados biométricos visam à prevenção à fraude, segurança nas transações e identificação inequívoca do titular dos dados, de modo que os critérios devem ser: (i) haver norma clara exigindo autenticação robusta; (ii) tratamento proporcional e necessário à finalidade; e (iii) uso dos dados apenas nos limites da obrigação legal. Como exemplos das normas mencionadas podem ser citadas a Lei nº 9.613/1998, a Circular BCB nº 3.978/2020 e a Resolução CMN nº 4.893/2021. Mesmo sem menção expressa à biometria, a exigência de medidas seguras pode legitimá-la. As salvaguardas incluem criptografia, controle de acesso, testes de segurança, registros de logs e due diligence com fornecedores. Como reforça o ICO, a proteção deve considerar o risco e a sensibilidade dos dados, não apenas a base legal. O STJ também exige medidas eficazes contra fraudes, como no REsp 2.052.228/DF", "940699": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: A ANPD esclarece que a anonimização não é obrigatória para tratamento de dados biométricos em pesquisas, pois a LGPD adota modelo flexível, equilibrando proteção e objetivos do estudo. Embora a anonimização não seja mandatória,

dados biométricos podem permitir reidentificação devido à inferência de dados sensíveis. Assim, conforme ANPD, ICO e Autoridade de Hong Kong, medidas proporcionais ao risco devem ser adotadas, incluindo irreversibilidade dos templates biométricos, mecanismos que evitem vinculação entre bases, restrição de acesso, segmentação de dados e políticas de uso e compartilhamento. A avaliação deve focar no risco concreto de reidentificação e mitigação adequada para proteger direitos dos titulares. ", "940700": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: O uso de reconhecimento facial no setor financeiro visa segurança, conformidade regulatória e inclusão, não vigilância. Aplica-se em contextos em que o titular espera o tratamento, como abertura de contas ou autenticação, sendo informado via aviso de privacidade acessível e oportuno. A biometria facial, com prova de vida, é proporcional frente a riscos como phishing e SIM swapping, e atende exigências regulatórias. O armazenamento da foto original pode ser necessário para fins probatórios e exercício regular de direitos. Práticas como verificação 1:1, finalidade específica e não inferência de outros dados sensíveis reforçam a minimização. Para mitigar vieses, adota-se qualificação de fornecedores e orientações do ICO: bases representativas, testes de viés, avaliação da acurácia e mecanismos para contestação de resultados. ", "940701": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Para garantir eficácia e confiabilidade de sistemas de reconhecimento facial, é fundamental adotar medidas proporcionais ao risco envolvido, conforme a finalidade e o potencial impacto do sistema. O projeto deve seguir boas práticas para modelos de IA, como: (i) definição prévia do nível mínimo de acurácia requerido; (ii) uso de bases de dados representativas e adequadas ao público-alvo, mitigando riscos de overfitting e underfitting; (iii) testes documentados de desempenho global e por grupos específicos, com retreinamentos ou ajustes, se necessário; e (iv) monitoramento contínuo e versões arquivadas de modelos que aprendem após implantação. Também é recomendável que os usuários tenham mecanismos para contestar resultados incorretos e que haja procedimentos eficazes para mitigar erros de identificação. ", "940702": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: O reconhecimento facial não deve ser usado quando existirem métodos adequados e proporcionais que atinjam a mesma finalidade com menor invasão à privacidade. Exemplos de contextos inadequados incluem controle de presença em escolas, monitoramento em espaços públicos sem justificativa, uso em processos seletivos que podem gerar vieses discriminatórios, e vigilância em eventos políticos. Alternativas recomendadas incluem autenticação por digital, cartões de acesso, senhas complexas, tokens temporários e verificações via serviços telefônicos automáticos. Dados de telecomunicações também auxiliam na prevenção de fraudes, por exemplo, identificando SIM swaps. É crucial que a ANPD fomente regulamentação que incentive o desenvolvimento de soluções seguras e eficazes, evitando o uso excessivo e inadequado do reconhecimento facial por falta de opções juridicamente seguras. ", "940704": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Medidas essenciais para proteger dados biométricos, com base no ICO, INAI e PIPC, incluem: (i) controle rigoroso de acesso; (ii) testes de penetração; (iii) políticas de segurança da informação; (iv) criptografia em trânsito e armazenamento; (v) varreduras regulares para identificar vulnerabilidades; (vi) registro de logs; (vii) armazenamento segregado; e (viii) due diligence e cláusulas contratuais robustas com terceiros. Para avaliação e monitoramento de riscos, segundo ISO/IEC 27005:2023, destacam-se: definição de critérios de risco,

identificação de ativos, ameaças (ex.: ataques de apresentação, interceptação, subversão, ameaças internas, ataques DDoS), análise do risco, decisão sobre mitigação e monitoramento contínuo para ajustes. Por fim, sobre o primeiro questionamento, destacam-se os pontos já apresentados na Pergunta 8.", "940707": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Em complemento às orientações apresentadas na Pergunta 8, é essencial considerar o princípio da acessibilidade no uso de ferramentas biométricas, especialmente indivíduos com deficiência visual, que podem enfrentar dificuldades significativas no uso dessa solução. Diante disso, é essencial que organizações implementem métodos alternativos de autenticação quando a biometria for inviável, ainda que com nível de proteção inferior. No consentimento, a recusa pode legitimar a indisponibilidade de funcionalidades que dependem da biometria, como confirmação de transações financeiras, mas não pode impedir o acesso a serviços que não exijam tais dados. Sem consentimento, a recusa é exercício do direito de oposição; a negativa de acesso é lícita se (i) tecnicamente inviável oferecer sem biometria; ou (ii) prevalecer interesse legítimo da organização, conforme parâmetros legais.

", "940708": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Retomando as orientações das Perguntas 2, 5, 8 e 11, destacam-se: Medidas de proteção e segurança: avaliação estruturada de riscos de cibersegurança (Pergunta 11) e controles técnicos/organizacionais conforme boas práticas do ICO, INAI e PIPC (Pergunta 8); Transparência: obrigação do art. 9º da LGPD, considerando finalidade, relacionamento e contexto; conforme o ICO, usos comuns exigem menos comunicação ativa, usos sensíveis demandam transparência reforçada; Risco de discriminação: prevenção de vieses, conforme orientações do ICO, conforme já abordado na Pergunta 8.", "940709": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: No que se refere ao direito à informação, e como já abordado na Pergunta 2, quando os titulares não possuem expectativa sobre a coleta de informações biométricas (em especial quando não há vínculo anterior com o controlador), é necessário empenho para garantir a transparência do tratamento. Para cumprir essa exigência, é possível, instalar sinalizações visíveis nos locais de coleta contendo informações básicas sobre o tratamento realizado, bem como indicar os canais pelos quais os titulares podem acessar dados mais completos e exercer seus direitos. Também é recomendável o uso de QR Codes posicionados em estruturas fixas, como paredes, painéis ou telas que direcionem para o aviso de privacidade da organização, onde devem constar todas as informações exigidas pela legislação. A ANPD já avaliou situação análoga e considerou adequadas as medidas mencionadas acima de prestação de informação, (Nota Técnica nº 29/2024/FIS/CGF/ANPD - § 6.1.4).", "940710": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Além das medidas de transparência, é essencial garantir o exercício dos direitos dos titulares no uso de biometria. O direito de acesso pode ser atendido com: (i) confirmação do tratamento e sua finalidade; (ii) tipo de dado tratado; (iii) origem da imagem; (iv) amostra original, se armazenada; e (v) dados contextuais, como data de uso. O direito à correção se aplica a erros de associação ou necessidade de recadastramento. Já a revogação do consentimento deve resultar na exclusão do template, exceto quando o dado for tratado com base em obrigações legais ou legítimo interesse, como prevenção à fraude. Nesses casos, a revogação impede novos usos, mas não exige exclusão retroativa de registros, que devem ser preservados para fins regulatórios, de auditoria e prevenção à lavagem de dinheiro, conforme exigido pelo BCB, CVM e demais órgãos do

SFN.", "940711": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Nos termos do Enunciado CD/ANPD nº 1/2023, o tratamento de dados biométricos de crianças e adolescentes pode se apoiar em qualquer base legal dos arts. 7º e 11 da LGPD, desde que respeitado o princípio do melhor interesse. Para garantir a participação informada dos responsáveis, recomenda-se, além de incluir o tratamento no Aviso de Privacidade: (i) enviar comunicações formais com explicações claras; (ii) informar canais de atendimento para exercício de direitos; e (iii) quando cabível, oferecer mecanismo de oposição. A análise do melhor interesse deve considerar: (i) o bem jurídico tutelado; (ii) a existência de alternativas menos invasivas; e (iii) o impacto do desenvolvimento físico nas características biométricas, que pode comprometer a eficácia do tratamento ao longo do tempo.

", "940712": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: Sobre bases legais aplicáveis e a necessidade de participação informada de pais ou responsáveis, valem as observações da Pergunta 16: Bases legais: conforme Enunciado CD/ANPD nº 1/2023, a ANPD admite que o tratamento de dados pessoais de crianças e adolescentes seja fundamentado nas hipóteses previstas nos arts. 7º e 11 da LGPD, desde que assegurado, como prioridade, seu melhor interesse. Assim, o uso de dados biométricos de menores de idade é permitido, desde que haja base legal devidamente fundamentada e o tratamento tenha como finalidade proteger os interesses dos menores. Transparência: além de incluir as informações no Aviso de Privacidade, é recomendável realizar a comunicação direta aos pais e/ou responsáveis, com explicações sobre a operação de tratamento e os meios disponíveis para o exercício dos direitos dos titulares. Por fim, quanto às medidas de segurança a serem adotadas, aplicam-se os parâmetros indicados nas Perguntas 5 e 11", "940714": "Contribuição da Zetta, CNPJ 37.253.906/0001-28: A verificação etária por biometria deve observar: (i) o contexto do serviço e seu risco para crianças e adolescentes; (ii) a precisão da tecnologia adotada; e (iii) a existência de métodos menos invasivos com eficácia semelhante. O princípio da necessidade não exige apenas minimizar a coleta, mas selecionar os dados essenciais para garantir o melhor interesse do menor. Conforme o ICO, a técnica deve ser proporcional ao risco. Tecnologias biométricas de estimação etária podem ter margem de erro alta, sendo mais seguras quando combinadas com verificação documental. Alternativas menos intrusivas incluem: autodeclaração de idade, confirmação via cartão de crédito, inferência por comportamento digital, checagem presencial de documentos e consentimento do responsável legal (desde que validado). A escolha do método deve ser sempre baseada em análise contextual e proporcionalidade.

Contribuinte: Laryssa de Menezes Silva

Número: OP-1005901

Data: 01/08/2025 - 11:25

Resumo: "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a

respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940688": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940690": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940693": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940695": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940697": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940699": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios;

Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940700": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940701": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940702": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940704": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940707": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940708": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes;

Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940709": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940710": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940711": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940712": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.", "940714": "A Associação Brasileira de Crédito Digital (ABCD) vem, por meio deste, informar que enviou as suas contribuições a respeito da Tomada de Subsídios sobre Tratamento de Dados Biométricos, publicada em 2 de junho de 2025, para o e-mail normatizacao@anpd.gov.br, em um arquivo único. Foram apresentadas contribuições a respeito das 18 questões apresentadas nos 5 blocos temáticos: Definições e Princípios; Hipóteses Legais; Tecnologias de Reconhecimento Facial e Tecnologias Emergentes; Segurança, Boas Práticas e Governança; Direitos dos Titulares e Grupos Vulneráveis.

Contribuinte: MARA REGINA GELSI DOS SANTOS

Número: OP-1005963

Data: 01/08/2025 - 12:08

Resumo: "A Abranet entende que a definição de dados biométricos do GDPR deve ser usada como inspiração para a ANPD. O GDPR (considerando 51, art. 4º (14) e art. 9º (1)) define que os dados biométricos são dados capazes de levar a identificação inequívoca ou a autenticação de uma pessoa singular quando processados por meios técnicos específicos, eliminando as fotografias do escopo de dado biométrico quando distantes desse contexto de identificação do usuário. O critério objetivo de capacidade de identificação inequívoca auxilia na definição de dado pessoal sensível/biométrico e aplicabilidade das medidas de segurança compatíveis. ", "940688": "A Abranet entende que as práticas de transparência ativa para garantir que os titulares possuem informações claras sobre o tratamento podem envolver: (i) Avisos de privacidade no momento da coleta / legal disclaimer nos pontos de coleta ativa de dados biométricos; (ii) Identificação dos controladores para exercício de direitos dos titulares e (iii) Política de privacidade que elenque as medidas de segurança utilizadas no tratamento de dados biométricos. ", "940690": "A Abranet entende ser necessário separar os padrões comportamentais que levam a identificação inequívoca dos usuários de análises de padrões comportamentais utilizados de maneira agregada para aferir métricas, por exemplo, qualidade do atendimento dos usuários ou análise de movimentações financeiras com a finalidade de identificar comportamentos suspeitos e prevenir fraudes. Quando a biometria comportamental for utilizada para identificar um usuário de maneira inequívoca, as mesmas regras e cuidados devem ser observados. ", "940693": "A Abranet entende que o consentimento não deve ser a hipótese legal quando a coleta de dados biométricos decorre de obrigação regulatória que busque prevenir fraudes e garantir segurança na autenticação do cadastro do usuário em seu aplicativo bancário. ", "940695": "A aplicação da hipótese legal de “garantia da prevenção à fraude” deve ser acompanhada de teste de balanceamento e medidas técnicas que mitiguem riscos aos titulares. O tratamento deve observar os princípios da necessidade, finalidade e segurança, com transparência nas políticas de privacidade. Boas práticas incluem: (i) criptografia; (ii) autenticação multifator (MFA); (iii) controle de acesso; (iv) monitoramento e resposta a incidentes; e (v) registro de logs. Diferentemente do monitoramento em espaços públicos, a biometria aplicada à autenticação em apps é uma solução segura e eficaz que protege o usuário e ajuda a prevenir fraudes, com baixa taxa de erro e tecnologias em constante evolução que reforçam a segurança do sistema e do próprio titular. ", "940697": "A coleta de dados biométricos deve ser informada ao titular de maneira clara e contextualizada sendo os mesmos cuidados necessários para possibilitar o exercício dos direitos dos titulares: (i) Avisos de privacidade no momento da coleta e legal disclaimer nos pontos de coleta ativa de dados biométricos; (ii) Identificação dos controladores para exercício de direitos dos titulares e (iii) Política de privacidade que elenque as medidas de segurança utilizadas no tratamento de dados biométricos. ", "940699": "A Abranet entende que em relação à pergunta 7, esclarecemos que a hipótese apresentada não se aplica ao nosso escopo, razão pela qual não temos elementos para uma contribuição adequada sobre os limites do tratamento de dados biométricos por órgãos de pesquisa, mesmo em contextos de anonimização e possíveis re-identificações, tampouco quanto às salvaguardas adicionais que poderiam ser implementadas nesses casos. ", "940700": "Entendemos que a metodologia Privacy by Design é essencial para identificar potenciais riscos no tratamento de dados biométricos e registrar as medidas de segurança capazes de mitigar riscos decorrentes do

tratamento de tais dados pessoais. Além disso, deve-se certificar de que os sistemas de reconhecimento facial são treinados com dados diversos para evitar vieses, especialmente em relação à aspectos de cor e raça. Isso ajuda a garantir que a tecnologia funcione de forma equitativa para diferentes grupos de indivíduos, prevenindo discriminação.

","940701": "Conforme exposto acima, através do Privacy By Design, deve-se buscar assegurar que os sistemas sejam desenvolvidos observando-se critérios como diversificação de dados de treinamento, ajustes algorítmicos, transparência e explicabilidade acerca do tratamento dos dados. Em suma, é crucial estar atento aos vieses incorporados nos algoritmos e adotar práticas que ajudem a mitigar esses vieses. Essa responsabilidade deve recair sobre os desenvolvedores dessa tecnologia cabendo aos utilizadores avaliar e arquivar os reports que demonstrem as diretrizes e bases utilizadas neste treinamento. ","940702": "A Abranet entende que o reconhecimento facial é a medida de segurança adequada para autenticar o usuário em aplicativos financeiros, e o avanço das tecnologias de reconhecimento contribuem para uma autenticação mais assertiva e segura, a exemplo da técnica liveness que coleta a biometria do usuário por meio de movimentos da face, impedindo que fotografias estáticas sejam utilizadas por terceiros para burlar o sistema. A documentoscopia, por exemplo, é um meio alternativo de autenticação do usuário, mas a possibilidade de fraude de documento de identidade fragiliza a utilização deste meio de autenticação, sendo menos seguro para o usuário e para o sistema financeiro de maneira geral. ","940704": "Além das obrigações da LGPD, como privacy by design, política de privacidade, aviso no ponto de coleta e relatório de impacto, é essencial adotar medidas como: (i) criptografia forte para armazenamento/transmissão; (ii) autenticação multifator; (iii) controle de acesso restrito; e (iv) auditorias periódicas. A segurança na biometria exige constante atualização tecnológica para reduzir vulnerabilidades, garantir a eficácia das proteções e minimizar os riscos de roubo de identidade, considerando que esses dados, uma vez vazados, não podem ser alterados. A gestão ativa de riscos e a adoção de boas práticas são fundamentais para a conformidade e proteção dos titulares. ","940707": "A Abranet entende ser essencial que os controladores apliquem o princípio da necessidade identificando se a coleta de dados biométricos é o único meio possível de fornecer o acesso a determinado produto ou serviço. Por se tratar de dado pessoal sensível, caso o serviço não seja essencial e a coleta de dados pessoais biométricos seja opcional, deve ser garantido ao usuário a utilização do produto ou serviço com forma diversa de autenticação. ","940708": "Para garantir proteção eficaz, o tratamento biométrico deve considerar a diversidade da população brasileira. As tecnologias devem ser treinadas com bases amplas, auditáveis e transparentes, promovendo equidade e reduzindo vieses. Os controladores devem arquivar os relatórios técnicos que demonstrem as diretrizes usadas no desenvolvimento das soluções. Medidas adicionais incluem: (i) criptografia; (ii) MFA; (iii) controle de acesso; (iv) monitoramento e resposta a incidentes; e (v) registro de logs. Transparência, responsabilidade e diversidade nos dados de treinamento são essenciais para evitar discriminação ilícita e abusiva. ","940709": "A Abranet entende que a transparência ostensiva em pontos de coleta de dados biométricos se faz necessária para garantir ao titular a possibilidade de exercer o seu direito à autodeterminação informativa entrando em contato com o Encarregado no canal também informado no aviso de privacidade.

","940710": "Entendemos que os avisos de privacidade em contexto, no ponto de coleta ativo

de dados pessoais, são a forma de garantir que o titular está ciente de quais dados serão coletados e para quais finalidades bem como terceiros envolvidos no fluxo de compartilhamento de dados pessoais. Por meio do canal do Encarregado o usuário terá a oportunidade de exercer seus direitos previstos no art. 9º da LGPD, inclusive sobre decisões automatizadas, obrigação que não limita aos dados biométricos. ",940711": "A Abranet entende ser importante que os pais ou responsáveis sejam claramente informados sobre a finalidade, a duração, e os destinatários dos dados biométricos, em linguagem acessível e inteligível, inclusive, para as crianças e adolescentes. O tratamento desses dados deve ocorrer sob hipóteses legais específicas, sempre prevalecendo o princípio do melhor interesse da criança ou adolescente. É necessário que se garanta a minimização de dados, além de implementar medidas de segurança rigorosas para proteger esses dados. As empresas devem também estabelecer um canal de comunicação aberto com os pais ou responsáveis para esclarecer dúvidas e fornecer informações adicionais sempre que necessário. ",940712": "O uso da biometria por menores para autenticação é seguro e contribui para evitar fraudes, mas não deve ser usada para verificação etária, pois os riscos superam os benefícios. As mesmas medidas aplicáveis a adultos devem ser observadas: (i) criptografia; (ii) MFA; (iii) controle de acesso; (iv) resposta a incidentes; (v) logs; (vi) aviso de privacidade; (vii) identificação do controlador; e (viii) política de privacidade com medidas de segurança. A participação dos pais deve ser garantida com linguagem acessível, transparência e consentimento livre e informado, respeitando o melhor interesse da criança e do adolescente.",940714": "Apesar de útil para identificação, a biometria ainda não é precisa para verificação de idade, especialmente na infância e adolescência, dada a variabilidade de traços físicos e fatores externos (luz, dispositivos, etc.). Há riscos de erro, discriminação e restrição indevida de direitos, além de preocupações com privacidade e vigilância. O princípio da necessidade exige minimizar a coleta de dados. Há alternativas mais seguras, como a documentoscopia, que não envolvem dados sensíveis. Assim, a biometria não é o meio mais adequado para essa finalidade, nem compatível com o melhor interesse da criança e do adolescente.

Contribuinte: LAURA ARANTES QUINTINO DOS SANTOS

Número: OP-1005982

Data: 01/08/2025 - 12:16

Resumo: "Concordamos com a definição da ANPD trazida na Nota nº 17/2025/CON1/CGN/ANPD que está em aderência ao Regulamento Geral de Proteção de Dados da União Europeia e define que dados biométricos são "...dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa". Complementando, para caracterizar um dado como biométrico, é preciso verificar a natureza do dado (se referir a uma característica física, fisiológica ou comportamental da pessoa natural), um tratamento técnico específico (uso de tecnologia especializada para extrair, analisar ou comparar essa característica) e a finalidade identificadora (o tratamento deve ter como finalidade permitir/confirmar a identificação única

e/ou autenticação). Uma simples foto não caracteriza, por exemplo, um dado biométrico, a menos que seja submetida a uma tecnologia para extrair este tipo de

dado.", "940688": "Recomenda-se que a ANPD estabeleça a obrigatoriedade das seguintes práticas de transparência ativa, sempre que houver tratamento de dados biométricos: 1. Aviso prévio claro e acessível no momento da coleta Informar, de forma destacada, que o dado a ser coletado é biométrico. Informar de forma destacada não significa pedir o consentimento, devendo ser observada a hipótese de tratamento cabível. É importante, também, explicitar a finalidade (ex: autenticação) e indicar se o fornecimento é obrigatório ou facultativo, conforme a hipótese de tratamento. 2. Meios acessíveis de comunicação: as informações devem ser fornecidas em linguagem clara, inclusive com recursos acessíveis (ex: leitura por voz, Libras ou contraste visual), sempre que possível. ", "940690": "Diferente da biometria física (como impressão digital ou íris), os padrões comportamentais não são fixos ou permanentes, pois eles podem sofrer alterações frequentes causadas por cansaço, estresse, enfermidades, além de mudanças no ambiente de uso (ex: teclado diferente, ruído na voz, iluminação), o que compromete a qualidade e a precisão dos dados tratados (art. 6º, V da LGPD), podendo gerar falsos positivos ou negativos, falhas de autenticação, ou até discriminação algorítmica. Diante disso, a exigência tecnológica é maior, com a necessidade de uma calibração contínua, clareza em relação a confiabilidade dos resultados e rotinas de atualização. ", "940693": "Deverá ocorrer a separação visual e funcional do campo de consentimento, de modo que o aceite para biometria deve estar destacado dos demais termos contratuais ou autorizações. O controlador deve, também, disponibilizar um meio alternativo de acesso ao serviço, sem uso de biometria, quando o consentimento for a única base legal. O consentimento não é adequado quando houver desequilíbrio de poder entre as partes (ex. relações de trabalho), não há liberdade de escolha real ao titular e o controlador pretende utilizar os dados biométricos para outras finalidades no futuro, comprometendo o ato volitivo inicial. Por ex.: sistemas bancários, em que a biometria tem sido considerada o padrão ouro para a segurança na identificação do titular, tal dado é necessário, e a hipótese adequada para o seu tratamento é a prevista no art. 11, “g”. Contudo, a utilização de biometria para a identificação do consumidor destinada a promoção de uma farmácia não representa nenhuma essencialidade.", "940695": "Tal tratamento deverá ter uma finalidade legítima e documentada, demonstrando que a biometria é empregada especificamente para prevenir fraudes, e não para conveniência ou controle genérico. Deve haver justificativa baseada em dados objetivos ou históricos que indiquem que o uso da biometria reduz riscos de fraude naquele contexto, e que para a segurança do titular o uso dela se tornou imprescindível. A biometria deve ser usada somente se não for possível ou viável a utilização de meios menos intrusivo (ex: autenticação em dois fatores, senhas...). Além da finalidade ser específica, a tecnologia deve ter uso limitado no escopo e no tempo (sem reutilização para marketing, perfilamento ou controle comportamental). Várias salvaguardas podem ser utilizadas como, por exemplo, deverá ser vedado expressamente a reutilização do dado biométrico para outros fins que não estejam vinculados à prevenção de fraude. Além disso, deverá ocorrer a exclusão imediata após o fim da necessidade.", "940697": "Primeiramente, a hipótese de tratamento é restritiva, e precisamos ter certeza de que a coleta e o tratamento de dados biométricos de fato são exigidos pela legislação ou pela regulação para que não seja feita uma coleta com base nesta

hipótese de tratamento sem que a legislação/regulação efetivamente demande. A legislação também não pode ser internacional, pois tal situação violaria a soberania brasileira (art. 1º e 4º da CF e LINDB). Os controladores devem fazer um Relatório de Impacto - RID (com teste de balanceamento) prévio para mitigar os riscos, inclusive em relação a proporcionalidade do que está sendo coletado. Além disso, as regras previstas na LGPD devem ser cumpridas, por exemplo, os dados biométricos devem ser retidos apenas pelo tempo necessário para cumprir a obrigação legal e, uma vez cumprida, devem ser eliminados de forma segura e irreversível.", "940699": "Precisa ser adotado um processo de anonimização que seja submetido a um teste antes da disponibilização para saber se é possível identificar o titular diretamente ou até mesmo indiretamente ("Risk-based approach" e "Procedure-based approach"). Diante disso, técnicas podem ser utilizadas para garantir a impossibilidade de reversão, ainda que diante de outras bases de dados, por exemplo, ruído. Outra questão importante é a definição de regras claras sobre a possibilidade de cruzamento de dados com outras bases. O cruzamento deve ser feito de maneira ética e supervisionada, com relevância ao objetivo da pesquisa. Na Austrália, por exemplo, um projeto baseado em blockchain feito em parceria com o provedor de nuvem seguro Vault Systems e a startup local Agile Digital garante o controle de acesso a dados de saúde para a pesquisa.", "940700": "É importante que o agente de tratamento se preocupe com a base de dados que será utilizada, evitando um determinado viés indevido. É fundamental, ainda, que verifique a validade da base de dados. A utilização da menor quantidade possível de dados para a biometria (pontos biométricos) é importante, para que o risco assumido não seja desnecessário e não seja violada a finalidade. Além disso, é fundamental que seja feito um teste de balanceamento. Entendemos que um aviso de privacidade claro e adequado para que próprio titular entenda os riscos antes de fornecer o dado é algo que falta no mercado e é capaz de gerar casos como o da WorldID. Uma solução para evitar riscos no mercado é a utilização de um sandbox regulatório de tecnologias de reconhecimento fácil que estão sendo desenvolvidas para teste e aperfeiçoamento, sob supervisão regulatória direta, antes de uma ampla adoção nos titulares de dados.", "940701": "Trabalhando uma fase de desenvolvimento em que são feitos testes para identificar o viés da ferramenta. Os desenvolvedores devem apresentar documentos sobre todos os detalhes que envolvem o sistema que coleta, armazena dados. Essa responsabilidade não deveria ficar a cargo apenas do controlador. Dados sintéticos também podem ser utilizados para tentar identificar os riscos da ferramenta antes do lançamento. Após o lançamento, medidas devem ser tomadas para monitorar a utilização do sistema, inclusive garantindo aos titulares de forma clara que possam fazer reclamações, caso necessário. Nesse caso, entendemos que também que pode ser utilizado o sandbox regulatório de tecnologias de reconhecimento fácil que serão desenvolvidas para teste e aperfeiçoamento, sob supervisão regulatória direta, antes de uma ampla adoção no mercado.", "940702": "Entendemos que em ambientes de coleta massiva de dados, de alta circulação, não recomendável a utilização de biometria. Locais, por exemplo, como presídios, hospitais, casas de repouso, e locais frequentados por pessoas vulneráveis como crianças e adolescentes, também não. Aliás, já existe caso concreto nessa linha em São Paulo, com a suspensão do reconhecimento fácil pela ViaQuatro concessionária de parte das linhas do metrô. Ademais, não é recomendado o uso de tais tecnologias onde não há necessidade da

biometria, por exemplo, condomínios (para entrada e saída) e farmácias (para obtenção de descontos). Quando necessário, podem ser utilizadas outras formas de biometria como, por exemplo, a digital ou outros mecanismos.", "940704": "Quem desenvolve o sistema deve adotar o Privacy by Design (art. 46 da LGPD), mitigando os riscos durante a construção das ferramentas, inclusive com a garantia da segurança adequada. Em relação a quem utiliza uma ferramenta que trata dados biométricos, é importante um RIPD prévio com teste de balanceamento antes da utilização dos dados tratamento. Sugerimos, ainda, medidas específicas de segurança já recomendadas pela ANPD e outras autorizadas como o controle de acesso ao banco de dados (M2FA), criptografia, registro de logs, firewall, conexão segura, garantir que o local de armazenamento é seguro e atende aos requisitos da LGPD, prazo de retenção, perfis de acesso, plano de resposta de incidentes, saneamento das informações coletadas para a manutenção apenas dos dados biométricos, dentre outras.", "940707": "O controlador deve buscar métodos menos intrusivos antes de implementar qualquer exigência de coleta de dado biométrico. Caso seja possível ou seguro a adoção de algum método não intrusivo como a biometria, devem ser dadas outras alternativas para acesso aos serviços. Por exemplo, o CNIL determinou que alunos podem recusar um sistema biométrico de acesso ao refeitório, obrigando a instituição a fornecer um “badge” ou meio alternativo, assegurando que o aluno não sofra nenhum prejuízo, como por exemplo, enfrentar filas maiores. Só em contextos em que não haja outra forma segura de acessar o serviço é que o uso obrigatório da biometria pode se justificar. O controlador deve justificar de forma transparente a necessidade e imprescindibilidade do uso da biometria. Em relação aos contextos e restrições quando utilizado o consentimento, o responsável pelo tratamento tem de demonstrar que é possível recusar ou retirar o consentimento sem que o titular dos dados seja prejudicado.", "940708": "Evitar discriminação ilícita significa também atentar para possíveis vieses algorítmicos nos sistemas biométricos. Tecnologias de reconhecimento facial ou de impressões digitais podem ter taxas de erro maiores para certos grupos demográficos (ex., falhas reconhecidas no acerto com pessoas de pele escura, idosos ou crianças). Portanto, entendemos que os controladores devem testar seus sistemas regularmente para identificar vieses e mitigá-los na origem. Isso pode envolver treinamento adicional do algoritmo com dados mais representativos da diversidade de usuários previstos, ajuste de “thresholds” de reconhecimento para equilibrar falsos positivos/negativos, ou mesmo optar por outra tecnologia se o viés não puder ser reduzido a níveis aceitáveis. Importante destacar que a justiça no tratamento vai além da acurácia estatística: mesmo um sistema perfeitamente preciso pode excluir pessoas se não for pensado para inclusão.", "940709": "Para assegurar o respeito à autodeterminação informativa em contextos de vigilância biométrica contínua e massiva, visando a segurança dos titulares, não basta confiar em boas intenções, são necessárias ações concretas de transparência e accountability. Os titulares devem ser informados de forma clara, devem ter algum grau de escolha ou influência sobre como seus dados são usados, e precisam ter à disposição meios eficazes de exercer seus direitos. Os exemplos internacionais mostram que é possível equilibrar segurança e inovação tecnológica com privacidade. Diversos países europeus reforçaram isso com ações concretas – p.ex., a autoridade holandesa determinou que projetos de smart city publiquem avaliações de impacto e respeitem proporcionalidade, na França, a CNIL autorizou experimentalmente câmeras

“inteligentes” em espaços públicos apenas sob condições rigorosas: anonimização de imagens, exclusão rápida de dados pessoais e proibição de identificar indivíduos em tempo real. ", "940710": "É importante entender o direito à informação clara como a necessidade de expor um determinado visando o público e com a sua finalidade. A título de exemplo, na saúde suplementar, podemos mencionar a RN 623/24 da ANS que dispõe sobre as respostas que as operadoras devem fornecer aos pedidos dos beneficiários, determinando que “não serão admitidas respostas genéricas para atendimento aos prazos de que trata este artigo, como, por exemplo, ‘em análise’, ‘em processamento’, ‘em auditoria’, devendo ser circunstanciada em linguagem de fácil compreensão para o beneficiário”. A ideia é evitar termos genéricos e técnicos que não permitam ao beneficiário compreender o que está sendo dito. Entendemos que, em observância do princípio da transparência deverá ocorrer o mesmo com relação ao direito dos titulares, por meio de avisos de privacidade que permitam, antes da coleta, a compreensão real do tratamento e suas consequências, evitando-se casos como o do WorldID. ", "940711": "Entendemos que essa garantia poderá ser feita por meio do letramento digital, com campanhas educativas para os pais, de modo que possam orientar seus filhos. É preciso, também, exigir dos agentes de tratamento que exijam a presença dos pais, quando necessário. ", "940712": "É fundamental garantir a participação informada dos pais ou responsáveis em todo tratamento de dados da criança. Isso requer que o controlador obtenha o consentimento do responsável de forma verificável. A LGPD manda envia todos os esforços razoáveis para confirmar que o consentimento foi realmente dado pelo responsável e não pela própria criança. As informações sobre a coleta e uso dos dados devem ser fornecidas de maneira simples, clara e acessível, em linguagem apropriada às capacidades da criança, inclusive com recursos visuais quando cabível. Dessa forma, os pais entendem exatamente quais dados do filho serão coletados, para que finalidade, por quanto tempo, com quem poderão ser compartilhados, e quais direitos eles podem exercer. Transparência e clareza aumentam a confiança e permitem a participação ativa dos responsáveis nas decisões, em linha com as normas internacionais que asseguram às crianças o direito à privacidade e à proteção contra uso indevido de seus dados. ", "940714": "Para compatibilizar a prática de verificação biométrica de idade com os princípios da necessidade e do melhor interesse, deve-se: (a) usá-la somente se realmente indispensável para proteger a criança/adolescente; (b) garantir que os dados biométricos sejam manejados de forma responsável, segura e transparente, com consentimento dos pais; e (c) manter o foco no benefício ao menor (mantê-lo fora de conteúdos impróprios, por exemplo) acima de quaisquer interesses comerciais. Assim, a verificação de idade servirá ao propósito legítimo de proteger os jovens, sem se tornar, ela própria, uma fonte de risco ou violação de direitos. Por fim, é essencial que os dados de crianças e adolescentes em contextos como jogos online sejam usados com responsabilidade e respeitando seu melhor interesse.

Contribuinte: LEONARDO HENRIQUE CARDONIA DA SILVA

Número: OP-1006036

Data: 01/08/2025 - 12:55

Resumo: :"" , "940688": "" , "940690": "Conforme as diretrizes da Autoriteit Persoonsgegevens e da ICO, o enquadramento como dado biométrico depende de três elementos: (i) a natureza do dado; (ii) o meio e a forma de tratamento; e (iii) a finalidade de identificação ou autenticação do indivíduo. Nesses casos, tanto a biometria comportamental quanto a tradicional se submetem a salvaguardas reforçadas nos termos da LGPD. Embora existam argumentos de que a biometria comportamental esteja mais sujeita a variações, o que exigiria parâmetros mais rigorosos de qualidade para evitar falsos positivos ou negativos é importante destacar que a biometria tradicional também apresenta variabilidades. Alterações estéticas na face ou nos olhos, cada podem comprometer a acurácia de sistemas de reconhecimento facial ou de íris. Assim, tanto a biometria comportamental quanto a tradicional estão sujeitas a fatores que impactam sua confiabilidade técnica. Por esse motivo, ambas devem ser submetidas ao mesmo regime jurídico. " , "940693": "" , "940695": "A base legal do art. 11, II, “g” da LGPD — prevenção à fraude — deve ser interpretada conforme os princípios da necessidade, proporcionalidade e mitigação de riscos, sobretudo em tratamentos envolvendo dados biométricos. O EDPB admite o uso legítimo da biometria, desde que precedido de RIPD e justificado como proporcional (Guidelines 3/2019, p. 18). Exigir que ela seja a única alternativa possível desconsidera a realidade operacional das instituições e compromete soluções eficazes de segurança. Embora não seja o único método, a biometria pode ser a opção mais apropriada por conjugar eficácia, praticidade e segurança. Oferecer alternativas pode, em certos casos, gerar brechas exploráveis. O STJ (REsp 1.197.929) reconhece a responsabilidade objetiva das instituições financeiras por fraudes, o que justifica o uso de mecanismos robustos como a biometria. Portanto, a ANPD deve reconhecer que a biometria pode ser legítima mesmo sem ser o único meio possível." , "940697": "" , "940699": "" , "940700": "" , "940701": "" , "940702": "" , "940704": "" , "940707": "" , "940708": "" , "940709": "" , "940710": "" , "940711": "" , "940712": "" , "940714": "Nos casos em que a verificação ou estimação de idade é realizada por biometria, o tratamento de dados de crianças e adolescentes deve observar com rigor os princípios da necessidade e do melhor interesse. A biometria, por se tratar de dado sensível, só pode ser utilizada se a plataforma comprovar que não há alternativas menos invasivas, como validação de CPF, análise documental ou autodeclaração acompanhada de controles técnicos eficazes. O uso deve ser proporcional ao risco envolvido, devidamente fundamentado e documentado, preferencialmente por meio de RIPD. Embora não exista norma que imponha a biometria como forma obrigatória de verificação, sua adoção exige justificativa robusta e salvaguardas que assegurem finalidade específica, limitação de acesso, descarte seguro, segurança da informação, minimização de dados e transparência. A definição do método cabe à plataforma, desde que a escolha seja tecnicamente justificada e eficaz para restringir o acesso indevido por menores.

Contribuinte: Gabriela Brasil Nascimento Almeida

Número: OP-1006049

Data: 01/08/2025 - 13:01

Resumo: "O dado biométrico deve, necessariamente, resultar de um processamento técnico específico de atributos biométricos, conforme o Decreto nº 10.046/2019 (art. 2º, II) – ou seja, de características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado. Assim, dados-base que antecedem tal processamento, como meras imagens faciais ou fotografias, devem ser excluídos desse escopo. É necessário considerar o dado biométrico com um atributo que permita, sem quaisquer dúvidas, a identificação e a individualização direta e automática de uma pessoa. Assim, deve ser um atributo físico único e infungível, que não se confunda com meras informações que possam apenas ser associadas a uma pessoa.", "940688": "Em uma interpretação sistemática que considera os princípios de proteção de dados do art. 6º e os requisitos de livre acesso previstos no art. 9º, os controladores responsáveis pelo tratamento de dados biométricos devem buscar, sempre que possível em relação à necessidade de proteção de seus segredos de negócio, divulgar informações sobre o tipo de processamento biométrico que será realizado, os dados tratados, os agentes de tratamento envolvidos e a duração da atividade.", "940690": "Sugere-se, de forma geral, que o foco do regulador não repouse sobre o tipo de atributo biométrico em si, mas no tratamento associado. Assim, em se tratando de um atributo físico capaz de, mediante processamento automatizado, resultar na identificação ou autenticação de uma pessoa, estaríamos diante de um tratamento de dados biométricos. Em todos os casos, as obrigações aplicáveis aos agentes de tratamento seriam aquelas diretamente relacionadas à LGPD, especialmente aquelas relacionadas ao atendimento das obrigações de transparência e utilização das bases legais aplicáveis. Em resumo, entendemos que a biometria comportamental deva ser tratada da mesma forma que a biometria tradicional, desde que tal técnica de fato envolva o tratamento de atributos biométricos conforme definição do art. 2º, II, do Decreto nº 10.046/2019.", "940693": "O consentimento deverá: (i) representar uma escolha do titular; (ii) ser obtido mediante a apresentação de informações que expliquem ao titular a atividade que será realizada; (iii) ser obtido por ação afirmativa que revele concordância com as condições da atividade, sendo certo que a própria decisão de fornecer os dados deve configurar tal ação; e (iv) ser obtido de forma que fique claro para o titular que a atividade envolverá dados sensíveis. Dadas as características e fragilidades do consentimento – uma vez que há, em certa medida, a atribuição de responsabilidade ao titular para manifestação de sua autorização –, os controladores devem sempre avaliar se o consentimento é a base legal mais adequada para fazer valer, no caso concreto, o regime protetivo da LGPD. Em caso contrário, outras bases legais devem ser avaliadas.", "940695": "Um dos critérios principais é a avaliação - por exemplo, através de Relatório de Impacto – sobre se existem outros mecanismos menos invasivos que poderiam conceder o nível de segurança necessário para garantia de prevenção à fraude. Em geral, a biometria costuma ser mais eficiente que mecanismos tradicionais de autenticação, o que justificaria seu uso em serviços financeiros, bancários ou de saúde, considerando o alto impacto que uma fraude de acesso a esses sistemas teria na vida do titular. Diante disso, é razoável presumir que para essas categorias de serviços, a biometria é necessária para garantir o maior nível de segurança possível ao titular, sendo compatível com o princípio da necessidade. Para fins de mitigação de riscos, é relevante considerar que os riscos potenciais decorrentes de um vazamento de dados biométricos possuem alta

severidade, de forma que a implementação de mecanismos adicionais de segurança para acesso aos dados é essencial.", "940697": "Caso exista uma obrigação legal ou regulatória que determine o tratamento de dados biométricos pelo órgão público, o descumprimento dessa obrigação pode acarretar consequências jurídicas. Assim, a adoção de critérios adicionais com o objetivo de contornar tal obrigação não é recomendada. Dessa forma, é essencial que o controlador verifique se a obrigação legal realmente se aplica à sua atividade e identifique quais critérios mínimos estão previstos na legislação para a implementação do mecanismo de biometria. Quanto às salvaguardas, recomenda-se a aplicação de medidas adicionais de segurança, como controle de acesso aos dados, uso de criptografia e elaboração de relatórios de avaliação para documentação de riscos e definição de medidas de mitigação aplicáveis, sempre lembrando que os órgãos públicos estão sujeitos a maior escrutínio público e sistemas institucionais de controle, o que demanda medidas efetivas e verificáveis.", "940699": "Os limites para o tratamento de dados biométricos em pesquisa devem ser avaliados caso a caso, considerando salvaguardas técnicas proporcionais ao risco e a necessidade do uso para atingir a finalidade da pesquisa, conforme exposto no Guia Orientativo da ANPD sobre o tema. A anonimização é recomendada como mitigação de riscos, mas sua aplicabilidade depende do contexto e da necessidade de identificação do titular, de forma que, apesar de recomendada em geral, ela pode não ser eficaz para certas finalidades de pesquisa. Vale ressaltar que, embora a anonimização pressuponha a impossibilidade de reidentificação, especialistas e autoridades internacionais reconhecem que sempre haverá um risco residual, que deve ser assumido pelo controlador. Assim, é essencial avaliar se a técnica empregada reduz suficientemente o risco, considerando o contexto de segurança da informação geral e planejando revisões periódicas, mas sem estipular metas de redução máxima da possibilidade de reidentificação.", "940700": "", "940701": "", "940702": "Sugere-se que eventual regulamentação do tema considere apenas aspectos gerais e principiológicos, em linha com a abordagem de riscos da LGPD. Deve-se, assim, evitar definir situações como de uso proibido, sem que se considere o contexto específico da atividade.", "940704": "É possível citar medidas como criptografia, controle de acesso físico, due-diligence com subcontratados, avaliação sistêmica de vulnerabilidades e planos de resposta a incidentes eficazes, que devem ser implementadas de forma compatível com o risco da atividade, conforme avaliado na fase de desenvolvimento. Em relação aos mecanismos de avaliação e monitoramento, é importante considerar a elaboração de Relatório de Impacto em casos de riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como a retenção de logs, permitindo identificar e analisar acessos, tratamentos e compartilhamentos no contexto do uso da tecnologia.", "940707": "", "940708": "A anonimização das imagens coletadas pode ser uma medida eficaz se utilizada de forma pontual quando a identificação posterior do titular não for essencial. Contudo, apesar de ser uma medida relevante para mitigação de riscos, a imposição da anonimização pode se revelar prejudicial em alguns casos, considerando os riscos à precisão do dado biométrico e limitação de treinamento algorítmico. Para redução dos riscos de discriminação ilícita e abusiva, é essencial que os fornecedores de tecnologias de biometria possam realizar o treinamento e calibragem com bases de dados amplas e balanceadas, que auxiliem na redução de vieses e imprecisão no reconhecimento facial, por exemplo. Além disso, é recomendável que os controladores, na medida do possível, realizem

revisões e atualizações periódicas das ferramentas para assegurar seu funcionamento em compatibilidade com a LGPD.", "940709": "", "940710": "Diante da complexidade envolvida no tratamento de dados biométricos, é necessário um cuidado adicional para traduzir os detalhes técnicos em linguagem acessível, explicando de forma compreensível a lógica de tratamento dos dados biométricos, as medidas de segurança adotadas e o modo como os dados podem ser utilizados para identificar o titular. Tudo isso, em conjunto com os meios cabíveis para o exercício de direitos Apesar dessa necessidade de fornecer informações claras, ressalta-se que o controlador também deve preservar os segredos de sua tecnologia. Assim, é preciso ponderar o grau de informação que pode ser disponibilizado ao titular.", "940711": "Conforme estabelece o Enunciado CD/ANPD nº1/2023, outras bases legais, que não o consentimento, podem ser utilizadas para fundamentar o tratamento de dados de crianças e adolescentes. Diante disso, apesar de o consentimento parental ser recomendado em alguns contextos, o controlador pode considerar outras bases legais aplicáveis caso a caso, desde que priorizado o melhor interesse da criança, como a garantia de segurança do menor para identificação e acesso controlado ao ambiente escolar. Nessas ocasiões, o pai ou responsável deveriam ser devidamente informados sobre a atividade, suas finalidades e as medidas de segurança implementadas através de cláusulas específicas nos documentos de matrícula ou de documentos institucionais, por exemplo. Para demonstração do alinhamento com o princípio do melhor interesse, sugere-se que as instituições elaborem Relatório de Impacto com análise aprofundada sobre a atividade, ponderando os riscos e benefícios aos titulares.", "940712": "O tratamento de dados de crianças e adolescentes pode acontecer sob diversas hipóteses legais previstas na LGPD, desde que respeitado seu melhor interesse, como já reconhecido pela ANPD no Enunciado CD/ANPD nº1/2023. Nesses casos, cabe ao controlador definir a hipótese legal cabível, avaliando o contexto, riscos aos titulares e benefícios esperados. Por exemplo, o tratamento de dados biométricos de menores pode ocorrer como mecanismo de verificação de idade sob a base legal da prevenção contra a fraude. A participação informada dos pais pode ser garantida com mecanismos de transparência que disponham de linguagem acessível e canais abertos de comunicação e atendimento.", "940714": "

Contribuinte: FERNANDO BOUSSO

Número: OP-1006052

Data: 01/08/2025 - 13:03

Resumo: "[TIM S.A.]: Alinhada a parâmetros internacionais, como o GDPR, dados biométricos podem considerar critérios ligados a características físicas, fisiológicas ou comportamentais, tratados tecnicamente para identificação ou autenticação. O uso de biometria não implica necessariamente identificar alguém, sendo possível diferenciar “prova de humanidade” de “reconhecimento individual”. Ao operar como filtro de unicidade, a biometria assegura que cada utilizador é único, sem revelar identidade civil, protegendo a privacidade. Quando bem aplicada, é ferramenta para ambientes digitais seguros, equilibrando inovação e direitos fundamentais.", "940688": "[TIM S.A.]: Considerando a falta

de padrões na legislação nacional, recomenda-se adotar boas práticas internacionais como as do ICO (Reino Unido) para transparência no uso de dados biométricos. É fundamental informar aos titulares sobre o tratamento, considerando o contexto (relação, finalidade, interação com a tecnologia e impacto das decisões automatizadas). A abordagem deve ser adaptada a realidade da operação e da empresa, ao público e ao uso específico, sempre prezando pela clareza, acessibilidade e respeito à privacidade.", "940690": "[TIM S.A.]: A LGPD não diferencia modalidades biométricas, portanto, regulamentações não devem impor obrigações distintas sem base legal, em respeito ao princípio da legalidade. Biometrias faciais, vocais e comportamentais precisam do mesmo rigor de proteção, considerando riscos e salvaguardas. Recomenda-se regulamentação uniforme baseada em princípios, requisitos proporcionais à complexidade técnica, avaliação de impacto quando necessário e transparência. O equilíbrio entre proteção de dados e inovação deve nortear a regulação dessas tecnologias.", "940693": "[TIM S.A.]: Em alguns contextos pode ser que o consentimento não seja considerado adequado, como por exemplo, processos de autenticação cadastral seja na contratação de um produto ou serviço ou ainda, a acesso a aplicações, nos casos em que a sua finalidade de tratamento esteja vinculada a prevenção a fraude.", "940695": "[TIM S.A.]: A biometria, como parte de autenticação, trata-se de uma medida comprovadamente eficaz na proteção dos consumidores de fraudes sofisticadas e empresas de tentativas de apropriação de identidades. Documentar riscos e justificativas técnicas é importante para demonstrar conformidade com a lei e manter a segurança jurídica e operacional dos serviços.", "940697": "[TIM S.A.]: Para aplicar essa fundamentação legal, é preciso demonstrar a existência da norma que determina a obrigação, ou que seja possível comprovar que tal medida é suficiente para o cumprimento da obrigação imposta em lei e foi utilizada para essa finalidade, isso assegura que a coleta de dados esteja alinhada e compatível com a finalidade prevista. Em qualquer medida para que seja justificado o seu uso amparado na hipótese legal da obrigação legal ou regulatória, para além da previsão na legislação vigente, é necessário igualmente observar princípios e diretrizes previstas na LGPD.", "940699": "", "940700": "[TIM S.A.]: Para garantir que o uso de FRTs, mesmo quando amparado por base legal, respeite os princípios de necessidade, proporcionalidade e transparência, evitando discriminação ilícita ou abusiva, é fundamental adotar um conjunto integrado de salvaguardas técnicas (como medidas robustas de segurança), jurídicas (como bases legais, finalidade, políticas e procedimentos) e institucionais (como treinamento, canais de atendimento aos titulares, avaliação de impacto).", "940701": "", "940702": "[TIM S.A.]: O uso do reconhecimento facial representa uma solução tecnológica válida e eficiente para autenticação e segurança, podendo ser implementada por organizações após análise de sua viabilidade técnica, vantagens e possíveis riscos, conforme o contexto de cada aplicação. Cabe às empresas decidirem, de maneira autônoma, se essa tecnologia é a opção mais adequada, levando em conta a natureza do serviço, o propósito do uso e os princípios previstos na LGPD, como necessidade, minimização de dados e não discriminação.", "940704": "[TIM S.A.]: As organizações que operam esse tipo de tecnologia precisam de liberdade para adotar medidas de segurança compatíveis com o seu tamanho, a quantidade de dados tratados e os riscos envolvidos em suas atividades. A proteção dos dados biométricos deve ser orientada por uma avaliação de risco, levando em conta a sensibilidade

do uso e a abrangência do processamento. Assim, recomenda-se implementar controles técnicos e administrativos adequados ao contexto, respeitando os princípios de proporcionalidade e eficácia. Essas definições devem seguir as melhores práticas de segurança da informação, evitando padrões inflexíveis que possam aumentar custos sem trazer benefícios reais à proteção dos dados.", "940707": "[TIM S.A.]: É fundamental que a regulamentação assegure a liberdade das empresas em escolher e implementar as inovações tecnológicas mais adequadas às suas necessidades. Isso permite equilibrar de forma eficiente a proteção dos usuários, a prevenção de fraudes e a manutenção da continuidade dos serviços. Além de garantir a segurança e a confiança nos ambientes digitais, essa autonomia facilita respostas rápidas diante de novas ameaças e mudanças no mercado, promovendo soluções flexíveis que acompanham a evolução tecnológica sem engessar processos ou limitar a competitividade.", "940708": "[TIM S.A.]: Principais mecanismos de segurança e mitigação de riscos: cláusulas de proteção de dados nos contratos; treinamento de quem acessa dados; análise de risco e de vulnerabilidades; pentest; desenvolvimento seguro; gestão de incidentes; segregação de ambientes; análise de riscos.", "940709": "", "940710": "[TIM S.A.]: As instituições devem garantir meios acessíveis para titulares exercerem seus direitos, oferecendo informações claras e compatíveis com sua capacidade operacional. Esses direitos se aplicam a todo tratamento de dados, mesmo fora de decisões automatizadas. Sobre o direito de acesso, conforme o ICO, dados biométricos são outputs matemáticos “ilegíveis” para humanos, podendo ser substituídos por uma explicação que justifique a impossibilidade de entrega, descreva a natureza do dado e esclareça como ele é mantido pela organização. Políticas de privacidade claras e canais de contato devem estar disponíveis para os titulares.", "940711": "", "940712": "", "940714": ""

Contribuinte: ANA CLARA ARAUJO MAIA

Número: OP-1006068

Data: 01/08/2025 - 13:16

Resumo: "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail A LGPD não define diretamente dados biométricos, e podemos recorrer a instrumentos como a GDPR e a ISO 24741 que indicam três critérios cumulativos para poder construir uma definição pátria: relação com características físicas, fisiológicas ou comportamentais; tratamento por meios automáticos; e identificação do titular. A biometria só deverá ser considerada dado sensível se permitir essa identificação mediante o tratamento por meios automáticos. Reconhecimento facial, por exemplo, será considerado dado biométrico se identificar a pessoa em tratamento automático. Dados biométricos anonimizados deixam de ser dados pessoais. A ISO/IEC 2382-37:2022 e autoridades como ICO e AEPD reforçam a necessidade de processo técnico na coleta para que se configure dado biométrico. ", "940688": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Não há padrão único para informar titulares sobre uso de biometria. Práticas devem ser compatíveis com o contexto, como avisos físicos, QR codes, materiais digitais ou orientação

presencial. A LGPD, ao não definir um rol fixo, permite adaptação conforme o modelo de negócio, finalidade e volume de dados. A comunicação deve ser clara, proporcional e respeitar os princípios da transparência e autodeterminação informativa."

","940690": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail A LGPD não distingue biometria comportamental da tradicional, ambas são dados sensíveis. A comportamental, no entanto, é mais suscetível a riscos por ser invisível, variável e vulnerável a falsificações. Controladores devem considerar essas diferenças em análises de risco, adotando salvaguardas proporcionais. O tratamento deve respeitar os princípios da LGPD conforme a configuração concreta do uso."

","940693": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail O consentimento deve ser livre, específico, destacado, informado e inequívoco, conforme a LGPD e a orientação do EDPB. Isso envolve ausência de coação, informação clara e ato afirmativo do titular.. A escolha da base deve considerar o contexto e a finalidade, com salvaguardas adequadas e análise de riscos e deve ser uma escolha do agente de tratamento. "

","940695": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Aplica-se com critérios similares ao legítimo interesse, exigindo finalidade legítima, necessidade do tratamento e mitigação de riscos. O uso de biometria deve ser estritamente necessário, com adoção de medidas como criptografia, anonimização ou uso de tecnologias PETs. Essa base é inovação brasileira e deve ser reconhecida como instrumento de política pública para segurança digital e prevenção de ilícitos. "

","940697": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Quando houver base legal, o tratamento deve ser proporcional, razoável e documentado, com atenção a princípios da LGPD como necessidade e transparência. O uso de biometria por órgãos públicos, como no caso do KYC bancário, pode ser legítimo se houver salvaguardas como anonimização e governança. A ANPD já oferece guias específicos sobre boas práticas para o setor público "

","940699": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Para se evitar risco de reidentificação recomenda-se uso de técnicas como privacidade diferencial, dados sintéticos, criptografia homomórfica, ZKP, computação multi-partidária segura, entre outras. Além disso, é essencial limitar acesso a dados brutos, conscientizar pesquisadores e estabelecer regras de compartilhamento e governança dos resultados."

","940700": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail O ideal é que os dados biométricos fiquem sob controle do titular. Quando isso não for possível, devem ser aplicadas salvaguardas como anonimização, transparência ativa, governança, comitês técnicos, testes de viés e acurácia, avaliações contínuas e canais para exercício de direitos. A escolha da tecnologia deve considerar o contexto, finalidade e riscos, promovendo proporcionalidade e conformidade com a LGPD. "

","940701": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail A eficácia de sistemas de reconhecimento facial depende de sua configuração técnica. O controlador deve escolher tecnologia conforme a finalidade, dados e ambiente de coleta. Devem ser previstos monitoramento contínuo, RIPD, testes de desempenho e canal de correção para titulares. A

solução mais eficaz e menos invasiva deve ser priorizada, seguindo padrões como ISO/IEC e NIST.", "940702": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail A decisão de uso de reconhecimento facial deve ser baseada em avaliação de risco. Mesmo quando usado, o RF deve observar necessidade, proporcionalidade, governança e segurança. Proibições genéricas não são adequadas – o contexto é decisivo. ", "940704": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Dados biométricos devem, idealmente, estar sob custódia do titular. Caso contrário, controladores devem aplicar medidas como criptografia, controle de acesso, tokenização irreversível e uso de PETs. A LGPD exige governança em privacidade, com RIPD, plano de resposta a incidentes, políticas internas e treinamento. Regras fixas não são recomendadas – a proteção deve se adaptar ao risco e ao contexto. ", "940707": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail A limitação de funcionalidades com base na recusa do titular em fornecer biometria só é lícita se o dado for estritamente necessário para a finalidade, como garantir segurança em operações de alto risco. A exigência deve ser informada claramente ao titular. A restrição deve ser proporcional e nunca afetar o serviço como um todo, apenas a funcionalidade específica. A recusa não deve gerar tratamento discriminatório. O controlador deve garantir canais de atendimento e meios alternativos, quando viável, sempre documentando as justificativas conforme os princípios da LGPD.", "940708": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Incluem limitação de finalidade, retenção mínima, uso proporcional dos dados, transparência com o titular, anonimização sempre que possível e acesso restrito. PETs como ZKP e computação multipartidária fortalecem essas práticas. Controladores devem revisar sistemas, mitigar vieses, permitir contestação de decisões automatizadas e promover governança contínua sobre o tratamento. ", "940709": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Em contextos como smart cities e eventos públicos, a transparência deve ser adaptada ao ambiente, com QR codes, avisos visuais e canais acessíveis. A retenção de dados deve ser mínima, e os dados anonimizados quando possível. O tratamento deve ter finalidade clara, e as tecnologias devem ser avaliadas continuamente quanto a eficácia, riscos e aderência à LGPD.", "940710": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Os titulares devem ter acesso claro a informações sobre tratamento, inclusive por meio de políticas e centrais de privacidade. Quando possível, dados biométricos devem ficar sob controle direto do titular. Tecnologias como ZKP e computação multipartidária possibilitam esse modelo. A revisão de decisões automatizadas deve ser garantida conforme previsto na LGPD. ", "940711": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail A LGPD exige proteção especial a crianças e adolescentes. O tratamento deve seguir o melhor interesse, com base legal adequada e comunicação clara aos responsáveis. A avaliação de riscos deve considerar proporcionalidade e alternativas menos invasivas. A biometria pode ser legítima em contextos como segurança escolar ou KYC, desde que com salvaguardas robustas e governança apropriada.", "940712": "Contribuição

Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail Controladores devem limitar o tempo de retenção, anonimizar ou pseudonimizar dados e adotar controle de acesso rigoroso. O controle parental deve equilibrar proteção e acessibilidade. A análise de riscos deve considerar contexto, finalidade, volume e grau de exposição. Políticas de descarte, auditorias e documentação reforçam a conformidade e a segurança.", "940714": "Contribuição Resumida do Movimento Inovação digital (MID) - a versão completa com argumentações será enviada no e-mail A verificação de idade por biometria deve ser adotada se atender ao melhor interesse do menor. Alternativas incluem autodeclaração, validação documental ou confirmação dos pais. Tecnologias como ZKP podem permitir a verificação preservando a privacidade. A escolha deve considerar risco, finalidade e governança do agente de tratamento.

Contribuinte: Ariel Uarian Queiroz Bezerra

Número: OP-1006073

Data: 01/08/2025 - 13:18

Resumo: "Para que um dado pessoal seja caracterizado como biométrico é necessário observar critérios objetivos relacionados à sua natureza, ao tratamento técnico específico que extraiam, interpretem ou analisem essas características físicas, fisiológicas ou comportamentais de uma pessoa natural de forma padronizada com finalidade de identificação. São exemplos de dados pessoais biométricos: impressões digitais, reconhecimento facial, leitura da íris, geometria da mão, padrão de voz ou até características comportamentais, como o modo de digitar ou caminhar.", "940688": "A transparência ativa exige que os controladores adotem medidas proativas, claras e acessíveis para garantir que os titulares compreendam, antes da coleta, como seus dados biométricos serão tratados. Portanto é importante a existência de Política de Privacidade específica ou seção dedicada à biometria facilmente disponível, inclusive em formato impresso ou digital nos pontos de coleta disponibilizando o canal para envio de esclarecimento de dúvidas. O auxílio de materiais visuais explicativos como o uso de vídeos curtos, animações ou infográficos pode tornar as informações mais compreensíveis, especialmente para públicos diversos ou com menor familiaridade com termos jurídicos ou técnicos.", "940690": "A biometria comportamental apresenta características e desafios distintos da biometria tradicional. Embora ambas sejam voltadas à identificação de pessoas a partir de aspectos únicos, a biometria comportamental baseia em padrões dinâmicos. Portanto, é fundamental avaliar se o dado está sendo tratado para autenticação, monitoramento ou análise preditiva, o que impacta diretamente nos riscos envolvidos, principalmente pela facilidade de uso indevido desses dados para fins de fraude, inclusive por terceiros mal intencionados que tenham acesso aos comportamentos registrados em redes sociais ou outras plataformas públicas. ", "940693": "Avaliar o consentimento para tratamento de dados pessoais biométricos na prática é um desafio, sobretudo em contextos de vulnerabilidade ou de alta dependência do serviço o que pode resultar na liberdade de escolha do titular. Quando o titular precisa fornecer sua biometria para obter atendimento de saúde pública, benefícios sociais ou educação, por exemplo, há um risco concreto de o

consentimento ser apenas formal, e não substancialmente livre. Cenários de alta volumetria e tratamento automatizado, como sistemas de autenticação em larga escala, o uso do consentimento como base legal também pode ser inadequado porque a gestão dos consentimentos se torna operacionalmente inviável, devendo optar por outra base legal como a segurança do titular, nos processos de identificação e autenticação de cadastro.", "940695": "Deve ser observado a demonstração concreta da necessidade e da adequação da medida ao risco que se pretende mitigar, por exemplo, prevenção de fraudes em operações bancárias, autenticação segura para acesso a contas digitais ou serviços financeiros. Além do mais, que a coleta seja estritamente indispensável para a finalidade declarada. Isso significa que o simples aumento da segurança ou da conveniência não justifica, por si só, o uso de biometria o tratamento só deve ocorrer quando houver proporcionalidade entre o risco enfrentado e o grau de sensibilidade dos dados coletados.", "940697": "Observar com rigor os princípios do Art.6 da LGPD em especial o princípio da necessidade, além de implementar regulamentação mais detalhada sempre considerando alternativas menos invasivas à biometria, quando viáveis. Um exemplo emblemático é o uso de reconhecimento facial em estádios de futebol para controle de acesso e segurança pública. Embora haja respaldo legal, o tratamento exige critérios técnicos claros, segregação de bases de dados, e limitação do compartilhamento de informações com outras entidades. A coleta e o uso devem estar claramente delimitados por norma específica, com escopo definido e regras de retenção e descarte. ", "940699": "Deve respeitar limites relacionados à finalidade científica, à necessidade dos dados utilizados e à segurança ao longo de toda a cadeia de tratamento. Mesmo em cenários em que os dados estejam anonimizados, os riscos à privacidade dos titulares permanecem relevantes, especialmente diante da possibilidade de cruzamento de bases de dados e reidentificação posterior, fenômeno cada vez mais comum com o avanço da tecnologia.", "940700": "O desenvolvimento da ferramenta deve considerar não apenas a eficiência da ferramenta, mas a proteção das pessoas, especialmente daquelas em situação de vulnerabilidade ou suscetíveis a discriminação algorítmica. Portanto, importante a adoção de calibragem do software, auditorias técnicas, realizar relatório de impacto, transparência ativa, governança de dados e treinamento.", "940701": "Devem ser implementadas rotinas de validação técnica periódica, com avaliação de desempenho em condições reais de uso, para medir e corrigir taxas de falsos positivos e falsos negativos, além de revisão humana qualificada, especialmente em casos de negativa de acesso, identificação incorreta ou consequências legais/sociais e documentação detalhada do sistema, incluindo arquitetura do modelo, métodos de coleta e treinamento de dados, limitações conhecidas e métricas de desempenho. ", "940702": "Sim, é possível e necessário identificar situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado, especialmente quando sua finalidade pode ser atingida por meios menos invasivos ou quando não se demonstrar a estrita necessidade da biometria facial. O princípio da minimização de dados, aliado ao princípio da necessidade (art. 6º, III, LGPD), impõe que o controlador escolha a solução proporcional ao risco e adequada à finalidade, evitando o uso de dados sensíveis sempre que possível.", "940704": "É indispensável que os controladores adotem medidas técnicas e administrativas, as quais destacam-se: Canal de atendimento funcional e acessível aos titulares; Política de retenção e

descarte seguro de dados biométricos, com prazos definidos e revisão periódica da necessidade de manutenção dos dados; Plano de resposta a incidentes, com protocolos definidos para contenção, investigação, notificação à ANPD e comunicação aos titulares, conforme o art. 48 da LGPD; Estrutura de engenharia de dados dedicada à organização e segregação dos bancos de dados, com controles de acesso, trilhas de auditoria e isolamento de dados sensíveis, de forma a facilitar a contenção e mitigação de danos em caso de vazamento.

","940707": "Proporcionar alternativas viáveis de autenticação, como uso de senhas, tokens ou múltiplos fatores de autenticação (MFA), garantindo que a recusa ao uso da biometria não inviabilize o acesso ao serviço como um todo, mas apenas, quando estritamente necessário, a uma funcionalidade específica cuja segurança técnica justifique a exigência. Além disso, é essencial que o tratamento seja acompanhado de transparência ativa em que o titular deve ser informado, de forma clara e acessível, sobre a finalidade do uso da biometria, as consequências da não adesão, os direitos que possui e os meios alternativos disponíveis."

","940708": "Entre as medidas essenciais, destaca-se a informação clara ao titular no momento da coleta, incluindo a finalidade do tratamento, a base legal utilizada, os direitos disponíveis e eventuais consequências da recusa ao fornecimento dos dados. Além disso, é fundamental que os algoritmos utilizados sejam treinados com bases de dados diversas, evitando viés discriminatório por raça, gênero, idade ou outras características. A falta de diversidade pode gerar padrões de reconhecimento errôneos e injustos, com impactos diretos sobre grupos vulneráveis."

","940709": "Criação de um portal de transparência acessível ao titular, contendo informações claras sobre a finalidade do monitoramento, tecnologias utilizadas, base legal, direitos dos titulares e canais para exercício desses direitos. Também é essencial implementar sinalização visível e compreensível nos locais monitorados, informando a existência do uso de tecnologias de reconhecimento facial ou outras formas de coleta biométrica, de forma que o titular não seja surpreendido."

","940710": "Para garantir o respeito aos direitos dos titulares em contextos de tratamento automatizado de dados biométricos, os agentes de tratamento devem implementar mecanismos acessíveis e eficazes que possibilitem o exercício desses direitos de forma contínua e transparente. Uma boa prática é a disponibilização de um portal de transparência integrado ao canal do titular."

","940711": "Participação informada dos pais ou responsáveis e à observância do princípio do melhor interesse da criança, conforme o art. 14 da LGPD e demonstrar que os benefícios superam os riscos, especialmente quando a biometria é utilizada para controle de acesso, proteção e segurança física dos menores. Importante evitar o armazenamento excessivo de dados, priorizando tecnologias que operem localmente ou com descarte automático após a verificação e celebrar contratos e/ou termo claro com os pais ou responsáveis, explicando a finalidade, os limites do uso, as medidas de segurança e os direitos envolvidos."

","940712": "O tratamento de dados pessoais sensíveis de crianças, como dados biométricos, pode ser admitido com base no art. 11, II, alínea "g" da LGPD, que permite o tratamento para segurança do titular, nos processos de identificação e autenticação de cadastro. Para participação informada dos pais ou responsáveis, é essencial envolvê-los desde o início por meio de reuniões explicativas, nas quais sejam apresentados os objetivos, os riscos e as medidas de segurança adotadas. Além disso, é fundamental que o tratamento esteja sempre alinhado ao princípio do melhor interesse da criança, inclusive com o desenvolvimento de

educação digital.", "940714": "Nos casos de verificação ou estimação de idade para acesso a plataformas digitais e jogos, especialmente no contexto de entretenimento, o tratamento de dados de crianças e adolescentes deve respeitar o princípio da necessidade e o melhor interesse do menor, conforme previsto na LGPD. Deve-se priorizar métodos menos invasivos, evitando o uso de dados biométricos sempre que possível. Soluções como verificações baseadas em comportamento, auto declaração com controle parental ou métodos técnicos que não envolvam identificação direta podem ser alternativas mais adequadas. Além disso, é recomendável oferecer uma segunda camada de controle familiar, como autorização ativa dos pais ou responsáveis, garantindo a participação e a supervisão no processo de acesso, reforçando a proteção dos direitos da criança e do adolescente sem recorrer, de imediato, a dados sensíveis.

Contribuinte: HORTENCIA RICARTE DE OLIVEIRA PAIZANTE

Número: OP-1006098

Data: 01/08/2025 - 13:29

Resumo: "Contribuição ABES: Nem todo dado biométrico é, por si só, um dado pessoal. Somente será considerado sensível quando utilizado para identificar ou tornar identificável uma pessoa natural. A LGPD não define dados biométricos, mas referências internacionais como o GDPR (art. 4º, 13) e a norma ISO 24741 estabelecem três critérios cumulativos: (i) relação com características físicas, fisiológicas ou comportamentais de um indivíduo; (ii) tratamento por meio de tecnologia automatizada; e (iii) finalidade de identificação. Dessa forma, tecnologias como o reconhecimento facial só envolvem dado biométrico sensível quando, no caso concreto, permitem identificar alguém de forma única. Caso não haja possibilidade de identificação, ainda que com uso de características físicas e tratamento automatizado, o dado não será considerado sensível. Da mesma forma, dados biométricos que tenham sido anonimizados deixam de ser considerados dados pessoais, por não permitirem a identificação do titular.", "940688": "Contribuição ABES: Controladores devem garantir transparência no tratamento de dados pessoais, conforme a LGPD, informando claramente os titulares sobre finalidades e formas de uso. No caso de dados biométricos, dada sua diversidade e contextos de aplicação, não há modelo único de transparência. Em linha com o ICO, recomenda-se avaliar o contexto específico, podendo-se usar avisos físicos, digitais (QR code), folhetos, vídeos ou orientação direta, sempre com linguagem clara. A LGPD não define “dado biométrico”, apenas o classifica como sensível. Assim, sua caracterização exige análise técnica e da finalidade do tratamento. A mera natureza comportamental não basta. Essa abordagem evita ampliação indevida do conceito e assegura equilíbrio entre proteção e inovação. Quando operadores processam biometria comportamental embarcada em softwares, cabe ao controlador definir se o uso configura dado sensível.", "940690": "Contribuição ABES: Ao incluir os dados biométricos entre os dados sensíveis, a LGPD não dispõe sobre hierarquias internas aos dados biométricos ou obrigações em específico para determinados tipos de dados biométricos. Os únicos dados sensíveis que têm obrigações específicas são os dados referentes à saúde, disciplinados especialmente nos § 4º e 5º do art. 11, mas estes não

se confundem com os dados biométricos, conforme redação ao inc. II do art. 5º, que os apresenta separadamente. Não há obrigações específicas à biometria comportamental, mas ela deve ser levada em consideração em análises de impacto e na definição do contexto e natureza do tratamento, respeitando os princípios da LGPD de forma adequada à sua configuração fática, a exemplo de todo tipo de dado biométrico. A biometria comportamental difere de traços estáticos como impressões digitais ou íris. Para manter a tecnologia legal e confiável, os reguladores devem impor salvaguardas adicionais além das regras biométricas usuais", "940693": "Contribuição ABES: Segundo o Guia de Consentimento do EDPB, o consentimento é válido quando atende aos seguintes requisitos: (i) livre, sem coerção, exigência desnecessária ou prejuízo em caso de recusa; (ii) específico, relacionado a finalidades determinadas e apresentadas de forma granular; (iii) destacado, com informação clara e ato afirmativo do titular (como clique ou marcação); (iv) informado, com conhecimento da identidade do controlador, finalidades, tipos de dados, direitos do titular e, quando aplicável, decisões automatizadas e transferências internacionais; e (v) inequívoco, expresso por ato afirmativo, não por omissão. O consentimento pode ser utilizado como base legal sempre que essas condições forem atendidas, podendo ser utilizado ainda quando houver interesse legítimo, obrigação legal ou execução de políticas públicas.", "940695": "Contribuição ABES: O tratamento de dados biométricos para prevenção à fraude é permitido pela LGPD (art. 11, II, “g”), desde que os direitos dos titulares não sejam sobrepostos. A ANPD, em seu Guia de Legítimo Interesse, orienta que essa base legal siga critérios semelhantes ao teste de balanceamento, exigindo análise de necessidade, proporcionalidade e medidas de mitigação. O controlador deve avaliar: (i) se a finalidade é de fato prevenção à fraude; (ii) se ocorre em ambiente eletrônico; (iii) se o uso de biometria é estritamente necessário; e (iv) quais salvaguardas podem ser aplicadas. Tecnologias de anonimização, como computação multipartidária segura e criptografia homomórfica, podem reduzir riscos, mas sua adoção deve considerar o contexto. Essa base legal, exclusiva da LGPD, visa promover segurança nos meios digitais e deve ser tratada como autônoma, com incentivos regulatórios que respeitem sua natureza e finalidade de interesse público.", "940697": "Contribuição ABES: A aferição de obrigação legal ou regulatória no mais das vezes não depende da identificação de titulares, devem ser estimuladas medidas de salvaguarda específicas para os dados biométricos sempre que eles materialmente apresentem risco de identificação indevida dos titulares. Exemplo as tecnologias oferecidas no relatório da ONU <https://11nq.com/vUaBT>. Computação Multipartidária Segura, criptografia homomórfica, privacidade diferencial, dados sintéticos, prova de conhecimento zero e ambientes de Execução Confiáveis e Enclaves Seguros. A lista é exemplificativa e não há possibilidade de obrigação ex ante relativa a uma ou outra tecnologia, já que cada uma se adequa a um certo ambiente ou contexto de tratamento. Ainda que devam operar sob a recomendação de anonimizar ou pseudonimizar dados biométricos antes de comunicações de dados e informações ao Poder Público, os controladores devem ter flexibilidade para escolher a melhor tecnologia que se adequa a seus dados e tratamento", "940699": "Contribuição ABES: O art. 13 da LGPD estabelece que pesquisas devem, sempre que possível, utilizar dados anonimizados ou pseudonimizados. Tecnologias como computação multipartidária segura, criptografia homomórfica, privacidade

diferencial, dados sintéticos, aprendizado distribuído, Prova de Conhecimento Zero e Ambientes de Execução Confiáveis são exemplos recomendados pela ONU, mas sua adoção depende do contexto, sem imposição prévia. Além disso, é importante adotar medidas especiais de controle de acesso a dados não anonimizados ou pseudonimizados e aos ambientes de pesquisa. A ANPD pode promover políticas de conscientização sobre riscos à privacidade em pesquisas, orientando quanto ao compartilhamento seguro de resultados, especialmente quando não for possível anonimizar os dados. Essas diretrizes reforçam a proteção à privacidade e a responsabilidade dos pesquisadores no tratamento de dados pessoais."

"940700": "Contribuição ABES: Segundo o EDPB, o ideal é que dados biométricos sejam armazenados sob controle exclusivo do titular, inclusive a chave de criptografia. Não sendo possível, outras salvaguardas devem ser adotadas conforme os princípios da LGPD. Destacam-se: (i) garantia de qualidade dos dados, (ii) anonimização, (iii) transparência ativa, (iv) governança com comitês especializados, (v) treinamento contínuo e (vi) acompanhamento periódico. O uso de reconhecimento facial deve respeitar os princípios da necessidade, proporcionalidade, transparência e não discriminação. Em contextos como prevenção à fraude, o uso pode ser legítimo e essencial, desde que proporcional ao risco e com salvaguardas adequadas. Em soluções embarcadas, a conformidade depende da configuração feita pelo controlador, cabendo ao operador assegurar aspectos técnicos, sem definir base legal ou finalidade. A proteção efetiva requer divisão clara de responsabilidades entre os agentes de tratamento (<https://11nq.com/8K2bt>)"

"940701": "Contribuição ABES: A acurácia é essencial no tratamento de dados biométricos, segundo o ICO. O controlador deve garantir a qualidade dos dados, escolher tecnologias adequadas à finalidade e minimizar riscos como falsos positivos ou negativos. Soluções menos invasivas devem ser priorizadas, respeitando o equilíbrio entre necessidade e impacto. O tratamento deve seguir o princípio do privacy by design, com salvaguardas técnicas e bases de dados diversas. Em sistemas operados por terceiros, o controlador deve parametrizar o uso conforme a LGPD. Na segurança pública, o reconhecimento facial deve focar em eficácia, não em infalibilidade. É essencial calibrar os sistemas ao contexto urbano, usar bases atualizadas, realizar testes contínuos e prever revisão humana. Falsos positivos devem ser corrigidos com transparência. A LGPD não se aplica a atividades de repressão penal (art. 4º, III), que seguem regime próprio e exigem soluções ágeis, auditáveis e proporcionais ao risco real."

"940702": "Contribuição ABES: O uso de reconhecimento facial deve ser evitado quando a finalidade pode ser atingida sem identificar o titular ou por meios menos invasivos, conforme o princípio da necessidade da LGPD. Tecnologias alternativas, como câmeras que apenas registram ocupação ou métodos de autenticação como cartões, senhas ou multifator, devem ser priorizadas. A escolha cabe ao controlador, conforme o contexto do tratamento. Mesmo quando o reconhecimento facial for necessário, recomenda-se o uso de soluções que preservem a privacidade, como tecnologias de zero knowledge proof (ZKP) ou agentes fiduciários de dados, que permitem autenticação sem compartilhamento excessivo de informações pessoais. Tais abordagens ajudam a evitar rastreamento, vigilância indevida e exposição desnecessária de dados, promovendo maior proteção à privacidade dos titulares."

"940704": "Contribuição ABES: Segundo o EDPB, o ideal é que dados biométricos fiquem sob controle do titular, com armazenamento local ou centralizado, mas com a chave

criptográfica em sua posse. Sempre que possível, o controlador deve permitir proteções adicionais, como senhas ou autenticação via dispositivo móvel, garantindo o direito de acesso e prevenindo incidentes de segurança. Quando isso não for viável, é essencial adotar medidas rigorosas de segurança, como controle de acesso e criptografia avançada. Tais medidas, por questões de segurança, nem sempre podem ser divulgadas publicamente. Para reforçar a proteção, recomenda-se o uso de tecnologias de aprimoramento de privacidade (PETs) e boas práticas de governança. O uso de modelos biométricos tokenizados e irreversíveis, processados com forte criptografia, impede a vinculação com pessoas reais mesmo em caso de vazamento, protegendo efetivamente os titulares contra exposições indevidas.", "940707": "Contribuição ABES: A restrição de funcionalidades por recusa do titular em fornecer dados biométricos deve atender a dois requisitos de legalidade: (i) o uso de biometria deve ser estritamente necessário para a finalidade do controlador, não havendo alternativa com igual eficácia para autenticação ou segurança; e (ii) a exigência do dado deve ser claramente comunicada, conforme o §3º do art. 9º da LGPD, por meios que garantam transparência, como banners, avisos físicos ou políticas de privacidade. Em contextos de alto risco, como acesso a contas com grandes valores, reemissão de credenciais digitais ou entrada em áreas seguras, a exigência de biometria pode ser proporcional e legítima. Nesses casos, deve-se oferecer ao titular opções como contato com um agente humano, registro de reclamações ou migração para outro fornecedor, evitando que a recusa resulte em tratamento desproporcional ou perda injustificada de serviço", "940708": "Contribuição ABES: Dentre as boas práticas no tratamento de dados biométricos, destacam-se: (i) limitação de finalidade, com uso restrito à finalidade originalmente informada; (ii) limitação do período de retenção, mantendo os dados apenas pelo tempo necessário; (iii) escolha de dados relevantes, garantindo necessidade, proporcionalidade e acurácia; (iv) transparência ao titular, com clareza sobre a coleta e uso dos dados; (v) anonimização, sempre que possível; e (vi) acesso restrito ao titular, com preferência por tecnologias que permitam seu controle direto. Tais práticas devem ser adaptadas ao contexto de cada operação. Destacam-se também as privacy-enhancing technologies (PETs), como computação multipartidária segura, criptografia homomórfica, privacidade diferencial, dados sintéticos, aprendizado distribuído, Zero Knowledge Proofs e ambientes de execução confiáveis. A adoção dessas tecnologias deve considerar a finalidade e o contexto do tratamento.", "940709": "Contribuição ABES: É essencial verificar se os dados biométricos são usados para identificar indivíduos de forma única. Se não houver essa finalidade, como em medições de fluxo de pessoas ou padrões de tráfego, os riscos são menores. Conforme o ICO, o controlador deve avaliar o contexto do tratamento e informar os titulares por meios acessíveis, como QR codes, avisos físicos ou digitais, sempre indicando os direitos e formas de exercê-los, salvo em casos de abuso ou frustração da finalidade legítima (como segurança pública). Relações prévias com o titular podem indicar interesse legítimo. A retenção deve ser limitada ao tempo estritamente necessário. Para mitigar riscos, recomenda-se: (i) anonimizar dados quando não for necessária a identificação; (ii) delimitar com precisão a finalidade do tratamento, evitando usos excessivos; e (iii) realizar avaliações contínuas sobre riscos, resultados e melhorias das soluções tecnológicas.", "940710": "Contribuição ABES: Os direitos da LGPD se aplicam a todos os dados pessoais, inclusive biométricos. Recomenda-se tratá-los como biométricos

apenas quando usados para identificar um titular de forma única, o que facilita a aplicação dos direitos dos titulares. O direito à informação exige transparência clara, concisa e adequada ao público, mas pode ser mitigado em situações de desproporcionalidade ou risco à finalidade do tratamento (como em pesquisas ou prevenção à fraude). Por conterem informações diretamente ligadas à identidade física, os dados biométricos devem, sempre que possível, ser mantidos sob controle exclusivo do titular, o que reduz riscos e facilita o exercício de direitos. Tecnologias de aprimoramento da privacidade (PETs), como computação multipartidária segura, criptografia homomórfica e testes de conhecimento zero, permitem que apenas o titular mantenha os dados, enquanto o controlador opera com dados anonimizados", "940711": "Contribuição ABES: É positiva a interpretação de que os grupos vulneráveis, segundo a LGPD, se restringem a crianças e adolescentes, que merecem proteção especial. Qualquer ampliação desse conceito exige base legal clara, evitando imposições arbitrárias ou a coleta excessiva de dados para identificar vulnerabilidades, em desacordo com os princípios da necessidade e minimização. Quanto à informação aos pais, deve-se adotar formas eficazes conforme o contexto, como avisos físicos e comunicação direta. Todas as bases legais são admissíveis para o tratamento de dados de menores, desde que observem o princípio do melhor interesse, conforme enunciado da ANPD. A aplicação desse princípio deve considerar, caso a caso, os benefícios do uso do serviço para o menor, como entretenimento, educação ou comunicação, sempre ponderando os riscos à integridade e aos direitos de crianças e adolescentes.", "940712": "Contribuição ABES: A resposta sobre participação informada e hipóteses legais se encontra na Questão 16. Sobre medidas técnicas e organizacionais para evitar abusos, vazamentos ou acessos indevidos, destacam-se, sem prejuízo de outras: (i) Limitação do período de retenção. Os controladores devem enviar esforços para limitar o tempo de retenção dos dados biométricos, mantendo-os em seus servidores apenas na exata medida da consecução da finalidade; (ii) Anonimização Os dados biométricos devem ser anonimizados, sempre que possível à luz da finalidade e da configuração fática do tratamento. Alternativamente, podem também ser pseudonimizados, com a manutenção da chave de reidentificação em localizações físicas ou virtuais diferentes daquela dos dados pseudonimizados; (iii) Acesso restrito aos titulares. Os dados biométricos, sempre que possível à luz da finalidade e configuração fática do tratamento, devem ter acesso restrito aos titulares, inclusive com a hipótese de exercício direto.", "940714": "Contribuição ABES: Quando a verificação de idade for feita por meio de dado biométrico, o controlador deve avaliar: (i) se o acesso ao serviço atende ao melhor interesse da criança ou adolescente, considerando conteúdos adequados e benefícios como entretenimento, educação ou comunicação, sempre ponderando riscos; e (ii) se existem meios alternativos e seguros para verificar a idade, como autodeclaração, autorização dos pais ou exame documental. Mesmo sendo possível o uso de biometria, é recomendável considerar tecnologias que preservem a privacidade, como zero knowledge proofs (ZKP) ou agentes fiduciários de dados, que permitem a verificação sem expor informações pessoais a múltiplos agentes. Essas alternativas evitam o tratamento excessivo de dados, práticas de vigilância e rastreamento indevido de menores em ambientes digitais.

Contribuinte: THOMAZ LOPES CORTE REAL

Número: OP-1006110

Data: 01/08/2025 - 13:35

Resumo: "1. O critério deve ser de origem biológica ou comportamental. O dado então deriva de características físicas ou comportamentais do indivíduo, como Impressão digital, reconhecimento facial, íris ou retina, geometria da mão, voz e padrões de digitação ou movimentação. Deve ser capaz de identificar de forma única um titular de dados, ou seja, permitir a identificação inequívoca de uma pessoa natural. A LGPD considera como biométricos os dados obtidos por meios técnicos, a exemplo dos scanners, câmeras, sensores) e tratados por sistemas informatizados com o objetivo de identificação (quem) e autenticação (quem diz ser). Mesmo que o dado biométrico não esteja inicialmente vinculado a uma pessoa, se possuir potencial de identificação futura (combinado com outras informações), ele já é considerado dado pessoal sensível. O dado só será considerado biométrico nos termos da LGPD se for tratado com a finalidade de identificar o titular.", "940688": "2. Nesse ponto, é necessário salientar que, embora o processo de autenticação do titular não tenha apresentado falha técnica, nem sempre é possível comprovar de forma inequívoca que o consentimento foi livre. Exemplifiquemos com base em casos reais de pessoas idosa de baixa escolaridade sendo induzidas por meio fraudulento a realizar uma operação financeira, a qual não faria se não fosse induzida. Além dessas situações, soma-se a possibilidade de fraude a sistemas de autenticação facial. É possível constatar que, em havendo possibilidade de fraude, o consentimento não goza de presunção absoluta de veracidade. Sobre este tópico específico e outros a seguir será apresentada uma nota técnica no endereço de e-mail indicado nesta tomada de subsídio.", "940690": "3. A biometria comportamental compartilha a mesma natureza sensível da biometria tradicional, mas apresenta riscos adicionais, que requerem considerações e medidas de mitigação de eventuais consequências mais rígidas, notadamente pelo fato de que o perfilamento de preferências pode desembocar na identificação de dados pessoais sensíveis, a exemplo da orientação sexual ou religiosa etc. O movimento do ocular, por exemplo, por si só não poderia ter considerado um dado pessoal sensível, mas, se um algoritmo que faz o cruzamento desses dados com as imagens, movimentos e intervalo de tempo de foco, então pode se revelar perfilamento de dados sensíveis do titular. Seria razoável, também, uma política de identificação e retenção clara dessas preferências, bem como a possibilidade de exclusão efetiva e definitiva desses dados a pedido do titular. Aplicações que usam dados com de biometria comportamental deveriam disponibilizar de maneira destacada a opção por exclusão desses dados.", "940693": "4. Com vista a reduzir o número de fraudes no sistema financeiro e garantir que realmente seja atendido o princípio da autodeterminação informativa, um fato que deveria ser melhor delineado pela regulamentação é a possibilidade de titular de dados antecipar o não consentimento para tratamento de seus dados biométricos para fins de processamento de operações de crédito sem revisão humana, ou sem sua confirmação de modo presencial. É possível concluir que sem a implementação dessa antecipação de negativa de consentimento para tratamento de dados biométricos, o princípio da autodeterminação não seria plenamente disponível ao titular. Esse quesito será explorado em outros pontos desse questionário e

também exaustivamente na nota técnica complementar, a qual será enviada por e-mail (cujo remetente será raphael.gomes@arsae.mg.gov.br).", "940695": "5. Também neste quesito, por mais que haja robustez nas implementações técnicas de segurança, sempre haverá possibilidade de fraude. À medida que a biometria facial se populariza, as tentativas de golpes digitais também avançam. Os fraudadores usam imagens montadas, edição de vídeos em movimento, fotos com fundo falso e deepfake, para tentar se passar para outra pessoa. Em tese, mesmo consolidada as melhores práticas em segurança, sempre haverá a probabilidade de que agentes de contrainteligência burlam os sistemas de autenticação. Somente a efetiva promoção da autodeterminação informativa, no sentido de o titular poder antecipar o não consentimento de tratamento de seus dados biométricos em sistemas de decisão automatizados e a vedação de operações de crédito por meios automatizados quando o beneficiário é pessoa idosa de baixa escolaridade poderiam mitigar os efeitos devastadores sofridos pelas milhões de vítimas de fraudes em operações de crédito.", "940697": "6. De forma genérica tem-se que haver consonância com os quesitos a seguir: previsão normativa clara, finalidade legítima e específica, adequação e necessidade, transparência institucional. Tem-se também as salvaguardas para mitigação de riscos, quais sejam: minimização de dados, criptografia dos dados biométricos, controle de acesso rigoroso, monitoramento e auditoria contínua, Relatório de Impacto, nomeação de encarregado, treinamento periódico de servidores públicos e ferramentas de promoção dos direitos dos titulares. Por fim deve se evitar discriminação ou exclusão, além de garantir que o uso da biometria não gere barreiras indevidas ao acesso a serviços públicos. Nesse diapasão, estando em consonância com o princípio da necessidade, o poder público não poderia excluir o consumo de um serviço público, se o reconhecimento de dados biométricos fosse essencialmente indispensável.", "940699": "7. O tratamento de dados biométricos para fins de pesquisa com base no artigo 11, inciso II, alínea “c” da LGPD — que permite o uso de dados sensíveis para a realização de estudos por órgãos de pesquisa — está sujeito a limites rigorosos, mesmo quando há anonimização. Isso se deve ao risco de reidentificação, especialmente em contextos de cruzamento de bases de dados. Devem ser observados os seguintes quesitos: finalidade científica, histórica ou estatística, anonimização sempre ou sempre que possível (a LGPD exige que os dados sejam anonimizados, exceto quando isso inviabilizar a pesquisa), proibição de uso discriminatório, vedação à reidentificação e base legal restrita. Salvaguardas adicionais recomendadas: avaliação de risco de reidentificação, evitar sempre que possível o cruzamento com bases externas que possam facilitar a identificação, supressão, generalização, randomização ou agregação, aplicação de métodos como k-anonymity, differential privacy, etc.", "940700": "8. Cumpre destacar com relação ao quesito da transparência que, mesmo existindo políticas bem elaboradas e publicadas, além da possibilidade de fraudes ou sistemas que burlam a autenticação de dados biométricos processados eletronicamente, existem grupos que estão sujeitos a serem induzidos a autenticação por meio fraudulento. Nesse contexto, como medidas adicionais, o controlador deve engendrar formas de garantir a licitude das operações, com destaque para aquelas que são notoriamente suspeitas. O Estado também pode agir no sentido de regulamentar, potencializar e dar pleno atendimento ao princípio da autodeterminação informativa. A LGPD dispõe que a revogação pode ocorrer a qualquer tempo, mas a legislação ainda não

prevê o registro de não consentimento prévio a operações de crédito tomadas sem revisão humana.", "940701": "9. Retomando a análise da necessidade da existência de revisão humana, é necessário ponderar que podem existir situações em que essa revisão seria imperativa. Ex: pessoa idosa de baixa escolaridade, cadastro de relacionamento recentes, faz contrato de uma operação de crédito, com pouca destreza para manipular dispositivos eletrônicos, e em seguida faz uma transação financeira com características suspeitas (beneficiário de outro Estado sem histórico de atividade empresarial). Agravantes: Brasil é o país em que mais sofre com tentativas de golpes e telemarketing invasivo e tem uma numerosa população idosa de baixa escolaridade. Na nota técnica em complementação a este questionário será apresentada com mais detalhes na dicotomia de “lentidão” do Direito para regular os fatos jurídicos em comparação com a alta velocidade do desenvolvimento de tecnologias.", "940702": "10. Não é recomendável que uma pessoa idosa baixa escolaridade tenha seus dados biométricos utilizados de forma automatizada para fins de concessão de crédito sem que haja uma revisão humana. O Estado brasileiro, além de no passado não promover acesso à educação para esse grupo vulnerável, falha mais uma vez ao não determinar medidas no combate a fraudes e uso indevidos de dados biométricos mediante fraudes. É inconcebível que o Estado não tome providências com uma situação que está ocorrendo massivamente contra uma população idosa, vulnerável e de baixa escolaridade. Tão pouco o sistema bancário conseguindo prevenir esses ilícitos. Está posta a necessidade de possibilitar, dando pleno significado ao princípio da autodeterminação, a antecipação do não consentimento para operações automatizada, uma vez que a LGPD que o consentimento pode ser revogado a qualquer tempo e a necessidade de se vedar operações de crédito exclusivamente na modalidade automatizada a idosos vulneráveis.", "940704": "11.

Conforme artigo 8, parágrafo 2º, seria possível o controlador comprovar a o consentimento do titular apenas com o log da autenticação, uma vez que caberia esse o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei? Do ponto de vista prático, muito idosos que são vítimas de fraude não conseguem reverter a operação e não têm recursos financeiros para buscar auxílio jurídico ou sabem que poderiam procurar a defensoria pública. Para além, caso as defensorias públicas fossem provocadas a agir em milhares de processos, a situação ficaria quase que insustentável. Analisando o parágrafo 4 do artigo 8, o consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. Uma autorização de concessão de crédito para pessoa idosa ou analfabeta ou de baixa escolaridade em um dispositivo móvel recém cadastrada poderia ser considerada, como regra, uma autorização genérica e, portanto, nula.", "940707": "12. A recusa ao fornecimento de dados biométricos pode resultar em tratamento discriminatório, salvo nos casos em que a funcionalidade dependa tecnicamente da biometria e não haja alternativa viável. Merece atenção o fato contrário ao exposto, no sentido de não haver previsto na legislação a possibilidade de o titular poder antecipar, notadamente junto ao Sistema Financeiro Nacional, o não consentimento ao tratamento de dados biométricos para fins de contratações de crédito. Esta aplicabilidade já está disponível para proteger o uso de um CPF contra a inclusão em empresas em todo o território nacional (<https://www.gov.br/pt-br/servicos/impedir-permitir-participacao-do-meu-cpf-no-cadastro-nacional-de-pessoas-juridicas-cnpj>). Essa opção pode

ser tida como um modelo a ser seguido para fortalecer e prever/criar outros casos em que o titular possa exercer o direito de autodeterminação informativa (negativa antecipada de consentimento), notadamente no que toca as operações de crédito.", "940708": "13.

Desde a concepção (Privacy by Design), incorporar medidas de segurança e privacidade desde o desenvolvimento de sistemas que utilizam biometria. Realizar avaliações de impacto à proteção de dados antes da implementação. Minimização e finalidade, coletando apenas os dados biométricos estritamente necessários para a finalidade pretendida. Não fazer reutilização para finalidades distintas sem nova base legal ou consentimento. Transparência (informando os titulares sobre finalidade, base legal, direitos disponíveis e consequências da recusa ao fornecimento). Consentimento livre e destacado (quando aplicável). No quesito segurança da informação implementar criptografia forte, controle de acesso baseado em perfil, monitoramento contínuo e resposta a incidentes e backups seguros e segregados. Além disso ter formalizado um programa de governança com a participação multidisciplinar do envolvidos, além da alta administração.", "940709": "14. O STF, ao reconhecer a autodeterminação informativa como direito fundamental autônomo (ADIn 6393), reforçou que o controle sobre os próprios dados deve ser garantido mesmo em contextos emergenciais ou de interesse público. Ponderemos que até em situações emergências, em tese, o princípio da autodeterminação informativa foi definido como sendo direito fundamental, mas na prática o titulares brasileiros ainda não gozam da prerrogativa de exercê-lo a qualquer tempo, no casos de querer antecipar o não consentimento (tal como já é feito para bloquear abertura de empresas para um determinado CPF, mas ainda não é feito no sistema bancário, no sentido de titular poder definir que seus dados para fins de contratação de operações de crédito tenham sempre passar por revisão humana ou confirmação presencial em caixas eletrônicos, por exemplo).", "940710": "15. O respeito aos titulares não é de competência exclusiva do agente de tratamento, embora esse possa contribuir de maneira significativa. Mesmo que somada a eventuais medidas de mitigação de riscos tomadas pelo controlador, tampouco a publicação das informações de maneira clara e ostensiva teria o condão de garantir o respeito aos direitos dos titulares, notadamente quando se tratar de operação fraudulenta, seja por meios técnicos capazes de burlar os sistemas de autenticação, seja por meio de estelionato, em que sempre estão presentes os métodos ardilosos. Três fatores agravam o cenário: o desenvolvimento de técnicas que burlam sistemas de autenticação, a quantidade de criminosos e o número de idosos de baixa escolaridade, além dos analfabetos. Medidas de mitigação: a possibilidade de antecipação de não consentimento e a vedação de empréstimos automatizados a analfabetos.", "940711": "16. Destacando inicialmente que não seria razoável supor que os tratamentos de dados biométricos de criança são sempre imprescindíveis para sua segurança. Em espaços escolares, por exemplo, o credenciamento de informações biométricas tais como reconhecimento facial ou controle de acesso por biometria não garantiram por si só a sua segurança e, numa visão pragmática, é difícil contemplar em que situação esse cadastramento contribuiria para o seu melhor interesse, principalmente por que a legislação não delineou esses casos. Caso exista esta previsão normativa, seria necessário criar políticas rigorosas de acesso, retenção, transferência e descarte dessas informações.", "940712": "17. O tratamento de dados biométricos de crianças e adolescentes é permitido pela LGPD em hipóteses legais específicas, mas exige medidas rigorosas de

proteção, especialmente em ambientes como escolas, creches e espaços recreativos. O artigo 14 da LGPD estabelece que esse tratamento deve sempre observar o princípio do melhor interesse da criança, além de garantir a participação informada dos pais ou responsáveis legais. De qualquer modo, em tese, salvo perigo eminente ou situação de risco detectada, não seria razoável colher dados biométricos de crianças em espaços escolares, dado que, salvo situação excepcionalíssima, essa medida não teria correlação direta com o aumento da segurança em escolas.", "940714": "18. Caso seja admissível a verificação ou estimação de idade por meio de dados biométricos em plataformas digitais e jogos — especialmente quando envolve crianças e adolescentes — deve seguir critérios rigorosos para estar em conformidade com a LGPD, em especial com o art. 14, que trata do tratamento de dados pessoais de menores de idade. O tratamento de dados biométricos de crianças e adolescentes pode ocorrer nas seguintes hipóteses: Consentimento específico e destacado de pelo menos um dos pais ou responsável legal, cumprimento de obrigação legal ou regulatória (ex: controle de acesso a conteúdos impróprios), proteção da vida ou da incolumidade física do menor ou de terceiros e atendimento ao legítimo interesse do controlador, desde que prevalecendo o melhor interesse da criança e com avaliação cautelosa. Também é necessário a avaliação de impacto, a minimização de dados, o consentimento informado e verificável, a transparência e linguagem acessível e alternativas não biométricas.

Contribuinte: RAPHAEL TADEU LEITE GOMES

Número: OP-1006120

Data: 01/08/2025 - 13:43

Resumo: : "Dados biométricos devem ser considerados sensíveis quando são utilizados para identificar ou autenticar uma pessoa. A coleta de características fisiológicas ou comportamentais — como impressões digitais, reconhecimento facial, íris, geometria da mão, voz, padrões de digitação ou movimento ocular — deve ser encarada como uma tecnologia essencial de autenticação e segurança. Assim, defendemos que a ANPD adotar critério semelhante: (i) considerar sensíveis apenas os dados biométricos usados para singularizar uma pessoa; (ii) excluir da categoria de sensíveis informações usadas para propósitos estatísticos ou de agregação, como contagem de fluxo de passageiros ou distinção entre pessoas e objetos; (iii) biometria para investigação criminal, defesa nacional ou segurança do Estado seja enquadrada nas exceções do art. 4º da LGPD. ", "940688": "Transparência é desejável, mas deve ser proporcional à finalidade. Em usos para segurança pública ou prevenção de fraudes, a divulgação de detalhes excessivos sobre algoritmos ou bases de dados pode prejudicar investigações e segurança dos sistemas e dos próprios policiais. Sugere-se informar ao público de forma geral quais dados são coletados e para que são usados, evitando revelar detalhes operacionais sensíveis. Em contextos menos críticos, avisos de privacidade claros e acessíveis, com iconografia e vídeos explicativos, ajudam a legitimar o uso sem embarçar as operações.", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "Em território brasileiro, o uso de tecnologias de reconhecimento facial (FRTs) para fins de segurança

pública está excluído do escopo da LGPD (art. 4º, III), devendo observar regime específico. Nesses casos, o consentimento não é requisito, devendo prevalecer o interesse público relevante, nos limites da legalidade, efetividade e proporcionalidade. A proteção de dados não pode inviabilizar o exercício do poder de polícia estatal, especialmente diante da crise de segurança no Brasil. A experiência europeia comprova que o reconhecimento facial em segurança pública é tratado fora das regras do GDPR, com salvaguardas específicas. Recomenda-se (i) avaliação de proporcionalidade e base legal clara; (ii) supervisão institucional e auditorias ex post; (iii) mitigação de vieses e controle humano; e (iv) salvaguardas técnicas e transparência. A diferenciação regulatória é essencial para proteger direitos sem comprometer a ordem pública. ", "940701": "Sistemas de reconhecimento facial voltados à segurança pública devem priorizar eficácia e aplicabilidade em ambientes reais, não exigindo infalibilidade. A redução de erros deve ocorrer com (i) calibração adequada ao contexto urbano brasileiro; (ii) uso de bases diversas e atualizadas; (iii) testes operacionais contínuos; e (iv) presença humana em decisões críticas. Em investigações e policiamento, eventuais falsos positivos devem ser corrigidos ex post, com relatórios públicos e mecanismos de revisão. O foco deve ser o desempenho do sistema, e não a adoção de barreiras ex ante que inviabilizem sua aplicação. A segurança pública exige soluções céleres, adaptáveis e auditáveis, não a antecipação de riscos hipotéticos. A LGPD não se aplica a essas hipóteses (art. 4º, III), devendo prevalecer regime próprio de proteção de dados em atividades de repressão penal. ", "940702": "O uso de FRTs deve ser orientado por finalidade legítima e proporcionalidade, sobretudo em segurança pública, investigação criminal ou defesa do Estado. Nessas hipóteses, o reconhecimento facial pode ser essencial para identificar foragidos, localizar desaparecidos ou prevenir crimes em áreas críticas. Já não se recomenda seu uso quando não houver risco relevante ou finalidade definida, como em campanhas comerciais, acesso a eventos privados ou serviços meramente promocionais, em que o impacto sobre a privacidade pode ser desproporcional. Métodos alternativos (senhas, tokens, QR codes) são adequados em contextos de baixo risco, mas não substituem a eficácia do reconhecimento facial em segurança pública. A discussão deve focar no uso proporcional e controlado da tecnologia, e não em sua restrição genérica. Governança, avaliação de impacto e supervisão institucional são mecanismos mais adequados para mitigar riscos. ", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Contribuinte: RODRIGO SARAIVA MARINHO

Número: OP-1006132

Data: 01/08/2025 - 13:51

Resumo: "A manifestação da Febraban e Abecs será enviada por email.", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Número: OP-1006155

Data: 01/08/2025 - 14:24

Resumo: "Abradee: Entendemos como critério a aplicação de um tratamento técnico específico ou tecnologia específica que torne hábil a identificação única e sistêmica de um indivíduo. Neste sentido, uma mera fotografia ou vídeo imagem não seriam considerados dados biométricos, o que ocorreria tão somente se e a partir da aplicação da tecnologia com a finalidade específica de identificação do titular.", "940688": "Abradee: Previsão em política, comunicação visual, script sobre a necessidade e finalidade da coleta e tratamento do dado sensível, e, quando for o caso, Termo de Consentimento, no local da coleta dos dados que serão objeto de aplicação da tecnologia de biometria; Em ambientes virtuais, inclusão ainda de checkbox para garantir que o titular leu a Política de Privacidade e que está ciente do tratamento de dados sensíveis e do seu direito de oposição e demais previstos na LGPD.", "940690": "Abradee: Sugerimos que o tratamento realizado com uso de biometria comportamental esteja restrito a finalidade primária, sendo limitada a possibilidade de tratamento com finalidades secundárias. Ademais, sugerimos maior cuidado com relação ao tratamento discriminatório decorrentes de decisões automatizadas por algoritmos.", "940693": "Abradee: Entendemos que todas as informações relacionadas ao tratamento de dados biométricos precisam estar disponíveis ao titular antes da coleta, por meios legíveis e de fácil entendimento ele. Contudo, a depender do contexto, por exemplo, tratamento de dados pessoais para fins de prevenção a fraude, é possível verificar uma confusão com relação a base legal utilizada, tendo em vista, que em muitos casos, especialmente quando os dados são coletados de forma online, o titular pode entender que a base legal é o consentimento, por entender que o “termo de ciência” é uma autorização. Nesses casos, a base legal utilizada é a prevenção a fraude e não o consentimento, por isso o “termo de ciência” possui caráter apenas informativo.", "940695": "Abradee: a) A transparência aos titulares quanto a finalidade e necessidade do tratamento; b) Inicialmente é importante reforçar que a garantia de prevenção à fraude não necessariamente é aplicável apenas em benefício do titular dos dados, mas do Controlador e/ou de terceiros. Nesse sentido, a coleta de dados biométricos para esta finalidade deverá considerar o contexto do tratamento, devendo ser proporcional à necessidade do mesmo e aos riscos envolvidos para o titular, o Controlador e/ou terceiros, garantindo que não haja coleta excessiva de dados. Há de ser considerado igualmente a sua utilização para acesso não só a soluções bancárias e financeiras, mas também a soluções disponibilizadas por empresas de setores que são amplamente conhecidos como alvo de fraudes e que precisam se valer de maior segurança em suas operações; c) Implementação de recursos de segurança desde a coleta até a eliminação do dado, como, por exemplo, criptografia, gestão de acesso, MFA, gestão lógica e etc.", "940697": "Abradee: Devem ser implementadas medidas técnicas de segurança, desde a coleta até a eliminação do dado, como, por exemplo, uso de criptografia, gestão de acesso, MFA e gestão lógica, conforme as boas práticas já adotadas pelo controlador e observados

parâmetros adicionais que podem ser impostos pelas obrigações legais ou regulatórias. Deve haver transparência ao titular com a informação, em aviso, de que ocorrem tratamentos com essas bases legais.", "940699": "Abradee: Utilização específica para pesquisas apenas mediante anonimização e sem possibilidade de reversão, o que deve ser garantido pelo órgão de pesquisa.", "940700": "Abradee: Para garantir o uso ético e legal de tecnologias de reconhecimento facial segundo a LGPD, é essencial a aplicação dos princípios de Privacy by Design, bem como realizar, quando for o caso, o teste de balanceamento, além de Análise de Impacto (DPIA), limitar a coleta de dados ao mínimo necessário, informar claramente os titulares sobre o tratamento de seus dados, aplicar controles técnicos como criptografia e acesso restrito, exigir auditorias de viés algorítmico, prever revisões humanas nas decisões automatizadas, estabelecer políticas internas, revisar contratos com cláusulas específicas de proteção de dados e manter governança ativa com a atuação de um DPO e plano de resposta a incidentes.", "940701": "Abradee: Foco em qualidade de dados, diversidade de amostras na fase de treinamento, validação contínua e uso de algoritmos auditados. Testes de acurácia por diferentes grupos demográficos para reduzir vieses, além de permitir revisões humanas das decisões automatizadas. Mecanismos de feedback, registros de erro e logs detalhados para detectar e corrigir falhas rapidamente. Políticas de atualização de modelos, reavaliação periódica de desempenho e canais acessíveis para contestação por parte dos titulares.", "940702": "Abradee: Contextos com alto risco de discriminação, como em espaços públicos sem consentimento ou sem a transparência adequada sobre as finalidades dos tratamentos realizados ou para prestação de serviços essenciais. Como alternativas, podem ser utilizados cartões de acesso, senhas, QR codes, tokens físicos, biometria por impressão digital, e demais tecnologias que possam trazer segurança nas operações do controlador com menor impacto aos titulares. ", "940704": "Abradee: Para mitigar riscos de violação de dados biométricos, indispensável adotar medidas como criptografia forte, controles de acesso rigorosos, autenticação multifator, armazenamento seguro com segregação de dados e registro de logs de acesso, mecanismos de detecção de fraude biométrica, como liveness detection e análise comportamental, e Sandboxing de sistemas de reconhecimento facial, especialmente quando utilizados em dispositivos de bordo (ex: câmeras, terminais físicos). Além disso, devem ser realizadas análises de risco periódicas, testes de vulnerabilidade, auditorias de segurança e atualização constante dos sistemas. As organizações devem implementar políticas internas claras, capacitar equipes, elaborar Relatório de Impacto à Proteção de Dados e manter um plano de resposta a incidentes. Parâmetros mínimos incluem monitoramento contínuo, indicadores de segurança, rastreabilidade de acessos e processos para notificação imediata à ANPD e aos titulares em caso de incidente.", "940707": "Abradee: Para evitar discriminação ilícita na exigência de biometria em serviços não essenciais, é fundamental garantir que a coleta seja realmente necessária e proporcional à finalidade, com oferta de alternativas viáveis de autenticação para quem não queira fornecer dados biométricos. O uso deve ser transparente, com consentimento livre e informado, sem condicionamento abusivo ao acesso geral ao serviço. A negativa do titular só pode justificar restrições aos serviços quando houver, por parte do Controlador, justificativa técnica clara e documentada, e a funcionalidade for opcional ou adicional, sem afetar o acesso ao serviço principal. Além disso, deve-se adotar o teste de balanceamento, quando for o caso, bem como

avaliação de impacto (DPIA) e revisão periódica das bases legais.", "940708": "Abradee: Boas práticas para proteção de dados biométricos incluem a adoção de medidas técnicas como criptografia, controle de acesso restrito, anonimização ou pseudonimização sempre que possível e armazenamento seguro. Juridicamente, é essencial definir base legal adequada, realizar Análise de Impacto (DPIA), garantir consentimento livre e informado (quando aplicável) e prever revisões humanas em decisões automatizadas. A transparência deve ser assegurada com políticas claras, comunicação acessível aos titulares e oferta de canais para exercício de direitos. Para evitar discriminação, os controladores devem auditar algoritmos, testar sistemas contra vieses e revisar periodicamente o tratamento para identificar e corrigir práticas abusivas.", "940709": "Abradee: Para assegurar a autodeterminação informativa em tratamentos contínuos e massivos de dados biométricos, os controladores devem adotar medidas como sinalização clara nos locais monitorados, políticas públicas de transparência, divulgação de informações acessíveis em sites e aplicativos, e canais específicos facilitados para o exercício dos direitos dos titulares, disponíveis nos mesmos locais de sinalização e transparência ao titular quanto ao monitoramento. É essencial realizar Análises de Impacto (DPIA), limitar a coleta ao estritamente necessário, adotar técnicas de minimização de dados e garantir revisões periódicas de proporcionalidade. Além disso, deve-se prever mecanismos de contestação, anonimização sempre que possível e processos eficazes de resposta a solicitações de acesso, correção ou exclusão de dados, mesmo em ambientes de difícil transparência como espaços públicos.", "940710": "Abradee: Devem garantir os direitos dos titulares por meio de políticas de privacidade claras e acessíveis aos titulares vulneráveis e responsáveis legais, disponibilizar canais específicos para solicitação de acesso, correção e revogação do consentimento, e oferecer respostas em prazos razoáveis considerando a complexidade envolvida no tratamento de tais dados. Em casos de tratamento automatizado de tais dados, fundamental assegurar a possibilidade de revisão humana das decisões, fornecer informações sobre a lógica e critérios usados nos processos automatizados, ressaltados segredos comerciais, registrar o consentimento de forma documentada, quando aplicável, facilitar sua revogação e implementar processos internos que permitam rápida localização e atualização dos dados, assegurando controle efetivo pelos titulares sobre eles. Caso o tratamento de dados biométricos esteja amparado por bases legais que não o consentimento, necessário garantir a autodeterminação informativa do titular.", "940711": "Abradee: O tratamento de dados biométricos de crianças e adolescentes só é admissível com o consentimento específico e destacado dos pais ou responsáveis, salvo quando necessário para proteger a vida ou a integridade física da criança ou de terceiros. Os controladores devem garantir a participação informada, com linguagem acessível e transparente sobre a finalidade, riscos e direitos dos titulares, respeitando o princípio do melhor interesse da criança previsto no art. 14 da LGPD. Além disso, é essencial limitar a coleta ao mínimo necessário, adotar medidas de segurança reforçadas, realizar Análise de Impacto (DPIA) e permitir fácil acesso, correção ou exclusão dos dados a pedido dos responsáveis.", "940712": "Abradee: Seria admissível legalmente apenas em hipóteses excepcionais previstas na LGPD: quando necessário para cumprimento de obrigação legal, para o exercício regular de direitos em processo judicial/administrativo, proteção da vida ou incolumidade física, a exemplo do controle de acesso a escolas. Para garantir participação

informada dos responsáveis, essencial obter consentimento específico e destacado dos responsáveis, com linguagem clara sobre finalidades, riscos e direitos. As medidas técnicas devem incluir criptografia forte, controle rigoroso de acesso, auditoria contínua e minimização de dados, limitando a coleta ao estritamente necessário. Organizacionalmente, deve-se implementar políticas de governança, treinamento de funcionários, avaliação de impacto à proteção de dados, e estabelecer canais para exercício de direitos dos titulares, sempre priorizando o melhor interesse da criança e adolescente conforme determina o ECA.", "940714": "Abradee: Devem ser observados critérios rigorosos de necessidade, proporcionalidade e adequação. Nesse contexto, a biometria não poderia estimar idade, mas sim ser aplicada de forma efetiva para garantir a vinculação com a informação correta, cruzando com bases oficiais do governo, por exemplo. O tratamento deve ser justificado pela necessidade e razoabilidade, garantindo uso proporcional e alinhado aos princípios da LGPD, exigindo base legal específica do art. 11. A compatibilização com o princípio da necessidade requer que a biometria seja o meio menos invasivo disponível para atingir o objetivo, limitando a coleta ao mínimo necessário e definindo prazo para retenção dos dados. O melhor interesse deve ser demonstrado através de avaliação de impacto, implementação de medidas de segurança robustas, transparência sobre os processos de verificação, garantia de que os benefícios superem os riscos à privacidade e desenvolvimento da criança e do exercício de direitos pelos responsáveis.

Contribuinte: Sarah Wallace escalante

Número: OP-1006158

Data: 01/08/2025 - 14:31

Resumo: : "CONTRIBUIÇÕES DA ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO - ABERT: Em razão do limite de caracteres da plataforma, a contribuição será encaminhada por e-mail.", "940688": "CONTRIBUIÇÕES DA ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO - ABERT: Em razão do limite de caracteres da plataforma, a contribuição será encaminhada por e-mail.", "940690": "CONTRIBUIÇÕES DA ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO - ABERT: Em razão do limite de caracteres da plataforma, a contribuição será encaminhada por e-mail.", "940693": "CONTRIBUIÇÕES DA ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO - ABERT: Em razão do limite de caracteres da plataforma, a contribuição será encaminhada por e-mail.", "940695": "", "940697": "", "940699": "", "940700": "", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": "

Contribuinte: Rafael Ferreira Larcher

Número: OP-1006162

Data: 01/08/2025 - 14:34

Resumo: : "CNseg: Considerando os pronunciamentos da ANPD, em especial a publicação do 2º volume da série “Radar Tecnológico”, que tratou de biometria e reconhecimento facial, bem como aqueles emitidos pela CNIL, pelo ICO, Office of the Privacy Commissioner (Canadá) e o GDPR, entendemos que devem ser considerados os seguintes critérios para caracterizar um dado como biométrico: (i) a informação deve ser relativa a características físicas, fisiológicas ou comportamentais únicas de uma pessoa natural identificada ou identificável; (ii) o tratamento do dado deve ter a finalidade de autenticar ou identificar (individualizar) a pessoa natural, mediante o uso de tecnologias específicas, dotadas da capacidade de reconhecimento automático. Embora a finalidade não seja uma característica do dado pessoal em si, no contexto do tratamento de dados biométricos, a finalidade estará associada ao uso da tecnologia para individualizar o titular de forma única ou inequívoca, de acordo com o que dispõe o GDPR.", "940688": "CNseg: Pelo art. 9º da LGPD, o controlador deve disponibilizar, de forma clara, adequada e ostensiva, as seguintes informações sobre o tratamento: (i) finalidade; (ii) forma e duração, ressalvados os segredos comercial e industrial; (iii) identificação do controlador (e do encarregado, se houver) e dados de contato; (iv) informações sobre o uso compartilhado de dados pelo controlador e a finalidade; (v) responsabilidade dos agentes que realizarão o tratamento; e (vi) direitos do titular. O controlador deve avaliar o tratamento realizado, podendo utilizar diversos meios eficazes para informar o titular, como: publicar, a seu critério, políticas e avisos de privacidade, bem como utilizar práticas de transparência ativa, como sinais visuais (placas, cartazes, adesivos) e folhetos físicos e/ou digitais (com QR code), com o objetivo de dar visibilidade aos titulares, por meio dos canais de coleta, sobre os detalhes do tratamento de dados realizado.", "940690": "CNseg: Não há razão para que a regulação diferencie a biometria comportamental da fisiológica (tradicional), pois ambas visam reconhecer ou identificar a pessoa natural. A biometria comportamental não desconsidera fatores fisiológicos, o que pode dificultar a identificação e classificação da biometria empregada. O modo de caminhar, p. ex., está relacionado à fisiologia da pessoa (tamanho da perna ou alguma doença). Os dados biométricos permitem a identificação única do titular, mas podem ser modificados ao longo do tempo e considerados, além de dados sensíveis, um dado dinâmico e não estático, exigindo maior atenção em todas as fases do tratamento. Para atender os princípios da segurança e da qualidade dos dados, o controlador poderá elaborar RIPD e adotar medidas para assegurar que os dados estarão protegidos e atualizados, à luz do caso concreto, levando em consideração os riscos à segurança da informação, as vulnerabilidades do sistema e os danos que poderão ser causados ao titular.", "940693": "CNseg: O consentimento para autorizar o tratamento de dado pessoal sensível, inclusive biométrico, deve observar os requisitos do pronunciamento da ANPD proferido no guia orientativo sobre a aplicação da LGPD no contexto eleitoral. Nem sempre o consentimento será a base legal apropriada para o tratamento de dados biométricos, como no caso do art. 11, II, “g” da LGPD, para a garantia da prevenção à fraude e à segurança do titular, o que ocorre, p. ex., para controle de acesso a sistemas com a verificação e autenticação do titular. Quando o consentimento for a base legal mais aplicável, deverá ser obtido por meio de manifestação clara e destacada. Não será adequado quando há assimetria de poder, como em relações trabalhistas ou quando o tratamento é necessário para prevenção à fraude. No mercado segurador, o uso de biometria

fundamentado na base legal prevenção à fraude é essencial tanto para a segurança das seguradoras quanto para proteger seus clientes.", "940695": "CNseg: Para garantia de prevenção à fraude, os critérios estão dispostos no próprio art. 11, II, "g", da LGPD. Assim, será possível avaliar a proporcionalidade do tratamento e identificar as salvaguardas apropriadas para resguardar o titular, como p. ex., criptografia, armazenamento seguro, auditorias e treinamento. O tratamento de dados biométricos com base na prevenção à fraude é essencial para as seguradoras, para garantir a manutenção da sustentabilidade do setor e a proteção dos titulares, sendo utilizada, p. ex., para 1. autenticação de operações no aplicativo da seguradora, impedindo acessos indevidos a informações, 2. validação de identidade na contratação de seguros, reduzindo fraudes e 3. prevenção de fraudes em sinistros, sendo utilizada, inclusive, como prova de vida.", "940697": "CNseg: Para cumprimento de obrigação legal/regulatória deve haver embasamento legal claro e específico, com estrita observância dos princípios do art. 6º, LGPD, recomendando-se que o controlador avalie a limitação do tratamento aos dados estritamente necessários e a existência de alternativa menos intrusiva. O controlador deve demonstrar a relação direta entre o tratamento do dado biométrico e o cumprimento da obrigação legal/regulatória, sendo que a finalidade do tratamento deve ser estipulada por lei/regulamento. As principais salvaguardas devem ser voltadas à transparência do tratamento, para assegurar que o titular exerça os direitos previstos na LGPD. Dentre as medidas para a mitigação de riscos e garantia de direitos dos titulares, destaca-se: realização do RIPD, uso de criptografia, controle de acesso, monitoramento e testes de vieses. Entidades e órgãos públicos devem observar as orientações já divulgadas pela ANPD no guia que aborda o tratamento realizado por esses agentes. ", "940699": "CNseg: Na realização de estudos por órgãos de pesquisa, o controlador pode observar orientações da ANPD no guia que aborda o tema, restringir os dados biométricos ao estritamente necessário e avaliar a necessidade e proporcionalidade do tratamento em relação à finalidade da pesquisa. O controlador pode adotar a seu critério técnicas de anonimização testada, pseudonimização, controle de acesso e proibição de reuso.", "940700": "CNseg: As tecnologias de reconhecimento facial são utilizadas como medida de segurança no setor de seguros para prevenção/combate à fraude, principalmente para confirmação da identidade, acesso a cadastros e resgate de valores, não devendo haver óbice desnecessário ao uso da biometria, dada a importância para o setor segurador. Para garantir o uso de tais tecnologias em conformidade com princípios do enunciado e mitigar riscos de discriminação ilícita/abusiva, o controlador poderá: 1. tratar somente dados estritamente necessários; 2. utilizar, quando possível, técnicas de anonimização/pseudonimização; 3. buscar alternativa de tratamento menos intrusiva; 4. utilizar meios eficazes para informar o titular; 5. disponibilizar canais para atendimento de direitos do titular; 6. estabelecer políticas de controle de acesso aos dados biométricos; 7. elaborar RIPD; e 8. adotar medidas compatíveis com os riscos do tratamento, as vulnerabilidades do sistema utilizado e possíveis danos ao titular.", "940701": "CNseg: O controlador deve considerar a acurácia dos sistemas como elemento central da conformidade do tratamento, devendo garantir: 1. sistema com precisão estatística compatível com a finalidade de uso; 2. realização de testes para identificar/corrigir vieses e evitar discriminação; 3. adoção de medidas de correção tempestiva de erros de identificação; e 4. adoção de medidas de transparência para titulares. O sistema deve estar

amparado em base robusta e diversa, ser validado tecnicamente e auditado periodicamente, com governança clara. As medidas de correção tempestiva de erros de identificação devem ser avaliadas à luz do caso concreto. Com efeito, recomenda-se a elaboração de RIPD visando à identificação dos riscos do tratamento e das medidas mitigatórias pertinentes. Não parece apropriado determinar antecipadamente as medidas que deverão ser adotadas pelo controlador, que precisam levar em consideração o contexto específico do tratamento e os reais riscos envolvidos. ", "940702": "CNseg: O uso de tecnologias de reconhecimento facial não é recomendado, por exemplo, em alguns tipos de serviços onde a autenticação de acesso não é necessária, pois os serviços ofertados não estão diretamente atrelados à autenticação da identidade do indivíduo, bem como em espaços públicos sem finalidade clara. Entretanto, para serviços que necessitam da garantia e validação automatizada da identidade do indivíduo, principalmente visando a prevenção à fraude e segurança, como por exemplo, de bancos e serviços de seguros e saúde, a utilização dessa tecnologia, observadas as adequadas salvaguardas técnicas e de segurança, tem se mostrado efetiva. Não se deve, portanto, que eventual, alteração regulatória desestime o seu uso de quando o objetivo for mitigar fraudes e garantir a segurança do titular. As alternativas ao uso de tecnologias de reconhecimento facial incluem autenticação multifatorial, tokens digitais e físicos ou validação documental assistida, conforme análise do caso. ", "940704": "CNseg: O controlador, de acordo com sua realidade, pode adotar as seguintes medidas para mitigar riscos de violação a dados biométricos: 1. controle de acesso, incluindo processos de autenticação, autorização e auditoria; 2. registro cronológico de alterações da base de dados de referência; 3. criptografia; 4. armazenamento de informações pelo tempo mínimo necessário; 5. plano de resposta a incidentes de segurança; 6. estabelecimento de obrigações contratuais; 7. uso de hash único e randomizado por dado; 8. mascaramento e embaralhamento de dados em ambientes não produtivos; 9. auditorias; e 10. monitoramento, MFA e registro de logs de acesso. A depender de seu porte e do contexto fático, o controlador poderá adotar como parâmetros de avaliação de riscos e monitoramento: plano de resposta a incidentes, backup seguro, testes de intrusão e descarte adequado dos dados, reavaliando periodicamente as medidas adotadas, para assegurar que continuem eficazes, através do RIPD.", "940707": "CNseg: É recomendável que o controlador, como boa prática, faça uma avaliação de proporcionalidade, considerando a necessidade do tratamento e possíveis riscos ao titular. Se houver riscos desproporcionais de discriminação, é recomendável que o tratamento não seja realizado, avaliando alternativas menos intrusivas. O risco ao titular não veda o tratamento, desde que possa ser mitigado. Se o controlador demonstrar a proporcionalidade do tratamento e mitigação de riscos, será legítima a restrição do uso de determinadas funcionalidades ao titular que se negar a fornecer dados biométricos, por exemplo, nos casos em que a segurança do titular ou da organização seja colocada em risco caso não se confirme a identidade do titular ou se não estiver disponível meio alternativo igualmente seguro. Para seguros de vida, a biometria pode ser essencial para prevenir fraudes, sendo que a recusa em fornecer selfie como prova de vida pode inviabilizar a aceitação/contratação digital do produto.", "940708": "CNseg: O controlador poderá adotar políticas e avisos de privacidade que registrem a realização de tratamento de dados biométricos e aplicar medidas organizacionais e técnicas para proteger o dado pessoal sensível, bem como realizar as comunicações necessárias aos titulares para dar

transparência quanto ao tratamento e sua finalidade, a depender do contexto do tratamento. Para garantir maior proteção ao tratamento, o controlador poderá realizar atualização periódica relativa à qualidade dos dados e avaliações periódicas de risco, com atualização contínua das medidas de segurança, bem como elaborar RIPD para avaliar discriminação ilícita e abusiva, garantindo proporcionalidade e aderência à LGPD.", "940709": "CNseg: Não aplicável às empresas seguradoras.", "940710": "CNseg: Os agentes de tratamento podem garantir o respeito aos direitos dos titulares mediante o uso de avisos de privacidade que descrevam o tratamento realizado, com destaque para a coleta do consentimento, bem como através de sinalizações de coleta e de monitoramento de ambiente, a depender do contexto do tratamento. Devem ser assegurados canais acessíveis para solicitação de informações, correção de dados e revogação do consentimento, com linguagem clara e registros que garantam rastreabilidade, o fornecimento da informação e a transparência das operações de tratamento, como, por exemplo, viabilizando o exercício de direitos via app, site ou SAC.", "940711": "CNseg: Não aplicável às empresas seguradoras. ", "940712": "CNseg: O tratamento de dados pessoais de crianças e adolescentes pode se basear em qualquer base legal, conforme enunciado nº 1/2023 da ANPD. A adequação do uso da base legal e a avaliação das medidas técnicas e organizacionais apropriadas para evitar abusos, vazamentos ou acessos indevidos dependerão do caso concreto. É recomendável que quando houver o tratamento de dados biométricos de crianças e adolescentes, o controlador elabore RIPD, observando a minimização dos dados e a finalidade legítima e específica do tratamento. A participação informada dos pais/responsáveis deve ocorrer com uso de linguagem adequada e sistema que garanta proteção contra acesso/uso indevidos. Como medidas técnicas e organizacionais para evitar abusos, vazamentos ou acessos indevidos, é possível citar a disponibilização de canal de contato, criptografia, controle de acesso, auditoria e revisão periódica contra acessos não autorizados.", "940714": "CNseg: Não aplicável às empresas seguradoras.

Contribuinte: MAISA LIMA DE ALMEIDA SALVADOR

Número: OP-1006187

Data: 01/08/2025 - 14:58

Resumo: "Associação Nacional dos Hospitais Privados (ANAHP) Adotamos o critério de que um dado biométrico é uma característica física ou fisiológica única que permite identificar uma pessoa de forma precisa e praticamente infalível.", "940688": "Associação Nacional dos Hospitais Privados (ANAHP): Comunicação clara sobre os dados coletados, sua finalidade e necessidade com a exibição de cartazes, panfletos e avisos visuais que reforcem essas informações ao titular.", "940690": "Associação Nacional dos Hospitais Privados (ANAHP): A biometria tradicional tem justificativa mais clara quanto à sua coleta e finalidade. Já a biometria comportamental é menos comum e sua necessidade é mais complexa de justificar.", "940693": "Associação Nacional dos Hospitais Privados (ANAHP): Por serem dados sensíveis, a coleta de dados biométricos exige consentimento explícito do titular, com total transparência sobre sua finalidade e necessidade. O consentimento só é

dispensado em casos previstos em lei, como obrigação legal, tutela da saúde, prevenção a fraudes ou proteção da vida.", "940695": "Associação Nacional dos Hospitais Privados (ANAHP): Embora dados biométricos sejam sensíveis, seu tratamento é permitido quando há obrigação legal ou regulatória. Nesses casos, a justificativa está na própria base legal. Ainda assim, é essencial avaliar se a coleta é estritamente necessária ou se outro dado menos invasivo pode atender à exigência.", "940697": "Associação Nacional dos Hospitais Privados (ANAHP): A LGPD permite o tratamento de dados pessoais e sensíveis, sem consentimento, por instituições de pesquisa com fins exclusivamente científicos. Sempre que possível, recomenda-se a anonimização dos dados, além da aplicação de medidas de segurança e a justificativa clara da necessidade, finalidade e adequação do tratamento.", "940699": "Associação Nacional dos Hospitais Privados (ANAHP): Os princípios da LGPD são aplicados desde a análise da atividade, com a adoção do Privacy by Design. Essa análise deve definir a finalidade do tratamento, os dados necessários, o mapeamento da operação e as possíveis vulnerabilidades, como riscos de vazamento ou discriminação. As ações de mitigação devem ser planejadas com base nesse estudo.", "940700": "Associação Nacional dos Hospitais Privados (ANAHP): Pode ser elaborada considerando os princípios da LGPD já desde o início da estruturação do projeto. É possível usar frameworks e regulamentos para apoiar, como RIPD, ROPA e ISO27701 para apoiar em mecanismos e regras.", "940701": "Associação Nacional dos Hospitais Privados (ANAHP): Pode ser elaborada considerando os princípios da LGPD já desde o início da estruturação do projeto. É possível usar frameworks e regulamentos para apoiar, como RIPD, ROPA e ISO27701 para apoiar em mecanismos e regras.", "940702": "Associação Nacional dos Hospitais Privados (ANAHP): O tratamento de dados pessoais fora das bases legais, sem comprovação de necessidade e adequação, não é recomendado. Quando a atividade visa proteger a liberdade, integridade, honra e privacidade do titular, ela se fundamenta na boa-fé e nas melhores práticas.", "940704": "Associação Nacional dos Hospitais Privados (ANAHP): Por possibilitarem identificação única e intransferível, os dados biométricos são uma forma segura de autenticação, dificultando fraudes e roubo de identidade. Na proteção de dados sensíveis, não há medidas mínimas: todas as recomendações e práticas de segurança devem ser tratadas com igual rigor.", "940707": "Associação Nacional dos Hospitais Privados (ANAHP): A coleta e o tratamento de dados biométricos devem respeitar princípios de bioética, a Constituição Federal e os direitos humanos, garantindo a integridade dos titulares. Qualquer prática discriminatória viola normas legais e é inconstitucional. Deve-se considerar alternativas de autenticação e informar claramente sobre a necessidade da biometria e permitir o uso parcial do serviço.", "940708": "Associação Nacional dos Hospitais Privados (ANAHP): Os princípios da LGPD — como finalidade, adequação, necessidade, transparência, segurança e não discriminação — devem ser aplicados a todo tratamento de dados, sem exceções. Ao desenvolver uma atividade que envolva dados biométricos, é essencial incorporar todos esses princípios desde o início do processo.", "940709": "Associação Nacional dos Hospitais Privados (ANAHP): O tratamento massivo e automatizado de dados biométricos sem consentimento claro representa uma vulnerabilidade para o controlador. É essencial garantir que os titulares estejam cientes do tratamento, por meio de canais informativos e comunicação visual. Também é importante

permitir contestação, limitar o uso aos fins éticos definidos e adotar medidas que evitem qualquer forma de discriminação.", "940710": "Associação Nacional dos Hospitais Privados (ANAHP): Criando um canal de comunicação e mecanismos eficazes e eficientes onde os direitos dos titulares sejam atendidos em sua totalidade.", "940711": "Associação Nacional dos Hospitais Privados (ANAHP): Deve haver a comunicação, transparência, q deve ser requerido o consentimento formal, legítimo, inequívoco e específico dos responsáveis quanto a coleta e o tratamento dos dados biométricos dos menores. Bem como os demais parâmetros de proteção e adequação também precisam estar acessíveis, e vizíveis.", "940712": "Associação Nacional dos Hospitais Privados (ANAHP): A coleta e o tratamento de dados biométricos de menores exigem comunicação clara e transparente, com consentimento formal, legítimo, inequívoco e específico dos responsáveis. Além disso, os parâmetros de proteção e adequação devem ser acessíveis e visíveis.", "940714": "Associação Nacional dos Hospitais Privados (ANAHP): A plataforma deve obter o consentimento formal, específico e inequívoco dos pais, conforme exige a LGPD. Também deve garantir transparência quanto à adequação, necessidade e finalidade do tratamento. O controlador deve avaliar alternativas à biometria para verificar a idade da criança, como a apresentação de documentos de identificação do menor e do responsável.

Contribuinte: LUCAS ALVES DA SILVA BONAFE

Número: OP-1006198

Data: 01/08/2025 - 15:04

Resumo: "Um dado biométrico deve ser analisado através de critérios jurídicos objetivos e cumulativos, baseada no GDPR e em autoridades como a Autoriteit Persoonsgegevens (Holanda) e ICO (Reino Unido). São três os critérios: (i) natureza do dado – deve referir-se a características físicas, fisiológicas ou comportamentais, geralmente permanentes; (ii) método de tratamento – uma operação de processamento - ou um conjunto de operações - que pode ser aplicada às características físicas, fisiológicas ou comportamentais de uma pessoa, tornando possível sua identificação exclusiva; e (iii) finalidade – tratamento voltado a identificar ou confirmar a identidade de uma pessoa física. A combinação cumulativa desses critérios evita interpretações excessivamente amplas e traz maior segurança jurídica. Portanto, um dado é caracterizado como biométrico não apenas pela sua origem em características pessoais, mas quando resulta de características pessoais e é tratado tecnicamente para identificar alguém.", "940688": "Controladores devem fornecer informações claras, completas e acessíveis no momento da coleta ou antes da coleta de dados biométricos. Com base em diretrizes como as da ICO, os titulares devem ser informados sobre: finalidades do tratamento, base legal, tipos de dados coletados, destinatários, prazo de retenção, direitos previstos na LGPD, possibilidade de revogar consentimento, eventuais obrigações legais e contatos do controlador. Entretanto, o dever de transparência deve ser equilibrado com a necessidade legítima de proteção a segredos comerciais e informações confidenciais dos controladores. Canais adequados incluem dashboards, notificações just-in-time e QR codes (no ambiente digital) e sinalização visual e equipes capacitadas (em espaços

físicos).", "940690": "A distinção entre biometria tradicional (características físicas) e comportamental (padrões de interação) não implica, por si só, em obrigações distintas. A avaliação deve considerar o contexto do tratamento, analisando riscos e eficácia caso a caso. Dado seu uso frequente para identificação e prevenção de fraudes, é essencial garantir a qualidade dos dados biométricos. Isso exige controle contínuo e monitoramento, tendo em vista que a falta de qualidade de dados biométricos pode levar a erros nessas finalidades e a uma redução da performance de sistemas que utilizam esses dados, podendo até mesmo gerar resultados falsos. Quanto à segurança, devem ser adotadas medidas técnicas e administrativas para proteger os dados de acessos indevidos e incidentes. Entretanto, destaca-se que os princípios da qualidade dos dados e da segurança se aplicam a todo tratamento de dados, independentemente de sua natureza.", "940693": "O consentimento como base legal para o tratamento de dados biométricos, embora previsto na LGPD, deve ser utilizado de forma cautelosa e não generalizada. Isto porque o consentimento livre e específico, destacado, informado e inequívoco pode ser difícil de obter diante de desequilíbrios informacionais, pressões indiretas e ausência de alternativas reais, o que pode comprometer sua validade e eficácia. Assim, sua generalização pode fomentar hipercoleta e transferir indevidamente aos titulares a responsabilidade por riscos sistêmicos, pois a exposição desse tipo de dado, uma vez vazado, não pode ser revertida, e seus efeitos podem ser permanentes. Recomenda-se priorizar hipóteses como a do art. 11, II, "g" (prevenção à fraude e segurança do titular). Nos casos em que o consentimento for excepcionalmente adotado, é essencial garantir medidas como alternativas não biométricas, transparência sobre riscos, exclusão imediata após revogação e avaliação de impacto para justificar sua adoção.", "940695": "A aplicação da base legal de prevenção à fraude exige prova concreta de que a biometria é indispensável para mitigar riscos, não havendo alternativa menos invasiva. No setor financeiro, pode ser usada para transações de alto risco, desde que com finalidades claras e justificativa técnica. Para respeitar o princípio da necessidade, é essencial restringir a coleta ao mínimo necessário, evitar reutilização para outras finalidades e justificar tecnicamente a escolha. A coleta ampla, preventiva ou desvinculada de risco real compromete a legalidade do tratamento, mesmo sob essa base. Ainda, devem ser adotadas salvaguardas como: realização de Relatório de Impacto à Proteção de Dados ("RIPD"), limitação de prazo de retenção, medidas de segurança avançadas (criptografia, controle de acesso, segregação de dados), transparência quanto às finalidades e garantia de revisão humana em decisões automatizadas. A biometria deve ser usada com parcimônia, nunca como atalho para conveniência.", "940697": "Quando o tratamento de dados biométricos se fundamenta no cumprimento de obrigação legal ou regulatória, é essencial que a norma em questão seja explícita quanto à exigência a tipo de dado sensível. Isto porque a mera existência de uma obrigação genérica não autoriza a coleta de biometria. Assim, a interpretação deve ser restritiva e orientada pelo princípio da necessidade, admitindo-se o tratamento apenas quando o dado biométrico for indispensável para cumprir o dever legal. O controlador, portanto, deve comprovar que não há meio menos invasivo de atingir a finalidade prevista na norma. Mesmo diante de obrigação legal, deve-se adotar salvaguardas já anteriormente mencionadas, como: RIPD, controle de acesso e rastreabilidade, políticas de retenção mínima, descarte seguro, segregação de bases, e transparência com os titulares.", "940699": "O tratamento de dados biométricos por órgãos de

pesquisa, nos termos do art. 11, II, “c”, da LGPD, deve estar vinculado a finalidades exclusivamente acadêmicas, científicas ou estatísticas, de interesse público, sendo vedado o uso para fins comerciais. A base legal deve ser definida a partir da finalidade do tratamento, e não da natureza biométrica dos dados. Embora a LGPD não exija anonimização, ela é recomendada para mitigar riscos devido ao alto potencial de identificação. Nesses casos, é essencial avaliar se a anonimização é tecnicamente suficiente para descaracterizar os dados como pessoais, conforme os critérios do art. 12. Se os dados não forem anonimizados, aplicam-se as regras para dados sensíveis. Mesmo com anonimização eficaz, devem ser adotadas salvaguardas: controle de acesso, registro, limitação ao escopo, avaliação ética e revisão periódica. Tentativas de reidentificação são proibidas e sujeitas a responsabilização, prevenindo riscos e insegurança jurídica.”, “940700”: “O uso de reconhecimento facial exige comprovação de que não há alternativa menos invasiva ou, se baseado em consentimento, que este seja plenamente válido, conforme detalhado anteriormente, e com alternativa funcionalmente equivalente. A justificativa não pode se basear em conveniência. A tecnologia pode apresentar riscos de discriminação, especialmente contra grupos vulneráveis, e não deve ser usada em contextos como vigilância indiscriminada. Entretanto, outras tecnologias biométricas e sistemas automatizados de tomada de decisão com base em dados pessoais sensíveis podem apresentar problemas similares. Assim, soluções normativas e técnicas não devem se restringir a uma tecnologia específica, sob pena de se tornarem insuficientes diante da evolução e diversificação de métodos de identificação e análise automatizada. Salvaguardas para minimização de riscos incluem: RIPD, auditorias algorítmicas independentes, revisão humana, treinamento com dados diversos e sistemas descentralizados.”, “940701”: “A criação de sistemas de reconhecimento facial, a minimização de erros de identificação e garantia de maior qualidade dos resultados pode ser obtida através da utilização de meios técnicos preventivos, incluindo técnicas avançadas de aprimoramento da qualidade de algoritmos, multi-scale feature fusion, spatial attention, verificação de vida e aprimoramento contínuo de algoritmos. Dados devem ser refinados com ajustes em brilho, rotação e diversidade. Correções exigem auditorias periódicas, supervisão humana ou automatizada e intervenção tempestiva diante de falhas ou vieses. Tais medidas devem respeitar o estado da arte, limitações técnicas e financeiras, evitando onerosidade desproporcional. A aplicação do princípio da necessidade deve ser não apenas quantitativa, mas qualitativa, permitindo o uso de novos dados para corrigir vieses e melhorar a acurácia, com transparência e respeito ao sigilo comercial.”, “940702”: “O uso de reconhecimento facial não deve ser generalizado: em contextos como vigilância massiva em locais públicos, especialmente por órgãos estatais, o tratamento é considerado desproporcional e arriscado para os direitos fundamentais — como reconhecido pelo EDPB. Nesses casos, os riscos de discriminação, perseguição e violação de liberdades individuais superam os potenciais benefícios. Já em ambientes privados, como condomínios ou instituições financeiras, o uso pode ser proporcional se houver finalidade legítima, medidas de mitigação, transparência e possibilidade de alternativas menos invasivas (como cartões ou senhas), exceto quando a biometria for indispensável para prevenção à fraude. Devem ser observados os princípios da necessidade, proporcionalidade e finalidade, além da implementação de salvaguardas técnicas e jurídicas (RIPD, segurança da informação, transparência, opção funcionalmente equivalente

e limitação de finalidades).", "940704": "Dada sua sensibilidade e irreversibilidade, a proteção de dados biométricos exige salvaguardas técnicas e administrativas robustas, baseadas em análise de risco contínua e proporcional. Medidas incluem uso de Biometric PETs conforme a ISO/IEC 24745/2022: irreversibilidade, desvinculação e revogabilidade dos templates. Recomenda-se armazenamento local (on-device), que mantém o template armazenado localmente, sob controle direto do titular, minimizando riscos relacionados à transmissão e ao armazenamento em servidores centrais. Ainda, é essencial implementar RIPD, protocolos de resposta a incidentes, testes de segurança recorrentes e auditorias. A capacitação contínua das equipes e uma cultura de minimização são pilares da conformidade. A atuação da ANPD deve ser flexível e orientadora, permitindo adaptações seguras e eficazes conforme o contexto, de forma que diferentes setores e agentes econômicos adaptem suas soluções de forma proporcional, segura e sem coibir a inovação. ", "940707": "Em serviços não essenciais, o uso de biometria, especialmente com base no consentimento, exige observância aos princípios da autodeterminação, necessidade, transparência e não discriminação (ainda que esse último não esteja expressamente previsto na LGPD). A biometria só pode ser exigida se for tecnicamente indispensável à funcionalidade, com justificativa clara. Em regra, a recusa do titular em disponibilizar seus dados biométricos não pode gerar restrições indevidas aos serviços não essenciais, devendo existir alternativa funcional equivalente — como senha ou token. Nesse contexto, exigir biometria como única via compromete a liberdade de escolha e invalida o consentimento, e a ausência de opções pode configurar prática abusiva. Portanto, a proteção do titular deve se apoiar tanto no princípio da necessidade quanto na validade estrita do consentimento, garantindo que o tratamento seja proporcional, justificado e não discriminatório.", "940708": "Para garantir a proteção eficaz de dados biométricos, controladores devem adotar boas práticas alinhadas à LGPD, considerando o risco, a finalidade do tratamento e o contexto de uso. Destacam-se: (i) elaboração consistente do RIPD, valorizado como instrumento estratégico de governança e evidência de accountability; (ii) políticas de minimização e uso necessário, com controles internos e restrições contratuais; (iii) incentivo ao uso de modelos treinados com dados representativos da população brasileira, prevenindo vieses; e (iv) transparência eficaz, contextualizada e proporcional, com avisos em camadas, linguagem acessível e proteção a segredos industriais. Ainda, destaca-se que a discriminação não decorre exclusivamente do uso de tais dados, sendo um fenômeno com raízes sociais mais amplas. Por fim, é essencial que eventuais diretrizes da ANPD sejam orientativas, e não prescritivas, permitindo adaptações pelos agentes. ", "940709": "O tratamento de dados pessoais realizado exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou repressão de infrações penais não está sujeito à LGPD, devendo ser regido por legislação específica. Nesses casos, a atuação da ANPD deve ser orientativa, respeitando os limites legais, mas ainda assim promovendo boas práticas e salvaguardas éticas. Quando a LGPD se aplica, controladores devem adotar medidas concretas como transparência contextualizada, mecanismos automatizados de informação e canais acessíveis para exercício de direitos. A ANPD, por sua vez, deve fomentar educação em privacidade, elaborar guias específicos, promover parcerias intersetoriais e valorizar soluções escaláveis e eficazes de governança informacional. A proteção dos direitos dos titulares, nesses cenários, depende de articulação institucional, inovação regulatória e

cooperação entre agentes públicos e privados.", "940710": "Para garantir os direitos dos titulares – especialmente informação clara, acesso, correção e revogação do consentimento – em tratamentos biométricos automatizados, é essencial adotar medidas específicas, sobretudo no caso de crianças e adolescentes. Devem ser usadas linguagens acessíveis e adequadas à idade, com comunicação contextualizada e contínua, como orientam o EDPB, ICO e PDPC (Singapura). O titular deve entender o tratamento, inclusive sua sensibilidade biométrica, e poder exercer seus direitos com facilidade. Em casos de crianças e adolescentes, a informação deve alcançar não só a criança, mas também seus responsáveis, garantindo o consentimento informado. Mecanismos de verificação da identidade do responsável legal e interfaces simples para revogação e correção de dados são boas práticas recomendadas. A transparência deve ser efetiva durante todo o ciclo do tratamento, e não apenas no momento da coleta.", "940711": "O tratamento de dados biométricos de crianças e adolescentes exige a participação informada dos pais ou responsáveis, com base no art. 14 da LGPD e no ECA, observando a autonomia progressiva dos menores. A base legal dependerá do contexto, podendo ser qualquer uma do art. 11 da LGPD, desde que atendido o melhor interesse do titular (Enunciado 01/2023 da ANPD). Em escolas e espaços recreativos, o tratamento deve ser proporcional, transparente, seguro e voltado a finalidades legítimas – como segurança e controle de acesso. Devem-se evitar usos discriminatórios e garantir revisão, minimização e possibilidade de oposição. A utilização desses dados provavelmente levará à necessidade de elaboração de RIPD, caso seja realizado em larga escala e/ou afete significativamente interesses e direitos fundamentais, conforme critérios da ANPD e do ICO. A proteção eficaz passa por mecanismos claros de informação, consentimento e governança adaptada ao público infantojuvenil.", "940712": "O tratamento de dados biométricos de crianças e adolescentes é admissível com base em qualquer hipótese legal prevista na LGPD, conforme Enunciado 01/2023 da ANPD, desde que respeitado o princípio do melhor interesse. Como referência internacional, a abordagem da ICO segue o mesmo entendimento, admitindo o uso de variadas bases legais para o tratamento desses dados. Não há hierarquia entre as bases legais, devendo o agente de tratamento escolher a mais adequada conforme finalidade, risco e maturidade do titular. A participação informada dos pais ou responsáveis varia conforme o contexto e a autonomia progressiva, especialmente para adolescentes, respeitando sua autodeterminação informativa. Medidas técnicas e organizacionais eficazes são essenciais, incluindo restrição de acesso, criptografia, anonimização ou pseudonimização, treinamento contínuo da equipe, revisão da finalidade e auditorias internas para evitar abusos, vazamentos e acessos indevidos. ", "940714": "A verificação ou estimativa de idade por meio de dados biométricos, como em plataformas digitais e jogos, deve respeitar análise contextual, considerando riscos e finalidades específicas. O TJDFT reconheceu a validade do uso de biometria para impedir acesso de menores a casas de apostas. Ou seja, o próprio Judiciário entende que a utilização de mecanismos de garantia de idade por meio do fornecimento de dados biométricos seria possível e não seria proibida no contexto brasileiro. O princípio da necessidade exige que só sejam tratados dados biométricos estritamente necessários para garantir a idade, sem uso para outras finalidades, e o princípio do melhor interesse impõe que o mecanismo proteja menores de conteúdos impróprios e riscos. Critérios incluem base legal

adequada, minimização de dados, transparência, segurança técnica e organizacional, contratos claros com terceiros e, se aplicável, elaboração de RIPD.

Contribuinte: MARCELA MATTIUZZO

Número: OP-1006212

Data: 01/08/2025 - 15:21

Resumo:

:"", "940688": "", "940690": "", "940693": "", "940695": "", "940697": "", "940699": "", "940700": "" A tecnologia de reconhecimento facial é crucial para a segurança contra fraudes em diversos setores. Para garantir seu uso ético, é essencial seguir boas práticas. A transparência deve ser priorizada, informando claramente o usuário sobre a coleta e uso de dados biométricos. A necessidade e a proporcionalidade justificam seu uso como uma camada de segurança robusta contra fraudes digitais, especialmente com a prova de vida (liveness). Para mitigar riscos, é preciso adotar salvaguardas técnicas, como a criptografia. É fundamental realizar testes de acurácia, documentando o desempenho da solução em diferentes grupos demográficos no br para mitigar vieses e prevenir a discriminação algorítmica. Para soluções de alto risco, a norma ISO/IEC 30107-3 é um padrão técnico internacional para atestar a capacidade do sistema em detectar fraudes.", "940701": "", "940702": "", "940704": "", "940707": "", "940708": "", "940709": "", "940710": "", "940711": "", "940712": "", "940714": ""

Contribuinte: ERICA ALEXANDROFF NETTO

Número: OP-1006211

Data: 01/08/2025 - 15:21

Resumo: : "[Resposta completa por e-mail - Idec] Todo dado pessoal vinculado a uma característica física do titular é considerado dado biométrico, incluindo atributos imateriais (como a voz), ou comportamentais, como o padrão de digitação e estilo de andar (também chamado de “gait”)[1]. Isso independe de o dado permitir uma identificação individual, como a íris ou a digital, ou apenas uma categorização genérica ou coletiva, como etnia ou gênero. Diversos países tratam dados biométricos como sensíveis, exigindo proteção reforçada.", "940688": "[Resposta completa por e-mail - Idec] controladores que tratam dados biométricos devem adotar práticas de transparência ativa que permitam ao titular compreender, antes da coleta, como e por que seus dados serão utilizados. É necessário fornecer aviso de privacidade claro, com destaque para a natureza sensível dos dados e (i) descrição objetiva das finalidades do tratamento, como autenticação, segurança ou marketing, e inclusive as finalidades secundárias. (ii) Devem ser identificados o controlador e seus canais de contato, bem como (ii) a base legal que fundamenta o tratamento. Também é essencial indicar (iii) os direitos do titular (como acesso, correção, exclusão e revogação do

consentimento) e os meios para exercê-los. ", "940690": "[Resposta completa por e-mail - Idec] A biometria comportamental exige tratamento tão, ou ainda mais, rigoroso quanto a biometria tradicional, pois ambas envolvem dados pessoais sensíveis, com direitos e deveres correspondentes. A jurisprudência e a atuação regulatória no Brasil já demonstraram a importância dessa diferenciação. No caso Hering [1], foi constatada a coleta indevida de expressões faciais em provadores inteligentes, sem informação clara ou consentimento dos consumidores. De forma similar, o projeto ViaQuatro instalou câmeras em portas de trens para análise de reações emocionais sem o devido aviso de privacidade [2] e, em 2024, o TikTok foi multado em R\$ 23 milhões de reais no Maranhão por coletar e compartilhar dados biométricos faciais de usuários, incluindo menores, sem consentimento [3].

", "940693": "[Resposta completa por e-mail - Idec] Deve-se estabelecer um conjunto normativo restritivo para exceção ao consentimento ao tratamento de dados biométricos. Sobretudo pela natureza sensível e invasiva da coleta desses dados, é necessário que o consentimento seja privilegiado em detrimento de outras bases legais, tal como protegido pela redação do art. 11 da LGPD. No entanto, sabe-se que o consentimento é, muitas vezes, sujeito à coleta “pró-forma”, sem efetivo conhecimento e aceitação do usuário. A adoção de boas práticas é fundamental para que o consentimento não seja fornecido de forma desinformada e viciada pelos titulares. Recomenda-se que os titulares permaneçam podendo ter acesso ao espaço, produto, serviço ou funcionalidade ainda que não consentam com a captura dos dados biométricos, quando possível. Ou seja, que se garanta uma alternativa aos usuários, independentemente da base legal mobilizada. É imprescindível que essa opção alternativa seja apresentada de maneira ostensiva", "940695": "[Resposta completa por e-mail - Idec] A base da “prevenção à fraude” (art. 11, II, g) só se aplica se houver necessidade, proporcionalidade e vínculo direto com a finalidade e a segurança da operação (art. 6º, incisos I, II, III e IV). O trecho final da alínea “g” (“exceto no caso de prevalecerem direitos e liberdades fundamentais do titular”) deve ser interpretado de maneira ampliativa. Na prática do tratamento de dados biométricos para prevenção a fraudes, embora comum como forma de autenticação, expõe o titular a riscos irreversíveis, como fraudes por imitadores de voz ou deepfakes, e perda definitiva do controle sobre seus dados, caso vazem. Nesse sentido, esta base legal deve ser interpretada de maneira a não impor somente uma modalidade de autenticação, mas com o fornecimento de alternativas menos invasivas ao titular de dados.

", "940697": "[Resposta completa por e-mail - Idec] A primeira diretriz diz respeito à transparência ativa: é essencial que os titulares sejam informados, de forma clara, acessível e destacada, sobre os dados que serão coletados, as finalidades específicas do tratamento, os prazos de retenção, as condições de armazenamento, as medidas de segurança adotadas, as hipóteses de compartilhamento com terceiros e os riscos envolvidos. Essa comunicação deve ser feita antes do início da coleta, de maneira visível e com profissionais capacitados para prestar esclarecimentos. Um estudo de Agrawal et al. (2020) [1] demonstra como arquiteturas públicas de dados devem ser construídas com base em princípios de finalidade limitada, controle de acesso e supervisão contínua, assegurando que o tratamento de dados sensíveis como biometria ocorra de forma ética e proporcional. ", "940699": "[Resposta completa por e-mail - Idec] Mesmo para esse tipo de tratamento haja previsão de anonimização “sempre que possível”, a anonimização por si só não elimina completamente os riscos ou as obrigações do

controlador. A coleta e o processamento inicial da biometria já configuram tratamento de dados pessoais sensíveis, e dados anonimizados ainda podem ser utilizados para formar perfis comportamentais de pessoas identificáveis. Informações como vetores faciais, padrões de íris ou digitais, mesmo sem identificação nominal, podem ser reconectadas a indivíduos com o uso de outras bases, técnicas estatísticas ou inteligência artificial. Nesses casos, o uso para fins acadêmicos ou científicos não elimina o dever de adotar medidas rigorosas de proteção e o respeito aos direitos dos titulares. ", "940700": "[Resposta completa por e-mail - Idec] O uso de tecnologias de reconhecimento facial para vigilância em espaços públicos e privados não pode ser normalizado sob pretexto genérico de segurança. A coleta de dados biométricos em locais de circulação comum, como estações de metrô, ruas ou shoppings, não necessariamente ocorre para fins estritamente relacionados à segurança pública, exceção prevista pela LGPD. Esse problema se intensifica quando infraestruturas privadas se apropriam da função de segurança pública, utilizando a vigilância biométrica como instrumento de gestão, sem a mediação ou qualquer controle estatal. ", "940701": "[Resposta completa por e-mail - Idec] Quando há sub-representação de determinados grupos, o sistema tende a falhar com eles, reproduzindo discriminações e desigualdades [1]. Durães (2024) relata que, em Sergipe, um homem negro foi preso por engano em um estádio após ser confundido por um sistema de reconhecimento facial. Em outro caso, uma mulher negra foi abordada três vezes em uma micareta, também por erro do sistema. Com receio de contribuírem para práticas discriminatórias e a escalada da violência institucional, intensificada pela repercussão internacional do assassinato de George Floyd, gigantes da tecnologia como IBM, Microsoft e Amazon decidiram interromper a venda dessas soluções a forças policiais e entidades governamentais (Idec, 2022). Esses exemplos evidenciam que, mesmo quando alegadamente “aperfeiçoados”, os sistemas de reconhecimento facial operam em contextos que favorecem a reprodução de desigualdades estruturais.

", "940702": "[Resposta completa por e-mail - Idec] Sim. Diferentemente de senhas, PINs ou endereços de e-mail que podem ser alterados após um vazamento, os dados biométricos são imutáveis e característicos de uma pessoa, agravando as consequências de um potencial vazamento causado por problemas de segurança da informação [1]. Logo, o uso dessas tecnologias deve ser evitado quando a coleta é obrigatória ou compulsória e não oferece alternativas menos intrusivas ao titular, violando o direito à liberdade de escolha e à proteção de direitos fundamentais do titular. Isso porque, como já afirmado diversas vezes nesta contribuição, o reconhecimento facial expõe os titulares ao risco de discriminação ilícita ou abusiva, sobretudo contra grupos vulneráveis como pessoas negras, que apresentam maiores índices de falha na verificação biométrica. Também é desaconselhável seu uso quando o reconhecimento de emoções é utilizado para tomada de decisões importantes que afetam a vida das pessoas, dada a questionável", "940704": "[Resposta completa por e-mail - Idec] Quando falhas ocorrem, os danos são profundos, duradouros e, muitas vezes, irreparáveis. Por isso, a prevenção deve ser encarada como núcleo estruturante de qualquer projeto que envolva dados sensíveis. Para mitigar esses riscos, medidas de segurança técnicas indispensáveis incluem (i) criptografia robusta dos dados; (ii) controle de acesso estrito com o mínimo privilégio (por exemplo, um funcionário do financeiro só pode acessar o módulo de faturamento, sem permissão para visualizar dados de RH); (iii) a exclusão permanente dos

dados biométricos após a extração das características desejadas [1]; (iv) e a realização de análises de vulnerabilidades e testes de intrusão/penetração (pentest) [2]. A lógica do “zero knowledge proof” (sistemas que processam os dados sem necessidade de acessar sua forma bruta) também pode ser adotada para reforçar a segurança [3]. É igualmente fundamental implementar controles de acesso rigorosos", "940707": "[Resposta completa por e-mail - Idec] As boas práticas devem priorizar a liberdade de escolha do titular e a oferta de alternativas menos intrusivas para acesso ao serviço principal, como a validação por documentos de identificação. Além disso, o controlador deve realizar avaliação prévia da real necessidade da biometria, adotando-a somente quando estritamente imprescindível para a funcionalidade específica [1]. Sempre que possível, recomenda-se limitar o uso da biometria a funções auxiliares ou complementares, que não comprometam o acesso básico ou essencial ao serviço, ou que haja alternativa à sua utilização. ", "940708": "[Resposta completa por e-mail - Idec] Quando falhas ocorrem, os danos são profundos, duradouros e, muitas vezes, irreparáveis. Por isso, a prevenção deve ser encarada como núcleo estruturante de qualquer projeto que envolva dados sensíveis. Para mitigar esses riscos, medidas de segurança técnicas indispensáveis incluem (i) criptografia robusta dos dados; (ii) controle de acesso estrito com o mínimo privilégio (por exemplo, um funcionário do financeiro só pode acessar o módulo de faturamento, sem permissão para visualizar dados de RH); (iii) a exclusão permanente dos dados biométricos após a extração das características desejadas [1]; (iv) e a realização de análises de vulnerabilidades e testes de intrusão/penetração (pentest) [2].", "940709": "[Resposta completa por e-mail - Idec] Em contexto de tratamento massivo de dados biométricos, como em cidades inteligentes, estádios ou espaços públicos, é indispensável a adoção de medidas que mitiguem os riscos inerentes à natureza sensível desses dados. Primeiramente, os controladores devem realizar uma análise prévia de proporcionalidade e necessidade para determinar se o reconhecimento facial é estritamente necessário, priorizando alternativas menos invasivas e a transparência, como já amplamente debatido na contribuição. ", "940710": "[Resposta completa por e-mail - Idec] Os agentes de tratamento devem adotar medidas que assegurem acesso fácil, transparente e contínuo às informações. O direito à informação clara exige que o titular seja informado, antes da coleta, sobre a natureza sensível dos dados, a finalidade específica do tratamento, os critérios da decisão automatizada, o tempo de retenção e os riscos envolvidos. Esse dever de transparência deve ser cumprido em linguagem acessível, sem termos técnicos ou vagos, e disponibilizado em canais visíveis e compreensíveis (Rodrigues et. al., 2024) [1]. Já o direito de acesso e correção pressupõe que o titular possa verificar quais dados estão sendo tratados, inclusive resultados de sistemas automatizados de reconhecimento biométrico, e solicitar a correção de eventuais imprecisões. Isso implica que os sistemas devem ser auditáveis e que os controladores mantenham registros adequados, com possibilidade de revisão humana, quando necessário. ", "940711": "[Resposta completa por e-mail - Idec] Para que esse tratamento seja legítimo, é indispensável garantir a participação informada, livre e específica dos pais ou responsáveis, mediante consentimento claro e destacado, precedido de informações acessíveis quanto à natureza dos dados coletados, finalidades, riscos, duração do tratamento e direitos assegurados ao titular. Esse tipo de tratamento só será admissível quando estritamente necessário e proporcional à finalidade, observando-se, prioritariamente,

o princípio do melhor interesse da criança ou do adolescente, conforme previsto no art. 14 da LGPD ", "940712": "[Resposta completa por e-mail - Idec] Será admissível, nos termos da LGPD, quando houver consentimento específico e em destaque dado por pelo menos um dos pais ou responsáveis legais, ou quando for indispensável para cumprimento de obrigação legal, execução de políticas públicas ou para a proteção da vida ou da incolumidade física do menor. A base mais comum em contextos escolares e recreativos é o consentimento, que deve ser precedido de informação clara, em linguagem acessível e compatível com a compreensão dos pais ou responsáveis, incluindo detalhes sobre a natureza dos dados biométricos, finalidade, duração do tratamento, riscos envolvidos e direitos garantidos. ", "940714": "[Resposta completa por e-mail - Idec] Por se tratar de dados sensíveis de hipervulneráveis, os agentes de tratamento devem demonstrar que a coleta é estritamente necessária para atingir a finalidade legítima e que não há alternativa menos invasiva que ofereça o mesmo grau de efetividade. A compatibilização com o princípio da necessidade exige a coleta mínima de dados, preferencialmente com técnicas de estimativa que não armazenem imagens ou padrões biométricos de forma identificável. A Yoti, por exemplo, desenvolveu uma tecnologia de estimativa de idade facial que funciona sem armazenar imagens identificáveis.

Contribuinte: LUCAS MARTHO MARCON

Número: OP-1006217

Data: 01/08/2025 - 15:26

Resumo: "a caracterização de um dado como biométrico, assim como estabelecido pelo GDPR, deve considerar as características físicas, biológicas e comportamentais de uma pessoa natural. Considerando que biometria se configura como uma “análise, realizada por meios matemáticos e estatísticos, das características físicas ou comportamentais de um indivíduo”¹, tais características só serão efetivamente consideradas como dados biométricos se forem processadas por uma tecnologia específica com a finalidade de identificar ou autenticar um indivíduo de maneira inequívoca. Assim, a caracterização de um dado como biométrico depende da combinação entre a sua origem (uma característica humana), o processamento tecnológico aplicado e o objetivo de individualizar uma pessoa.", "940688": "conforme estabelece o art. 9º da LGPD, os agentes de tratamento têm o dever de fornecer informações claras e de fácil acesso aos titulares a respeito do tratamento de seus dados pessoais. No âmbito dessa obrigação, os agentes de tratamento podem abrir uma seção específica em suas políticas e avisos de privacidade relacionada ao tratamento dos dados biométricos, indicando as respectivas finalidades para tanto. (Complemento enviado por e-mail).", "940690": "como premissa inicial, tanto a biometria comportamental quanto a biometria tradicional devem ser tratadas com altos níveis de segurança e proteção, considerando que são classificadas como dados sensíveis e, portanto, as medidas legais devem ser devidamente observadas. No entanto, a coleta da biometria comportamental, apesar de ser uma técnica menos invasiva do que a da biometria tradicional, demanda requisitos específicos, uma vez que pode ser coletada de maneira passiva, mesmo sem a

ciência do titular, bem como pode ser alterada a depender de diversos fatores. Para mitigar tais riscos, propõe-se que os sistemas adotem um conjunto de medidas técnicas, como criptografia de ponta a ponta, pseudonimização, controles de acesso, auditoria algorítmica e adoção de padrões de segurança reconhecidos pelo mercado, minimização dos dados e a adoção do Privacy by Design.", "940693": "quando o consentimento for a base legal para o tratamento dos dados, é fundamental que ele seja obtido em conformidade com as exigências da LGPD. A garantia principal é que o consentimento jamais deve ser presumido, mas, sim, concedido por meio de uma manifestação de vontade ativa, livre e inequívoca por parte do titular. Para ser válido nesse contexto, o consentimento precisa ser informado, específico para uma finalidade legítima e apresentado de forma destacada e acessível. Na prática, isso implica o dever de informar claramente ao titular quais dados estão sendo tratados e com qual propósito. (Complemento enviado por e-mail)", "940695": "o uso de dados biométricos para prevenção à fraude requer uma justificativa definida e contextualizada, de modo que o agente de tratamento consiga demonstrar a existência do risco de fraude e a indispensabilidade do uso da biometria para mitigá-lo. Para tanto, o bem jurídico a ser protegido deve ser devidamente especificado. A utilização de dados biométricos para prevenção à fraude deve considerar os princípios de necessidade e minimização, de forma que o tratamento deve ser limitado à identificação e autenticação do titular. Dentre as salvaguardas para garantir a segurança dos dados tratados, destacamos: (i) elaboração de um Relatório de Impacto à Proteção de Dados, (ii) transparência aos titulares sobre a coleta de referidos dados e respectivas finalidades; (iii) auditorias e avaliações sistêmicas; (iv) criptografia robusta, tal como o padrão AES-256 e pseudonimização.", "940697": "o tratamento de dados biométricos para cumprimento de obrigação legal ou regulatória pelo controlador deve se basear nos critérios de necessidade, proporcionalidade e, evidentemente, da legalidade, cuja finalidade deve ser vinculada ao cumprimento da obrigação legal ou regulatória. Dentre as salvaguardas, destacamos (i) transparência com relação às informações sobre o tratamento, (ii) elaboração de Relatório de Impacto à Proteção de Dados; e (iii) adoção de medidas técnicas e administrativas, com governança em todo o ciclo.", "940699": "não aplicável, considerando o escopo de atuação da ABIPAG.", "940700": "sendo uma técnica naturalmente invasiva, a utilização de reconhecimento facial deve ser realizada quando outra tecnologia não for suficiente para atingir a finalidade pretendida com o tratamento. Para que os princípios da LGPD sejam observados, os agentes de tratamento devem adotar salvaguardas técnicas, administrativas e institucionais para garantir a proteção dos dados que serão tratados, bem como a integridade do titular. As salvaguardas incluem pseudonimização, criptografia, políticas claras para garantir transparência aos titulares, fiscalização de vieses algorítmicos e governança robusta. No mais, para evitar resultados discriminatórios, é importante que as tecnologias de reconhecimento facial sejam treinadas com bases de dados diversificadas, que reflitam as diversas raças e etnias da população. A ausência dessa diversificação pode levar a vieses nos resultados das análises.", "940701": "para garantir a eficácia, a confiabilidade e, principalmente, para mitigar riscos de discriminação, os sistemas de reconhecimento facial devem ser projetados e mantidos por meio de um ciclo de vida que integre aspectos técnicos e de governança. Para tanto, esse ciclo de vida deve ser projetado a partir de uma base de dados diversificada, com uma pluralidade de rostos, expressões, iluminação e imagens de qualidade.

Além disso, as melhores práticas de arquitetura para os modelos de reconhecimento facial devem ser empregadas. Revisão humana periódica para monitoramento das respostas do algoritmo testes e auditorias contínuas também são medidas para mitigar eventuais falhas dessas tecnologias. (complemento por e-mail)", "940702": "a utilização de tecnologias de reconhecimento facial deve ser precedida de uma análise da finalidade, do contexto e da proporcionalidade da medida. O uso dessas tecnologias não é recomendado em situações sem uma finalidade legítima e específica, ou quando envolve um impacto desproporcional à privacidade e aos direitos fundamentais, como é o caso de vigilância em massa de espaços públicos. O uso dessas tecnologias em hospitais e escolas também deve ser cuidadosamente analisado, uma vez que envolve titulares de dados em situação de vulnerabilidade. Contudo, no contexto específico do mercado de meios de pagamento, a ABIPAG ressalta que os casos de uso são frequentemente essenciais para a prevenção a fraudes e segurança das operações, não identificando, a princípio, a dispensabilidade da tecnologia para essas finalidades críticas. Como medida de mitigação, é recomendável que os agentes de tratamento (i) elaborem um Relatório de Impacto à Proteção de Dados, de forma a avaliar a

proporcional", "940704": "dentre as medidas técnicas, podemos listar: (i) criptografia forte, tanto aos dados em trânsito quanto aos em repouso, (ii) utilização de templates biométricos em vez das imagens brutas, (iii) controles de acesso com a implementação de MFA, (iv) monitoramento constante de riscos e testes de segurança, como pentests e varreduras de vulnerabilidades. Como medidas organizacionais e de governança apropriadas, recomenda-se: (i) desenvolvimento de políticas e procedimentos internos sobre o tratamento de dados biométricos, (ii) atualização dos registros de operações de tratamento (RoPA) para as novas finalidades que demandem a coleta de dados biométricos, (iii) elaboração de Relatório de Impacto à Proteção de Dados, (iv) treinamento e conscientização de colaboradores, (v) atualização e implementação de um plano de resposta a incidentes, e (vi) procedimentos para avaliação prévia de fornecedores relacionados à segurança da informação e proteção de dados.", "940707": "em serviços não essenciais, a utilização da biometria deve ser justificada por uma finalidade legítima e critérios de razoabilidade previamente definidos, especialmente em cenários de alto risco. Nessas ocasiões, a recusa do titular em fornecer sua biometria deve ser analisada com base no risco. Em eventuais recusas ou situações externas, o controlador deve oferecer alternativas que garantam nível mínimo de segurança para garantir o acesso, como tokens, senhas únicas ou mesmo certificados digitais. Importante destacar que a limitação de acesso a determinadas finalidades em decorrência da verificação da identidade do titular, por si só, não configura prática discriminatória ou abusiva. (Complemento por e-mail)", "940708": "conforme já destacado em outras respostas, medidas de segurança devem ser implementadas em todo o ciclo de vida do tratamento de dados biométricos. Dentre as medidas de segurança que podem ser implementadas, destacamos: (i) análise prévia, que justifique a necessidade e razoabilidade do tratamento de dados biométricos e posterior elaboração de um Relatório de Impacto à Proteção de Dados, (ii) implementar medidas de minimização durante a coleta dos dados, como, por exemplo, selecionar apenas os dados de entrada estritamente necessários para o atingimento da finalidade, bem como utilizar templates ao invés de dados brutos, (iii) implementar políticas para controle de acesso, retenção dos dados, criptografia e expurgo de dados, (iv) fornecer informações claras e

acessíveis aos titulares sobre o tratamento dos dados, (v) realizar testes e monitoramento contínuo nos sistemas .", "940709": "a transparência é fundamental para preservar a autodeterminação informativa dos titulares. Assim, mesmo na ocorrência de eventos de tratamento massivo de dados, os controladores devem informar aos titulares, através de avisos claros, portais públicos ou outros veículos de comunicação, que seus dados pessoais serão coletados. Além disso, garantir a transparência também implica a disponibilização de canais de comunicação acessíveis, por meio dos quais os titulares possam tirar dúvidas, obter mais detalhes e exercer seus direitos.", "940710": "para garantir respeito aos direitos dos titulares, os agentes de tratamento devem prover informação clara, acessível e de fácil compreensão. Além disso, a disponibilização de canais de comunicação direta com os titulares é essencial para o correto atendimento aos direitos dos titulares. Tais canais devem possibilitar que os titulares questionem sobre a existência de decisões automatizadas e revoguem seu consentimento quando este for a base legal utilizada para amparar o tratamento.", "940711": "o tratamento de dados biométricos de crianças e adolescentes é uma atividade que exige cuidados específicos, sendo sempre pautada pelo princípio fundamental do melhor interesse do menor. Conforme o Enunciado 1 da ANPD, o tratamento não se limita ao consentimento parental específico e pode se basear em outras hipóteses legais claras do artigo 11 da LGPD, como o cumprimento de obrigação legal ou a garantia da prevenção à fraude, desde que a escolha sempre vise proteger a criança ou o adolescente. No contexto financeiro, por exemplo, em que a abertura de contas para menores não emancipados depende da representação de seus responsáveis legais e a biometria é considerada uma boa prática de segurança, a aplicação dessa tecnologia é admissível. Para que isso ocorra de forma legítima, é essencial garantir a participação informada dos responsáveis, oferecendo-lhes explicações transparentes sobre porque o uso dos dados biométricos do menor é uma medida necessária e proporcional para a finalidade", "940712": "O tratamento de dados biométricos de crianças e adolescentes deve ser sempre guiado pelo princípio do melhor interesse do menor e, nos termos do Enunciado nº1 da ANPD, o tratamento não se restringe apenas ao consentimento parental específico, uma vez que pode ser amparado em outras bases legais do artigo 11 da LGPD. Para que os pais ou responsáveis legais possam participar, o controlador deve fornecer as informações pertinentes sobre o tratamento, além de disponibilizar um canal de contato para que os pais possam contatar o controlador. Em complemento, os controladores devem implementar medidas de segurança robustas, como criptografia, templates, controles de acesso, firewalls e antivírus, além de elaborar políticas internas e Relatório de Impacto à Proteção de Dados.", "940714": "a operação de um sistema de verificação de idade precisa estar alinhada aos pilares da LGPD, o que inclui transparência, um propósito determinado e a minimização dos dados. Acima de tudo, deve prevalecer o melhor interesse do menor, exigindo que o controlador documente sua análise de risco e necessidade de Relatório de Impacto à Proteção de Dados (RIPD). A observância do princípio da necessidade implica comparar a eficácia da biometria com métodos alternativos e restringir a coleta de dados ao essencial. Por exemplo, não se deve coletar a impressão digital se a análise facial já cumpre o objetivo pretendido. Adicionalmente, o sistema deve garantir que os dados biométricos não sejam retidos além do tempo estritamente necessário, respeitando-se sempre as obrigações legais ou regulatórias de manutenção de dados que recaiam sobre o controlador.

Número: OP-1006220

Data: 01/08/2025 - 15:37

Resumo: "Nos termos do art. 5º, II, da LGPD, um dado é considerado biométrico quando resulta do tratamento técnico de características físicas, fisiológicas ou comportamentais de uma pessoa, de forma a permitir sua identificação única. Entre os critérios objetivos, destacam-se: a origem em atributo próprio e estável do indivíduo (como íris, face ou voz); o uso de tecnologia para captação e processamento com finalidade de identificação ou autenticação; a capacidade de individualizar o titular; e o vínculo direto com pessoa identificada ou identificável. Referida vinculação enquadra o dado como sensível, sendo a possibilidade concreta de identificação o critério central da definição de dado biométrico. As Resoluções BCB nº 406 e 407, que tratam do Open Finance, poderão viabilizar a implementação do "Pix por Biometria" no setor de pagamentos, com autenticação de transações via impressão digital ou reconhecimento facial, exemplificando a aplicação prática dos critérios de identificação única.", "940688": "No tratamento de dados biométricos, especialmente em ambientes digitais e financeiros, os controladores devem adotar mecanismos informativos proativos, que permitam ao titular compreender, de forma clara e antecipada, como seus dados serão utilizados. Isso inclui a apresentação de avisos específicos sobre a finalidade do tratamento (ex.: autenticação de transações), o tipo de dado coletado (como reconhecimento facial ou impressão digital), a base legal aplicada, os responsáveis envolvidos, bem como as formas de uso, armazenamento, proteção e eventuais compartilhamentos. No setor de pagamentos, uma prática recomendada é o uso de pop-ups explicativos no onboarding de aplicativos de banking, antes da ativação da câmera ou leitor biométrico, informando a necessidade da coleta. O titular deve ser informado sobre a voluntariedade do fornecimento e as consequências da recusa, garantindo, assim, uma decisão consciente e alinhada aos princípios da LGPD.", "940690": "As biometrias tradicional e comportamental são classificadas como dados pessoais sensíveis pela LGPD e exigem o mesmo nível de proteção jurídica e técnica. A biometria comportamental, contudo, impõe desafios adicionais quanto à qualidade e segurança dos dados, pois suas múltiplas variantes (inerentes à natureza humana) elevam o risco de falsos positivos/negativos, o que impõe aos controladores a revisão periódica da acurácia dos sistemas. Por ser menos perceptível ao titular, sua coleta exige maior transparência e, quando possível, oferta de alternativas ou direito de oposição. No setor financeiro, por exemplo, a biometria comportamental pode ser usada para autenticação e prevenção a fraudes a partir do perfil comportamental do usuário e da elaboração de score de risco individualizado. Por serem dados sensíveis, os dados coletados a partir de biometria comportamental devem ser tratados com segurança robusta, uso ético e não discriminatório.", "940693": "Para garantir o correto consentimento para o tratamento de dados biométricos nos termos da LGPD, é necessário apresentar ao titular, de maneira clara e acessível, solicitação autônoma relativa ao uso da biometria, com indicação expressa da finalidade, sem recorrer a cláusulas genéricas ou implícitas. A manifestação deve

ser voluntária, sem vícios de vontade, especialmente em contextos de desequilíbrio, como relações de trabalho ou serviços essenciais, nos quais o titular não dispõe de escolha real e pode ser compelido a consentir por necessidade. Nesses casos, o consentimento não constitui base legal válida, sendo mais adequado recorrer a outra hipótese legítima prevista no art. 11 da Lei. A definição da base legal deve resultar de análise criteriosa do contexto e da finalidade do tratamento, de modo a assegurar não apenas a conformidade normativa, mas também maior estabilidade jurídica à atividade do controlador e a efetiva proteção dos direitos do titular.", "940695": "A aplicação da base legal do art. 11, II, “g”, da LGPD exige que o uso de dados biométricos para prevenção à fraude seja necessário, proporcional e restrito à finalidade de segurança. É imprescindível demonstrar que não há alternativa menos intrusiva com eficácia equivalente. No setor financeiro, por exemplo, a biometria pode ser empregada para autenticação, desde que acompanhada de salvaguardas técnicas (criptografia, tokenização, anti-spoofing), organizacionais (políticas internas, treinamentos, RIPD) e jurídicas (limitação de finalidade e acesso). O tratamento não se legitima se representar risco desproporcional às liberdades do titular. Assim, deve-se realizar teste de balanceamento, garantir a transparência e permitir revisão em caso de erro, assegurando, em última análise, respeito à autodeterminação informativa.", "940697": "Nesses casos, os controladores devem observar os princípios da necessidade, proporcionalidade e segurança. A coleta deve se restringir ao mínimo necessário para cumprir a obrigação legal expressa, vedados excessos ou desvios. Devem ser adotadas salvaguardas técnicas e organizacionais, como controle de acesso restrito, criptografia, governança interna, RIPD e contratos que garantam proteção por terceiros. Órgãos públicos devem assegurar transparência ativa (art. 23), e todos os controladores, mesmo amparados por obrigação legal, devem respeitar os demais princípios da LGPD, como não discriminação, adequação, transparência, prevenção e responsabilização. No setor de pagamentos, a biometria pode ser integrada como fator adicional de segurança, desde que seu uso seja proporcional, transparente e alinhado à regulação, nos limites legais e constitucionais.", "940699": "Apesar da autorização de uso de dados biométricos em pesquisas (art. 11, II, “c”), preferencialmente anonimizados, havendo risco razoável de reidentificação (ex.: cruzamento de bases), devem ser integralmente aplicadas as ressalvas utilizadas no tratamento de dados sensíveis. Os limites incluem: (i) uso estrito à finalidade científica; (ii) anonimização sólida e, se não for possível, pseudonimização em ambiente seguro; (iii) proibição técnica e contratual de reidentificação e compartilhamento não autorizado; e (iv) transparência sobre a pesquisa. Portanto, nesse cenário, a realização de avaliação ética e de relatório de impacto (RIPD) são de extrema importância. Destaca-se também a vedação ao uso secundário de dados biométricos coletados para finalidade de pesquisa, sob pena de violar a legalidade do tratamento. O objetivo da pesquisa não pode servir de pretexto para desviar a biometria para finalidades econômicas sem nova base legal.", "940700": "O uso de FRT deve observar os princípios da necessidade (ausência de alternativa menos invasiva), proporcionalidade (uso mínimo e por tempo limitado), transparência (informação clara ao titular) e não discriminação. Constituem formas de mitigar riscos a (i) realização de testes no sistema com dados diversos, medindo erros por grupos e corrigindo vieses; (ii) vedação de decisões automatizadas, sem revisão humana (art. 20); (iii) a adoção de políticas internas e treinamentos sobre FRT para evitar abusos; (iv) a realização de avaliações de impacto (RIPD)

prévias e periódicas. Salvaguardas técnicas incluem descarte da imagem após verificação, anonimização, criptografia e mecanismos anti-spoofing. Institucionalmente, recomenda-se supervisão contínua, logs auditáveis e canais acessíveis para contestação. A FRT deve ser projetada com “privacy by design” e só aplicada quando os benefícios forem superiores aos riscos aos direitos fundamentais.”, "940701": "Para garantir eficácia e confiabilidade, os FRTs devem ser concebidos com algoritmos robustos, treinados em bases amplas e diversas, com capacidade de ajustar-se à parâmetros e contextos de uso. Testes periódicos e monitoramento de taxas de erro (falsos positivos e negativos) são essenciais para a calibragem dessas tecnologias. Para a correção de falhas, devem ser adotados mecanismos de revisão humana imediata, com possibilidade de contestação pelo titular (art. 20 da LGPD). Também se recomenda a implantação de canais para reporte de falhas e retificação de dados. Em aplicações sensíveis, deve-se combinar a FRT com outros fatores de autenticação e manter registros das decisões automatizadas para posterior auditoria. Comitês técnicos ou responsáveis internos são fundamentais na supervisão do desempenho e da governança algorítmica, assegurando transparência nos critérios de decisão. Dessa forma, é possível conciliar o uso de tecnologia eficiente com o respeito aos direitos dos titulares.”, "940702": "O uso de reconhecimento facial (FRT) não é recomendado em contextos de vigilância massiva, identificação indiscriminada em espaços públicos ou aplicação a grupos vulneráveis, como crianças, sem finalidade legítima e proporcional. Também é desaconselhado para inferências subjetivas, como reconhecimento de emoções para fins comerciais, pois fere direitos constitucionais à privacidade, intimidade e imagem. Em certos casos, o FRT pode comprometer garantias individuais, que devem ser priorizadas. Assim, recomenda-se o uso de tecnologias alternativas, como autenticação multifatorial, biometria local no dispositivo, tokens físicos ou digitais, QR codes ou cartões eletrônicos. Essas soluções respeitam os princípios da necessidade e proporcionalidade (art. 6º da LGPD), promovendo segurança com menor invasividade.”, "940704": "Dados biométricos exigem proteção técnica e administrativa rigorosa, dada sua natureza sensível e o caráter irreversível de eventuais violações. Como medidas de mitigação, recomenda-se: criptografia em repouso e trânsito; uso de templates em vez de imagens brutas; armazenamento segregado em módulos seguros; controle de acesso com autenticação multifator e registro de logs. No âmbito administrativo, destaca-se a importância de programas de governança em privacidade, com avaliações periódicas de risco, testes de invasão, resposta a incidentes e monitoramento contínuo, conforme arts. 46 e 50 da LGPD. Normas como ISO/IEC 27001 e 24745 devem orientar a avaliação de riscos e inspeção de conformidade. Também são boas práticas: due diligence de fornecedores, capacitação das equipes e orientação dos responsáveis por segurança, garantindo abordagem preventiva, auditável e centrada na proteção dos titulares.”, "940707": "Quando a autenticação biométrica não for essencial ao serviço contratado, o controlador deve oferecer formas alternativas de acesso ao titular, sob risco de configurar discriminação, em violação ao art. 6º, IX, da LGPD. A recusa do titular em fornecer dados biométricos, sobretudo quando baseada em consentimento, não pode gerar penalidades nem restringir funcionalidades de forma desproporcional, tampouco impedir o acesso ao serviço principal. A limitação será válida apenas se: (i) a funcionalidade for opcional; (ii) houver justificativa técnica clara para o uso de biometria; e (iii) o titular for previamente informado sobre os motivos e os efeitos da

recusa (art. 18, VIII). A política de privacidade deve explicitar as hipóteses de exigência de biometria, e o consentimento, se adotado, deve ser livre, informado e inequívoco, vedando-se qualquer forma de coação, ainda que indireta.", "940708": "Para proteção eficaz no tratamento de dados biométricos, os controladores devem adotar boas práticas que integrem segurança, governança e ética. Dentre elas, destacam-se (i) a adoção de “privacy by design”, minimizando a coleta e preferindo processamento local no dispositivo do titular; (ii) políticas internas específicas para biometria, com definição clara de responsabilidades, avaliação prévia de riscos e resposta a incidentes; (iii) transparência e controle do titular, com mecanismos de informação, acesso e exclusão de dados; (iv) prevenção à discriminação, com auditoria de algoritmos e garantia de alternativas para grupos afetados por falhas de acurácia; (v) limitação de finalidade e retenção, com descarte seguro ao término do uso; e (vi) supervisão contínua, com auditorias e documentação das decisões. Tais medidas concretizam os princípios da LGPD e promovem um uso legítimo e confiável da biometria.", "940709": "Em tratamentos contínuos e massivos de dados biométricos, como em cidades inteligentes ou vigilância em estádios e espaços públicos, os controladores devem adotar medidas que garantam a autodeterminação informativa dos titulares (art. 2º, II, LGPD). Isso inclui sinalização visível em áreas monitoradas, campanhas educativas, políticas de privacidade acessíveis e canais permanentes para exercício dos direitos previstos no art. 18, ainda que o tratamento não se baseie em consentimento. Devem ser implementadas revisões humanas em decisões automatizadas (art. 20) e mecanismos de anonimização ou minimização de dados sempre que possível. A limitação da finalidade, a transparência ativa e o engajamento com a sociedade civil, sobretudo com grupos vulneráveis, integram o dever de governança e boas práticas (art. 50), reforçando uma atuação ética, preventiva e proporcional no uso de biometria em espaços públicos.", "940710": "Para proteger os direitos dos titulares no tratamento de dados biométricos, o controlador deve adotar medidas transparentes e eficazes. O direito à informação (arts. 6º, VI e 9º) exige políticas acessíveis, em linguagem clara, que informem a base legal, a finalidade e o uso de decisões automatizadas. O acesso aos dados (art. 18, II) deve ocorrer por canais seguros, permitindo ao titular visualizar suas informações e o histórico de uso. A correção (art. 18, III) requer mecanismos para ajustar associações incorretas, como templates vinculados a dados errados. A revogação do consentimento e a eliminação dos dados (art. 18, VI e §5º) devem ser simples e registradas. No caso de decisões automatizadas, o direito à revisão humana (art. 20) deve ser garantido, com procedimentos claros e auditáveis. A manutenção de logs dessas interações reforça a transparência e a autodeterminação informativa.", "940711": "O tratamento de dados biométricos de crianças e adolescentes exige cuidados redobrados e só é admissível com base legal clara e respeito ao princípio do melhor interesse (art. 14 da LGPD). A coleta requer consentimento específico e destacado dos pais ou responsáveis (art. 14, §1º), com informações claras e adequadas à compreensão do menor, sempre que possível. Esse consentimento deve ser verificável e revogável a qualquer tempo. O uso da biometria só se justifica quando estritamente necessário para finalidades legítimas, como segurança escolar ou controle de acesso. Nesses casos, devem ser observadas a minimização dos dados, segurança reforçada e transparência contínua. Além do consentimento, são admitidas as bases legais da obrigação legal e da proteção da vida ou integridade física (art. 11, II, “e”). Fora

dessas hipóteses, o uso tende a ser abusivo. A biometria só é compatível com a LGPD se for proporcional, necessária e efetivamente benéfica ao menor.", "940712": "O tratamento de dados biométricos de crianças é admissível quando houver consentimento específico e verificável dos pais ou responsáveis (art. 14, §1º, LGPD), e deve sempre observar o princípio do melhor interesse da criança. A participação informada exige que os responsáveis recebam informações claras, destacadas e compreensíveis sobre a finalidade do tratamento, os riscos envolvidos e os direitos do titular. Devem ser asseguradas alternativas não biométricas sempre que possível, especialmente em verificações de idade, evitando a retenção indevida de imagens. Para prevenir abusos, vazamentos e acessos não autorizados, o controlador deve implementar salvaguardas técnicas e organizacionais robustas, como criptografia, controle de acesso restrito, políticas internas específicas, avaliação de impacto e auditorias periódicas. A biometria só deve ser utilizada quando estritamente necessária, proporcional e efetivamente protetiva à criança, jamais como forma invasiva ou discriminatória.", "940714": "A verificação ou estimação de idade por biometria em plataformas digitais e jogos deve seguir os princípios da necessidade e do melhor interesse (art. 14, LGPD). Só será legítima se não houver alternativa eficaz menos invasiva, com finalidade específica e legítima, como proteger contra conteúdos inadequados, sendo vedado seu uso para marketing ou criação de perfis (profiling). O tratamento deve ser mínimo: processamento local, sem retenção de imagens e com descarte imediato. A tecnologia deve ter acurácia adequada, evitando exclusões indevidas, e prever meios alternativos de verificação. Exige-se consentimento dos pais (em caso de crianças) ou, no mínimo, ciência dos responsáveis (art. 14, §6º). A biometria só se justifica se indispensável, proporcional e acompanhada de salvaguardas técnicas e organizacionais robustas. Sempre que possível, devem ser adotados métodos menos intrusivos, desde que atendam ao melhor interesse do menor.

Contribuinte: DIEGO PEREZ MARTIN DE ALMEIDA

Número: OP-1006221

Data: 01/08/2025 - 15:38

Resumo: "A caracterização como dado biométrico deve considerar a presença cumulativa de três elementos: (i) aplicação de tratamento técnico específico sobre características físicas, fisiológicas ou comportamentais; (ii) finalidade deliberada de identificação ou autenticação do titular; e (iii) potencial de individualização do titular. Nem todo dado biométrico é dado pessoal, pois podem não servir para identificar ou tornar pessoas identificáveis. Definições excessivamente inclusivas podem capturar dados relacionados ao corpo, mas não capazes de identificação, levando a encargos de conformidade desnecessários. Portanto, dados biométricos devem ser tratados como informação sensível apenas quando usados para identificação única. Essa abordagem é coerente com a prática internacional, como no GDPR da UE e nas diretrizes do Comitê Europeu de Proteção de Dados e da ICO do Reino Unido, que reconhecem dados biométricos como sensíveis quando há uso efetivo para identificação de um indivíduo específico. ", "940688": "Os controladores devem adotar medidas em conformidade com o princípio da transparência da LGPD, cujo objetivo é garantir que os

titulares de dados tenham informações claras sobre como seus dados pessoais são tratados. Os controladores também estão sujeitos à obrigação prevista no Artigo 9º de fornecer informações sobre o tratamento, incluindo as finalidades para as quais os dados pessoais são processados.

","940690": "As tecnologias somente devem ser regulamentadas como tratamento de dado biométrico quando utilizadas para identificar pessoas de forma única. É necessário ainda avaliar com cuidado se e quando os traços comportamentais se enquadram como dados biométricos, considerando que nem sempre possuem estabilidade ou singularidade suficientes para uma identificação confiável. Assim, o uso meramente funcional ou estatístico, sem finalidade identificadora, não deve ser regulado da mesma forma que aplicações com intenção identificar indivíduos específicos. Limitar o escopo da definição é essencial para evitar que a regulação capture dados não identificáveis, o que geraria exigências desproporcionais. O fator decisivo é a finalidade do tratamento: se os dados são usados efetivamente para individualizar alguém, devem ser tratados como sensíveis; do contrário, não.

","940693": "O consentimento para dados biométricos deve ser livre, informado, específico, destacado e inequívoco, conforme a LGPD. Em contextos de baixa intrusão, como autenticação em dispositivos pessoais, são válidas soluções simplificadas (painéis de preferência, aceites digitais). Quando o tratamento for necessário à prestação do serviço ou à prevenção à fraude e segurança do titular (art. 11, II, “a” e “g”), o consentimento pode ser inadequado ou dispensável. Exigir consentimento nesses casos pode comprometer a finalidade do tratamento. Também é inadequado em situações com múltiplos titulares não identificáveis individualmente (ex: imagens com transeuntes). A presença de remuneração ou benefícios não compromete, por si só, a liberdade do consentimento. Autoridades como o ICO e a autoridade holandesa reconhecem que o consentimento não é sempre a base mais eficaz nesses contextos.

","940695": "Dados biométricos podem ser utilizados para prevenir atividades fraudulentas, beneficiando tanto os consumidores quanto as empresas. O Artigo 11 da LGPD permite expressamente o tratamento para essa finalidade, salvo se o interesse nesse tratamento for superado pelos direitos dos indivíduos. O reconhecimento dessa base legal é fundamental e sua aplicação deve ser pautada por uma análise proporcional, que avalie as necessidades de proteção e os riscos desse tratamento. A interpretação dessa base legal deve ser ampla para abranger o uso de dados biométricos para combater fraudes e ameaças à integridade. É legítimo seu uso, por exemplo, na recuperação de contas hackeadas, na detecção de deepfakes de figuras públicas e na investigação de possíveis falsificações de identidade.

","940697": "Os controladores devem identificar e avaliar suas obrigações legais e regulatórias para o tratamento de dados pessoais sensíveis, incluindo dados biométricos. Para o setor privado, tais obrigações podem decorrer de leis e regulamentos, ou de ordens específicas de órgãos governamentais. As orientações devem reconhecer claramente a importância desse tipo de tratamento.

","940699": "Entidades de pesquisa devem conduzir estudos em conformidade com as proteções previstas na LGPD. Isso inclui a anonimização de dados pessoais sensíveis sempre que possível.

","940700": "É importante reconhecer que tecnologias que tratam dados pessoais estão sujeitas não apenas à LGPD, mas também a outras leis vigentes. Pode ser necessário examinar como leis que proíbem a discriminação ilícita se aplicam ao uso de novas tecnologias. Essas leis devem continuar protegendo contra a discriminação à medida que novas tecnologias são

adotadas.", "940701": "", "940702": "", "940704": "Reconhecemos que a ANPD está considerando emitir orientações sobre relatórios de impacto à proteção de dados pessoais (RIPDs) para tratamentos que apresentem determinados riscos. Somos favoráveis à exigência de que os controladores realizem RIPDs ao tratar dados pessoais sensíveis, incluindo dados biométricos, o que está em conformidade com o GDPR da União Europeia e outras legislações globais de proteção de dados.", "940707": "", "940708": "Os controladores devem adotar práticas em conformidade com a LGPD, incluindo limites ao tratamento de dados sensíveis. Além disso, a LGPD exige que os controladores que tratam qualquer dado pessoal sejam transparentes quanto às suas atividades e adotem medidas de segurança apropriadas. Leis além da LGPD também podem proibir a discriminação e outros atos ilícitos.", "940709": "É importante compreender se os dados, nesses cenários, estão sendo tratados com a finalidade de identificar indivíduos de forma única. Se for o caso, eles devem ser protegidos como dados biométricos. No entanto, o tratamento de dados que apenas revela o número de pessoas em uma multidão ou fornece informações agregadas sobre padrões de tráfego não gera as mesmas sensibilidades.", "940710": "", "940711": "Os direitos previstos na LGPD se aplicam a todos os dados pessoais, inclusive os biométricos. Recomenda-se que esses dados sejam tratados apenas quando necessários para identificar uma pessoa de forma única, o que facilita a aplicação dos direitos dos titulares, como acesso, correção, informação clara e revogação do consentimento. Cabe aos agentes de tratamento garantir mecanismos internos que viabilizem esses direitos de forma efetiva e transparente, respeitada sua autonomia na definição dos fluxos e procedimentos operacionais.", "940712": "", "940714": "Os dados dos mecanismos de garantia de idade devem ser cuidadosamente avaliados sob os princípios de necessidade e proporcionalidade. A proporcionalidade exige que as soluções biométricas sejam adaptadas ao nível de risco.

Contribuinte: Kaike Boni de Mathis Silveira

Número: OP-1006225

Data: 01/08/2025 - 15:43

Resumo: "BRASSCOM: A LGPD não fornece uma definição expressa do que se entende por "dado biométrico", limitando-se a incluí-lo como uma das espécies de dado pessoal sensível. Portanto, é necessária a conjugação dos critérios previstos na própria LGPD com referências internacionais consolidadas, especialmente o GDPR. É possível extrair três critérios objetivos que devem ser cumulativamente observados para que determinado dado possa ser considerado biométrico à luz da LGPD: 1.Referência a características físicas, fisiológicas ou comportamentais inerentes a uma pessoa natural (por exemplo: impressões digitais, traços faciais, voz, marcha); 2.Submissão a tratamento técnico específico, mediante uso de tecnologias que extraíam, codifiquem ou convertam essas características em medições ou templates; 3.Finalidade de identificação ou autenticação individual, ou seja, o uso do dado com o propósito de permitir ou confirmar quem é o titular. ", "940688": "BRASSCOM: Conforme a Autoridade de Dados do Reino Unido (ICO), não existe metodologia única aplicável a todos os casos sobre como a transparência pode ser garantida, incluindo medidas

ativas a serem adotadas pelos controladores. A forma mais eficiente de transparecer o uso de dados biométricos ao titular deverá ponderar fatores, como: i) o caso de uso; ii) a natureza de relacionamento com o titular; e iii) os dados envolvidos na atividade de tratamento. Nesse sentido, quanto mais óbvia a atividade de tratamento em análise, considerando as práticas habituais de mercado e a natureza do relacionamento com o titular, menor a exigência de práticas ativas de transparência. De qualquer forma, as boas práticas de transparência devem balizar todo e qualquer tratamento de dados, independentemente do dado ser caracterizado como dado pessoal sensível, como é o caso do dado biométrico.", "940690": "BRASSCOM: A biometria comportamental não deve ser automaticamente equiparada à biometria tradicional apenas por estar vinculada ao corpo humano. Dessa forma, enquanto a biometria tradicional se baseia em características físicas relativamente estáveis e imutáveis (como digitais, íris ou estrutura facial), a biometria comportamental envolve padrões que podem variar significativamente conforme o contexto. Por exemplo, a forma de caminhar de uma pessoa pode se modificar se ela sofrer uma lesão, passar por treinamento militar ou envelhecer. O mesmo se aplica a padrões de digitação, ritmo de voz ou movimento ocular. Tais variabilidades impactam diretamente a exatidão e confiabilidade desses dados, e devem ser levadas em conta na aplicação dos princípios da qualidade e da segurança.", "940693": "BRASSCOM: Para que o consentimento para o tratamento de dados biométricos seja considerado livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD, é fundamental que o titular tenha clareza sobre a finalidade do tratamento, compreenda suas implicações e possa manifestar sua vontade de forma autônoma, sem coerção ou engano. A exigência de que o consentimento seja livre não implica, necessariamente, a ausência de qualquer condicionamento. O que a LGPD veda é a coação, a ausência de transparência ou a imposição de desvantagens excessivas ao titular. A simples oferta de um serviço vinculada ao tratamento de dados pessoais — inclusive biométricos — não invalida, por si só, o consentimento, desde que: Haja transparência quanto à necessidade dos dados para a prestação do serviço; e O titular não seja compelido a consentir sob pena de sofrer desvantagens desproporcionais ou discriminatórias.", "940695": "BRASSCOM: A utilização de dados biométricos com a finalidade de prevenção à fraude deve ser analisada à luz da LGPD a partir de uma ponderação entre os direitos fundamentais à privacidade e à proteção de dados, de um lado, e o interesse coletivo na segurança, na estabilidade econômica e na prevenção de ilícitos, de outro. Trata-se de uma típica aplicação do princípio da proporcionalidade, que exige a verificação da adequação, necessidade e proporcionalidade em sentido estrito da medida. No contexto brasileiro, marcado por altos índices de fraudes bancárias, golpes digitais e uso indevido de identidades falsas, o tratamento de dados biométricos para fins de autenticação representa, muitas vezes, a medida mais segura, eficaz e menos invasiva disponível para proteger os usuários e o sistema financeiro como um todo - contexto que faz com que a base legal de prevenção à fraude seja extremamente relevante.", "940697": "BRASSCOM: No que tange o princípio da necessidade, observam-se medidas que visem à utilização dos dados biométricos apenas de forma estritamente necessária para o atingimento da finalidade, atentando-se para a disponibilização de informação aos titulares acerca da finalidade do tratamento, de forma clara, precisa e facilmente acessível. Em relação às salvaguardas a serem adotadas para mitigação de riscos,

entendemos que devem ser as mesmas aplicáveis aos agentes de tratamento que utilizam a base legal de “prevenção à fraude”. Isso porque as medidas de proteção de dados devem ser proporcionais aos riscos envolvidos, independentemente da base legal utilizada para justificar o tratamento. Assim, os controles e as salvaguardas adequados para mitigar os riscos decorrentes do uso de dados biométricos permanecem os mesmos, seja a base legal “prevenção à fraude”, “cumprimento de obrigação legal” ou outra prevista na LGPD.”, "940699": "BRASSCOM: Nesse sentido, é importante esclarecer que o dado anonimizado se caracteriza pelo dado que não é capaz de permitir a reidentificação posterior. Corrobora esse entendimento o conceito de dado anonimizado previsto no art. 5º, III da LGPD. Diante desse cenário, em caso de uso de dados anonimizados, medidas técnicas de anonimização, bem como a aplicação de testes de robustez para validar se o dado está efetivamente anonimizado, conforme recomenda a ANPD em Guia de Boas Práticas de Anonimização e Pseudoanonimização, podem ser consideradas como salvaguardas para garantir a eficácia do processo de anonimização do dado. Uma vez garantido o processo de anonimização, referido dado não é considerado como dado pessoal, em conformidade com o art. 12º da LGPD, tendo em vista que não é possível identificar o titular. Consequentemente, portanto, o dado deixa de figurar como dado pessoal.”, "940700": "BRASSCOM: Na ótica do princípio da transparência, é necessário garantir que o titular tenha ciência do tratamento de reconhecimento facial, disponibilizando informações acerca da finalidade deste reconhecimento. No aspecto técnico, medidas de mitigação de vieses e testes de acurácia utilizando uma base ampla e diversificada contribuem para evitar situações de discriminação ilícita ou abusiva. Na visão jurídica, entende-se como mitigador a correta identificação da base legal amparada pelo atingimento dos princípios acima observados. No que tange à visão institucional, as medidas de monitoramento, controle de acesso e rastreamento do tratamento dos dados, conforme já explicitado, visam contribuir com os riscos mapeados neste item. É importante reconhecer que, em determinados contextos, como a prevenção à fraude no sistema financeiro ou em serviços digitais, o uso de tecnologias de reconhecimento facial pode ser não apenas legítimo, mas essencial para proteger direitos de usuários.”, "940701": "BRASSCOM: Os sistemas de reconhecimento facial devem ser concebidos e implementados desde sua origem com base no princípio do privacy by design, adotando salvaguardas técnicas e organizacionais que garantam alta acurácia e minimizem riscos aos direitos dos titulares. Para garantir eficácia e confiabilidade, é essencial que esses sistemas sejam treinados com bases de dados amplas, diversificadas e representativas da população, a fim de reduzir vieses e minimizar erros de identificação, como falsos positivos (identificação incorreta) e falsos negativos (falha na identificação de quem deveria ser reconhecido). O tratamento de dados biométricos que não permitem a identificação de uma pessoa natural — ou seja, que não configuram dados pessoais nos termos da LGPD — é essencial para o treinamento e aprimoramento de sistemas de reconhecimento facial.”, "940702": "BRASSCOM: O reconhecimento facial não será mecanismo apropriado quando existirem meios adequados e proporcionais para se alcançar o mesmo resultado sem uso dessa tecnologia, especialmente se houver forma de tratamento menos intrusiva e capaz de atender à finalidade pretendida, inclusive outras formas de autenticação biométrica. Em outras palavras, o reconhecimento facial deve ser evitado sempre que métodos alternativos

possam garantir nível de identificação equivalente, ou minimamente suficiente diante dos riscos envolvidos. Por exemplo: solução alternativa para auxiliar na verificação da identidade do titular: Soluções de prevenção a fraudes baseadas em dados para verificar se o número de telefone e outras informações de contato coincidem com as informações apresentadas pelo titular no momento de registro junto à empresa, confirmar se a localização de uma transação corresponde à localização do dispositivo do titular e identificar indícios de práticas fraudulentas, como o SIM Swap." , "940704": "BRASSCOM: Diante do alto potencial lesivo decorrente de eventuais violações de dados biométricos, como o roubo de identidade, é indispensável a adoção de medidas técnicas e administrativas robustas para mitigar esses riscos. O setor de tecnologia tem atuado proativamente nesse sentido, incorporando mecanismos avançados de segurança da informação — como criptografia, segmentação de bases, anonimização, controle de acesso e rastreabilidade — desde as fases iniciais do desenvolvimento de produtos e sistemas. Além disso, muitas empresas já implementam práticas sofisticadas de privacy by design e by default, realizando o tratamento de dados biométricos de forma parametrizada, com o objetivo de identificar padrões ou calibrar sistemas, sem que haja identificação ou reidentificação de uma pessoa natural, o que reduz significativamente os riscos à privacidade. Para garantir a conformidade com a LGPD, é essencial que as organizações adotem parâmetros mínimos de avaliação contínua de riscos(...)" , "940707": "BRASSCOM: Para evitar que a exigência de autenticação biométrica em serviços não essenciais configure discriminação ilícita ou prática abusiva, é fundamental que o tratamento desses dados observe os princípios da LGPD bem como esteja devidamente enquadramento em uma das bases legais autorizativas para o tratamento, em especial, da necessidade, não discriminação e transparência, como todo e qualquer tratamento de dados deve observar. Na situação em que o tratamento do dado biométrico é amparado no consentimento, o titular deve ter garantido o direito ao opt-out, de forma simples, acessível e sem que isso implique em restrições desproporcionais do serviço. A limitação de funcionalidades pode ser considerada legítima, entretanto, quando houver justificativa técnica concreta para sua implementação. Nessa ocasião, tal limitação deve ser previamente comunicada de forma clara e transparente." , "940708": "BRASSCOM: A proteção eficaz no tratamento de dados biométricos exige adoção de boas práticas voltadas à transparência, necessidade e mitigação de riscos discriminatórios. Entre essas práticas, destacam-se: Treinamento e Capacitação: oferecer treinamento específico quanto ao tema; Políticas e Procedimentos: reforçar as informações de forma detalhada sobre como deve ser realizado o tratamento de dados para essa categoria de dados; Relatório de Impacto à Proteção de Dados Pessoais (DPIA), quando aplicável. Em relação às medidas de transparência, a obrigatoriedade legal se refere ao fornecimento das informações previstas no art. 9º, da LGPD. A forma adequada de disponibilização dessas informações, conforme indicado nos questionamentos nºs 2 e 8, com base no posicionamento do ICO, dependerá de uma série de fatores – como o caso de uso, a natureza do relacionamento com o titular e os elementos envolvidos na atividade de tratamento." , "940709": "", "940710": "BRASSCOM: Os agentes de tratamento, especialmente no setor de tecnologia, têm avançado significativamente na implementação de práticas que asseguram o respeito aos direitos dos titulares, inclusive em contextos complexos como o tratamento automatizado de dados biométricos. Empresas de

tecnologia vêm adotando medidas técnicas e organizacionais que facilitam o exercício dos direitos previstos na LGPD — como o direito à informação clara, ao acesso, à correção de dados e à revogação do consentimento — por meio de interfaces amigáveis, políticas de privacidade mais acessíveis e canais digitais eficientes de atendimento ao titular. Além disso, o setor tem investido em soluções inovadoras para promover maior transparência, como painéis de controle de dados, logs de acesso e funcionalidades que permitem ao titular visualizar, corrigir ou apagar dados de forma autônoma. ", "940711": "BRASSCOM: O princípio do melhor interesse, previsto no art. 14 da LGPD, deve ser interpretado de forma concreta, contextualizada e não apriorística. Essa abordagem está em consonância com o Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU, que destaca o caráter flexível, relacional e multidimensional do conceito, exigindo sua ponderação em conjunto com outros direitos fundamentais. Reconhece-se, ainda, a condição peculiar da criança e do adolescente como pessoas em desenvolvimento, conforme o Estatuto da Criança e do Adolescente (ECA). Nesse sentido, recomenda-se que a ANPD assegure margem de autonomia aos controladores para que possam demonstrar, caso a caso, como o tratamento atende ao melhor interesse, inclusive com a possibilidade de adotar ajustes e salvaguardas adicionais. A base legal para o tratamento de dados biométricos, ainda que envolva crianças e adolescentes como titulares dos dados, decorre do art. 11 da LGPD.

", "940712": "BRASSCOM: A hipótese de Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (Art. 11, II, “g”, LGPD”). Quando a hipótese legal é o consentimento, este deve ser inequívoco e contemplar as finalidades para a qual o representante do titular concorda com o tratamento. O tratamento dos dados biométricos de crianças e adolescentes também pode ser amparado em outras bases legais que não o consentimento, especialmente considerando as disposições do Enunciado nº 1/2023 da ANPD. Nesse cenário, é imprescindível que haja a devida transparência do tratamento e suas finalidades para os representantes do menor. Sobre as medidas técnicas e organizacionais, destacam-se as medidas de segurança relevantes para todo e qualquer tratamento de dados, independentemente do titular figurar como criança ou adolescentes, quais sejam: implementação de programas de Segurança da Informação, medidas de controle e gestão de acesso.", "940714": "BRASSCOM: Para compatibilizar a prática de verificação de idade com o princípio da necessidade, é essencial que a coleta de dados biométricos seja limitada ao mínimo necessário para atingir a finalidade pretendida, evitando excessos, tratamentos desproporcionais ou tratamentos a posteriori para outras finalidades. A biometria, por ser um dado sensível, deve ser utilizada apenas quando não houver outra forma menos invasiva de verificar a idade do usuário. Além disso, é fundamental garantir a transparência do processo, com informações claras e acessíveis aos pais ou responsáveis, incluindo a finalidade da coleta, os direitos dos titulares e os mecanismos disponíveis para exercer esses direitos. O tratamento de dados biométricos para casos de verificação ou estimação de idade de crianças e adolescentes deve priorizar a proteção do menor, evitar riscos à sua dignidade, liberdade e segurança, de forma a se garantir o melhor interesse do menor.

Contribuinte: GABRIELY DA CONCEICAO DOS SANTOS

Número: OP-1006230

Data: 01/08/2025 - 15:46

Resumo: "Para caracterizar dado biométrico nos termos da LGPD deve-se observar a origem biológica ou comportamental; o caráter unívoco de identificação e singularização da pessoa; ser tecnicamente mensurável, ou seja, a característica (física, fisiológica ou comportamental) captada por um sistema ou dispositivo e convertida em dados numéricos que permitam comparação, identificação ou autenticação; e tratado com a finalidade de identificar ou autenticar uma pessoa natural. Ademais, como critério adicional de acurácia, pode-se observar a estabilidade a longo prazo do dado biométrico, como a inalterabilidade da íris ou impressão digital. ", "940688": "Os controladores devem assegurar transparência ativa no tratamento de dados biométricos por meio da elaboração e ampla divulgação de aviso de privacidade com disposições específicas acerca de informações claras sobre a finalidade do tratamento, base legal, dados coletados, prazos de retenção e medidas de segurança. Ainda, o aviso deve ser acessível e estar disponível nos pontos de coleta, previamente ao tratamento, com sinalização visível e adequada ao contexto, além de conter canal eficaz para exercício dos direitos dos titulares previstos na LGPD. Quando a base legal for o consentimento, este deve ser obtido de forma livre, específica, informada e destacada, com explicitação clara da finalidade, base legal, tipo de dado biométrico tratado e medidas de segurança adotadas. A coleta do consentimento deve ser registrada de forma segura, permitindo sua verificação e auditoria, em conformidade com os princípios da transparência, necessidade e responsabilização. ", "940690": "A biometria comportamental apresenta maior variabilidade devido ao tempo, ambiente e condições individuais, o que pode afetar a precisão dos sistemas de identificação. Por isso, entendemos que os controladores precisarão ter atenção a verificação rigorosa de acurácia e taxa de erro, considerando contextos específicos para prevenir falsos positivos ou negativos, como variações naturais de voz por idade, doença ou interferências ambientais. Além disso, recomenda-se que a ANPD estabeleça diretrizes sobre medidas de segurança robustas, alinhadas a padrões internacionais como a ISO | IEC JTC 1/SC 37 (que é o subcomitê técnico permanente responsável pela padronização de tecnologias biométricas) e a ISO/IEC 24.745. Essas medidas devem incluir autenticação forte para acesso aos dados biométricos, avaliação de riscos, testes periódicos de robustez, registros auditáveis das operações de tratamento e eliminação segura dos dados biométricos ao final do ciclo de vida. ", "940693": "Para que o consentimento seja livre, o controlador deve oferecer alternativa viável ao uso da biometria, sem imposições, garantindo que a recusa não cause exclusão ou limitação dos direitos dos titulares. O consentimento deve ser específico (vinculado a finalidades determinadas e sem cláusulas genéricas); destacado (com apresentação visual separada e, no caso de opt-in, sem pré-seleção definida para o titular); informado (com linguagem clara sobre quem coleta os dados, finalidades, forma e tempo de tratamento, compartilhamento e direitos do titular) e inequívoco (com ação proativa do titular, nunca presumido), em observância ao art. 5º, XII da LGPD. Não se identifica que o consentimento, nos termos do art. 11, I da LGPD, seria a base mais adequada em contextos com assimetria de poder, como nas relações trabalhistas e, nos casos, em que o titular não tiver real

possibilidade de escolha, como no acesso condicionado a serviços ou ambientes.

","940695": "Para aplicação da hipótese legal de prevenção à fraude, devem ser observados critérios como a indispensabilidade do uso de biometria, inexistência de meios menos invasivos, proporcionalidade e respeito aos princípios da LGPD, em especial o da necessidade. É essencial garantir os direitos dos titulares, elaborar um RIPD e preencher Teste de Balanceamento, atualizar o ROPA e adotar medidas robustas de segurança, como criptografia, base segregada e controle de acesso. A compatibilização com o princípio da necessidade requer minimização de dados e tratamento contextualizado para o titular, bem como maior observância de medidas de segurança quando houver autenticações críticas e transações financeiras de alto valor por exemplo, vedando a reutilização dos dados para fins distintos, como marketing etc. Referente as salvaguardas, recomenda-se observar padrões técnicos internacionais, como a ISO |IEC JTC 1/SC 37 (Biometrics) e ISO/IEC 24745.", "940697": "Para aplicação da hipótese legal de cumprimento de obrigação legal ou regulatória, devem ser observados a priori a existência de norma clara e específica acerca do tratamento pretendido, com identificação objetiva da finalidade que justifique o tratamento do dado biométrico; observância dos princípios da LGPD, como finalidade, necessidade, transparência e segurança; avaliação da estrita necessidade, demonstrando que o dado biométrico é imprescindível, sem alternativas menos invasivas; elaboração de RIPD e adoção de medidas robustas. Como salvaguardas, recomenda-se a observância de padrões técnicos como a ISO |IEC JTC 1/SC 37 (Biometrics) e ISO/IEC 24745, que trata da proteção de templates biométricos, uso de criptografia, controle de acesso, auditoria e rastreabilidade. Ademais, entidades e órgãos públicos devem garantir a especificação legal ou regulatória e divulgação de aviso de privacidade institucional, com linguagem clara e acessível ao público, reforçando a transparência.", "940699": "Para aplicação da hipótese legal de realização de estudos por órgãos de pesquisa, deve-se verificar a priori se a entidade se enquadra como órgão de pesquisa, considerando registro formal e natureza técnico-científica. É essencial elaborar o RIPD e observar os princípios da LGPD, especialmente finalidade, transparência, necessidade e segurança. Quando possível, a anonimização deve garantir ausência de reidentificação do titular, inclusive com cruzamento de bases. Se não for possível, devem ser adotadas medidas como controle rigoroso de acesso, pseudonimização, segregação de bases, registro das operações, uso exclusivo para fins acadêmicos ou estatísticos, e descarte seguro. Recomenda-se revisão ética e técnica por comitês especializados. Como salvaguardas adicionais, recomenda-se avaliação de risco para estimar a probabilidade de reidentificação, técnicas avançadas de anonimização, termos de responsabilidade assinados por pesquisadores e políticas claras de descarte e retenção.", "940700": "É preciso verificar se o reconhecimento facial é essencial para o fim proposto e se não há alternativa menos invasiva. Também é necessário observar o princípio da minimização em linha com o princípio da finalidade e não discriminação, o que significa ao final aplicar o princípio da big data de exaustão. A transparência deve ser assegurada com avisos visuais nos pontos de captação e avisos de privacidade acessíveis, informando base legal, finalidade, tempo de retenção e direitos dos titulares. A acurácia do sistema deve ser validada para prevenir falsos positivos ou negativos, especialmente com grupos vulneráveis. Ademais, é indispensável capacitar profissionais para evitar abordagens abusivas. Como salvaguardas, recomenda-se o uso de Privacy by Design,

Avaliação de Impacto Algorítmico, correção de viés algorítmico, limitação do escopo de tratamento, elaboração de RIPD e avaliação contratual com fornecedores, com cláusulas sobre uso ético, segurança e responsabilização.", "940701": "Para que sistemas de reconhecimento facial sejam eficazes, confiáveis e em conformidade com a LGPD, devem seguir os princípios do privacy by design e default, com avaliação prévia e contínua de riscos e atenção a vieses algorítmicos. É importante garantir diversidade no time de desenvolvimento e avaliações rigorosas de desempenho, com testes periódicos e métricas baseadas em condições reais. Deve-se adotar medidas robustas de segurança, como autenticação multifator, técnicas anti-fraude, controle de acessos, registros de logs e auditoria. Além disso, a intervenção humana qualificada deve ser assegurada em decisões automatizadas assim como feedbacks críticos devem ser incorporados, com ajustes contínuos. Da mesma forma, é essencial elaborar o RIPD e a AIA, com análises técnicas e jurídicas sobre os riscos envolvidos, as medidas de mitigação e os controles implementados. Os sistemas devem permitir revisão de decisões automatizadas, conforme o art. 20 da LGPD.", "940702": "O uso de reconhecimento facial deve levar em consideração as liberdades civis e os princípios da LGPD, podendo ser utilizado para o desenvolvimento de smart cities e para fins de segurança pública. No contexto educacional, o uso de biometria para fins de controle de frequência deve assegurar a transparência para os titulares, por meio de aviso de privacidade e/ou instrumento contratual, sem prejuízo de que em alguns contextos no âmbito do poder público, o tratamento seja respaldado na execução de políticas públicas. Nesses cenários, em especial, os princípios da transparência, segurança e não discriminação devem ser considerados. ", "940704": "A proteção de dados biométricos exige medidas técnicas e administrativas robustas, conforme a LGPD e a ISO/IEC 24745. São indispensáveis: criptografia irreversível, segregação de bases, gestão de acessos, registros de logs passíveis de auditorias, além de testes de vulnerabilidades e avaliações de privacidade. Como boas-práticas, recomenda-se o armazenamento do template biométrico no dispositivo do titular ou criptografado com chave sob sua posse, além de limitar o prazo de armazenamento à finalidade. Administrativamente, destacam-se: cláusulas contratuais com fornecedores, RIPD e plano de resposta a incidentes.", "940707": "O uso da biometria deve ser justificado como tecnicamente indispensável e informado ao titular, incluindo as consequências da recusa. O consentimento, quando aplicável, deve ser livre, informado, destacado e inequívoco. E a decisão pela aplicação da biometria deve ser respaldada por RIPD. A demonstração da necessidade do dado biométrico deve observar os princípios do art. 6º da LGPD e envolver equipe multidisciplinar. O canal de atendimento (arts. 18 e 20) deve ser eficaz. Contratos com fornecedores devem prever cláusulas protetivas e responsabilização. A restrição de funcionalidades em caso de recusa só é válida se for proporcional, não discriminatória e legalmente fundamentada.", "940708": "Os controladores devem observar os princípios da LGPD, adotar medidas de segurança alinhadas à ISO/IEC 24745 e implementar governança robusta em privacidade, com normativos claros. É essencial realizar RIPD e AIA que identifiquem riscos de viés, incluindo testes de acurácia e balanceamento em diferentes públicos. Antes do uso, deve-se mapear falhas e prevenir discriminação. Auditorias periódicas, testes de viés e coleta de feedbacks fortalecem a responsabilidade. A coleta deve ser proporcional, com base legal válida, uso transparente, canal de atendimento eficaz e

consentimento livre e informado, quando necessário. A limitação de funcionalidades deve ser justificada e não discriminatória. Deve-se prever revisão contínua e evidência de conformidade com segurança e direitos dos titulares.", "940709": "Para assegurar a autodeterminação informativa no tratamento massivo de dados biométricos em espaços públicos, os controladores devem garantir a transparência ativa, com placas informativas visíveis, canais eficazes para exercício de direitos, dúvidas e denúncias. É essencial investir em conscientização da população por meios acessíveis e abrangentes. Devem ser realizadas avaliações de impacto (RIPD, AIA) e testes de balanceamento para prevenir discriminações. As medidas técnicas devem priorizar anonimização ou pseudonimização, sempre que possível, e aplicar protocolos robustos de segurança. O tratamento deve ter base legal clara, finalidade legítima e ser limitado no tempo e na forma. A governança deve incluir auditorias, controle social e revisão periódica, garantindo que o uso da biometria seja proporcional, responsável e conforme os princípios da LGPD.", "940710": "Os agentes devem disponibilizar Aviso de Privacidade com texto claro, acessível e em linguagem adequada às características dos titulares, incluindo recursos audiovisuais para ampliar a compreensão. A comunicação deve ser multicanal, alcançando diferentes públicos. Recomenda-se abordagem em camadas: informações resumidas e visuais (placas, vídeos) num primeiro nível, e detalhamento aprofundado em segundo. É fundamental garantir o exercício dos direitos, especialmente revisão de decisões automatizadas, oferecendo canais eficientes, como formulários padronizados para solicitações. Embora o art. 20 da LGPD não exija revisão humana obrigatória, a ANPD poderia destacar que em tratamentos biométricos com IA, o controlador deve adotar o seguinte fluxo de revisão: a) revisão por IA (1º Nível), b) revisão por humano (2º Nível) e c) revisão por Comitê de Ética (3º Nível), reforçando transparência e confiança no processo automatizado.", "940711": "No ambiente educacional, a instituição deve garantir transparência aos responsáveis por meio de informativos online ou físicos e interações com os pais, explicando o uso da biometria, os tipos de dados tratados, a finalidade e os meios para exercício dos direitos. Deve realizar avaliações de riscos para assegurar o melhor interesse do menor, conforme art. 14 da LGPD. O tratamento de dados biométricos estaria relacionado à hipótese legal de exercício regular de direito (inclusive em contratos), consentimento ou de prevenção à fraude e segurança do titular (art. 11, II, g), por exemplo, para o reconhecimento facial em catracas. O tratamento deve ser mínimo, seguro, transparente e possibilitar acesso e correção, sempre priorizando a proteção integral da criança ou adolescente.", "940712": "O tratamento biométrico deve levar em consideração se será realizado por entidade privada ou pública. No contexto da Administração Pública, o tratamento poderá ser respaldado na execução de políticas públicas, nos termos do art. 11, II, "b", podendo em alguns casos ser fundamentado na obrigação legal ou regulatória (art. 11, II, "a"). Outrossim, no contexto privado, o tratamento poderá ser respaldado no exercício regular de direitos, inclusive em contrato (art. 11, II, "d"), no consentimento dos responsáveis (art. 11, I c/c art. 14, §1º) ou na prevenção à fraude e segurança do titular (art. 11, II, "g"). Em todos os casos, as medidas técnicas e organizacionais devem ser adotadas para proteger os dados, de modo a garantir a segurança e evitar abusos ou acessos indevidos, devendo sempre ser respeitado o princípio do melhor interesse do menor. A instituição deve, ainda, oferecer canais oficiais para que os direitos dos titulares, previstos no art. 18 e 20 da LGPD, sejam

assegurados.", "940714": "No tratamento de dados biométricos para verificação de idade, deve-se observar o princípio da necessidade (art. 6º, III, LGPD), evitando coletar múltiplas modalidades, como reconhecimento facial e de voz simultaneamente. Os dados só podem ser usados para esse fim, proibindo perfilamento ou publicidade. Deve-se avaliar alternativas menos invasivas e oferecer meios alternativos de validação. O armazenamento da biometria do menor deve ser evitado, preferindo tecnologias de verificação em tempo real (que em alguns casos, como biometria neonatal, não é aplicável). Por serem dados sensíveis de titular vulnerável, é obrigatório realizar RIPD. As hipóteses legais válidas são o consentimento específico dos responsáveis (art. 14, §1º c/c art. 11, I) e prevenção à fraude e segurança do titular (art. 11, II, g). O princípio do melhor interesse do menor deve sempre ser respeitado.

Contribuinte: GABRIEL HERINGER ZIGONI OLIVEIRA

Número: OP-1006232

Data: 01/08/2025 - 15:48

Resumo: : "[SAÚDE DIGITAL BRASIL - SDB] Nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD), um dado é caracterizado como biométrico quando atende aos seguintes critérios objetivos: (i) origem física, comportamental ou fisiológica: o dado deve ser resultante de características biológicas do indivíduo (ex: impressões digitais, geometria da face ou mão, reconhecimento da voz, íris ou retina, dinâmica de digitação ou marcha); (ii) obtenção por meio de tratamento técnico específico: o dado biométrico decorre de um processo técnico ou tecnológico, como sensores, algoritmos ou softwares especializados, que capta e transforma essas características físicas/comportamentais em dados digitais tratáveis; (iii) finalidade de identificação: o dado biométrico deve ser usado para identificar ou autenticar uma pessoa natural de forma única ou singularizada; e (iv) potencial de individualização: ainda que a finalidade não seja declaradamente de identificação, se o dado tiver sua capacidade técnica real. ", "940688": "[SAÚDE DIGITAL BRASIL - SDB] Como medida de transparência no tratamento de dados biométricos, especialmente no setor da saúde, é possível exigir dos agentes de tratamento práticas já previstas na LGPD, sem criação de novas obrigações legais. Entre essas práticas, destaca-se a indicação clara e destacada das finalidades específicas do uso biométrico, como a identificação do paciente em exames, autenticação em prontuários eletrônicos e segurança no acesso a sistemas críticos. Também é recomendável explicitar, em políticas de privacidade, os tipos de biometria coletados e as tecnologias envolvidas, como sensores faciais, leitores de digitais e dispositivos de voz. Além disso, deve-se informar de forma transparente que os dados são compartilhados com o fornecedor da tecnologia utilizada. Todas essas informações devem ser apresentadas em linguagem simples, visual e acessível, garantindo que o titular compreenda de forma clara o tratamento de seus dados biométricos. ", "940690": "[SAÚDE DIGITAL BRASIL - SDB] Na saúde, a biometria tradicional é essencial para identificar pacientes, prevenir fraudes e proteger o sigilo médico. Também autentica o acesso a prontuários e registra atualizações de dados sensíveis. Já a biometria comportamental auxilia no monitoramento clínico, como em disfunções cognitivas e uso de ECGs vestíveis para detectar fibrilação atrial. Contudo, exige

cautela por envolver inferências sobre emoções e saúde, com riscos discriminatórios. O Parlamento Europeu diferencia “biometric categorisation” e “biometric detection”, destacando sua sensibilidade. O aumento de dados exige mais governança e precisão. Apesar disso, a LGPD trata qualquer dado biométrico como sensível, sem distinguir tecnologias. Assim, a ANPD não pode criar categorias distintas ou impor obrigações extras à biometria comportamental, sob pena de violar os princípios da legalidade e reserva legal. Por isso, não propomos novas obrigações além das já previstas em lei.”, "940693": "[SAÚDE DIGITAL BRASIL - SDB] No contexto da saúde, há um evidente desequilíbrio entre o agente de tratamento e o paciente, o que pode comprometer a liberdade do consentimento. Por isso, entendemos que, sempre que possível, deve-se considerar o uso de outra base legal mais adequada ao tratamento de dados biométricos, como a prevenção à fraude e a tutela da saúde. Na prática, o consentimento nem sempre é a base legal mais apropriada, já que o paciente pode se sentir compelido a aceitar o tratamento de seus dados como condição para acessar serviços essenciais, o que compromete sua validade jurídica. Diante disso, é recomendável que os agentes de tratamento avaliem outras bases legais previstas nos incisos II (f) e (g) do artigo 11 da LGPD, como a tutela da saúde — quando o tratamento for indispensável à prestação de serviços médicos, hospitalares ou laboratoriais — e a prevenção à fraude e garantia da segurança do titular. Essas bases são mais adequadas ao contexto da saúde.”, "940695": "[SAÚDE DIGITAL BRASIL - SDB] A base legal de prevenção à fraude (art. 11, II, “g”, da LGPD) exige: (i) finalidade concreta; (ii) uso proporcional e sem alternativas menos intrusivas; e (iii) transparência ao titular. Na saúde, a biometria é compatível com a necessidade, dada a urgência, rotatividade e vulnerabilidades dos métodos tradicionais, como senhas e cartões. A biometria garante acesso seguro, rastreabilidade e reduz riscos de violação. O tratamento deve incluir salvaguardas técnicas e administrativas, como o RIPD, quando houver riscos aos direitos dos titulares. Também se aplica o princípio da segurança, com controles e políticas adequadas. Essas medidas, já previstas na LGPD, são suficientes para mitigar riscos, sem necessidade de novas obrigações regulatórias.”, "940697": "[SAÚDE DIGITAL BRASIL - SDB] O tratamento de dados pessoais biométricos deve observar a indicação de bases legais claras e específicas, com uma finalidade clara quanto à obrigatoriedade do uso de dados. O uso de dados biométricos com base em obrigação legal ou regulatória deve ser excepcional, transparente e tecnicamente justificado, com salvaguardas robustas para proteger os direitos fundamentais dos titulares em medidas de mitigação. As entidades e órgãos públicos devem implementar medidas ainda mais robustas, considerando que, em muitos casos, os titulares de dados compartilham suas informações pessoais para o acesso a serviços públicos, como o direito à saúde. A LGPD permite o tratamento de dados sensíveis sem consentimento quando necessário para o cumprimento de obrigação legal ou regulatória pelo controlador. No entanto, essa hipótese não é uma autorização irrestrita: ela deve ser interpretada à luz dos princípios da LGPD.”, "940699": "[SAÚDE DIGITAL BRASIL - SDB] O tratamento de dados biométricos em pesquisas exige atenção redobrada, dado seu caráter sensível e risco elevado de reidentificação. Segundo o ICO, seu uso só é admissível se necessário, proporcional e o meio mais adequado ao objetivo científico. A anonimização enfrenta desafios técnicos, sendo recomendada sua combinação com técnicas como differential privacy, criptografia

homomórfica, segregação de dados e controle de reuso. É essencial a revisão ética, cláusulas de exclusão e proteção a grupos vulneráveis. Os dados devem ser usados exclusivamente para fins científicos, vedada sua aplicação prática sem nova base legal. A LGPD exige salvaguardas técnicas e administrativas, como o RIPD e políticas de segurança, que são suficientes para mitigar riscos, conforme reforçado pela Resolução CNS nº 674/2022.

","940700": "[SAÚDE DIGITAL BRASIL - SDB] O tratamento de dados biométricos deve ser submetido a critérios rigorosos de conformidade com os princípios da proteção de dados pessoais e com os direitos fundamentais, especialmente no que se refere à não discriminação, transparência e proporcionalidade. É essencial garantir que o uso da tecnologia não resulte em discriminação direta ou indireta, especialmente contra grupos vulneráveis, com atenção especial ao treinamento dos algoritmos e à composição das bases de dados utilizadas. Recomenda-se ainda a elaboração de um Relatório de Impacto antes de qualquer implementação, com a submissão dos sistemas à auditorias e alternativas ao reconhecimento facial. A justificativa se baseia em três pilares fundamentais: a natureza sensível da tecnologia de reconhecimento facial, os princípios da LGPD e as evidências empíricas de riscos discriminatórios associados a essa tecnologia. Sendo assim, é essencial que a ANPD estabeleça critérios técnicos e salvaguardas.

","940701": "[SAÚDE DIGITAL BRASIL - SDB] Recomendamos para garantir a eficácia, confiabilidade e justiça no uso de tecnologias de reconhecimento facial, é essencial que esses sistemas sejam desenvolvidos com base no princípio de “privacidade desde a concepção” (privacy by design) e com foco em precisão técnica, mitigação de vieses e mecanismos de correção contínua. Para tanto, recomendamos que testes sejam realizados em base diversificada, para a redução de vieses, constante calibração e validação externa de suas medidas. A revisão humana e um canal específico para o tratamento de requerimentos são essenciais na correção de erros com o uso da tecnologia. A justificativa está fundamentada em três eixos principais: os princípios da LGPD, as características técnicas dos sistemas de reconhecimento facial e as evidências empíricas sobre falhas e riscos associados a essas tecnologias.

","940702": "[SAÚDE DIGITAL BRASIL - SDB] O uso de reconhecimento facial deve ser restrito a contextos de alto risco e com justificativa técnica robusta, sempre acompanhado de salvaguardas jurídicas e institucionais. Em muitos casos, tecnologias alternativas podem oferecer segurança equivalente com menor impacto à privacidade e aos direitos fundamentais. Recomendamos a adoção de tecnologias de menor impacto, tais como a Autenticação Multifator (MFA), cartões de identificação (Chip/QR Code), e a biometria comportamental. A justificativa está fundamentada nos princípios da LGPD, as evidências empíricas sobre riscos do reconhecimento facial, e a viabilidade de alternativas tecnológicas menos invasivas. Portanto, a recomendação de evitar o uso de reconhecimento facial em determinados contextos também se justifica pela alta sensibilidade da tecnologia, pelos riscos de danos irreversíveis aos titulares de dados pessoais e pela disponibilidade de soluções menos invasivas e proporcionais.

","940704": "[SAÚDE DIGITAL BRASIL - SDB] A adoção de criptografia, segregação de bases, controle de acesso, logs e testes regulares são indispensáveis. Recomendamos práticas alinhadas às ISOs 27001 e 27701, com RIPD, revisão periódica de riscos e plano de resposta a incidentes para garantir proteção e conformidade com a legislação vigente e as regulamentações de proteção de dados. A LGPD (art. 46 a 49) impõe

aos agentes de tratamento o dever de adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais, especialmente os sensíveis, como os biométricos. A violação desses dados pode gerar danos irreparáveis. Diferentemente de senhas ou tokens, dados biométricos não podem ser alterados após um vazamento. Por isso, a proteção deve ser preventiva, contínua e proporcional ao risco.", "940707": "[SAÚDE DIGITAL BRASIL - SDB] A biometria só deve ser exigida quando tecnicamente indispensável à funcionalidade, desde que não viole direitos fundamentais do titular e, como boa prática, oferecer alternativa viável. A recusa do titular só pode restringir funcionalidades adicionais se houver justificativa informada previamente. A LGPD (art. 6º, IV e IX) estabelece os princípios da não discriminação e da transparência, que devem ser observados mesmo quando o tratamento se baseia no consentimento. O uso de biometria em serviços não essenciais não pode ser uma forma de coerção indireta, nem pode excluir ou limitar desproporcionalmente o acesso de determinados grupos.", "940708": "[SAÚDE DIGITAL BRASIL - SDB] Limitar a coleta à finalidade, usar anonimização sempre que possível, revisar algoritmos quanto a vieses e garantir supervisão humana. Transparência exige informar claramente as finalidades, bases legais e direitos, com canais acessíveis para o titular. É altamente recomendado que haja a indicação de maneira pública do responsável pela atuação como Encarregado pelo tratamento de dados pessoais na organização, de maneira preferencial em seu sítio eletrônico. A LGPD impõe aos controladores o dever de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais (art. 46), com especial atenção aos dados sensíveis, como os biométricos (art. 11). Além disso, os princípios da transparência, não discriminação, prevenção e responsabilização (art. 6º) exigem uma abordagem proativa e ética.", "940709": "[SAÚDE DIGITAL BRASIL - SDB] Para assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos, os controladores devem adotar um conjunto de medidas concretas, proporcionais e transparentes, mesmo em ambientes de difícil controle individual.. Garantir sinalização clara nos locais, informar previamente o tratamento, adotar tecnologias menos intrusivas, criar canais acessíveis para exercício de direitos. O tratamento deve ser justificado, auditável e reversível. A autodeterminação informativa é um direito fundamental implícito na LGPD, que garante ao titular o controle sobre seus dados pessoais, mesmo em contextos de tratamento automatizado e em larga escala. O art. 6º da LGPD estabelece os princípios da transparência, necessidade, não discriminação e responsabilização, que devem ser observados com ainda mais rigor em ambientes de vigilância biométrica pública.", "940710": "[SAÚDE DIGITAL BRASIL - SDB] Recomenda-se a adoção de medidas técnicas, organizacionais e comunicacionais que assegurem a efetividade, acessibilidade e transparência desses direitos. Garantir linguagem clara em todas as etapas, canais acessíveis para consulta sobre seus direitos. Deve-se prever supervisão humana, logs auditáveis e resposta com linguagem acessível às solicitações. A LGPD assegura aos titulares uma série de direitos (arts. 9º, 18 e 20), que devem ser respeitados mesmo em contextos de tratamento automatizado e de difícil transparência, como ocorre com dados biométricos. A adoção de mecanismos acessíveis, auditáveis e transparentes é essencial para garantir que a autodeterminação informativa seja efetiva e não apenas formal.", "940711": "[SAÚDE DIGITAL BRASIL - SDB] Compreendemos que a adoção de critérios rigorosos de legalidade, necessidade,

proporcionalidade e proteção integral, conforme o art. 14 da LGPD e o princípio do melhor interesse da criança. Os pais ou responsáveis legais devem ser informados sobre o tratamento realizado, seja por meio de cartazes, contrato celebrado com a escola, aviso de privacidade no site, sempre em benefício do menor. O art. 14 da LGPD estabelece que o tratamento de dados pessoais de crianças deve ser realizado com consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal, e sempre com base no melhor interesse da criança.", "940712": "[SAÚDE DIGITAL BRASIL - SDB] Seria admissível em alguma das hipóteses previstas no art. 11 da LGPD. Recomendamos garantir a participação informada dos responsáveis mediante um canal de comunicação de fácil acesso e com linguagem acessível, bem como a própria divulgação de informações de maneira física em locais e pontos de coleta de dados pessoais, sobretudo para dados pessoais sensíveis como os biométricos. A LGPD (art. 14) estabelece que o tratamento de dados pessoais de crianças deve ser realizado com consentimento específico e em destaque de pelo menos um dos pais ou responsável legal, e sempre com base no melhor interesse da criança.", "940714": "[SAÚDE DIGITAL BRASIL - SDB] A verificação ou estimação de idade por meio de dados biométricos deve ser considerada uma prática de alto risco, especialmente quando envolve crianças e adolescentes. A verificação biométrica demanda proporcionalidade e deve ser usada apenas se não houver método menos intrusivo. Exigir minimização, transparência, retenção limitada, anonimização e supervisão humana, sempre priorizando o melhor interesse e a segurança da criança. A LGPD (art. 14) estabelece que o tratamento de dados de crianças deve ser realizado com consentimento dos pais ou responsáveis e sempre com base no melhor interesse da criança. A coleta de dados biométricos para verificação de idade, embora possa ter finalidades legítimas, como a proteção contra conteúdos impróprios, pode envolver riscos significativos para os titulares de dados pessoais, sobretudo para crianças e adolescentes.

Contribuinte: Teresa de Souza Dias Gutierrez

Número: OP-1006256

Data: 01/08/2025 - 16:28

Resumo: :", "940688": "Mesmo quando o tratamento de dados biométricos não se baseia no consentimento, os controladores devem adotar práticas de transparência ativa, com informações claras, acessíveis e antecipadas. Isso inclui o uso de linguagem simples, recursos visuais adequados e comunicação prévia sobre os riscos, permitindo que os titulares compreendam o tratamento e exerçam seus direitos, inclusive se opondo a usos indevidos ou ilegais. Deve-se informar qual tecnologia está sendo utilizada, a finalidade do tratamento e o ciclo de vida dos dados. Devem ser evitados documentos genéricos e longos, priorizando resumos objetivos, avisos em camadas ou “just in time”. Recomenda-se ainda oferecer versões acessíveis dos RIPDs, voltadas ao público leigo. O Registro de Operações de Tratamento deve estar sempre atualizado. Por fim, o encarregado pelo tratamento de dados deve garantir canais de atendimento eficientes e inclusivos. Detalhes no documento expandido. ", "940690": "", "940693": "O consentimento só é válido quando livre, ou seja, não

pode estar condicionado a penalidades ou restrições. Isso pode ser verificado analisando as consequências de uma eventual recusa: se a negativa resultar na impossibilidade de acessar um serviço essencial (em sentido estrito ou ampliado), há um indicativo de que o consentimento não foi verdadeiramente livre, mas sim condicionado. Isso indica que o tratamento deve se basear em outra hipótese legal mais adequada. Caso o consentimento seja escolhido como a base legal adequada, a coleta dos dados biométricos só pode ocorrer após a obtenção de um consentimento válido. Por fim, o consentimento não é considerado livre quando condicionado a incentivos financeiros que afetam a capacidade do titular de avaliar criticamente os riscos. A preocupação central não é o pagamento em si, mas seu impacto na decisão do titular, reforçando a fragilidade do consentimento, muitas vezes dado sem real compreensão. ", "940695": "O uso de tal base legal para tratar dados biométricos exige cautela, pois, embora legítima, não deve ser aplicada de forma automática sob o pretexto genérico de segurança. Sem critérios claros, corre-se o risco de abusos, como o uso indiscriminado de reconhecimento facial. O Guia de Legítimo Interesse equipara sua aplicação à lógica do legítimo interesse, mas a operacionalização dessa equivalência é incerta. A dúvida sobre como aplicar o teste de balanceamento quando a segurança do próprio titular é o objetivo revela uma lacuna conceitual. Nesses casos, não há um interesse "externo" a ser ponderado, o que pode enfraquecer a análise crítica. O uso da base de prevenção à fraude com dados biométricos deve seguir exigências rigorosas: demonstração da necessidade, análise de proporcionalidade, avaliação de alternativas menos invasivas e salvaguardas robustas. Isso não impede seu uso, mas evita a banalização de práticas invasivas. Mais detalhes no documento expandido. ", "940697": "Nos casos de obrigação legal ou regulatória, o tratamento de dados biométricos deve atender aos critérios de necessidade, proporcionalidade e finalidade específica. Normas genéricas, como diretrizes de modernização tecnológica, não são suficientes: é preciso justificar tecnicamente e com evidências que o uso da biometria é indispensável - inclusive frente a opções menos invasivas - para cumprir a obrigação. Órgãos públicos devem basear suas decisões em análises técnicas e claras, com detalhamento dos objetivos e da adequação da tecnologia ao fim proposto. O simples fato de existir uma meta ampla de uso de tecnologias, como no Plano Nacional de Educação, não autoriza o uso automático de biometria, especialmente em ambientes escolares. O salto entre a diretriz genérica e a medida concreta precisa ser tecnicamente justificado e registrado em documentos como o RIPD. Detalhes no documento expandido. ", "940699": "", "940700": "Para garantir que o uso de TRFs observe os princípios da LGPD e evite resultados discriminatórios, é essencial impor um ônus regulatório mais elevado, dado o caráter invasivo e sensível da biometria. A adoção dessas tecnologias deve estar ancorada em finalidade legal, específica e clara, com demonstração técnica de que a TRF é a alternativa mais adequada e menos intrusiva. Finalidades genéricas como "segurança" ou "eficiência" não bastam. É preciso restringir o uso à finalidade declarada, vedando reuso indevido. Transparência deve ser garantida com informações claras, RIPDs em linguagem acessível e ROPA atualizado. A definição de responsáveis pelo tratamento deve ser pública, especialmente em arranjos com múltiplos atores. Devem-se prever auditorias regulares, avaliação de riscos discriminatórios e canais acessíveis e ágeis de comunicação com o encarregado. A LAI deve ser aplicada, e justificativas genéricas de sigilo empresarial não devem limitar o acesso à informação.

", "940701": "", "940702": " É importante avaliar a aplicação de tecnologias de reconhecimento facial com base na proporcionalidade. Em contextos sensíveis, como ambientes escolares, usos preditivos ou monetização de dados biométricos, os riscos envolvidos podem, em certas situações, superar os possíveis benefícios, apontando para a necessidade de cautela e eventuais restrições. No contexto educacional, por exemplo, TRFs são comumente justificadas para finalidades administrativas ou pedagógicas, mas, na prática, podem se converter em tecnologias de vigilância. Quando associadas a sistemas preditivos, levantam preocupações quanto à transparência, acurácia e possíveis efeitos discriminatórios. Já no campo da segurança pública, a aplicação dessas tecnologias exige atenção redobrada, especialmente diante de dúvidas sobre eficácia, riscos de generalização e potenciais impactos sobre direitos fundamentais. A proteção de dados pode desempenhar papel relevante nesse debate. Detalhes no documento expandido. ", "940704": "", "940707": "A biometria em serviços não essenciais deve atender à LGPD, sobretudo a minimização e a proporcionalidade. Só é válida se tecnicamente indispensável, com justificativa concreta e a ausência de alternativas viáveis. Tais titulares de dados devem receber informações claras sobre o uso, segurança e descarte dos dados. Principalmente pela não essencialidade do uso, o consentimento deve ser livre e informado, sem implicar restrição injusta do serviço. Nesse sentido, o recomendado é que haja meios alternativos de autenticação. A manutenção de ROPAs atualizados é importante, porque o uso da biometria exige revisão periódica para averiguação de proporcionalidade e práticas não discriminatórias. ", "940708": "", "940709": "", "940710": "O tratamento de dados pessoais sensíveis de crianças e a deve seguir critérios rigorosos de legalidade, transparência e proporcionalidade, com finalidades específicas e compatíveis com seu melhor interesse. A coleta de dados biométricos só deve ocorrer se não houver meios menos invasivos, sendo os dados limitados ao necessário, protegidos em todo o ciclo de vida. O consentimento, quando base legal, deve ser livre, informado e não condicionado à perda de direitos/benefícios. Devem ser garantidas informações acessíveis, adequadas à faixa etária, e canais eficazes para que titulares, pais ou responsáveis acessem e corrijam os dados. Dados biométricos de crianças e adolescentes não podem ser usados para fins comerciais. A LAI também se aplica ao setor público, exigindo transparência, inclusive em parcerias com entes privados, sem uso genérico de sigilo empresarial. ", "940711": "O princípio do melhor interesse da criança deve orientar o tratamento de dados biométricos de crianças e adolescentes, que só deve ocorrer se comprovadamente necessário, com finalidade legítima, segurança robusta e medidas para evitar vieses. Em contextos escolares e recreativos, esse uso tende a ser desproporcional, com riscos de erro, discriminação e impactos duradouros. Se adotado, deve contar com salvaguardas como RIPDs, protocolos de segurança, minimização de dados e auditorias, com transparência pública. Além do consentimento, outras bases legais são possíveis, desde que com análise rigorosa de riscos. Gestores públicos devem apresentar relatórios auditáveis e garantir canais acessíveis para que titulares ou responsáveis possam exercer seus direitos. A base de prevenção à fraude (art. 11, II, “g”) exige justificativa concreta, proporcionalidade e garantias adicionais. O uso comercial de dados biométricos de crianças é vedado. ", "940712": "", "940714": "

Contribuinte: ISABELLA PEREIRA DE MOURA LIMA

Número: OP-1006297

Data: 01/08/2025 - 17:29

Resumo: "O conceito de dado biométrico deve considerar elementos que, cumulativamente, (i) estejam ligados a características físicas, fisiológicas ou comportamentais do titular e (ii) sejam tecnicamente tratados com a finalidade de identificá-lo de forma única. Fotografias, vídeos ou voz não são, por si, dados biométricos. Apenas se tornam quando processados com esse propósito. Reguladores como EDPB, INAI e PIPC distinguem dados biométricos de informações biológicas gerais, estas usadas apenas para inferir características pessoais (como idade ou emoções). A regulamentação brasileira deve seguir abordagem técnica e funcional, distinguindo usos voltados à autenticação e identificação de aplicações experimentais ou científicas, especialmente quando envolvem dados sintéticos ou modelos pré-treinados. Essa distinção evita insegurança jurídica e favorece a inovação tecnológica responsável.", "940688": "A transparência no tratamento de dados biométricos deve ser proporcional ao contexto do uso, como reconhece a ICO. Quando o uso é previsível e há relação com o titular (como desbloqueio de celular ou autenticação em serviços bancários), bastam práticas simples, como avisos na interface ou QR Codes. Já em casos inesperados, como videomonitoramento em via pública, são necessárias medidas ativas e visíveis. A regulamentação deve permitir flexibilidade para que controladores adaptem suas práticas conforme o setor. No caso de fabricantes de dispositivos móveis, como a Samsung, a biometria é processada localmente, sem envio de dados, com alertas exibidos ao usuário durante a ativação dos sensores. A experiência da indústria demonstra como aplicar o Privacy by Design de forma eficaz, aliando segurança e transparência. Uma abordagem setorial garante maior efetividade e incentiva boas práticas.", "940690": "A legislação vigente não distingue entre tipos de biometria, razão pela qual a regulamentação não pode criar obrigações distintas sem respaldo legal, sob pena de violar o princípio da legalidade. Autoridades como INAI e ICO diferenciam biometria física e comportamental, mas sem impor obrigações específicas a cada tipo. A regulamentação deve considerar as particularidades técnicas da biometria comportamental, em especial em contextos científicos. Dados de tremores, equilíbrio ou expressões faciais usados para fins de pesquisa, sob controle ético, não devem ser submetidos às mesmas exigências aplicáveis à autenticação biométrica em larga escala. Adotar exigências proporcionais ao risco e contexto estimula a pesquisa responsável e desenvolvimento de soluções com relevância social, sem comprometer a proteção aos titulares.", "940693": "O consentimento válido deve ser livre, informado, específico, destacado e inequívoco. Deve haver opção real de recusa sem prejuízo, salvo quando o tratamento for necessário para evitar riscos ao titular. O titular deve receber informações claras, em camadas ou por meio de TCLE aprovado por comitês de ética, no caso de pesquisas. O consentimento não pode ser presumido, deve ser individualizado por finalidade e destacado quando envolver dados sensíveis. Não é base adequada quando não for possível satisfazer esses requisitos, como em casos de prevenção à fraude ou monitoramento público, em que não há alternativa viável nem relação direta com o titular. A regulamentação deve reconhecer tais limitações e permitir o uso de outras bases legais, como prevenção à

fraude, conforme o art. 11, II, “g” da LGPD.”, "940695": "A base legal de “prevenção à fraude” (art. 11, II, “g”, LGPD) admite o tratamento de dados biométricos quando este for proporcional à finalidade e adequado ao risco. O Teste de Balanceamento pode auxiliar na avaliação, mas não é exigência legal. A biometria é viável, por exemplo, para autenticação em serviços bancários, considerando o bem jurídico envolvido (vida financeira do titular). O princípio da necessidade exige tratamento direcionado e proporcional, conforme entendimento do ICO. Deve-se permitir modelos biométricos embarcados e sem armazenamento em dispositivos móveis, por reduzirem riscos. Salvaguardas incluem: criptografia, segregação de dados, controle de acesso, registros de logs, due diligence de fornecedores e políticas de segurança. Recomenda-se ainda observar normas como a ISO/IEC 24745:2022 para proteção de dados biométricos.”, "940697": "A base legal de “obrigação legal ou regulatória” exige salvaguardas proporcionais aos riscos, independentemente da hipótese jurídica adotada. Assim, devem ser aplicadas medidas equivalentes às previstas para a “prevenção à fraude”, conforme já explicado. O tratamento pode se fundamentar tanto em obrigações legais expressas quanto em situações nas quais a biometria é meio legítimo para o cumprimento de normas, como a verificação de identidade prevista na Circular BCB nº 3.978/2020. São legítimos, por exemplo, usos embarcados de biometria para autenticação local em dispositivos, como carteiras digitais e acessos protegidos por senha, sem transferência para servidores centrais. Também são admissíveis projetos de P&D em saúde baseados em normas da Anvisa ou do CNS, com controles de finalidade, anonimização e acesso restrito. Negar tal enquadramento comprometeria a coerência normativa e geraria insegurança jurídica aos agentes privados.”, "940699": "A anonimização não é obrigatória para a base legal do art. 11, II, “c”, da LGPD, mas, se adotada, deve considerar o risco de reidentificação. Dados biométricos dificilmente são anonimizáveis de forma irreversível, podendo revelar informações sensíveis. Por isso, a ANPD deve incentivar salvaguardas proporcionais ao risco, como irreversibilidade dos templates e não vinculabilidade entre bases. Pesquisas com sinais sensoriais anonimizados e sem metadados identificáveis, como padrões de digitação ou marcha, aprovadas por Comitês de Ética e com TCLE demonstram boas práticas. A regulamentação deve reconhecer o uso seguro desses dados para inovação, mesmo fora do escopo clínico tradicional. Técnicas como a conversão de áudio para espectros ou uso de vídeo sem semântica reduzem o risco de reversão. Garantir segurança jurídica para pesquisas com dados biométricos anonimizados é essencial para promover avanços em áreas de interesse público.”, "940700": "A transparência no uso de reconhecimento facial deve ser contextual: em espaços públicos, exige sinalização visível e acessível; em serviços já consolidados, o aviso de privacidade na jornada do usuário pode ser suficiente. O princípio da necessidade demanda avaliação da proporcionalidade da biometria frente à finalidade, privilegiando templates em vez de amostras e coleta mínima. O uso deve ser evitado se houver meios menos invasivos com eficácia equivalente. Para mitigar discriminações, o ICO recomenda: bases de treinamento diversas, testes de vieses, verificação de critérios discriminatórios, aferição da acurácia e mecanismos de contestação. No caso de detecção facial local e em tempo real, sem armazenamento ou identificação, o uso de bibliotecas embarcadas pode ser legítimo e alinhado ao privacy by design. Reconhecer essa distinção é crucial para garantir segurança jurídica sem inibir a inovação em segurança

embarcada.", "940701": "O desempenho de sistemas de reconhecimento facial deve ser compatível com os riscos de sua aplicação. Soluções usadas em segurança pública, por exemplo, exigem mais robustez do que aquelas voltadas à autenticação predial. Com base no ICO, recomenda-se: (i) definir previamente níveis mínimos de acurácia; (ii) usar dados representativos e rotulados corretamente; (iii) realizar testes por subgrupos populacionais e ajustar o sistema em caso de falhas; e (iv) manter rotinas de monitoramento, mecanismos de contestação e cópias de versões anteriores, especialmente em IA de aprendizado contínuo.

Em contextos experimentais, devem ser valorizadas práticas seguras, como o uso de dados sintéticos ou embarcados, que permitam validar mecanismos antifraude com baixo risco aos titulares. Tais medidas favorecem o princípio do privacy by design e fomentam a inovação responsável sem comprometer a proteção de dados.", "940702": "O reconhecimento facial não é recomendado quando houver alternativas menos invasivas com eficácia equivalente.

Exemplos incluem: (i) controle de frequência em escolas; (ii) vigilância em massa sem justificativa proporcional; (iii) triagem em processos seletivos, devido a riscos de viés algorítmico; e (iv) identificação de manifestantes, que pode comprometer direitos fundamentais. Alternativas eficazes incluem senhas, tokens, autenticação multifator e dados de telecomunicação, como alertado pela Anatel no combate a fraudes com SIM Swap. Além disso, a regulamentação deve preservar o uso experimental em ambientes controlados, como laboratórios, desde que sem coleta persistente ou identificação. Reconhecer usos de baixo risco e fomentar soluções alternativas é essencial para mitigar riscos, evitar discriminações e incentivar inovação responsável, criando caminhos seguros para a substituição da biometria facial em contextos sensíveis.", "940704": "A proteção de dados biométricos exige medidas técnicas e administrativas robustas, como: controle de acesso, criptografia, testes de penetração, varredura de vulnerabilidades, logging de acessos, segregação dos dados e due diligence de fornecedores. A análise de riscos deve seguir parâmetros como os da ISO 27005:2023 e considerar ataques específicos, como deepfakes e fraudes por apresentação.

Mesmo com boas práticas, fraudes externas — como impressões digitais falsas ou manipulação facial — nem sempre são integralmente evitáveis. Por isso, deve-se aplicar o art. 43, III, da LGPD, que afasta a responsabilidade do controlador se demonstrado que não deu causa direta ao dano e adotou todas as medidas razoáveis de prevenção. A regulamentação deve exigir avaliação contínua de riscos e monitoramento, mas reconhecer limites técnicos e assegurar uma lógica de responsabilização baseada na diligência e na

proporcionalidade.", "940707": "Para evitar discriminação no uso de biometria, é fundamental considerar limitações técnicas e barreiras de acessibilidade, como no caso de pessoas com deficiência visual. Nesses casos, recomenda-se adotar métodos alternativos de autenticação. Quando o tratamento se baseia no consentimento, a recusa do titular pode justificar, de forma proporcional e transparente, a limitação de funcionalidades que dependam tecnicamente da biometria, como acesso por reconhecimento facial. A negativa, contudo, não pode restringir o uso de funcionalidades que não exijam esse tratamento. Em outras hipóteses, a recusa à biometria equivale ao exercício do direito de oposição. A restrição será legítima se (i) a funcionalidade for inviável sem a biometria, ou (ii) houver justificativa legítima para o uso do dado que prevaleça sobre a oposição do titular. O reconhecimento dessas condições é essencial para garantir segurança jurídica e o uso legítimo de soluções seguras e

eficientes.", "940708": "Boas práticas de proteção incluem os controles indicados nos quesitos 2, 5, 8 e 11, com base em orientações do ICO, INAI e PIPC: criptografia, testes de segurança, segregação de dados, due diligence e monitoramento contínuo. A transparência exige o fornecimento das informações do art. 9º da LGPD, cuja forma de apresentação dependerá do contexto da operação. Em soluções claras e padronizadas, são dispensáveis mecanismos ativos. Quanto à prevenção de discriminação, é essencial atentar aos riscos de perfilamento e segmentação. Projetos experimentais com dados biométricos — como rastreamento ocular ou análise de marcha — não devem ser equiparados, em exigências, ao uso comercial. A regulamentação deve permitir estratégias de privacy by design ajustadas ao papel do agente de tratamento, diferenciando obrigações de fabricantes de hardware e plataformas. A abordagem baseada em risco e contexto é essencial para evitar barreiras desproporcionais à inovação responsável.", "940709": "Em contextos de tratamento contínuo e massivo de dados biométricos, como cidades inteligentes ou monitoramento de multidões, recomenda-se adotar medidas escaláveis e proporcionais para garantir transparência e autodeterminação informativa. Entre as práticas viáveis, destacam-se sinalizações visuais em locais acessíveis, com explicações gerais sobre a coleta e tratamento de dados, além da disponibilização de QR Codes vinculados ao aviso de privacidade e canais de contato. Tais medidas já foram consideradas adequadas pela ANPD (Nota Técnica nº 29/2024/FIS/CGF/ANPD, §6.1.4). Quando não houver vínculo direto entre titular e controlador, como em tecnologias embarcadas e testes sem coleta persistente de dados, a transparência tradicional deve ser substituída por estratégias alternativas que preservem a proporcionalidade, sem inviabilizar o uso responsável e seguro da tecnologia. O respeito aos direitos do titular exige adaptação aos diferentes contextos de operação.", "940710": "O exercício de direitos em contextos de biometria exige adaptações técnicas. Para o direito de acesso, o ICO reconhece que os dados biométricos, por serem representações numéricas ilegíveis, podem ser substituídos por comunicação explicativa, com descrição do dado, forma de armazenamento e motivo da não entrega direta. O direito de correção é aplicável se houver erro na vinculação do template biométrico ou modificação física relevante, sendo essencial que os templates sejam revogáveis e renováveis. A revogação do consentimento também depende dessa característica técnica, mas não implica exclusão automática de registros anteriores, quando houver fundamento legítimo, como obrigações legais. Em soluções embarcadas, deve-se assegurar que os dados possam ser substituídos sem vínculo técnico com os anteriores. Por fim, a responsabilidade de controladores que usam modelos de IA pré-treinados deve se restringir à sua esfera de controle, sob pena de insegurança jurídica e desincentivo à inovação", "940711": "O tratamento de dados biométricos de crianças e adolescentes pode se basear em qualquer hipótese do art. 11 da LGPD, desde que respeitado o princípio do melhor interesse. A finalidade deve estar alinhada à proteção da criança e à proporcionalidade do tratamento. Para garantir a participação informada dos pais ou responsáveis, recomenda-se: (i) comunicação formal com informações claras sobre a operação de tratamento; (ii) inclusão da biometria no aviso de privacidade; (iii) canais de atendimento acessíveis; e (iv) meios de oposição, quando aplicável. A análise do melhor interesse deve considerar: o bem jurídico protegido; a existência de alternativas menos invasivas; e a instabilidade de certas características biométricas em menores, como traços faciais durante a puberdade. Diretrizes

britânicas podem ser referência, desde que adaptadas à LGPD. A adoção dessas práticas assegura transparência e proteção adequada a esse grupo hiper vulnerável.", "940712": "O tratamento de dados biométricos de crianças e adolescentes pode se apoiar em qualquer hipótese do art. 11 da LGPD, desde que respeitado o princípio do melhor interesse, conforme Enunciado CD/ANPD nº 1/2023. A base legal escolhida deve estar claramente justificada e vinculada à proteção dos direitos da criança. Recomenda-se, além do Aviso de Privacidade, a comunicação direta e formal aos pais ou responsáveis com informações objetivas sobre a operação de tratamento e canais para exercício de direitos. Boas práticas incluem dissociação entre dados biométricos e identificadores, anonimização desde a origem e acesso restrito à equipe. Tais medidas são aplicáveis inclusive em ambientes de pesquisa, promovendo segurança e ética. Por fim, é indispensável seguir os controles técnicos e administrativos destacados nos quesitos 5 e 11, a fim de prevenir abusos, vazamentos ou acessos indevidos, assegurando a proteção dos dados dos menores.", "940714": "A verificação de idade por biometria deve considerar: (i) o contexto da verificação; (ii) a acuracidade da tecnologia; e (iii) a existência de métodos menos intrusivos. Conforme o ICO, o método deve ser proporcional ao risco que o serviço representa. Para serviços de alto risco (ex: jogos com interação online), o uso de biometria facial pode ser justificado; já para serviços de baixo risco (ex: envio de newsletters), autodeclaração pode ser suficiente. A acuracidade é essencial: tecnologias imprecisas exigem cautela, sendo recomendável combiná-las com análise documental. Métodos alternativos incluem validação por cartão de crédito simbólico, análise comportamental, verificação presencial ou consentimento validado dos responsáveis. Em serviços de risco elevado, pode-se adotar soluções híbridas (ex: verificação facial sem armazenamento), desde que acompanhadas de salvaguardas adequadas e mecanismos de controle pelos responsáveis legais.

Contribuinte: Giovanna Milanez Tavares

TOMADA DE SUBSÍDIOS - DADOS BIOMÉTRICOS

O objetivo da presente Tomada de Subsídios é coletar informações, evidências e perspectivas de diversos setores da sociedade sobre o tratamento de dados biométricos, visando a elaboração de materiais orientativos ou regulamentos que promovam a proteção de dados pessoais e a inovação responsável.

As contribuições abordam eixos como hipóteses legais para o tratamento de dados biométricos, reconhecimento facial e aplicação de tecnologias emergentes e inovadoras, governança e boas práticas e direitos dos titulares e grupos vulneráveis.

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo “dados biométricos”, mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos — que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Um dado deve ser caracterizado como biométrico, nos termos da LGPD, quando atender cumulativamente aos seguintes critérios objetivos:

- a) Origem biológica ou comportamental – decorre de características físicas, fisiológicas ou comportamentais de um indivíduo (ex: impressão digital, reconhecimento facial, íris, voz, padrões de digitação);
- b) Unicidade individual – permite identificar ou autenticar um indivíduo de forma única e inequívoca;
- c) Tratamento automatizado – é coletado e processado por sistemas computacionais com finalidade de identificação ou autenticação;
- d) Finalidade identificatória – seu uso visa estabelecer a identidade de uma pessoa natural ou verificar sua autenticidade de forma direta ou indireta.

Assim, a mera existência de uma característica física não configura dado biométrico, sendo necessário que ela seja capturada e processada com fins de identificação/autenticação automatizada.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Os controladores que tratam dados biométricos devem adotar as seguintes práticas de transparência ativa, antes da coleta dos dados:

- A) Aviso de Privacidade Específico – fornecer documento claro, destacando a natureza sensível dos dados biométricos, finalidade do tratamento, base legal, tempo de retenção e direitos do titular;
- B) Sinalização Visual nos Locais de Coleta – uso de avisos visíveis (físicos ou digitais) indicando que há coleta de dados biométricos, com QR Code ou link para o aviso de privacidade completo;
- C) Consentimento Informado (quando aplicável) – em casos em que a base legal for o consentimento, este deve ser obtido de forma destacada, livre, específica e inequívoca, com opção clara de recusa sem prejuízo indevido;

D) Canal de Atendimento Ativo – disponibilizar canal facilitado (e-mail, telefone ou formulário digital) para esclarecimento de dúvidas e exercício de direitos por meio do Encarregado de Dados (DPO);

E) Descrição dos Riscos e Medidas de Segurança em políticas internas – informar, em linguagem acessível, os principais riscos associados ao tratamento de dados biométricos e as medidas técnicas e administrativas adotadas para mitigá-los, bem como as demais informações associadas à coleta.

Essas práticas asseguram a autodeterminação informativa e o cumprimento dos princípios da LGPD, especialmente os da transparência, necessidade e responsabilidade.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A biometria comportamental deve ser tratada com o mesmo grau de proteção da biometria tradicional, pois ambas envolvem dados sensíveis com potencial de identificação individual como, por exemplo, o uso da voz. No entanto, há particularidades que exigem obrigações específicas adicionais, especialmente em razão de seu caráter dinâmico, contínuo e contextual.

1. Tratamento diferenciado justificado por características técnicas:

A) Variabilidade temporal: padrões comportamentais mudam ao longo do tempo, exigindo mecanismos robustos de atualização e validação contínua para garantir a qualidade dos dados;

B) Dependência de contexto: o desempenho e precisão podem variar conforme dispositivos, ambiente e condições de uso e minimização de falsos positivos/negativos.

2. Obrigações específicas recomendadas:

A) Auditorias frequentes de precisão dos sistemas de reconhecimento comportamental, com métricas claras de desempenho e revisão periódica dos modelos;

- B) Documentação técnica acessível à ANPD, demonstrando a aderência a critérios de minimização, necessidade e proporcionalidade no uso da biometria comportamental;
- C) Limitação de finalidade e reuso: proibir o reuso desses dados para finalidades não inicialmente informadas, dada sua capacidade de traçar perfis complexos e comportamentos;
- D) Anonimização ou pseudonimização sempre que possível, com destaque nos fluxos em que a identificação não for estritamente necessária;
- E) Camadas adicionais de segurança: dado o risco elevado de rastreamento contínuo e vigilância, recomenda-se a implementação de criptografia forte, segregação de bases e controles de acesso reforçados.

Embora compartilhe a natureza sensível da biometria tradicional, a biometria comportamental demanda regras técnicas e organizacionais específicas para garantir os princípios de qualidade dos dados (exatidão, relevância, atualização) e segurança (proteção contra acessos não autorizados e vazamentos).

BLOCO II – HIPÓTESES LEGAIS

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Para garantir que o consentimento para o tratamento de dados biométricos atenda aos requisitos da LGPD, o controlador deve adotar as seguintes práticas:

1. Garantias para um consentimento válido:

- A) Livre: assegurar que o titular possa negar ou revogar o consentimento sem sofrer prejuízo, discriminação ou restrição de acesso a serviços essenciais;
- B) Específico: indicar de forma clara e separada a finalidade exata do uso dos dados biométricos, evitando consentimentos genéricos ou em bloco;
- C) Destacado: apresentar o pedido de consentimento em seção separada, com destaque visual e textual, sem estar embutido em outros termos ou contratos;
- D) Informado: fornecer informações completas e acessíveis sobre: Finalidade do tratamento; Base legal; Riscos envolvidos; Compartilhamentos; Direitos do titular; e, Prazo de retenção dos dados.
- E) Inequívoco: exigir ação afirmativa clara do titular (ex: clicar em “Aceito”, assinar digitalmente ou marcar uma caixa de seleção não pré-preenchida).

2. Contextos em que o consentimento não é adequado como base legal:

- A) Relações assimétricas de poder, como: Relações de emprego; Relações com o Estado; Ambientes educacionais ou prisionais; Serviços que dependem da coleta para funcionarem (sem alternativa ao titular).
- B) Situações em que a recusa do consentimento impediria o cumprimento de obrigação legal ou regulatória, como: Controle de acesso em ambientes de alta segurança; Verificação de identidade em serviços bancários regulados; Cumprimento de exigência legal de identificação.

Nesses casos, o uso de outras bases legais como cumprimento de obrigação legal, execução de contrato, legítimo interesse (com a elaboração do teste de balanceamento / avaliação de impacto), ou proteção do crédito, deve ser considerado mais apropriado e transparente.

O consentimento deve ser usado apenas quando houver real liberdade de escolha e compreensão do titular. Quando isso não for possível, deve-se recorrer a bases legais mais compatíveis com o princípio da necessidade e da boa-fé. Ainda, sugere-se a ANPD a possibilidade de instituir uma nova base legal específica que poderá ser utilizada para essa regulamentação, bem como a exigência de documentos próprios como forma de boa prática.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

1. Critérios para aplicar a base legal de “prevenção à fraude” (art. 11, II, "g") no tratamento de dados biométricos:

Para o uso legítimo dessa hipótese legal, devem ser observados os seguintes critérios:

- I. Finalidade específica e legítima: o tratamento deve estar claramente vinculado à prevenção de fraudes reais e identificáveis, como acesso indevido a contas, roubo de identidade, lavagem de dinheiro ou fraudes bancárias;
- II. Comprovação de risco concreto: o controlador deve demonstrar, por meio de análise de risco, que há ameaças significativas à segurança ou integridade das operações que justifiquem o uso de biometria;
- III. Impossibilidade de medidas menos intrusivas: deve ser comprovado que outros meios menos invasivos (ex: senha, token, verificação em dois fatores) são insuficientes para alcançar o mesmo nível de proteção.

2. Compatibilização com o princípio da necessidade (art. 6, III, LGPD):

A biometria deve ser limitada ao mínimo necessário para atingir a finalidade de segurança:

- I. Modularidade e seletividade: aplicar biometria apenas em situações de risco elevado (ex: transações acima de determinado valor ou acessos sensíveis), evitando uso indiscriminado;
- II. Descarte ou anonimização após uso: sempre que possível, adotar biometria temporária ou transformada em hash irreversível, para mitigar risco de exposição indevida;
- III. Finalidade restrita: proibir o reuso dos dados biométricos para outras finalidades (ex: marketing, perfilamento ou publicidade comportamental).

3. Salvaguardas recomendadas para mitigar riscos:

- I. Relatório de Impacto à Proteção de Dados (RIPD): obrigatório para tratamento de alto risco, deve avaliar riscos à privacidade, proporcionalidade do uso e medidas mitigadoras;
- II. Pseudonimização ou criptografia forte dos dados biométricos;
- III. Controle de acesso rigoroso e registros de auditoria sobre quem acessa os dados e para qual finalidade;
- IV. Treinamento contínuo das equipes técnicas e operacionais sobre a natureza sensível e os riscos associados à biometria;
- V. Política de retenção restritiva: guardar os dados biométricos apenas pelo tempo necessário à finalidade de prevenção à fraude, com exclusão automática após esse período.

A aplicação da base legal de prevenção à fraude exige justificativa técnica, proporcionalidade e salvaguardas robustas. A proteção das liberdades fundamentais deve ser preservada mediante uso seletivo da biometria, transparência, minimização de dados e governança contínua.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Quando o tratamento de dados biométricos for realizado com base no “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD), especialmente por órgãos e entidades públicas, devem ser observados os seguintes critérios e salvaguardas:

1. Critérios para aplicação legítima da base legal:

- A) Previsão legal ou normativa expressa: o tratamento deve decorrer de lei ou regulamento específico que exija, de forma clara, a coleta de dados biométricos para uma finalidade definida (ex: identificação civil, segurança pública, controle migratório);
- B) Finalidade pública legítima e específica: o tratamento deve atender ao interesse público ou ao exercício regular de autoridade legal, com vinculação direta à missão institucional do órgão;
- C) Limitação de escopo: o uso dos dados biométricos deve se restringir exclusivamente à finalidade legal prevista, sendo vedado o compartilhamento com terceiros para outras finalidades (ex: marketing, perfilamento ou vigilância ampliada).

2. Salvaguardas recomendadas para mitigar riscos e garantir direitos:

- A) Transparência ativa: ampla divulgação, em linguagem acessível, da base legal, finalidades, período de retenção e direitos do titular — inclusive nos pontos de coleta (físicos ou digitais);
- B) Minimização de dados: coleta apenas dos elementos biométricos estritamente necessários à finalidade legal, evitando excesso e uso generalizado;
- C) Avaliação de impacto (RIPD): elaboração e atualização periódica de Relatório de Impacto à Proteção de Dados Pessoais, detalhando riscos à privacidade, medidas de segurança e mitigação;
- D) Segurança da informação reforçada: adoção de protocolos robustos de criptografia, controle de acesso, registro de logs, monitoramento contínuo e política de resposta a incidentes;

E) Governança e responsabilização: definição clara de papéis e responsabilidades, incluindo a atuação de um Encarregado (DPO) e a supervisão da cadeia de tratamento (inclusive com operadores);

F) Direitos dos titulares garantidos: canais eficazes para solicitação de acesso, correção, informação sobre uso e revisão de decisões automatizadas, inclusive nos casos em que o titular não possa recusar o tratamento.

A base legal do “cumprimento de obrigação legal ou regulatória” impõe obrigação de proporcionalidade e legalidade estrita, especialmente ao poder público. Para que o tratamento seja legítimo e constitucional, deve haver previsão normativa clara, salvaguardas técnicas e organizacionais eficazes, e mecanismos reais de transparência e controle social.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

1. Limites ao tratamento de dados biométricos por órgãos de pesquisa (art. 11, II, “c”):

Mesmo com base na LGPD para fins de pesquisa, o tratamento de dados biométricos deve respeitar os seguintes limites legais e éticos:

A) Finalidade exclusivamente científica ou estatística: o uso deve estar claramente vinculado à produção de conhecimento, sem fins comerciais, promocionais ou de controle individual;

B) Necessidade de anonimização eficaz: o dado biométrico só pode ser tratado quando irreversivelmente anonimizado, exceto quando houver base legal e salvaguardas adicionais para uso em formato pseudonimizado;

C) Proibição de reidentificação: é vedado o cruzamento de bases de dados com o propósito ou efeito de reidentificar os titulares, mesmo que de forma indireta;

D) Minimização e proporcionalidade: uso limitado ao mínimo necessário de atributos biométricos, evitando coleta ou tratamento de dados excessivos, detalhados ou desnecessários para a finalidade da pesquisa.

2. Riscos com o cruzamento de bases e possibilidade de reidentificação:

Dados biométricos, mesmo quando anonimizados, possuem alto grau de singularidade e persistência, o que os torna vulneráveis à reidentificação por correlação com outras bases (ex: dados de saúde, localização, registros públicos).

3. Salvaguardas adicionais recomendadas:

A) Avaliação de risco de reidentificação: testes periódicos para aferir a robustez dos métodos de anonimização aplicados (ex: k-anonimato, diferencial de privacidade);

B) Segregação de bases de dados: manter separação técnica e organizacional entre dados biométricos e outras bases que contenham identificadores diretos ou indiretos;

C) Governança ética e revisão por comitês de ética em pesquisa, quando aplicável, inclusive para projetos conduzidos por instituições públicas;

D) Cláusulas contratuais restritivas: em parcerias ou compartilhamentos com terceiros, impor obrigações legais de não reidentificação, uso limitado e confidencialidade;

E) Descarte controlado ou irreversível dos dados ao final do ciclo da pesquisa, salvo quando houver justificada necessidade de arquivamento científico, sob controle rigoroso;

F) Transparência científica: sempre que possível, comunicar publicamente os objetivos, metodologia e cuidados adotados para garantir a privacidade dos titulares, inclusive em relatórios públicos.

Embora a LGPD permita o uso de dados biométricos anonimizados para pesquisa, esse tratamento está sujeito a limites técnicos, éticos e legais rigorosos, com especial atenção ao risco de reidentificação. A adoção de salvaguardas adicionais é indispensável para garantir que o interesse público da pesquisa não viole os direitos fundamentais dos titulares.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

A utilização das tecnologias de reconhecimento facial (Facial Recognition Technologies, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento. Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou

abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

1. Garantia do cumprimento dos princípios no uso do reconhecimento facial

A) Necessidade: Limitar o uso da tecnologia estritamente ao mínimo indispensável para a finalidade legalmente prevista e Avaliar alternativas menos invasivas antes da adoção do reconhecimento facial.

B) Proporcionalidade: Adequar o grau de intervenção ao risco envolvido, aplicando o reconhecimento facial apenas quando os benefícios superarem os potenciais impactos aos direitos dos titulares e Evitar o uso em massa ou indiscriminado, priorizando casos específicos e justificados.

C) Transparência: Informar claramente os titulares sobre o uso da tecnologia, finalidade, bases legais, riscos, direitos e canais de atendimento e Publicar relatórios de impacto de privacidade acessíveis ao público e às autoridades regulatórias.

D) Prevenção de discriminação ilícita ou abusiva: Realizar testes de viés e auditorias técnicas para identificar e corrigir possíveis falhas que afetem grupos sociais vulneráveis ou minorias e Garantir que os algoritmos sejam desenvolvidos e avaliados com diversidade de dados e sob supervisão independente.

2. Salvaguardas técnicas, jurídicas e institucionais

A) Técnicas: Uso de modelos de inteligência artificial auditáveis e explicáveis, Criptografia e pseudonimização dos dados biométricos para limitar o acesso indevido e Monitoramento contínuo da performance e impactos do sistema, com atualizações regulares para corrigir vieses.

B) Jurídicas: Formalização clara da base legal que autoriza o tratamento, com documentação completa, Implementação de políticas internas e termos de uso específicos, detalhando responsabilidades e restrições e Adoção obrigatória de Relatório de Impacto à Proteção de Dados (RIPD) específico para reconhecimento facial.

C) Institucionais: Criação ou fortalecimento de comitês multidisciplinares para governança ética e controle do uso da tecnologia, Capacitação contínua de equipes envolvidas para garantir conformidade e sensibilidade aos riscos sociais e

Estabelecimento de canais independentes para denúncia e revisão de decisões automatizadas, Auditorias e fiscalizações para garantir o cumprimento e adequação à LGPD e a possibilidade de instituição de um selo específico de certificação.

O uso do reconhecimento facial deve ser cuidadosamente calibrado para respeitar direitos fundamentais, exigindo governança robusta, transparência efetiva, controles técnicos rigorosos e contínua supervisão institucional para mitigar riscos de discriminação e violações à privacidade.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

1. Projetar sistemas de reconhecimento facial para alta eficácia e confiabilidade

A) Treinamento com bases de dados diversificadas e representativas: Para minimizar vieses e melhorar a precisão, o sistema deve ser treinado com amostras variadas que representem diferentes etnias, gêneros, idades e condições ambientais.

B) Uso de algoritmos avançados e validados: Aplicar modelos de aprendizado de máquina state-of-the-art, com testes extensivos de desempenho (precisão, recall, F1-score).

C) Validação contínua e testes em ambientes reais: Monitorar o sistema em operação para identificar variações de desempenho e ajustar o modelo conforme necessidade.

D) Criação de regulamentos para verificação de critérios específicos.

2. Mecanismos para correção tempestiva de falhas:

A) Mecanismos de feedback humano (human-in-the-loop): Incorporar revisão manual em casos de baixa confiança do sistema ou decisões críticas, para evitar decisões automatizadas equivocadas;

B) Monitoramento e auditoria em tempo real: Implementar dashboards que acompanhem métricas de erro (falsos positivos e negativos), permitindo identificação rápida de problemas.

C) Procedimentos de contestação e retificação: Estabelecer canais acessíveis para titulares contestarem resultados errôneos e solicitarem revisão humana.

D) Atualização periódica dos modelos: Revisar e re-treinar os algoritmos regularmente com novos dados para corrigir desvios e adaptar-se a mudanças no ambiente.

E) Registro detalhado de logs e rastreabilidade: Manter registros auditáveis de todas as decisões automatizadas para análises posteriores e comprovação de conformidade.

A eficácia e confiabilidade dos sistemas de reconhecimento facial dependem de dados diversificados, modelos robustos, supervisão humana, monitoramento contínuo e mecanismos claros para correção de erros, especialmente quando o tratamento é automatizado e impacta direitos dos titulares.

10.É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

1. Contextos e situações em que o uso de reconhecimento facial não é recomendado:

A) Espaços públicos com vigilância massiva e indiscriminada: O uso amplo em praças, ruas, transportes ou eventos sem base legal clara e sem consentimento configura risco elevado à privacidade e pode gerar vigilância abusiva.

B) Ambientes com alta probabilidade de erro ou viés algorítmico: Como escolas, concursos públicos ou processos seletivos, onde falsos positivos ou negativos podem resultar em discriminação ou exclusão indevida de indivíduos.

C) Ausência de justificativa proporcional e de risco real identificado: Sempre que não houver uma ameaça concreta à segurança ou fraude que justifique o tratamento de dados biométricos sensíveis.

D) Utilização por agentes públicos sem legislação específica e controles independentes: A falta de base legal e de mecanismos de prestação de contas pode transformar o uso da tecnologia em violação aos direitos fundamentais.

Importante se faz destacarmos o cuidado especial que os grupos vulneráveis precisam ter a fim de garantir que não haja uso indiscriminado, ou seja, que o reconhecimento facial seja utilizado para práticas ilícitas e abusivas.

2. Tecnologias alternativas com menor impacto à proteção de dados:

A) Autenticação multifator (MFA): Combinação de senha + token + biometria opcional, onde a biometria não seja armazenada de forma centralizada.

B) Tokens físicos ou digitais temporários: Cartões com chip, QR codes dinâmicos ou chaves de autenticação com expiração rápida e sem identificação permanente do titular.

C) Reconhecimento de comportamento contextual (autenticação adaptativa): Análise de padrões de uso (localização, horário, dispositivo) sem identificação biométrica direta.

D) Senha segura com verificação por canal secundário (ex: SMS, e-mail, aplicativo autenticador): Soluções de autenticação de dois fatores com menor risco à privacidade.

O reconhecimento facial não é recomendável em contextos de baixa justificativa, risco elevado à privacidade, ou ausência de regulamentação clara. Tecnologias alternativas como MFA, tokens temporários e autenticação contextual podem oferecer segurança equivalente com menor impacto sobre os dados sensíveis dos titulares, alinhando-se melhor aos princípios da LGPD.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

O tratamento de dados biométricos exige uma abordagem cautelosa e

estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos.

Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes.

Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados.

Com base nisso, questiona-se:

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos

das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

1. Medidas de segurança técnicas e administrativas indispensáveis para mitigar riscos com dados biométricos:

A) Técnicas: Criptografia forte e específica para dados biométricos; Template biométrico em vez de imagem bruta; Segregação de ambientes e controle de acesso; Registro de logs e rastreabilidade completa; Análise de anomalias e detecção de intrusão.

B) Administrativas: Política específica de segurança para dados sensíveis; Treinamento contínuo das equipes; Contrato e due diligence com operadores e fornecedores; Plano de resposta a incidentes com foco em dados sensíveis.

2. Parâmetros mínimos de avaliação de riscos e monitoramento exigíveis:

I. Elaboração e revisão periódica do RIPD (Relatório de Impacto à Proteção de Dados);

II. Classificação de risco com base em impacto e probabilidade;

III. Testes periódicos de segurança (pentests e auditorias);

IV. Indicadores-chave de risco (KRIs) e conformidade (KPIs);

V. Supervisão do DPO (Encarregado) e sua obrigatoriedade.

Devido ao caráter permanente, sensível e irrecuperável dos dados biométricos, é essencial adotar medidas de segurança específicas, robustas e contínuas, tanto técnicas quanto administrativas. A gestão de riscos deve ser estruturada, documentada e auditável, garantindo conformidade com a LGPD e proteção efetiva dos titulares contra violações e seus efeitos irreversíveis.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se

baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

1. Boas práticas para evitar discriminação ilícita ou abusiva em serviços não essenciais que utilizam biometria:

I. Oferecimento de alternativas viáveis à autenticação biométrica;

II. Proporcionalidade na exigência biométrica;

III. Transparência prévia e completa;

IV. Evitar coerção disfarçada;

V. Política de uso clara e baseada em princípios de não discriminação.

2. Quando a negativa do titular pode justificar restrição de funcionalidades?

A funcionalidade depende diretamente da biometria por exigência técnica de segurança elevada, como em transações financeiras de alto valor, assinatura eletrônica qualificada ou autenticação sensível.

A base legal adotada é o consentimento, e este é recusado ou revogado — desde que: a biometria não seja requisito geral para uso do serviço e/ou a finalidade e os riscos estejam claramente informados ao titular.

Exemplo de aplicação legítima:

Um app bancário pode restringir o uso de reconhecimento facial apenas para autenticação de transações de alto risco, oferecendo alternativas (como token físico ou senha temporária) para quem não fornecer a biometria e, caso a biometria seja imposta como um único meio disponível sugere-se que sejam estabelecidas medidas de segurança específicas para isso.

A coleta de dados biométricos em serviços não essenciais deve ser voluntária, justificada e proporcional, com garantia de alternativas seguras e não discriminatórias. A recusa do titular pode justificar restrições específicas, desde que haja transparência, proporcionalidade e respeito à autodeterminação informativa, conforme previsto na LGPD.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como

garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

1. Boas práticas específicas para proteção eficaz de dados biométricos:

A) Minimização e finalidade clara: Coletar apenas os dados biométricos estritamente necessários e vinculá-los a finalidades legítimas, específicas e informadas, vedando usos secundários ou ampliados sem nova base legal.

B) Relatório de Impacto à Proteção de Dados (RIPD): Elaborar obrigatoriamente antes do início do tratamento de dados biométricos, detalhando os riscos, medidas de mitigação, hipóteses legais e alternativas menos intrusivas.

C) Pseudonimização ou uso de templates biométricos: Sempre que possível, evitar o armazenamento de imagens brutas. Optar por templates matemáticos que reduzam o risco de reidentificação em caso de violação.

D) Criptografia e controle de acesso rigoroso: Implementar criptografia forte nos dados em trânsito e em repouso. Restringir o acesso com autenticação multifator e gestão baseada em perfis de risco.

E) Auditorias e testes regulares de segurança e viés: Avaliar periodicamente os sistemas de reconhecimento quanto a falhas, vieses e desempenho. Corrigir de imediato distorções que afetem determinados grupos sociais.

F) Capacitação contínua das equipes: Promover treinamentos periódicos sobre proteção de dados, riscos da biometria e prevenção à discriminação algorítmica.

G) Política interna e código de conduta específico: Estabelecer diretrizes formais para o tratamento de dados biométricos, com responsabilização clara de gestores e operadores.

H) DPO:

I) Eliminação após o uso.

2. Como garantir uso transparente e responsável dos dados biométricos:

A) Informações claras e destacadas ao titular: Fornecer políticas de privacidade acessíveis, com linguagem simples, explicando a finalidade, base legal, riscos, direitos e canais de atendimento.

B) Consentimento livre, informado e específico (quando aplicável): Garantir que o titular possa exercer sua escolha de forma autônoma e que a recusa não resulte em penalidade indevida, exceto quando tecnicamente justificada.

C) Governança algorítmica: Criar estruturas de governança que incluam revisão humana de decisões automatizadas, auditoria de algoritmos e mecanismos para contestação de resultados.

D) Prevenção à discriminação: Testar continuamente os sistemas para detecção de vieses, especialmente em relação a gênero, cor de pele, idade ou deficiência, com correções documentadas.

A proteção eficaz de dados biométricos exige medidas técnicas, jurídicas e éticas integradas, com foco na minimização, segurança, transparência e equidade. Controladores devem adotar uma postura ativa de responsabilidade e prestação de contas, prevenindo abusos e garantindo que o tratamento não comprometa a dignidade ou os direitos fundamentais dos titulares.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

1. Como assegurar o respeito à autodeterminação informativa em tratamentos contínuos e massivos de dados biométricos:

A) Planejamento e base legal adequada:

I. Avaliação prévia de impacto (RIPD): Obrigatória, considerando a escala, o contexto público e os riscos elevados à privacidade. Deve demonstrar a necessidade, proporcionalidade e justificar a base legal utilizada (ex: obrigação legal, execução de políticas públicas, etc.).

II. Base legal clara e específica: O tratamento não pode ser baseado em consentimento em contextos de difícil manifestação de vontade, como em vias públicas. Deve haver respaldo legal e normativo para legitimar o uso.

2. Medidas concretas para garantir a informação e o controle do titular:

A) Transparência proativa:

I. Sinalização clara e visível nos locais monitorados: Informar de forma destacada e compreensível sobre a presença de tecnologia de reconhecimento facial ou biometria (ex: placas com QR Code para acessar política de privacidade).

II. Campanhas públicas de conscientização: Explicar à população o funcionamento do sistema, sua finalidade, direitos dos titulares e canais de contato com o controlador ou com o DPO.

III. Portal de privacidade ou aplicativo acessível: Permitir que o cidadão acesse informações, visualize se seus dados foram capturados, entenda os tratamentos realizados e possa exercer seus direitos (acesso, oposição, anonimização, etc.).

3. Medidas para garantir o exercício de direitos:

I. Canal de atendimento simplificado e multicanal: Suporte por site, telefone, aplicativo ou presencial, com linguagem acessível e prazo razoável de resposta.

II. Mecanismo de contestação de decisões automatizadas: Sempre que o uso de biometria resultar em alguma decisão ou triagem automática (ex: barramento em entrada), deve haver revisão humana garantida.

III. Limitação de retenção e descarte seguro: Dados biométricos coletados em ambientes públicos devem ter prazo de retenção mínimo necessário, com descarte seguro e documentado.

4. Responsabilidade ativa do controlador:

I. Governança e prestação de contas (accountability): Controladores devem manter registro das operações, justificar o uso da tecnologia com base em critérios técnicos e legais, e submeter-se à fiscalização da ANPD.

II. Auditorias independentes e relatórios públicos periódicos: Avaliação de eficácia, riscos e eventuais abusos com divulgação dos resultados à sociedade, reforçando a confiança e o controle democrático.

Para garantir a autodeterminação informativa em contextos massivos, como smart cities ou estádios, os controladores devem adotar medidas concretas de transparência, prestação de contas, mecanismos de informação acessível e canais eficazes de exercício de direitos, respeitando os princípios da necessidade, proporcionalidade e não discriminação, conforme determina a LGPD.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

1. Direito à informação clara:

A) Transparência ativa desde a coleta que pressupõe informar previamente e de forma clara, acessível e destacada: Finalidade do tratamento; Tipo de dado biométrico coletado; Base legal utilizada; Período de retenção; Possibilidade de revogação ou oposição; e, Contato do encarregado (DPO).

B) Política de privacidade específica e objetiva: Adaptada ao tratamento de dados biométricos, com linguagem não técnica, disponível no ponto de coleta e em meios digitais.

C) Uso de linguagem visual (ex: infográficos, vídeos, QR Codes): Especialmente útil em ambientes físicos com tratamento automatizado (ex: catracas com reconhecimento facial).

D) Implementação de técnicas e medidas específicas para portadores com deficiência (PCD).

2. Direito de acesso e correção de dados:

A) Mecanismo digital ou físico de fácil acesso como a criação de portais, aplicativos ou canais presenciais para que o titular possa: Solicitar confirmação da existência de tratamento; Visualizar dados biométricos (quando possível, sem risco à segurança); Corrigir dados associados (ex: erro de vinculação com identidade).

B) Prazos razoáveis e automação com supervisão humana: Atender as solicitações dentro dos prazos legais (até 15 dias) e, sempre que automatizado, garantir revisão humana para correções ou esclarecimentos.

C) Registro de logs de tratamento: Manter histórico de acesso, coleta e alterações de dados, que possa ser auditado em caso de solicitação.

3. Direito à revogação do consentimento:

- A) Canal simples e gratuito para revogação: Quando o tratamento se basear em consentimento, deve ser possível revogá-lo com a mesma facilidade com que foi concedido, sem ônus ao titular.
- B) Consequências da revogação devem ser informadas: O controlador deve indicar claramente se a revogação limita ou inviabiliza o uso de determinada funcionalidade, de forma proporcional e justificada.
- C) Cessaç o imediata do tratamento ap s revoga o: Com posterior exclus o ou anonimiza o dos dados biom tricos, salvo quando houver outra base legal que justifique sua manuten o (ex: obriga o legal).

4. Medidas adicionais em contextos automatizados:

- A) Preven o de decis es exclusivamente automatizadas prejudiciais: Quando o tratamento resultar em efeitos jur dicos ou significativos, deve haver possibilidade de revis o por pessoa humana, conforme art. 20 da LGPD.
- B) Auditoria de algoritmos e mitiga o de vi s: Testes peri dicos para evitar discrimina o, erros e falsas negativas/positivas na identifica o biom trica.

16. Diante da sensibilidade dos dados biom tricos de crian as e adolescentes, especialmente em contextos como escolas e espa os recreativos, como garantir a participa o informada dos pais ou respons veis e em quais hip teses legais esse tipo de tratamento seria admiss vel? Quais condi  es devem ser observadas para que esse tratamento esteja alinhado ao princ pio do melhor interesse, nos termos do art. 14 da LGPD?

- I) Deve haver consentimento livre, espec fico, destacado e informado de ao menos um dos pais ou respons veis.
- II) O tratamento deve seguir o princ pio do melhor interesse da crian a/adolescente (art. 14 da LGPD).
- III) A coleta de dados biom tricos s    leg tima se for estritamente necess ria para a finalidade proposta.
- IV)   obrigat ria a transpar ncia com os respons veis, com informa  es claras sobre uso, riscos e direitos.

V) Dados devem ser tratados com medidas de segurança adequadas e acesso controlado.

VI) O uso para controle de frequência, por exemplo, deve ter justificativa proporcional e documentada.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

I) Consentimento dos pais ou responsáveis é a principal base legal em instituições privadas (art. 14, §1º).

II) Em instituições públicas, pode-se aplicar cumprimento de obrigação legal ou execução de política pública.

III) A transparência com os responsáveis é obrigatória em todos os casos, mesmo sem consentimento formal.

IV) Devem ser adotadas medidas técnicas e organizacionais eficazes, como: Criptografia; Controle de acesso; Segregação de dados; Auditorias de segurança; Descarte seguro após a finalidade.

V) Recomenda-se a elaboração de Relatório de Impacto à Proteção de Dados (RIPD).

VI) O tratamento deve respeitar os princípios da necessidade, proporcionalidade e segurança.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

I) O uso de biometria para estimar idade exige justificativa técnica robusta e deve ser indispensável.

II) Sempre que possível, devem ser usadas alternativas menos invasivas (ex: autodeclaração ou documentos).

III) A base legal, em geral, será o consentimento dos responsáveis, salvo obrigação legal expressa.

IV) O uso da biometria deve respeitar o melhor interesse do menor, sem finalidade comercial indevida.

V) Os dados biométricos não devem ser armazenados após a verificação, salvo se estritamente necessário.

VI) Devem ser adotadas medidas de segurança reforçadas, como criptografia, revisão de algoritmos e minimização de riscos.

VII) A prática deve ser transparente, proporcional e acompanhada de mecanismos para exercício dos direitos dos responsáveis.

É a contribuição.

SOLINTEL - SOLUCOES INTELIGENTES EM TELECOMUNICACOES LTDA
CNPJ nº 08.429.293/0001-39



“Contribuição da Claro à Tomada de Subsídios sobre Dados Biométricos”

I. BLOCO I - DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Com base no entendimento da Autoridade de Proteção de Dados do México (INAI) [1]¹, e do art. 16 ter da Lei de Proteção de Dados Chilena [2]², consideram-se dados biométricos aqueles que, cumulativamente, atendem aos seguintes requisitos:

- (a) estejam relacionados a características físicas, fisiológicas, comportamentais ou traços de personalidade de um titular de dados; e
- (b) resultem de um tratamento específico (em regra, uma forma de medição), cuja finalidade seja identificar, de maneira única, o titular.

Dessa forma, imagens captadas em vídeo, fotografias, gravações de voz ou dados semelhantes não devem ser, isoladamente, considerados dados biométricos. Apenas o resultado do tratamento específico dessas informações que objetive identificar unicamente indivíduos pode ser considerado um dado biométrico.

Para evitar dúvidas imaginemos os seguintes cenários:

- Uma operadora de telefonia utiliza sistema de reconhecimento facial para validar a identidade de seus clientes, no qual pontos de biometria (características únicas do indivíduo, como distância entre os olhos e formato do maxilar [3]³) são extraídos do documento de identidade do cliente e comparados com pontos extraídos de uma fotografia (*selfie*) tirada na hora pelo titular. Nesse exemplo, os dados biométricos não são as fotografias (do documento de identidade ou da *selfie*), mas os pontos biométricos dela extraídos. Assim, eventual armazenamento da foto isoladamente não deverá ser considerado dado biométrico.
- Uma empresa pode gravar as ligações de seu SAC com a finalidade de cumprir o Decreto nº 11.034/2022 e para avaliar a qualidade do atendimento prestado. Essas gravações, por si só, não constituem dados biométricos. No entanto, se a organização utilizar essas gravações em modelo de inteligência artificial capaz de extrair características biométricas da fala (como padrões de frequência e amplitude das ondas sonoras [4]⁴) com o objetivo

¹

Disponível em: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf. Acesso em 09.06.2025

Disponível em: <https://www.diariooficial.interior.gob.cl/publicaciones/2024/12/13/44023/01/2583630.pdf>. Acesso em 09.06.2025

Disponível em: <https://blog.zapsign.com.br/en/reconhecimento-facial/>. Acesso em 09.06.2025

Disponível em: <https://sciforce.solutions/blog/voice-biometrics-recognition-and-opportunities-it-gives-bw9hqop9moas5bzwemea2zbt>. Acesso em 13.06.2025

⁴ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>. Acesso em 09.06.2025



de gerar identificador único do titular, então esses pontos biométricos extraídos (e não a gravação em si) configuram dados biométricos, nos termos da LGPD.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Conforme a Autoridade de Dados do Reino Unido (ICO⁵), não existe metodologia única aplicável a todos os casos sobre como a transparência pode ser garantida, incluindo medidas ativas a serem adotadas pelos controladores. A forma mais eficiente de transparecer o uso de dados biométricos ao titular deverá ponderar fatores, como: i) o caso de uso; ii) a natureza de relacionamento com o titular; e iii) os dados envolvidos na atividade de tratamento [1].

Nesse sentido, quanto mais óbvia a atividade de tratamento em análise, considerando as práticas habituais de mercado e a natureza do relacionamento com o titular, menor a exigência de práticas ativas de transparência. Exemplificamos:

Quando o tratamento de dados pessoais ocorre no contexto da validação da identidade do titular, durante a contratação ou utilização de produto ou serviço — por exemplo, a verificação biométrica no processo de contratação ou portabilidade de plano de telefonia. Trata-se de prática consolidada no mercado, em que a coleta de dados biométricos é clara e previsível para o titular, inclusive devido a:

(i) existência de regulamentações que requerem que empresas de telefonia adotem mecanismo de prevenção a fraudes, como o art. 65-M, da Resolução ANATEL 738/2020; e (ii) o fato de que fraudes no acesso às linhas de telefone dos usuários podem servir de ponto de partida para a realização de novas práticas criminosas, incluindo a obtenção de contas de e-mail, a estes vinculadas enquanto mecanismos de recuperação de senhas, e, a partir destas, contas de diversos serviços em que o titular está inscrito.

Nesses casos, o fornecimento do Aviso de Privacidade ao longo da jornada do usuário, nos termos de seu contrato de prestação de serviço ou, no caso de atendimento presencial, por meio de QR Codes disponibilizados em telas, cartazes ou materiais similares dentro do local físico, ou mesmo breve explicação pelo atendente, é suficiente para assegurar o atendimento do dever de transparência.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Não existem obrigações legais específicas que distingam as diferentes modalidades de biometria facial, não podendo eventual regulamentação sobre a legislação criar obrigação distinta, em situação na qual a legislação não a traz, o que implicaria em violação do princípio da legalidade.

Assim, por exemplo, soluções antifraude pautadas no reconhecimento da voz para permitir a realização de compras de produtos e serviços de forma segura por telefone não devem ser tratadas de forma distinta da coleta de biometrias faciais em aplicativos para o mesmo fim.



Além disso, não existe na LGPD definição específica para “dato biométrico”, há apenas a classificação como uma categoria de dato pessoal sensível. Nesse contexto, a caracterização de um dato como biométrico exige uma análise baseada em critérios objetivos que levem em conta a finalidade e a forma de tratamento do dato. Um dato só será considerado pessoal se puder tornar o titular identificado ou identificável. Essa premissa é essencial para o enquadramento dos dados biométricos, pois apenas informações capazes de individualizar o titular podem ser qualificadas como tal.

Dessa forma, dados que possam conter características biométricas, sejam elas imagens captadas em vídeo, fotografias ou gravações de voz, não devem ser, isoladamente, considerados dados biométricos ou mesmo dados pessoais sensíveis. Se uma fotografia, por exemplo, for empregada para treinar um modelo de IA com o objetivo de aprimorar funcionalidades gerais — como detecção de objetos, identificação de padrões de métrica facial, ou classificação de imagens — sem a intenção de identificar ou autenticar uma pessoa natural de forma individualizada, não há que se falar em tratamento de dato pessoal sensível.

A interpretação deve se apoiar na finalidade específica e concreta do tratamento, conforme preceitua o princípio da necessidade (art. 6º, III) e da finalidade (art. 6º, I). A mera possibilidade teórica de que um dato possa vir a ser utilizado para identificação não é suficiente para que se imponha, de forma automática, o regime jurídico mais rigoroso aplicável aos dados sensíveis.

A simples natureza comportamental do dato não é suficiente para enquadrá-lo automaticamente como dato pessoal sensível. É imprescindível avaliar o modo de tratamento técnico e a finalidade de uso. Essa abordagem evita uma interpretação excessivamente ampla e desproporcional da categoria de dados biométricos, e assegura um equilíbrio entre proteção de direitos e inovação tecnológica, em consonância com os princípios da LGPD.

BLOCO II - HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Existem diversas bases legais previstas na LGPD, e a mais apropriada dependerá do contexto específico, não havendo nenhum tipo de hierarquização entre elas, isto é, todas as hipóteses previstas são igualmente válidas e podem ser utilizadas sem haver a necessidade de se priorizar uma em detrimento de outras.

Para que o consentimento para o tratamento de dados biométricos seja considerado livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD, é fundamental que o titular tenha clareza sobre a finalidade do tratamento, compreenda suas implicações e possa manifestar sua vontade de forma autônoma, sem coerção ou engano.

A exigência de que o consentimento seja livre não implica, necessariamente, a ausência de qualquer condicionamento. O que a LGPD veda é a coação, a ausência de transparência ou a imposição de desvantagens excessivas ao titular. A simples oferta de um serviço vinculada ao tratamento de dados pessoais — inclusive biométricos — não invalida, por si só, o consentimento. A simples oferta de um serviço em troca do consentimento não o invalida, desde que: haja



transparência quanto à necessidade dos dados para a prestação do serviço; e o titular não seja compelido a consentir sob pena de sofrer desvantagens desproporcionais ou discriminatórias.

Diante da relevância do consentimento como base legal no tratamento de dados pessoais sensíveis, é fundamental que a ANPD reconheça, em suas orientações e interpretações normativas, as nuances e particularidades envolvidas na aferição do consentimento livre, especialmente no contexto da economia digital. Tal reconhecimento é essencial para evitar abordagens excessivamente restritivas que possam comprometer a viabilidade jurídica e econômica de modelos de negócio legítimos, amplamente utilizados na oferta de serviços digitais.

De fato, há casos em que o consentimento não será a base legal mais adequada - e mesmo a efetivamente correta - para o tratamento de dados pessoais sensíveis, razão pela qual o art. 11, em seu inciso II, traz outras hipóteses nas quais o tratamento do dado biométrico dispensa o consentimento. Nesse sentido, destaca-se a alínea “g”, a qual prevê expressamente a dispensa do consentimento para garantia da prevenção à fraude em processos de identificação e autenticação de cadastro. Nota-se, portanto, que o referido tratamento tem por finalidade proteger a segurança do próprio titular do dado contra usos indevidos de sua identidade. A exigência do consentimento poderia inviabilizar mecanismos de segurança automatizados, como as autenticações por reconhecimento facial ou impressão digital.

O consentimento não será a base legal adequada nas situações em que os requisitos de validade não podem ser satisfeitos, tipicamente isso transcorrerá em situações como quando não for viável oferecer alternativa à biometria facial ao titular de dados. Por exemplo, em processos de prevenção a fraudes, nos quais eventual opção poderia facilitar a atuação de fraudadores, ou nos casos em que a biometria é essencial para a prestação do serviço ou funcionamento do produto. Essa hipótese admite exceção quando não houver outra base legal aplicável e a ausência de consentimento tornar inviável o prosseguimento do tratamento biométrico - nesses casos, o prejuízo decorrente da negativa do titular é consequência necessária da própria impossibilidade de realizar a atividade.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Conforme Guia sobre o Legítimo Interesse da ANPD [1]⁶, os requisitos para o enquadramento do tratamento de dados biométricos na base legal de “prevenção à fraude” são semelhantes aos aplicáveis ao legítimo interesse. Nesse sentido, são aplicáveis os mesmos critérios do Teste de Balanceamento para enquadramento no “legítimo interesse”, ressalvada a proibição de tratamento de dados pessoais sensíveis.

Isso não implica dizer que a realização prévia de Teste de Balanceamento (“LIA”) seja medida obrigatória para garantir a licitude da atividade, pois inexistente obrigação legal nesse sentido.

⁶ Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em 09.06.2025



Assim, o Teste de Balanceamento auxilia a organização a demonstrar o enquadramento na base legal, mas sua ausência, por si só, não implica em ilicitude da atividade de tratamento – o que requererá demonstração concreta de ausência de atendimento dos requisitos mínimos.

No setor de telecomunicações, o uso de dados biométricos é, em regra, legítimo com base no art. 11, II, “g”, da LGPD. Essa prática encontra respaldo nas condutas usualmente adotadas pelo mercado e se justifica não apenas pela prevenção a fraudes no acesso aos serviços de telecomunicações, mas também pela necessidade de proteger a segurança de diversos serviços da sociedade da informação acessados por esses canais.

A apropriação indevida de uma linha telefônica (que em várias situações é mecanismo de autenticação para a recuperação de senhas) pode ter impactos severos sobre a vida do titular. Entre os riscos concretos estão o acesso não autorizado a e-mails, redes sociais e contas bancárias, expondo o titular a perdas financeiras e violações de privacidade por agentes mal-intencionados.

Observa-se tendência global entre reguladores do setor de telecomunicações em exigir a adoção da biometria facial pelas operadoras. Em diferentes países, a autenticação biométrica tem sido considerada medida proporcional e necessária para mitigar riscos de fraude e de apropriação indevida de identidade.

Na Tailândia⁷, o órgão regulador passou a exigir a autenticação biométrica para o registro de cartões SIM. Na Índia, a vinculação de SIM cards a dados biométricos tornou-se obrigatória como forma de aumentar a segurança na identificação dos titulares. No Chile, a autoridade reguladora determinou a adoção de biometria para todas as transações no setor.

Esse movimento regulatório dialoga diretamente com os princípios da Convenção 108+, da qual o Brasil é signatário. O artigo 5º da Convenção modernizada dispõe que o tratamento de dados pessoais (inclusive sensíveis, como biométricos) deve observar os critérios de necessidade, proporcionalidade e finalidade legítima, especialmente quando se busca proteger a segurança das comunicações e dos serviços da sociedade da informação.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

A biometria facial deve ser passível de enquadramento na mencionada base legal sempre que for meio razoável e proporcional de se atender a obrigação regulatória em análise. Por exemplo, no setor de telecomunicações, a Resolução ANATEL 738/2020, prevê, em seu art. 65º-M, *caput*:

Art. 65-M. As prestadoras devem adotar as **medidas técnicas e administrativas necessárias e disponíveis para prevenir e cessar a ocorrência de fraudes** relacionadas à prestação do serviço e ao uso das redes de telecomunicações, bem como para reverter ou mitigar os efeitos destas ocorrências.

A adoção de medidas de validação biométrica da identidade para prevenir fraudes se enquadra no atendimento deste dispositivo, razão pela qual, desde que seja adotada de forma razoável e proporcional aos riscos de fraude, deve ser apta a enquadramento na hipótese do art. 11º, II, a, da

⁷ <https://idtechwire.com/thailand-mandates-biometric-authentication-for-sim-cards-to-combat-fraud/>. Acesso em 13.06.2025
<https://www.biometricupdate.com/202501/biometric-authentication-required-for-sim-card-registration-in-india-and-thailand>. Acesso em 13.06.2025
<https://c-prav.com/2025/02/17/chile-mandates-biometric-verification-for-telecommunications-transactions/>. Acesso em 13.06.2025



LGPD – interpretar de forma contrária implicaria em verdadeira distorção da razão de ser desta base legal, que é fornecer aos agentes de tratamento segurança jurídica para as atividades de tratamento executadas com o fim de cumprir a legislação (que seria o caso), garantindo harmonia do sistema regulatório.

No caso do setor de telecomunicações, a própria ANATEL elenca a biometria facial como mecanismo utilizado no setor, como parte das medidas coordenadas pelo regulador na prevenção do sequestro de linha:

“O que a Anatel e setor estão fazendo? A Agência determinou a inclusão de segundo fator de autenticação ao procedimento de portabilidade. Trata-se do envio de uma mensagem de texto para o terminal objeto da solicitação de Portabilidade, para confirmar a solicitação. Sendo confirmado com SIM a portabilidade ocorre normalmente, sendo respondido NÃO a solicitação de portabilidade é cancelada automaticamente. Também são utilizados procedimentos de identificação dos consumidores por meio do uso de técnicas de biometria facial ou de voz. Para prevenir fraudes no sistema financeiro, as prestadoras disponibilizam informações para os bancos, possibilitando que adotem providências preventivas relativas às movimentações financeiras atreladas ao número do celular envolvido em troca de chip[1]⁸”.

Em relação às salvaguardas a serem adotadas para mitigação de riscos, entendemos que devem ser as mesmas aplicáveis aos agentes de tratamento que utilizam a base legal de “prevenção à fraude”, conforme descrito no quesito nº 5. Isso porque as medidas de proteção de dados devem ser proporcionais aos riscos envolvidos, independentemente da base legal utilizada para justificar o tratamento.

Assim, os controles e as salvaguardas adequados para mitigar os riscos decorrentes do uso de dados biométricos permanecem os mesmos, seja a base legal “prevenção à fraude”, “cumprimento de obrigação legal” ou outra prevista na LGPD.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

O questionamento apresentado busca resposta para três questionamentos: a) como garantir a transparência no uso de reconhecimento facial; b) como garantir a sua necessidade e proporcionalidade; e c) como evitar a discriminação.

Em relação aos questionamentos de transparência, aplicam-se as considerações já apresentadas no questionamento nº 2: as medidas de transparência devem ser definidas conforme análise contextual, levando em conta diversos fatores, especialmente o caso de uso, a natureza do relacionamento com o titular e as características da atividade de tratamento. De modo geral,

⁸ Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/dicas-contra-fraudes/golpes-atuais-mais-comuns>. Acesso em 13.06.2025



quanto mais evidente for a atividade de tratamento para o titular, menor será a exigência de práticas adicionais de transparência ativa.

Assim, quando o tratamento de dados biométricos é prática consolidada e conhecida no mercado, como no contexto da validação da identidade do titular durante a contratação ou alteração de um produto ou serviço, especialmente no contexto das telecomunicações, o fornecimento do Aviso de Privacidade ao longo da jornada do usuário, em seu contrato, durante o atendimento ou acessível por meio de informações visíveis em caso de atendimento presencial (como sinalizações com o QR Code para o Aviso de Privacidade), é suficiente para assegurar o dever de transparência.

Em relação ao princípio da necessidade, como visto no questionamento nº 5, ele não se refere a absoluta essencialidade, mas na necessidade de que a atividade de tratamento seja “uma forma direcionada e proporcional” de alcançar a finalidade do tratamento.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

O reconhecimento facial não será mecanismo apropriado quando existirem meios adequados e proporcionais para se alcançar o mesmo resultado sem uso dessa tecnologia, especialmente se houver forma de tratamento menos intrusiva e capaz de atender à finalidade pretendida, inclusive outras formas de autenticação biométrica. Em outras palavras, o reconhecimento facial deve ser evitado sempre que métodos alternativos possam garantir nível de identificação equivalente, ou minimamente suficiente diante dos riscos envolvidos.

Particularmente, o setor das telecomunicações pode contribuir significativamente com a verificação da identidade do titular:

- Desenvolvendo soluções de prevenção a fraudes baseadas em dados originados do setor, por exemplo, verificar se o número de telefone e outras informações de contato coincidem com os registros das operadoras, confirmar se a localização de uma transação corresponde à localização do dispositivo do titular e identificar indícios de práticas fraudulentas, como o SIM Swap.
- Utilizar seu conhecimento especializado em tecnologias de captação e transmissão de voz para desenvolver formas de verificação da identidade baseadas em validação biométrica da voz – as quais podem ser consideradas menos intrusivas do que a biométrica facial, vez que tende a permitir a inferência de menos dados pessoais sensíveis (como dados de saúde ou etnia) do que a biometria facial.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?



Como já apontado no questionamento de nº 5, com base nos posicionamentos do ICO, INAI e da Autoridade de Dados da Coreia, estas são as medidas de segurança que entendemos essenciais para a proteção de dados biométricos:

- Controles de acesso aos dados;
- Implementação de política de segurança da informação;
- Quando houver contratação de fornecedor, realização de processo adequado de *due diligence*.

Em relação aos parâmetros mínimos a serem adotados para a mensuração e o monitoramento de riscos de segurança, não entendemos existir diferença entre a metodologia empregada no contexto da biometria facial e as práticas adotadas para outros riscos de cibersegurança. Nesse sentido, alguns parâmetros básicos são:

- a. **Definir critério de riscos:** estabelecer, com base no apetite de risco organizacional, as regras e os parâmetros para aceitação de riscos;
- b. **Identificar os Riscos:** contemplando identificar os(as): i) ativos envolvidos; ii) ameaças potenciais a esses ativos; iii) controles existentes; e iv) vulnerabilidades.
- c. **Analisar os riscos:** identificar os potenciais consequências decorrentes da concretização dos riscos e a probabilidade de sua ocorrência, definindo, por meio de ambos os elementos, o nível do risco.
- d. **Tomar decisão:** avaliar, de acordo com o critério de riscos, se ele é aceitável e tomar uma decisão – isto é, modificar (mitigar), reter (aceitar), compartilhar ou evitar (eliminar) o risco.
- e. **Monitoramento:** é necessário que os elementos que compuseram a identificação do risco sejam monitorados, para que, em caso de sua modificação (por exemplo, o surgimento de nova ameaça) os efeitos desta alteração sejam computados na análise do risco.

Em relação ao primeiro questionamento (isto é, quais boas práticas devem ser observadas para garantir que a limitação não configure discriminação ilícita ou abusiva), reiteramos os pontos já descritos no questionamento nº 8.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Em relação ao primeiro questionamento, entendemos que, além das medidas já indicadas no questionamento nº 8, é fundamental considerar a acessibilidade da ferramenta utilizada (por exemplo, indivíduos com deficiência visual podem ter significativa dificuldade na utilização de soluções dessa natureza) [1]⁹.

Assim, é importante que as organizações ponderem esse desafio de acessibilidade e busquem a adoção de mecanismos para mitigá-los. Por exemplo, em situações nas quais seja possível

⁹ <https://www.vice.com/en/article/facial-recognition-apps-are-leaving-blind-people-behind/>. Acesso em 12.06.2025



confirmar a deficiência visual do indivíduo, buscar, excepcionalmente, fornecer processos alternativos de autenticação, ainda que não ofertem o mesmo grau de proteção.

Solução adequada para garantir a acessibilidade na adoção de mecanismos alternativos pode ser encontrada no desenvolvimento de soluções de prevenção a fraude com base em dados de telecomunicação, especialmente os apresentados no questionamento de nº 10 – os quais, além de representar mecanismos menos intrusivos do que a biometria facial tipicamente utilizada, se perfazem suficientemente adequados para grande parte dos riscos apresentados por produtos, serviços e funcionalidades não essenciais.

Nesse sentido, recordamos que dados do setor de telecomunicação, conforme elencado pela própria ANATEL, já são utilizados para auxiliar instituições financeiras a detectar fraudes: “para prevenir fraudes no sistema financeiro, as prestadoras disponibilizam informações para os bancos, possibilitando que adotem providências preventivas relativas às movimentações financeiras atreladas ao número do celular envolvido em troca de chip” [2]¹⁰.

Entendemos que a recusa em fornecer a biometria implicaria em exercício de fato do direito de oposição. Consequentemente, o não oferecimento da funcionalidade, serviço ou produto resguardado pelo acesso biométrico será lícito se uma das seguintes condições for satisfeita: (a) não seja faticamente possível ofertar a funcionalidade sem o tratamento de dados biométricos, aplicando-se aqui o mesmo descrito quanto ao consentimento; **ou** (b) os direitos e interesses protegidos ao se exigir a biometria não sejam sobrepujados pelo direito do titular de não a ofertar – isto é, existe razão pela qual a validação biométrica é necessária, como a existência de bem protegido relevante[3]¹¹ – é o caso típico dos serviços de telecomunicação, cuja fraude, nos termos já vistos, são comumente meio para condutas criminosas significativamente mais lesivas, para o titular afetado ou para a sociedade globalmente considerada – seja obtendo indevidamente a linha do titular para obter acesso a outros bens e serviços vinculados a ela, inclusive serviços bancários, seja se utilizando da linha fraudulentamente obtida para a práticas de crimes, incluindo fraudes movidas a engenharia social.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Retomamos as respostas já oferecidas aos questionamentos nºs 2, 5, 8 e 11.

Em relação aos mecanismos adequados de proteção, além da necessidade de avaliação de riscos de cibersegurança, seguindo os passos já elencados no questionamento de nº 11, reforçamos os controles apontados no questionamento de nº 8, com base nos guias de diversas autoridades de dados (ICO, INAI, Autoridade de Dados da Coreia)

Em relação às medidas de transparência, a obrigatoriedade legal se refere ao fornecimento das informações previstas no art. 9º, da LGPD. A forma adequada de disponibilização dessas informações, conforme indicado nos questionamentos nºs 2 e 8, com base no posicionamento do ICO, dependerá de uma série de fatores – como o caso de uso, a natureza do relacionamento com o titular e os elementos envolvidos na atividade de tratamento.

¹⁰ <https://www.gov.br/anatel/pt-br/assuntos/dicas-contras-fraudes/golpes-atuais-mais-comuns>. Acesso em 13.06.2025

¹¹ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>. Acesso em 12.06.2025



Em síntese, quanto mais evidente for a atividade de tratamento analisada – considerando, inclusive, as práticas habituais de mercado e obrigações regulatórias –, menor será a exigência de adoção de práticas ativas de transparência para o fornecimento das informações legalmente requeridas ao titular. A título exemplificativo, dadas as obrigações regulatórias que atingem o setor de telecomunicações, as práticas habituais de mercado e os riscos já abordados relacionados a ocorrência de fraudes no setor e a própria divulgação do uso de biometria facial no setor pela própria ANATEL, entendemos que a disponibilização do Aviso de Privacidade é suficiente para atender as obrigações regulatórias em proteção de dados.

Por fim, em relação ao risco de discriminação, reiteramos as medidas já apontadas no questionamento de nº 8, baseadas no posicionamento do ICO.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Para além das práticas de transparência já expostas nos questionamentos anteriores, entendemos que o atendimento aos direitos dos titulares deve ser assegurado, considerando as especificidades da tecnologia biométrica.

Em relação ao direito de acesso, conforme o ICO [1]¹², há dificuldade técnica em fornecer os dados biométricos propriamente ditos, uma vez que, em geral, são *outputs* matemáticos complexos, não compreensíveis (“ilégíveis”) por seres humanos. Diante disso, o fornecimento pode ser substituído por uma declaração explicativa, que:

- (a) justifique a impossibilidade de entrega direta do dado;
- (b) descreva a natureza do dado em questão; e
- (c) esclareça como esse dado é mantido pela organização.

¹² <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>. Acesso em 12.06.2025

São Paulo, 31 de julho de 2025.

Para: Autoridade Nacional de Proteção de Dados - ANPD

De: Telefônica Brasil S.A.

Ref.: Tomada de Subsídios: Dados pessoais sensíveis - Dados biométricos

Telefônica Brasil, uma das principais operadoras de telecomunicações do país, apresenta à ANPD suas contribuições à Tomada de Subsídios¹ sobre o tratamento de dados biométricos. Nosso objetivo é colaborar na definição de diretrizes práticas e equilibradas, que atendam à realidade operacional das empresas brasileiras e reforcem a proteção dos titulares.

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Entendemos que é fundamental que a definição de dado biométrico, conforme prevista na Lei Geral de Proteção de Dados Pessoais ("LGPD"), seja guiada por critérios claros e objetivos e sempre atrelada à exigência prevista no próprio inciso II do artigo 5º da LGPD ("vinculado a uma pessoa natural"). Isso ajuda tanto a proteger os direitos dos titulares quanto a dar segurança jurídica para quem trata esses dados no dia a dia - empresas, órgãos públicos e demais organizações.

Com base no artigo 5º, inciso II, da LGPD, entende-se que três elementos cumulativos devem estar presentes para que determinada informação seja caracterizada como dado biométrico:

- a) Características físicas, fisiológicas ou comportamentais de uma pessoa natural:** o dado deve derivar de atributos únicos e inerentes ao indivíduo, como impressões digitais, traços faciais únicos, padrões da íris, timbre específico de voz, forma de caminhar ou dinâmica de digitação (*keystroke dynamics*). Esses elementos são capazes de identificar uma pessoa de maneira exclusiva, especialmente quando processados por tecnologias específicas de reconhecimento. Essa definição está alinhada ao artigo 4º, item 14², do Regulamento Geral sobre a Proteção de Dados (GDPR), que considera dados biométricos aqueles resultantes de tratamento técnico relacionado a características físicas, fisiológicas ou comportamentais que permitam a identificação única de uma pessoa natural. O Information Commissioner's Office (ICO) do Reino Unido também adota entendimento semelhante, reconhecendo como dados biométricos tanto

¹ Disponível em <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-tratamento-de-dados-biometricos>.

² Article 4(14), General Data Protection Regulation – GDPR: “‘Biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.”

atributos físicos estáticos (como impressões digitais e imagens faciais), quanto padrões comportamentais mensuráveis, desde que utilizados com finalidade identificatória³.

- b) Uso de tecnologia para análise ou tratamento:** essas características só se tornam de fato biométricas quando são tratadas por meios técnicos específicos, como softwares de reconhecimento facial ou sistemas de autenticação por voz. Por exemplo, uma simples foto não é um dado biométrico por si só, mas pode se tornar, caso seja usada por um sistema de reconhecimento facial.

Esse entendimento inclusive é destacado pelo ICO: *“Embora as características físicas de alguém possam ser mostradas em uma foto, isso não é suficiente para tornar essa foto um dado biométrico. É apenas quando algo mais acontece com essa foto – uma operação de tratamento específica ou conjunto de operações que resulta em algo que permite ou confirma a identificação única de alguém – que o resultado se torna um dado biométrico. Por exemplo, se técnicas específicas são aplicadas à foto para extrair as características faciais de alguém, então a foto foi ‘tratada através de meios técnicos específicos’ que permitem que a pessoa seja identificada de forma única”*⁴.

- c) Finalidade de identificar uma pessoa de forma única:** a intenção (ou o resultado prático) do uso desse dado deve ser identificar, autenticar ou rastrear uma pessoa específica. Se a informação é usada apenas para fins estatísticos, por exemplo, e não permite individualização, esta não será considerada dado pessoal nem tampouco dado biométrico.

Consideramos importante que as empresas tenham flexibilidade para interpretar e aplicar esses critérios de acordo com suas realidades operacionais específicas, sempre respeitando os princípios da LGPD. Um ambiente regulatório que permita essa flexibilidade interpretativa favorece a inovação responsável e a adequação proporcional às diferentes realidades empresariais do país.

É importante ressaltar que dados biométricos não devem ser considerados intrinsecamente perigosos ou de alto risco. O nível de risco está diretamente relacionado ao contexto de uso, finalidade, escala do tratamento e salvaguardas implementadas. Uma impressão digital usada para desbloquear um celular pessoal apresenta riscos muito diferentes de um sistema de reconhecimento facial em espaços públicos. A regulamentação deve reconhecer essas distinções contextuais ao invés de adotar uma abordagem única para toda e qualquer utilização de dados biométricos.

³ Disponível em

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/#scd4>

⁴ Cf. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/>.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Entendemos que o princípio da transparência é fundamental quando se trata de dados sensíveis como os biométricos. Contudo, é essencial que as práticas de transparência sejam proporcionais ao porte da empresa, ao contexto do tratamento e aos riscos envolvidos.

Recomenda-se que os controladores adotem medidas de transparência adequadas à sua realidade operacional, podendo incluir:

- a) disponibilização de informações claras em seus canais habituais de comunicação com os titulares, seja através de políticas de privacidade, avisos ou outros meios já utilizados pela empresa;
- b) linguagem adaptada ao público-alvo, respeitando o princípio da inteligibilidade sem criar obrigações excessivas de produção de múltiplos materiais; e
- c) canais de atendimento já existentes na empresa para esclarecimento de dúvidas, com indicação do canal de contato do Encarregado de Proteção de Dados (DPO), conforme previsto no art. 41 da LGPD.

É importante que a regulamentação permita às empresas escolherem os meios mais eficazes de comunicação com seus públicos, evitando prescrever métodos específicos que podem não ser adequados a todos os contextos empresariais.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Entendemos que a biometria comportamental constitui uma vertente emergente e especialmente complexa do tratamento de dados biométricos, por sua natureza dinâmica, contextual e, muitas vezes, coletada de forma passiva e contínua.

Em contraste com a biometria tradicional (como impressões digitais, reconhecimento facial e de íris), que se apoia em traços corporais relativamente estáveis e de coleta pontual, a biometria comportamental opera com variabilidade temporal e reflete o contexto situacional em que o dado é gerado.

Diante dessas especificidades, mas também considerando que a LGPD não traz distinção entre essas modalidades de biometria, entendemos que a regulamentação deve permitir flexibilidade para que as empresas possam desenvolver suas próprias abordagens de governança, contemplando:

- a) a possibilidade de realizar avaliações de risco internas quando a empresa julgar necessário, especialmente em casos de maior complexidade;

- b) transparência adequada ao contexto, permitindo que as empresas expliquem o uso desses dados de forma proporcional ao público e ao risco;
- c) desenvolvimento de alternativas conforme a viabilidade técnica e operacional de cada empresa.

Entendemos que a regulamentação deve promover um equilíbrio entre o incentivo à inovação tecnológica e a proteção adequada dos dados pessoais, sem criar barreiras desnecessárias ao desenvolvimento de novas tecnologias.

BLOCO II - HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Entendemos que o consentimento, quando utilizado como base legal para o tratamento de dados pessoais sensíveis, deve observar os requisitos legais estabelecidos no art. 5º, XII e no art. 8º da LGPD.

Entretanto, reconhecemos que existem contextos nos quais outras bases legais podem ser mais apropriadas, especialmente quando há necessidade de proteção contra fraudes ou quando o consentimento poderia comprometer a eficácia de medidas de segurança.

Entendemos que a escolha da base legal mais adequada deve considerar aspectos específicos de cada caso concreto e ficar a critério do controlador, que possui melhor conhecimento de sua operação e dos riscos envolvidos, sempre respeitando os princípios da LGPD e documentando adequadamente suas decisões.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de "garantia da prevenção à fraude" (art. 11, II, "g", LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Entendemos que a base legal da "garantia da prevenção à fraude" (art. 11, II, "g", da LGPD) é a hipótese jurídica mais adequada e proporcional para sustentar o uso de dados biométricos em diversos contextos legítimos de identificação e autenticação de titulares, especialmente em operações de risco elevado, como transações bancárias, contratações digitais, ativação de chips, validação de identidade em serviços financeiros e telecomunicações.

Em um país como o Brasil, que enfrenta índices altíssimos e crescentes de tentativas de fraude digital, inclusive com uso de identidades falsas, biometria forjada e engenharia social, a adoção de tecnologias biométricas confiáveis é indispensável para proteger o próprio titular contra danos, como roubo de identidade, contratação indevida de serviços ou movimentações financeiras não autorizadas.

Nesse cenário, limitar o uso da biometria em nome de uma suposta intrusividade, sem considerar o risco real e atual do mercado brasileiro, representa retrocesso regulatório e compromete diretamente a segurança jurídica e operacional de soluções que hoje são amplamente aceitas e valorizadas pelos próprios consumidores.

Para a adequada aplicação dessa base legal, sugerimos que as empresas possam:

- a) Documentar internamente a análise de necessidade do uso de biometria, considerando o contexto específico de suas operações e os riscos de fraude enfrentados;
- b) Estabelecer políticas internas sobre o uso e proteção desses dados, com limitações de acesso, finalidade e compartilhamento;
- c) Implementar medidas de segurança proporcionais ao risco, incluindo criptografia e controles de acesso adequados;
- d) Manter transparência com os titulares sobre o uso de seus dados para prevenção à fraude.

A flexibilidade regulatória nesse aspecto é fundamental para permitir que as empresas continuem protegendo eficazmente seus clientes contra fraudes cada vez mais sofisticadas.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o "cumprimento de obrigação legal ou regulatória" (art. 11, II, "a", LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Entendemos que quando o tratamento de dados biométricos for realizado para cumprimento de obrigação legal ou regulatória, a legitimidade da base legal não afasta a necessidade de observância aos demais princípios da LGPD.

Para garantir o uso adequado dessa base legal, é importante que os controladores interpretem de forma razoável o escopo das obrigações legais, levando em consideração tanto o texto quanto o espírito da lei, bem como mantenham documentação sobre as obrigações legais que fundamentam o tratamento e implementem medidas de segurança adequadas ao contexto.

Entendemos que deve haver espaço para que as organizações avaliem, de acordo com sua realidade, as melhores formas de cumprir suas obrigações legais respeitando os direitos dos titulares.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, "c", LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Entendemos que o uso de dados biométricos para pesquisa deve respeitar os princípios da LGPD, especialmente quando há risco de reidentificação.

As organizações de pesquisa devem ter flexibilidade para implementar salvaguardas apropriadas ao contexto de suas pesquisas, podendo incluir técnicas de anonimização ou pseudonimização

adequadas ao risco; protocolos éticos quando apropriado ao tipo de pesquisa; medidas contratuais para proteção dos dados, e segurança da informação proporcional ao risco.

É importante que a regulamentação não crie barreiras desnecessárias à pesquisa científica legítima, permitindo que os órgãos de pesquisa desenvolvam suas próprias abordagens de proteção de dados.

BLOCO III - TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Entendemos que o reconhecimento facial é uma tecnologia legítima e valiosa quando utilizada adequadamente, especialmente para fins de segurança e prevenção à fraude.

Para seu uso responsável, as organizações devem ter autonomia para:

- a) avaliar internamente quando o uso da tecnologia é apropriado para seus objetivos legítimos;
- b) definir finalidades específicas de uso conforme suas necessidades operacionais;
- c) implementar controles proporcionais ao contexto de uso; e
- d) desenvolver processos de melhoria contínua conforme apropriado.

Entendemos que uma abordagem baseada em princípios, ao invés de requisitos prescritivos, permite melhor adaptação às diversas realidades empresariais e evolução tecnológica.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Entendemos que a qualidade dos sistemas de reconhecimento facial deve ser uma preocupação das organizações que os utilizam, considerando seus contextos específicos de aplicação.

As empresas devem ter flexibilidade para desenvolver ou adquirir sistemas adequados às suas necessidades; estabelecer níveis de precisão apropriados ao risco envolvido; implementar processos de melhoria conforme identificarem necessidades; e oferecer canais de correção quando apropriado ao contexto.

É importante que a regulamentação não estabeleça padrões técnicos rígidos que possam rapidamente se tornar obsoletos ou inadequados para diferentes usos legítimos da tecnologia.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao

reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Entendemos que o reconhecimento facial é uma ferramenta tecnológica eficaz e legítima para fins de autenticação e segurança. Sua utilização, quando bem empregada, contribui significativamente para a proteção do titular - prevenindo fraudes, acessos indevidos e prejuízos financeiros, inclusive para os próprios titulares - e para a eficiência operacional de serviços digitais amplamente utilizados pela população.

As organizações devem ter autonomia para avaliar quando o reconhecimento facial é a tecnologia mais apropriada para seus objetivos legítimos de negócio, considerando (i) o nível de segurança necessário; (ii) a experiência do usuário; (iii) a viabilidade técnica e econômica de alternativas; (iv) a eficácia concreta e a facilidade de utilização de alternativas (que muitas vezes não alcançam os mesmos objetivos com qualidade), e (v) o contexto específico de uso.

A escolha da tecnologia mais adequada deve permanecer com quem melhor conhece os riscos e as necessidades operacionais específicas de cada contexto.

BLOCO IV - SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Entendemos que as organizações devem ter flexibilidade para implementar medidas de segurança proporcionais ao seu porte, volume de dados tratados e riscos específicos de suas operações.

Recomenda-se uma abordagem baseada em risco, na qual:

- a) A avaliação de risco considere o contexto específico de uso, reconhecendo que dados biométricos não apresentam riscos intrínsecos elevados, mas sim riscos variáveis conforme sua aplicação, escala e finalidade;
- b) Relatórios de Impacto (RIPDs) sejam realizados quando a organização identificar riscos realmente elevados, e não como requisito universal para qualquer uso de biometria;
- c) Políticas de controle de acesso sejam desenvolvidas de acordo com a estrutura e necessidades de cada organização; e
- d) Medidas de segurança sejam proporcionais ao contexto, evitando requisitos únicos que possam ser excessivos para pequenas empresas ou inadequados para grandes operações.

Entendemos que prescrever medidas específicas como "indispensáveis" pode criar custos desnecessários e inadequados para muitas organizações, especialmente as de menor porte.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva?

Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Entendemos que as organizações devem ter autonomia para determinar quando a biometria é tecnicamente necessária para determinadas funcionalidades, especialmente em contextos de segurança e prevenção à fraude.

É importante reconhecer que: a) em setores com alta incidência de fraude, a biometria pode ser essencial para proteger tanto a empresa quanto os próprios usuários; b) as empresas devem poder comunicar claramente quando certas funcionalidades dependem de autenticação biométrica por razões técnicas ou de segurança; e c) a decisão sobre oferecer alternativas deve considerar a viabilidade técnica, a eficácia concreta dessas alternativas (que muitas vezes não têm a mesma qualidade de soluções que fazem uso de biometria) e os riscos envolvidos.

A regulamentação deve respeitar a autonomia empresarial para fazer escolhas tecnológicas que protejam adequadamente seus usuários e suas operações.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Entendemos que as organizações devem desenvolver práticas de proteção de dados adequadas à sua realidade operacional.

Recomenda-se que as empresas integrem a governança de dados biométricos em suas políticas gerais de proteção de dados, evitando a necessidade de criar documentos e estruturas separadas, utilizem suas estruturas existentes de privacidade e proteção de dados, incluindo o DPO já designado e comuniquem adequadamente sobre o uso de biometria em suas políticas de privacidade existentes.

É importante evitar a criação de requisitos burocráticos adicionais que não agreguem valor real à proteção dos dados, mas apenas custos operacionais.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos -- como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

Entendemos que em contextos de tratamento de grande volume de dados, as organizações devem buscar soluções de transparência proporcionais e viáveis operacionalmente.

Sugere-se flexibilidade para que as organizações possam utilizar os canais de comunicação mais eficazes para cada contexto; desenvolver abordagens de transparência que sejam operacionalmente viáveis; e implementar mecanismos de exercício de direitos adequados à escala da operação.

É fundamental que a regulamentação reconheça os desafios práticos desses contextos e permita soluções proporcionais.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Entendemos que as organizações devem poder utilizar seus canais e processos existentes de atendimento aos titulares para garantir o exercício de direitos relacionados a dados biométricos.

Recomenda-se permitir que as empresas integrem o atendimento sobre dados biométricos em seus canais já estabelecidos; utilizem tecnologias que já possuem para facilitar o exercício de direitos; e desenvolvam processos proporcionais ao volume e contexto de suas operações.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

Entendemos que o uso de biometria em ambientes educacionais pode ser justificado quando visa à segurança e proteção das crianças.

As instituições devem ter flexibilidade para comunicar-se com pais e responsáveis por meio dos canais já utilizados pela escola, bem como avaliar a necessidade do uso de biometria conforme sua realidade específica, além de implementar medidas de proteção proporcionais ao seu porte e recursos.

É importante não criar requisitos que inviabilizem o uso legítimo da tecnologia por instituições educacionais, especialmente as de menor porte.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Reconhecemos que o uso de biometria por instituições educacionais é uma realidade crescente e muitas vezes necessária para segurança.

Deve-se permitir flexibilidade para que as instituições escolham a base legal mais apropriada para sua situação, sempre implementando medidas de segurança proporcionais ao seu porte e capacidade, e desenvolvam processos de comunicação adequados à sua comunidade escolar.

É importante que a regulamentação reconheça as diferentes realidades das instituições educacionais brasileiras e não imponha requisitos uniformes que possam ser inadequados ou excessivamente onerosos.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Entendemos que o uso de dados biométricos para verificação de idade representa uma solução tecnológica importante e eficaz para a proteção de crianças e adolescentes no ambiente digital.

As empresas devem ter autonomia para implementar soluções de verificação de idade adequadas aos riscos de suas plataformas (evitando-se, assim, uma única solução padronizada que pode não ser adequada a certos serviços), bem como escolher tecnologias que equilibrem eficácia e privacidade e desenvolver abordagens proporcionais ao conteúdo oferecido.

Entendemos que a verificação eficaz de idade é fundamental para proteger menores de conteúdos inadequados, e a biometria pode ser uma ferramenta legítima quando utilizada com as devidas salvaguardas e apenas para as finalidades descritas. As empresas devem poder avaliar quando seu uso é a melhor solução disponível para cumprir esse objetivo de proteção, que está alinhado com o princípio do melhor interesse dos menores.

São Paulo, 1 de agosto de 2025

À

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Coordenação Geral de Normatização – CGN/ANPD

Ref.: Tomada de Subsídios: dados pessoais sensíveis - dados biométricos (“Tomada de Subsídios”).

Prezado Sr. Coordenador Geral de Normatização,

A B3 S. A. – Brasil, Bolsa, Balcão (“B3”) submete a esta Autoridade de Proteção de Dados Pessoais (“ANPD”) seus comentários à Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos, que foi organizada em cinco blocos: (i) Definições e princípios; (ii) Hipóteses legais; (iii) Tecnologias de reconhecimento facial (FRTS) e aplicação de tecnologias emergentes e inovadoras no tratamento de dados biométricos; (iv) Segurança, governança e boas práticas e (v) Direitos dos titulares e grupos vulneráveis. A participação da B3 está restrita aos tópicos nos quais ela considera apta a contribuir.

Bloco 1 – PRINCÍPIOS DA LGPD

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Para caracterizar um dado pessoal como dado biométrico, é necessário verificar a finalidade do tratamento desse dado. Não é eficaz estabelecer uma lista exaustiva dos dados que devem ser considerados biométricos, devido à constante evolução tecnológica no tratamento dessas informações. Propõe-se a conceituação de dado biométrico como o dado que é tratado com a finalidade de identificação de uma

pessoa natural, medindo características físicas, biológicas, fisiológicas e/ou comportamentais únicas de um indivíduo. São características do dado biométrico:

- Origem biológica, fisiológica ou comportamental: o dado biométrico é derivado de características físicas ou comportamentais do indivíduo.
- Único: o dado biométrico é unicamente atribuível ao indivíduo.
- Inalterável: o dado biométrico não é facilmente alterável, exceto em situações excepcionais de acidentes, intervenções cirúrgicas, procedimentos invasivos ou situações semelhantes.
- Inequívoco: o dado biométrico pode ser atribuído ao titular de dados pessoais de forma precisa, sem margem para ambiguidade.

A ISO/IEC 2382-37:2022, norma que estabelece uma descrição sistemática de conceitos biométricos relativos ao reconhecimento de seres humanos, conceitua a característica biométrica pautada na finalidade de tratamento, qual seja: a característica biológica e comportamental de um indivíduo da qual podem ser extraídas atributos biométricos distinguíveis e repetíveis, para a finalidade de reconhecimento biométrico, como por exemplo: topografia do rosto, textura da pele facial, estrutura de íris, padrão retiniano, dentre outros.

Em sentido semelhante e pautada na finalidade do tratamento, prevê o Regulamento Geral de Proteção de Dados da União Europeia, definindo como dados biométricos “aqueles resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única da pessoa singular, nomeadamente imagens faciais ou dados datiloscópicos”.

Por exemplo, a coleta de digitais de um indivíduo para controle de acesso a um prédio deve ser considerado tratamento de dados biométricos, visto que é tratado com a finalidade de medir características físicas, biológicas e fisiológicas únicas do indivíduo, para controle de acesso a um espaço. Já a foto presente em um crachá não deve ser considerado tratamento de dado biométrico, visto que não é tratado

com a finalidade de medir características físicas, biológicas e fisiológicas únicas do indivíduo.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

As práticas de transparência ativa a serem exigidas dos controladores para o tratamento de dados pessoais biométricos devem ser as já previstas na legislação, conforme disposto no artigo 9º da Lei Geral de Proteção de Dados – Lei Nº 13.709/2018 (“LGPD”), ou seja, o acesso facilitado, de forma clara, adequada e ostensiva às seguintes informações:

- i. Finalidade específica do tratamento;
- ii. Forma e duração do tratamento;
- iii. Identificação do controlador;
- iv. Informações de contato do controlador;
- v. Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- vi. Responsabilidade dos agentes que realizarão o tratamento;
- vii. Direitos dos titulares.

Quando o tratamento de dados biométricos se basear no consentimento, além das informações mencionadas acima, é necessário garantir transparência durante a coleta, informando de maneira clara e específica sobre a finalidade do uso desses dados. Pautado nesta base legal, caso os dados sejam tratados para outras finalidades e compartilhados com outros controladores, além da necessidade de coleta de uma nova autorização específica para este compartilhamento, considera-se uma boa prática a transparência de quem são esses outros agentes.

Além disso, deve-se dar transparência da identidade e canal de contato do Encarregado de Proteção de Dados. A transparência para o tratamento de dados

peçoais biométricos não necessariamente deve constar em documento apartado e específico para esta operação de tratamento de dados, podendo constar no âmbito de Políticas de Proteção de Dados ou documentos congêneres.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Para o tratamento do tema, deve-se conceituar a biometria comportamental e biometria tradicional:

- Biometria comportamental: conjunto de técnicas de autenticação ou identificação baseadas em padrões dinâmicos e recorrentes de comportamento individual relacionados a forma de interação do indivíduo com sistemas ou ambientes. Exemplos: padrões de digitação, padrões de uso de dispositivos, movimentação corporal, assinatura dinâmica, etc.
- Biometria tradicional: conjunto de técnicas de identificação pessoal baseadas em características físicas únicas e invariáveis de um indivíduo, tais como: impressão digital, reconhecimento facial, padrões de natureza morfológica ou fisiológica, utilizadas para fins de verificação ou autenticação de identidade.

É necessário estabelecer uma distinção no tratamento de dados biométricos tradicionais e dados biométricos comportamentais. Conforme conceito acima sugerido, os dados biométricos comportamentais não devem ser compreendidos como dados sensíveis.

Para garantir a qualidade dos dados biométricos comportamentais, considerando que estes mudam com mais facilidade ao longo da vida do titular, diferentemente dos dados biométricos tradicionais, deve-se realizar o tratamento dos dados durante o período em que o dado se mantém relevante e com acurácia.

como sanções ou consequências adversas a descontinuidade de acesso a determinado sistema, local, software ou serviço sem que os dados biométricos possam ser confirmados ou tratados. Quanto ao consentimento, é recomendável que seja destacado, podendo, contudo, fazer parte do mesmo documento em que sejam estabelecidas as demais cláusulas contratuais ou termos de uso, desde que seja facilitada sua identificação e compreensão. Mecanismos claros, como caixas de seleção não pré-marcadas, podem, facultativamente, ser utilizados para que o titular manifeste sua autorização de forma afirmativa.

A transparência deve ser mantida ao fornecer todas as informações necessárias para que o titular compreenda plenamente como seus dados biométricos serão tratados. É importante manter o titular informado sobre quaisquer mudanças nas políticas de tratamento de dados ou nas específicas para quais dados são utilizados, garantindo uma comunicação contínua e atualizada.

Ressalte-se que, em determinados contextos, o consentimento não é uma possibilidade legal adequada para o tratamento de dados biométricos. Conforme previsto na legislação, o tratamento de dados pessoais realizado com base no consentimento deve ser interrompido quando na retirada deste por parte do titular de dados. Ocorre que em determinadas situações a retirada do consentimento pode inviabilizar a continuidade de determinadas relações. Por exemplo: em uma aplicação bancária para celular, para acesso e realização de transações financeiras é necessário validação facial para garantir que o titular da conta é de fato quem está utilizando a aplicação, autenticando o acesso ao sistema com segurança e prevenindo fraudes. Em situações como essa, a exigência de consentimento compromete tanto a funcionalidade do aplicativo bancário quanto a segurança do ambiente, pois revogar o consentimento impossibilitaria seu uso.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a

finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A legislação prevê que o tratamento de dados pessoais sensíveis para garantia de prevenção à fraude e segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos deve ser realizado resguardando os direitos dos titulares, exceto se prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Conforme disposto no “Guia do Legítimo Interesse da ANPD”, tanto a base legal do legítimo interesse como da prevenção à fraude e segurança do titular são bases legais que devem ser utilizadas. Portanto, dentre os critérios e salvaguardas que devem ser observados no tratamento de dados biométricos para a prevenção de fraudes e a segurança do titular, a realização do Teste de Balanceamento deve ocorrer previamente à realização do tratamento.

O Teste de Balanceamento para tratamento de dados pessoais para prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos deve avaliar os seguintes requisitos: i) finalidade: verifica-se se o tratamento tem um propósito legítimo, específico e compatível com a lei, e se está baseado em interesse válido do controlador ou de terceiros; ii) necessidade: analisa-se se os dados usados são estritamente necessários para atingir a finalidade, evitando excessos e priorizando formas menos invasivas; iii) balanceamento e salvaguardas: compara-se o interesse do controlador com os direitos do titular, avaliando riscos e adotando salvaguardas para proteger os dados.

Portanto, a utilização da base legal referente à prevenção de fraudes e à segurança do titular no tratamento de dados biométricos poderá se dar se o Teste de Balanceamento demonstrar a compatibilidade com os direitos e liberdades fundamentais e com as legítimas expectativas dos titulares.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Nos casos em que o tratamento de dados biométricos decorre do cumprimento de obrigação legal ou regulatória, nos termos do art. 11, II, “a”, da LGPD, é fundamental que sejam observados critérios técnicos e jurídicos rigorosos para mitigação de riscos e garantia dos direitos dos titulares. Recomendam-se as seguintes diretrizes:

- Existência de obrigação regulatória expressa e justificável: O uso de dados biométricos deve estar claramente vinculado ao melhor cumprimento ou adequação da observância de uma obrigação legal ou regulatória específica (ex: normas da Receita Federal, BACEN, entre outras). Para isso, o controlador deve ser capaz de demonstrar que o tratamento e a coleta do dado biométrico são indispensáveis para o melhor cumprimento da norma a que está sujeito.
- Observância dos Princípios da LGPD: Ainda que exista uma obrigação legal, o tratamento deve respeitar os princípios previstos na LGPD, especialmente: 1) finalidade: o dado biométrico só pode ser tratado para atender à obrigação específica ou dela decorrente; 2) necessidade: deve ser avaliado se não há alternativa menos intrusiva para cumprir a obrigação; 3) segurança e prevenção: devem ser adotadas medidas para evitar acessos não autorizados, vazamentos ou uso indevido; 4) transparência com os titulares: O controlador deve garantir que os titulares tenham acesso à informação, de maneira clara e acessível, sobre a finalidade do uso de dados biométricos, a base legal que fundamenta o tratamento, os direitos assegurados e como exercê-los e a quem recorrer em caso de dúvidas ou reclamações.

- **Minimização e Limitação de Retenção:** os dados biométricos devem ser coletados e armazenados apenas na medida estritamente necessária e eliminados assim que deixarem de ser exigidos pela obrigação legal ou regulatória correspondente. Além disso, só devem ser acessíveis apenas por profissionais autorizados, com registro e controle de acesso.
- **Cautela no uso para Outras Finalidades:** A reutilização dos dados biométricos para fins distintos daqueles para os quais foram tratados para atendimento de obrigação legal só será possível se houver nova base legal compatível com a nova finalidade.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Para garantir que o uso de tecnologias de reconhecimento facial esteja de acordo com os princípios da necessidade, proporcionalidade e transparência, as organizações devem adotar diversas práticas essenciais desde a concepção até a operação contínua desses sistemas.

Sugere-se a realização de avaliações de impacto sobre a proteção de dados antes da implementação da tecnologia de reconhecimento facial. Essas avaliações identificam e mitigam riscos, assegurando que a coleta e o tratamento de dados biométricos sejam justificados e proporcionais aos objetivos perseguidos. Além disso, deve-se aplicar a limitação por escopo e contexto, utilizando a tecnologia

apenas quando estritamente necessário e comprovadamente mais eficaz que outros métodos disponíveis.

Para minimizar vieses e promover a equidade, é justo treinar os algoritmos com conjuntos de dados diversificados, representando diferentes etnias, gêneros, idades e condições ambientais. Paralelamente, a proteção dos vetores faciais deve ser garantida através de criptografia robusta, armazenamento segregado e restrição rigorosa de acesso, protegendo os dados biométricos contra acessos não autorizados.

A governança dos modelos de IA deve abranger o monitoramento das atualizações dos algoritmos, a clareza dos resultados produzidos e a documentação minuciosa das decisões automatizadas. Isso garante que as atualizações preservem a integridade do sistema e que os resultados sejam claros e compreensíveis para os usuários.

Implementar auditorias periódicas é essencial para avaliar a eficácia e a conformidade com os princípios da LGPD. Essas auditorias monitoram o desempenho do sistema, identificam falhas e garantem que as práticas de tratamento de dados estejam alinhadas com as normas legais e éticas. Além disso, auditoria e rastreabilidade exigem a manutenção de logs completos das capturas, decisões e acessos ao sistema, facilitando a identificação e correção de irregularidades.

A transparência no tratamento de dados deve ser promovida através da publicação de informações claras sobre como e por que os dados biométricos são coletados e utilizados. Comunicações acessíveis fortalecem a confiança dos usuários, permitindo que compreendam os benefícios e as implicações do uso da tecnologia. Além disso, disponibilizar canais para relatar abusos ou discriminação é essencial para que os usuários possam expressar preocupações e denunciar irregularidades de forma eficaz.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Para projetar e implementar sistemas de reconhecimento facial que garantam alta eficácia e confiabilidade, minimizando erros de identificação como falsos positivos e negativos, é essencial adotar uma abordagem abrangente desde a concepção até a operação contínua. Inicialmente, os sistemas devem ser submetidos a testes rigorosos antes de sua implementação. Esses testes envolvem a validação da precisão, utilizando conjuntos de dados diversificados que representem diferentes etnias, gêneros, idades e condições de iluminação para reduzir vieses e aumentar a robustez. Simulações de cenários reais ajudam a identificar e corrigir limitações antes do lançamento.

Após a implementação, é crucial estabelecer mecanismos de feedback contínuo que permitam a correção imediata de erros e a atualização dos algoritmos. Isso inclui a coleta de feedback dos usuários e a implementação de sistemas de monitoramento automatizado que detectem anomalias ou padrões de erro, facilitando ajustes rápidos e eficazes. Além disso, deve-se acompanhar e avaliar continuamente a performance do sistema através de indicadores de desempenho chave (KPIs), realizando análises regulares para manter altos níveis de precisão e eficácia.

Manter registros detalhados de todas as falhas e implementar um plano de resposta a incidentes eficaz é fundamental para a gestão de erros. Logs detalhados devem capturar a natureza e o contexto de cada falha, permitindo respostas rápidas e prevenindo recorrências através de análises pós-incidente.

Além disso, é fundamental implementar mecanismos de auditoria e explicabilidade para assegurar a transparência e a responsabilidade. Os sistemas precisam rastrear

as decisões automatizadas e oferecer justificativas claras para os resultados, o que aumenta a confiança dos usuários e facilita a conformidade com as regulamentações de proteção de dados. Auditorias independentes realizadas regularmente são essenciais para garantir a conformidade com as normas de segurança e privacidade, além de identificar oportunidades para a melhoria contínua.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Dado o impacto significativo de uma violação de dados biométricos, como o roubo de identidade, é essencial que as organizações adotem medidas de segurança técnicas e administrativas robustas para mitigar esses riscos e garantir a conformidade com a LGPD.

Medidas técnicas incluem o uso de criptografia forte para proteger dados biométricos tanto em armazenamento quanto em transmissão, assegurando que informações interceptadas permaneçam ilegíveis. Controles de acesso rigorosos devem ser implementados para limitar quem pode visualizar ou manipular esses dados, reduzindo riscos de exposição indevida. A segregação de redes que lidam com dados biométricos das demais redes corporativas impede que uma possível invasão afete diretamente esses sistemas sensíveis. Além disso, a realização regular de auditorias de segurança, testes de penetração e varreduras de vulnerabilidades ajuda a identificar e corrigir falhas antes que sejam exploradas por atacantes.

Medidas administrativas envolvem a definição de parâmetros mínimos para avaliação de riscos, como análises de impacto e monitoramento contínuo, permitindo uma gestão eficaz da segurança. É crucial desenvolver um plano de resposta a incidentes específico para violações de dados biométricos, garantindo

uma reação rápida e minimizando danos. O treinamento contínuo de conscientização em segurança para funcionários que lidam com esses dados também é fundamental para reduzir erros humanos que possam comprometer a integridade das informações.

Parâmetros de avaliação e monitoramento devem incluir a análise de impacto para entender o potencial dano de uma violação, bem como o monitoramento constante de anomalias e tentativas de acesso não autorizado. Revisões periódicas de conformidade com a LGPD asseguram que as práticas de tratamento de dados estejam alinhadas com os requisitos legais, evitando sanções e fortalecendo a confiança dos titulares. Relatórios detalhados de auditoria e compliance proporcionam transparência sobre as medidas de segurança adotadas e sua eficácia, enquanto a atualização constante das políticas de segurança garante que as defesas evoluam conforme novas ameaças e tecnologias surgem.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Em serviços não essenciais, a autenticação via biometria pode, ainda assim, ser o método mais seguro para a identificação do titular. Para evitar que essa escolha configure discriminação ilícita ou abusiva, é fundamental que as organizações adotem boas práticas que garantam a equidade e a transparência no uso de dados biométricos.

Os agentes de tratamento devem viabilizar formas de acesso tão seguras quanto a biometria, oferecendo alternativas não biométricas, como senhas tradicionais ou cartões de acesso. No entanto, caso a autenticação biométrica seja considerada essencial para a segurança do serviço, é importante informar claramente aos

titulares que a utilização desse método confere maior segurança ao processo de identificação, destacando seus benefícios adicionais.

Além disso, é crucial garantir que os titulares sejam plenamente informados sobre a necessidade do uso dos dados biométricos e as consequências de sua recusa em fornecê-los. A comunicação deve ser clara e acessível, explicando detalhadamente por que a autenticação biométrica é necessária para determinadas funcionalidades específicas do serviço. Caso haja restrição de funcionalidades quando a autenticação é realizada por métodos alternativos, essa limitação deve ser devidamente informada, acompanhada de explicações claras e justificativas proporcionais.

Quando a negativa do titular em fornecer dados biométricos resulta na restrição de determinadas funcionalidades, essa decisão deve ser implementada de maneira transparente e fundamentada. As organizações devem assegurar que tais restrições sejam proporcionais à necessidade de segurança e que não comprometam direitos fundamentais dos titulares. Explicações detalhadas sobre o motivo da restrição reforçam a confiança dos usuários e demonstram o compromisso da organização com a proteção dos dados pessoais e a conformidade com a LGPD.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Para garantir o respeito aos direitos dos titulares, os agentes de tratamento devem, principalmente através de instrumentos acessíveis, conferir transparência ao tratamento de dados que realizam por meio de políticas de privacidade e ao mecanismo que viabiliza o exercício desses direitos através de canais de atendimento ao titular.

Esses instrumentos devem possuir acesso facilitado, sendo de fácil utilização nas plataformas disponibilizadas pelo controlador, como sites, aplicativos e espaços físicos. Além disso, é essencial proporcionar uma experiência intuitiva para o titular, utilizando uma linguagem clara, oferecendo uma interface amigável e assegurando uma comunicação transparente durante todo o processo de atendimento. Isso inclui fornecer informações detalhadas sobre como os dados são coletados, utilizados, armazenados e compartilhados, permitindo que o titular compreenda plenamente o processo de tratamento de seus dados.

Para garantir a segurança e a integridade dos dados, devem ser implementados métodos de verificação de identidade do titular que assegurem a confirmação da identidade de forma segura e eficiente. Também é crucial assegurar um atendimento inclusivo para pessoas com deficiência (PCDs), adaptando os serviços de atendimento às necessidades específicas desse público, garantindo assim a acessibilidade universal.

Adicionalmente, é necessário disponibilizar opções para a solicitação de direitos por representantes legais, permitindo que os titulares exerçam seus direitos através de procuradores e representantes legais quando necessário. Essa flexibilidade é fundamental para atender às diversas circunstâncias em que os titulares possam necessitar de assistência para o exercício de seus direitos.

A transparência no tratamento de dados deve ser priorizada, fornecendo informações claras e detalhadas sobre todas as etapas do tratamento de dados pessoais. Isso assegura que os titulares tenham pleno conhecimento de como seus dados estão sendo manipulados, fortalecendo a confiança nas práticas adotadas pelos agentes de tratamento.

Por fim, é fundamental estabelecer auditorias regulares que criem rotinas de verificação da conformidade com os direitos dos titulares. Essas auditorias permitem identificar e corrigir eventuais falhas, garantindo que as práticas de tratamento de dados estejam alinhadas com as normas e regulamentos aplicáveis, promovendo assim a proteção contínua dos direitos dos titulares.

Em síntese, ao implementar essas características nos instrumentos de tratamento de dados, os agentes de tratamento não apenas respeitam e garantem os direitos dos titulares, mas também fortalecem a transparência e a confiança nas suas práticas de gestão de dados.

Por fim, agradecemos a oportunidade de contribuir com esta Tomada de Subsídios e colocamo-nos à disposição para quaisquer esclarecimentos adicionais.

Atenciosamente,

B3 S.A. – BRASIL, BOLSA, BALCÃO

São Paulo, 1º de agosto de 2025.

À Autoridade Nacional de Proteção de Dados (ANPD)

Ref.: Tomada de Subsídios: Dados Pessoais Sensíveis – Dados Biométricos

Na qualidade de representantes da **Samsung Eletrônica da Amazônia LTDA.**, apresentamos, a seguir, comentários aos quesitos levantados pela ANPD na Tomada de Subsídios em referência¹, elaboradas à luz das diretrizes institucionais da Samsung.

- Resposta aos Quesitos -

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Com base nos entendimentos da Autoridade de Proteção de Dados do México (“INAI”)², do Comitê Europeu de Proteção de Dados (*European Data Protection Board* – “EDPB”)³ e do artigo 16 da Lei de Proteção de Dados do Chile⁴, consideram-se dados biométricos aqueles que atendem, cumulativamente, aos seguintes critérios: **(i)** estejam vinculados a características físicas, fisiológicas, comportamentais ou traços de personalidade do titular de dados; e **(ii)** sejam resultado de tratamento técnico específico, vinculado a uma forma de medição, cuja finalidade seja identificar o titular de maneira única.

Assim, **imagens de vídeo, fotografias, gravações de voz ou dados semelhantes não devem ser classificados, por si sós, como dados biométricos.** Só serão considerados dados biométricos quando tratados com a finalidade de permitir a identificação única do indivíduo em questão e armazenados com esse propósito. Nesse sentido, dispõe o Considerando 51 do Regulamento Geral de Proteção de Dados da União Europeia (“GDPR”). O EDPB reforça esse entendimento ao afirmar: *“The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual”*⁵.

Para ilustrar, considere o seguinte cenário: determinada empresa de tecnologia utiliza sistema de controle de acesso com reconhecimento de íris para permitir a entrada de seus colaboradores em áreas restritas do prédio. Neste sistema, a imagem da íris do colaborador é capturada e, a partir dela, o sistema extrai dados biométricos, como padrões na textura da íris, que são então transformados em modelo matemático e armazenados para validação em acessos futuros. Nesse contexto, a imagem original do olho não é, por si só, considerada um dado biométrico. O dado biométrico é o conjunto de pontos ou padrões extraídos da imagem e então processados com o

¹ <https://www.gov.br/participamaisbrasil/ts-dados-biometricos>

² https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf

³ https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

⁴ <https://www.diariooficial.interior.gob.cl/publicaciones/2024/12/13/44023/01/2583630.pdf>

⁵ https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

objetivo específico de identificar de forma única aquele colaborador. Portanto, caso ocorra um incidente em que apenas a imagem original, e não o modelo biométrico, seja exposta, o dado comprometido seria classificado apenas como dado pessoal e não como biométrico (sensível).

Nessa mesma linha, a **Autoridade de Proteção de Dados da Coreia do Sul** (*Personal Information Protection Commission* ou “PIPC”) apresenta uma conceituação mais sofisticada ao diferenciar informações biológicas de informações biométricas.

De acordo com as Diretrizes para Tratamento de Dados Biométricos da PIPC (“Diretrizes”), o conceito de “**informações biológicas**” refere-se a dados sobre características físicas, biológicas e comportamentais, como impressões digitais, rosto, íris, veias, voz, escrita manual, entre outros. Esses dados podem ser usados para autenticar ou identificar indivíduos, através da comparação de traços únicos com informações previamente armazenadas, como no reconhecimento facial ou leitura de digitais para acesso a serviços. Ainda, podem ser processados com meios técnicos para compreender as características pessoais, como a idade, gênero ou estado emocional, sem envolver autenticação, por exemplo, os sistemas que sobrepõem elementos visuais ao rosto com base na posição dos olhos e boca.⁶

Já as **informações biométricas** são aquelas tratadas com o objetivo de autenticar ou identificar a pessoa com base em dados biológicos. Assim, os dados biológicos podem ser divididos em dois tipos: as **informações biométricas**, utilizadas para autenticação e identificação, e as **informações biológicas gerais**, utilizadas para compreender características pessoais, como idade, gênero ou emoções, sem fins de identificação direta.

Logo, quando as informações sobre características físicas, biológicas e/ou comportamentais não são tecnicamente processadas para fins de autenticação, identificação ou compreensão de suas características pessoais (como idade ou emoções), esses dados são considerados **informações pessoais comuns**, e não dados biométricos. O quadro abaixo resume essa conceituação proposta pela PIPC nas Diretrizes:

Classification		Definition
Personal information	It is possible to identify a certain person with the information itself or it is information can be comprehensible by easily aggregating with other information	
Bio information	Information on an individual's physical, biological, and behavioral features is processed through a certain technical means to either authenticating/identifying a specific individual or understanding the individual's features (age, gender, emotion, etc.) .	
Biometric information	This is a person's bio information that is processed to authenticate/identify a certain person .	
	Original information	This biometric information is used in creating feature information , collected and entered via an input device.
	Feature information	Information created through a certain technical means , extracting features from original information

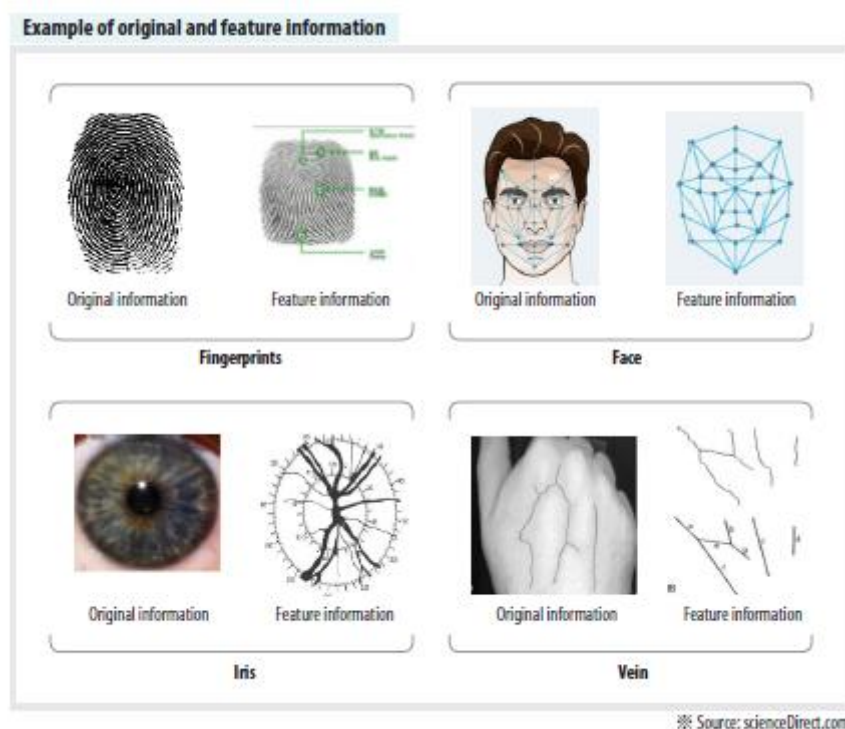
Por exemplo, a imagem de um rosto é considerada **informação biométrica** quando utilizada para autenticar ou identificar a pessoa, como em sistemas de controle de acesso por reconhecimento facial. Se for usada para interpretar características pessoais, como gênero ou estado emocional

⁶ <https://www.pipc.go.kr/eng/user/lgp/law/ordinancesDetail.do#none>

(por exemplo, se a pessoa está feliz ou irritada), trata-se de **informação biológica geral**, mesmo que haja extração técnica de traços faciais.

Da mesma forma, a voz é tratada como **informação biométrica** quando utilizada para identificar a pessoa que está falando, como em assistentes virtuais que reconhecem usuários previamente cadastrados. Porém, se a voz é usada apenas para inferir emoções (como alegria e/ou irritação), sem objetivo de identificar quem fala, ela se classifica como **informação biológica geral**.

A PIPC ainda divide as informações biométricas em: **(i) informação biométrica original**, coletada diretamente por dispositivos de entrada (como sensores) para autenticar ou identificar alguém, e **(ii) informação de características biométricas**, gerada com base na extração técnica dos traços individuais. Quando a **informação original** é vazada ou mal utilizada durante o tratamento de dados por meio eletrônico, há alto risco de violação da privacidade. Por isso, se essa informação for armazenada, é essencial adotar medidas de proteção, como o armazenamento separado de outros dados pessoais e aplicação de técnicas de codificação para garantir sua segurança. Abaixo, um exemplo da classificação proposta pela PIPC extraído das Diretrizes:



Adicionalmente, é importante que a regulamentação adote abordagem tecnicamente orientada e funcional sobre o conceito de dado biométrico, de forma a distinguir com clareza situações de coleta ou uso experimental, voltadas à pesquisa científica ou validação de modelos, daquelas em que há efetivo processamento com finalidade de identificação de titulares. Essa diferenciação é essencial para evitar insegurança jurídica nas iniciativas de inovação tecnológica que envolvam, por exemplo, o uso de dados sintéticos ou a aplicação de modelos pré-treinados, amplamente utilizados em ambientes acadêmicos e de P&D.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Segundo a **Autoridade de Proteção de Dados do Reino Unido** (“ICO”), não há uma metodologia única aplicável sobre como garantir a transparência ativa em todos os casos, incluindo medidas adotadas pelos controladores. O modo mais efetivo de fornecer transparência ao titular com relação ao uso de seus dados biométricos é considerar fatores como: i) caso de uso; ii) natureza de relacionamento com o titular; e iii) dados envolvidos na atividade de tratamento⁷.

Quanto mais evidente ao titular a atividade de tratamento com dados biométricos, considerando práticas habituais de mercado e natureza de relacionamento com o titular, menor a necessidade de práticas ativas de transparência. Vejamos as situações hipotéticas abaixo:

- **Situação 1:** uma empresa de segurança privada para condomínios instala câmeras na calçada de prédios para realizar a identificação biométrica de indivíduos. Neste caso, o titular – que são toda e qualquer pessoa que passe em frente às câmeras – não possui a expectativa de que seus dados biométricos sejam coletados e tampouco possui relacionamento prévio com a empresa. Cabe ao controlador adotar medidas adicionais para garantir a transparência e isso pode ser realizado, por exemplo, por meio da instalação de placas, em local de fácil visualização, antes da entrada na área monitorada, fornecendo informações gerais sobre o tratamento e o modo como obter informações mais detalhadas e para o exercício de direitos dos titulares, como QR Code para o Aviso de Privacidade. Em cenário semelhante, a ANPD entendeu que as medidas sugeridas acima foram suficientes, vide Nota Técnica nº 29/2024/FIS/CGF/ANPD, § 6.1.4⁸.
- **Situação 2:** uma instituição financeira precisa realizar a verificação biométrica de clientes para realizar a abertura de conta ou autorização de empréstimo. Esta é uma prática consolidada no mercado, tendo em vista que a coleta de dados biométricos é clara e previsível pelo titular. Assim, conceder o acesso ao Aviso de Privacidade durante a jornada do usuário – ou, em caso de atendimento presencial, por meio da disponibilização de QR Codes de fácil acesso ou informações prestadas oralmente durante o atendimento – basta para assegurar o dever de transparência.

Somado a isso, é fundamental que as práticas de transparência ativa estejam alinhadas com as especificidades setoriais de cada controlador. Caberá à ANPD garantir **flexibilidade regulatória** para que as empresas de diferentes segmentos (incluindo as fabricantes de dispositivos móveis e *hardware*) possam adaptar suas estratégias de governança conforme o seu modelo de negócio, canal de interação com usuário e nível de acesso aos dados biométricos.

Especificamente no caso de **fabricantes de dispositivos móveis** (como a Samsung, que integra sensores biométricos em dispositivos, incluindo leitores de impressão digital ou reconhecimento facial para desbloqueio de aparelhos), já são implementadas múltiplas práticas de transparência ativa diretamente na interface de configuração do dispositivo, como avisos e banners exibidos no momento de ativação dos sensores biométricos. A experiência da indústria de dispositivos móveis, em especial, traz lições valiosas sobre como aplicar princípios como a transparência e o *Privacy by Design* de forma eficaz desde a concepção dos produtos, com foco em segurança dos dados e experiência do usuário.

⁷ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>

⁸ https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-29_2024.pdf

A experiência da indústria de dispositivos móveis é particularmente relevante nesse ponto. As tecnologias embarcadas de biometria, como o desbloqueio facial ou por digital, são estruturadas com base em algoritmos locais (*hashes*), sem envio ou armazenamento dos dados sensíveis fora do dispositivo. Nesses casos, práticas como a exibição de alertas no momento da ativação da função, ou a inclusão de explicações no menu de configurações, são bem eficazes para garantir a transparência necessária.

Por isso, é importante que não se adote abordagem única de práticas de transparência ativa para todos os setores, mas sim incentive o desenvolvimento de boas práticas adaptadas ao contexto do controlador, considerando o grau de risco do tratamento, a proximidade com o usuário final e capacidade técnica.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Na legislação vigente, não há obrigações legais que distingam as diferentes modalidades de biometria, de modo que não pode haver eventual regulamentação sobre a legislação que crie uma obrigação distinta sendo que a própria legislação não traz, o que implicaria na violação do princípio da legalidade. Nesse sentido, embora tanto a INAI^{9 10} quanto a ICO¹¹ diferenciem dados biométricos físico e fisiológicos de comportamentais, nenhuma das autoridades traz obrigações específicas aplicáveis de forma diversa.

Portanto, é essencial que a regulamentação considere as especificidades técnicas da biometria comportamental, sobretudo quando ela é aplicada em contextos científicos e não comerciais. A utilização de dados como padrões de marcha, equilíbrio, tremores ou emoções faciais, para fins exclusivamente investigativos e sob controles éticos institucionais, não deve ser equiparada, em termos de exigências regulatórias, ao uso de biometria para a autenticação ou identificação em larga escala. Ao permitir níveis diferenciados de exigência regulatória a depender do risco e do contexto do tratamento, a ANPD pode estimular a pesquisa responsável e o avanço de soluções com potencial social relevante.

BLOCO II - HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

No que se refere aos requisitos de validade do consentimento, entendemos que os seguintes cuidados devem ser aplicados:

⁹ https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf

¹⁰ <https://home.inai.org.mx/wp-content/uploads/GuiaBiometricos-Dic2024.pdf>

¹¹ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/>

a) **Livre:** o consentimento deve ser genuinamente opcional para o titular. De acordo com o Guia da ICO¹², isso significa que: i) o titular deve poder recusar ou revogar o consentimento sem sofrer qualquer tipo de prejuízo – ressalvadas, conforme orienta o EDPB¹³, as situações em que o tratamento de dados biométricos seja essencial para evitar esse prejuízo ao titular e o consentimento represente a única base legal aplicável; e ii) devem ser oferecidas alternativas ao titular que permitam o acesso a produtos, serviços ou benefícios sem a necessidade de tratamento da biometria facial – salvo nos casos em que tais produtos, serviços ou benefícios dependam, por sua própria natureza, do uso dessa tecnologia. Além disso, o consentimento deve ser específico e vinculado a uma finalidade determinada, sem vícios de vontade, como coação, erro ou fraude.

b) **Informado:** conforme o Guia de *Cookies* da ANPD¹⁴, o titular precisa ter informações completas e adequadas para que o consentimento seja válido, garantindo que ele tenha acesso ao conjunto mínimo de informações necessárias, conforme determina o art. 9º da LGPD, para que ele possa decidir de forma consciente. De acordo com Guia do EDPB¹⁵ e na NBR ISO/IEC 29184¹⁶, há duas formas principais que essas informações podem ser apresentadas, sendo que elas são apropriadas para o contexto do consentimento em tratamento de dados biométricos:

- Termo de consentimento único, que deverá ser lido e assinado pelo titular. Prática mais recomendável para a coleta de consentimento por meios físicos.
- Fornecer informações em camadas, principalmente em ambientes digitais. Geralmente, as informações são apresentadas em duas etapas: na primeira, em que o titular manifesta o seu consentimento (por exemplo, ao selecionar um *checkbox*), apresentam-se as informações mais importantes e marcantes, como a finalidade do tratamento e a necessidade de uso de dados biométricos. Depois, ainda nessa etapa, deve ser permitido o acesso à segunda etapa, como, por exemplo, um link escrito “clique aqui para saber mais”. Neste momento, é fornecido ao titular todas as informações elencadas no art. 9º da LGPD, por meio do Aviso de Privacidade ou do Termo de Consentimento; e
- Em especial no âmbito de pesquisas científicas, é importante que se reconheça o Termo de Consentimento Livre e Esclarecido (TCLE), que é aprovado por Comitês de Ética em Pesquisa, como um instrumento hábil para viabilizar o tratamento de dados biométricos, inclusive comportamentais. Essa prática é essencial para a continuidade de estudos que buscam desenvolver soluções tecnológicas voltadas à saúde mental e cognitiva, a partir de dados anonimizados e armazenados de forma segura e restrita. A previsibilidade regulatória sobre o consentimento em pesquisas pode fomentar iniciativas socialmente relevantes, sem comprometer os direitos dos titulares.

c) **Inequívoco:** não pode haver dúvida quanto à manifestação de vontade do titular. O consentimento não pode ser presumido ou tácito, conforme o já citado guia da ANPD¹⁷.

¹² <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>

¹³ https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

¹⁴ <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>

¹⁵ https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

¹⁶ <https://www.normas.com.br>

¹⁷ <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>

d) Específico: de acordo com o EDPB¹⁸, caso tenha a probabilidade de o dado biométrico ser utilizado para mais de uma finalidade, se uma dessas finalidades necessitar do consentimento, ele deve ser obtido individualmente para cada uma. Embora o consentimento seja aplicável para finalidade delimitadas, a sua coleta não é necessária quando o tratamento de dados pessoais para finalidades adicionais puder ocorrer com fundamento em outras bases legais. Por exemplo: caso uma organização colete dados biométricos de voz, com base no consentimento, para personalização de experiência e detecção de emoção, ela não precisa coletar para fins de autenticação, pois esta atividade estaria amparada no art. 11, II, “g”, da LGPD.

e) Destacado: a fim de que o titular tenha uma experiência mais fluida e que o fluxo seja otimizado, o consentimento pode ser coletado, ao mesmo tempo, para dados pessoais e sensíveis, principalmente, quando a finalidade não puder ser alcançada sem o tratamento dos dois tipos de dados, sendo necessário haver um destaque específico para o tratamento dos dados pessoais sensíveis.

O consentimento, porém, não será a base legal adequada quando pelo menos dentre os quatro elementos de validade destacado acima não puderem ser satisfeitos. Isto ocorrerá principalmente nos seguintes casos:

- Quando não houver uma alternativa viável à coleta da biometria, como nos casos de prevenção à fraude, por exemplo, em que o uso de outras formas de verificação poderia reduzir a segurança de processos e facilitar a ação de pessoas má intencionadas, ou nas hipóteses em que a biometria é fundamental para a prestação de certo serviço ou uso de determinado produto; e
- Quando não houver uma relação direta com o controlador, como nos casos de monitoramento de vias públicas, por exemplo, em que coleta do consentimento é inviável.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Segundo o Guia de Legítimo Interesse da ANPD ¹⁹, as condições para que um tratamento de dados biométricos seja fundamentado na base legal de “prevenção à fraude” são semelhantes àquelas aplicáveis ao legítimo interesse. Assim, aplicam-se os mesmos parâmetros do Teste de Balanceamento para aplicar o “legítimo interesse”, exceto a proibição de dados pessoais sensíveis.

A elaboração prévia do Teste de Balanceamento, porém, não é uma condição obrigatória para garantir a legalidade da atividade, pois não há obrigação legal nesse sentido. Destaca-se aqui a posição do ICO²⁰:

¹⁸ https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

¹⁹ https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf

²⁰ https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/#why_LIA

“There is no obligation in the UK GDPR to do an LIA, but it is best practice to conduct one and it is difficult to meet your obligations under the accountability principle without it.

The LIA encourages you to ask yourself the right questions about your processing and objectively consider what the reasonable expectations of the individuals are and any impact of the processing on them.

Conducting an LIA helps you ensure that your processing is lawful. It helps you to think clearly and sensibly about your processing and the impact it could have on the individual.

Recording your LIA also helps you demonstrate compliance with the principles and appropriate organisational measures in line with your accountability obligations under Articles 5(2) and 24”.

Assim, o Teste de Balanceamento assiste à organização a atestar a aplicação da base legal, contudo, a sua ausência, por si só, não significa ilicitude da atividade de tratamento, sendo que, para chegar a esta conclusão, será necessário comprovar a ausência do cumprimento dos requisitos mínimos.

Com relação ao princípio da necessidade, a ICO elucida que ele não significa absoluta essencialidade, mas sim que a atividade de tratamento seja “uma forma direcionada e proporcional de alcançar o objetivo” (*“targeted and proportionate way of achieving your purpose”*) – ou seja, a finalidade do tratamento. Esta também foi a premissa elencada pelo ICO para o tratamento de dados biométricos para a “prevenção ou detecção de atos ilícitos”²¹.

Desse modo, no caso de soluções bancárias, por exemplo, considerando a prática do mercado, a utilização da biometria é, geralmente, viável com base no art. 11, II, “g”, da LGPD, devido ao bem jurídico protegido contra fraudes, que é a vida financeira do titular, e as consequências negativas que o titular pode ter se indivíduos mal-intencionados acessem serviços financeiros em seu nome.

Para além dos critérios já expostos, destaca-se a relevância de permitir o uso de modelos públicos e algoritmos de detecção biométrica embarcados em dispositivos móveis, em especial quando utilizados exclusivamente em tempo real, sem armazenamento dos dados capturados. Essa abordagem é fundamental para viabilizar o desenvolvimento e teste de soluções de segurança embarcada voltadas à proteção de dispositivos e prevenção de fraudes, respeitando limites técnicos e reforçando o *privacy by design*. A regulamentação da ANPD poderá promover segurança jurídica e inovação se reconhecer a legitimidade do uso de tais modelos em ambientes controlados e de risco reduzido.

Com relação às proteções a serem adotadas, destacamos as medidas aplicadas por ICO²², INAI²³ e Autoridade de Proteção de Dados da Coreia do Sul²⁴, que resumizamos em dois tipos:

(a) Medidas mais relevantes

²¹ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>

²² <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

²³ https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf

²⁴ <https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do#none>

- Controles de acesso robustos aos dados biométricos;
- Realização de testes de penetração;
- Implementação de política de segurança da informação;
- Criptografia dos dados pessoais, tanto em trânsito quanto em repouso;
- Realização de varredura (*scan*) de vulnerabilidades nos sistemas que tratam dados biométricos, com adoção de medidas corretivas;
- Registro, em logs, de todos os acessos aos dados biométricos;
- Armazenamento de dados biométricos de forma segregada de outras informações; e
- Quando houver contratação de fornecedor, realização de processo adequado de *due diligence*.

(b) Medidas adicionais:

- Restringir o armazenamento de dados biométricos ao *template* com minúcias das impressões digitais, evitando a guarda da representação completa da impressão; e
- Avaliar a adoção de controles previstos em normas reconhecidas internacionalmente, como a ISO/IEC 24745:2022.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Para a base legal de “cumprimento de obrigação legal ou regulatória”, entendemos que devem ser aplicados as mesmas salvaguardas e critérios aplicáveis aos agentes de tratamento que utilizam a base legal de “prevenção à fraude”, conforme explicado no quesito nº 5. Adotamos essa posição, pois entendemos que as medidas de proteção de dados devem ser equivalentes aos riscos da atividade de tratamento independentemente da base legal que a justifique. Desse modo, os critérios e salvaguardas para reduzir os riscos decorrentes do uso de dados biométricos devem ser os mesmos independentemente da base legal aplicável.

O ICO²⁵, por exemplo, adota este raciocínio ao não trazer distinções com relação às medidas de segurança recomendadas conforme a base legal adotada para o tratamento de dados biométricos.

Com relação às condições para justificar o tratamento de dados biométricos na base legal de “cumprimento de obrigação legal ou regulatória”, defendemos que ela deve abranger tanto as hipóteses expressamente previstas na legislação quanto os casos em que o tratamento de dados biométricos é meio legítimo para estar de acordo com as normas legais. A Circular BCB nº 3.978/2020, por exemplo, determina que instituições financeiras devem possuir processos que permitam verificar e validar a identidade de clientes:

Art. 16. As instituições referidas no art. 1º devem adotar procedimentos de identificação que permitam verificar e validar a identidade do cliente.

§ 1º Os procedimentos referidos no caput devem incluir a obtenção, a verificação e a validação da autenticidade de informações de identificação do cliente, inclusive, se necessário, mediante confrontação dessas informações com as disponíveis em bancos de dados de caráter público e privado.

²⁵ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

Nesse cenário, é importante reconhecer também a legitimidade do uso de biometria embarcada para fins de autenticação local do titular em soluções críticas, como o uso de carteiras digitais, substituição de crachás físicos ou acesso a serviços protegidos por senha. Essas soluções, por operarem exclusivamente no dispositivo do usuário e não armazenarem dados em servidores centrais, refletem modelo de segurança centrado na autodeterminação informativa do titular, compatível com o princípio da minimização e do *privacy by design*.

É igualmente importante que a regulamentação considere que, em determinados contextos regulados, como os de saúde e pesquisa clínica, o tratamento de dados biométricos pode ser condição necessária para o cumprimento de obrigações legais e éticas previstas em resoluções do Conselho Nacional de Saúde (ANS) e da Agência Nacional de Vigilância Sanitária (Anvisa). Isso inclui, por exemplo, a coleta de dados comportamentais ou motores para a análise científica em conformidade com protocolos aprovados por comitês de ética, salvaguardas de anonimização, finalidade determinada e acesso restrito. Reconhecer tais práticas como alinhadas ao art. 11, II, “a”, da LGPD confere coerência sistêmica ao ordenamento jurídico e assegura segurança jurídica para projetos de P&D voltados à saúde.

Desproporcional seria sustentar que o uso de dados biométricos, quando adotado por uma Instituição Financeira com base em riscos concretos, não se enquadra como forma legítima de cumprimento da obrigação legal de verificação de identidade. Um posicionamento nesse sentido contrariaria a finalidade da base legal aplicável, cuja razão de existir é justamente promover a coerência do ordenamento jurídico, conferindo segurança jurídica aos agentes de tratamento ao realizarem operações indispensáveis para atender exigências legais.

Por fim, no que tange às atividades de tratamento conduzidas por entes do Poder Público, para garantir o atendimento aos direitos dos titulares, torna-se essencial adotar mecanismos de transparência eficazes, especialmente nos casos em que não há vínculo direto entre o titular dos dados e o órgão público responsável. Isso é fundamental para que o titular tenha ciência da realização do tratamento e possa exercer, de forma efetiva, os direitos que lhe são garantidos.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Segundo o posicionamento da ANPD em seu Guia para tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas, a anonimização não é condição para órgãos de pesquisa elaborarem estudos:

“Em conjunto, esses dispositivos legais indicam que a anonimização ou a pseudonimização de dados pessoais não foram instituídas pela LGPD como medidas de segurança impositivas, isto é, que devem ser adotadas em todo e qualquer caso de estudos e pesquisas.

Da mesma forma, a LGPD não estabeleceu a anonimização ou a pseudonimização como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais para fins de realização de estudos e pesquisas, devendo-se reconhecer, inclusive, que, em alguns casos, a

identificação dos titulares pode ser imprescindível para os objetivos da pesquisa.

A leitura mais adequada – e que decorre, em especial, do uso da expressão “sempre que possível” tanto nos arts. 7º e 11 quanto nos arts. 13 e 16 – é a de que a LGPD optou por um modelo mais flexível, que busca equilibrar a proteção de dados pessoais com as peculiaridades e os propósitos de realização dos mais diversos estudos e pesquisas”²⁶.

Dessa forma, o uso do termo “necessária” no questionamento apresentado mostra-se inapropriado, uma vez que, sendo a anonimização uma medida facultativa e não compulsória, não se impõe automaticamente a adoção de salvaguardas adicionais com base no risco de reidentificação.

Feito esse esclarecimento, é importante destacar, conforme apontam tanto a Autoridade de Proteção de Dados de Hong Kong²⁷ quanto o ICO²⁸, que, em diversas situações, dados biométricos não podem ser verdadeiramente anonimizados. Isso ocorre porque, ainda que tais dados não estejam diretamente associados a uma pessoa identificável, eles podem possibilitar a dedução de informações sensíveis — como origem étnica, traços físicos distintivos ou condições de saúde — que podem levar à reidentificação do indivíduo. Por esse motivo, eventuais técnicas complementares de anonimização devem ser avaliadas com base na probabilidade e no impacto do risco de reidentificação.

Assim, as salvaguardas implementadas devem ser compatíveis com o nível de risco concreto identificado. Ainda assim, recomenda-se que incluam mecanismos voltados à mitigação de possíveis prejuízos aos titulares, caso ocorra uma violação ou tentativa de reidentificação. Nesse sentido, como ressalta o ICO²⁹, é essencial garantir a irreversibilidade e a não vinculabilidade (*unlinkability*) dos *templates* biométricos — isto é, adotar técnicas que complexifiquem a engenharia reversa para obter informações sobre a aparência do titular e impossibilite que tais dados possam ser facilmente associados ao titular a quem se referem os dados ou reutilizados em diferentes sistemas e bases de dados.

Ainda no contexto de estudos científicos, é importante que a regulamentação reconheça que, quando os dados biométricos são tratados exclusivamente sob a forma de sinais sensoriais anonimizados, o risco de reidentificação é significativamente mitigado, sobretudo quando não há conservação de dados semânticos e/ou metadados identificáveis. Ao permitir o uso desses dados de forma segura e controlada, inclusive fora do escopo de estudos clínicos formais, será possível contribuir para a ampliação de aplicações benéficas em áreas como detecção precoce de distúrbios neuropsiquiátricos, sem comprometer os direitos dos titulares.

Diversas iniciativas de pesquisa existentes no Brasil envolvem análise de dados comportamentais extraídos de sensores móveis, como os padrões de digitação, equilíbrio, marcha ou expressões faciais, anonimizados na origem e dissociados de qualquer identificador direto. Tais estudos são conduzidos com base em protocolos éticos aprovados por Comitês de Ética em Pesquisa e

²⁶ <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>

²⁷ https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

²⁸ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

²⁹ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

respaldados por Termos de Consentimento Livre e Esclarecido (TCLE), refletindo padrão robusto de proteção de dados.

Contudo, ainda há insegurança jurídica quanto à legalidade do uso desses dados biométricos em projetos de pesquisa aplicada, em especial os voltados ao desenvolvimento de funcionalidades inovadoras em dispositivos móveis fora do escopo clínico tradicional. A ausência de diretriz clara sobre a possibilidade de utilização de dados biométricos anonimizados para fins exclusivamente científicos ou tecnológicos poderia gerar entraves indevidos à inovação, inclusive em áreas de relevante interesse público como saúde mental e envelhecimento cognitivo.

Nesse sentido, deve-se incorporar parâmetros proporcionais ao risco de reidentificação e ao grau de controle técnico sobre os dados. Técnicas como a transformação de sinais de áudio para o domínio de frequência, ou uso de vídeos sem conservação de conteúdo semântico, são exemplos de boas práticas que reduzem drasticamente a possibilidade de reversão ou de vinculação dos dados a indivíduos específicos. Ao reconhecer e incentivar tais práticas, a ANPD pode estabelecer marco regulatório que assegure tanto a proteção de direitos quanto o fomento à pesquisa e à inovação responsável.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

A dúvida apresentada busca esclarecer três aspectos principais: (i) de que forma assegurar a transparência no uso de reconhecimento facial; (ii) como garantir que esse uso atenda aos princípios da necessidade e proporcionalidade; e (iii) quais medidas adotar para prevenir discriminações.

No que diz respeito à transparência, aplicam-se os mesmos fundamentos já discutidos na resposta ao quesito nº 2: as medidas de proteção à privacidade devem ser definidas de acordo com uma análise contextual, considerando múltiplos elementos — em especial, a finalidade do tratamento, a relação existente entre o agente de tratamento e o titular, e as características da atividade de tratamento de dados³⁰. Assim, quanto mais perceptível for a atividade de tratamento para o titular, menor será a necessidade de aplicação de práticas adicionais de transparência ativa.

Se, por exemplo, uma empresa de segurança utiliza câmeras em vias públicas para fins de identificação biométrica de indivíduos, devem ser adotadas medidas ativas de transparência, como a instalação de placas informativas ou sinalizações visuais de fácil e rápida visualização antes do ingresso na área monitorada, contendo informações gerais sobre o uso da biometria e canais de acesso a informações detalhadas, bem como meios para exercício dos direitos dos titulares. Em contraste, nos contextos em que o uso de biometria facial já constitui prática

³⁰ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>

consolidada e de conhecimento do mercado — como na verificação da identidade do titular durante a contratação de serviços ou produtos —, a disponibilização do Aviso de Privacidade ao longo da jornada do usuário basta para atender ao dever de transparência.

Quanto ao princípio da necessidade, conforme analisado no quesito nº 5, ele não se refere à absoluta essencialidade, mas sim na necessidade de que o tratamento seja “uma forma direcionada e proporcional” para atingir a finalidade do tratamento (*“targeted and proportionate way of achieving your purpose”*)³¹. Assim, com base no Guia da INAI³², é pertinente que o controlador aplique, dentre outros, as seguintes precauções:

- Evitar a utilização de dados biométricos sempre que a mesma finalidade puder ser alcançada, com eficácia equivalente, por meio de outras formas de tratamento menos invasivas.
- Sempre que possível, eliminar as amostras biométricas originais, mantendo apenas os *templates* gerados a partir dessas amostras, os quais servirão para futuras comparações. No entanto, essa prática pode não ser adequada em situações em que a preservação da amostra seja necessária como evidência da ação realizada pelo titular — como, por exemplo, a manutenção de uma fotografia facial em casos em que a biometria é utilizada para assinatura contratual, possibilitando comprovação posterior em eventual disputa judicial.
- Limitar a coleta à menor quantidade possível de amostras biométricas, priorizando, sempre que não comprometer a finalidade desejada, sistemas de verificação em lugar de sistemas de identificação.
- Evitar a coleta de dados biométricos que possam, por sua natureza, revelar outras informações sensíveis — por exemplo, priorizar impressões digitais em vez de dados de íris, uma vez que estes últimos podem indicar condições de saúde.
- Buscar sempre garantir a maior precisão possível na coleta das amostras, reduzindo, com isso, o volume necessário de dados tratados.

No tocante à redução de vieses discriminatórios, recomenda-se, conforme diretrizes do ICO em seus guias sobre biometria e inteligência artificial^{33 34}, a adoção das seguintes providências:

- Assegurar que a base de dados utilizada para o treinamento de modelos contenha amostras representativas de diferentes perfis étnicos e de gênero;
- Conduzir testes e auditorias para identificar e avaliar a presença de possíveis vieses discriminatórios no sistema;
- Realizar verificações, por meio de ferramentas disponíveis no mercado, para analisar se a estrutura e os critérios utilizados pelo modelo (*features*/métricas) podem gerar distorções;
- Avaliar a acurácia da solução empregada; e
- Implementar procedimentos voltados ao tratamento de erros, priorizando a redução de impactos negativos aos titulares, incluindo mecanismos que permitam contestar os resultados gerados pelo sistema de reconhecimento facial.

³¹ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>

³² https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf

³³ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-fairly/>

³⁴ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/>

No desenvolvimento experimental de tecnologias embarcadas de detecção facial, é igualmente importante diferenciar o tratamento de dados para fins de detecção em tempo real – sem armazenamento ou identificação individual – de aplicações voltadas à autenticação ou vigilância. Modelos utilizados exclusivamente em ambiente local, com base em bibliotecas públicas, configuram práticas alinhadas aos princípios de *privacy by design* e minimização. Reconhecer essas distinções técnicas pode evitar entraves indevidos à inovação e garantir segurança jurídica para iniciativas voltadas à segurança do usuário.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Todas as iniciativas destinadas a assegurar elevados níveis de precisão e confiabilidade — ou seja, a melhoria do desempenho — de sistemas de reconhecimento facial devem ser compatíveis com os riscos concretos envolvidos em sua aplicação. A título de exemplo, um sistema utilizado para monitorar espaços públicos com o intuito de identificar pessoas procuradas pela justiça, em geral, exige uma performance mais robusta do que aquele voltado à autenticação de usuários para entrada em edifícios corporativos, considerando os possíveis impactos morais e sociais decorrentes de uma identificação equivocada. Por esse motivo, as medidas listadas a seguir devem ser interpretadas como boas práticas recomendadas, a serem adotadas de acordo com a análise de risco específica do sistema, e não como obrigações absolutas ou universalmente exigidas.

Atentando-se para o fato de que sistemas de reconhecimento facial são sistemas de inteligência artificial, as práticas recomendadas para garantir seu desempenho são as mesmas aplicáveis a modelos de IA. Com base no Guia de Inteligência Artificial e Proteção de Dados publicado pelo ICO³⁵, bem como em seu respectivo toolkit de avaliação de riscos³⁶, destacamos os seguintes controles a serem considerados:

- **Planejamento:** recomenda-se estabelecer, desde o início do projeto, o nível mínimo de acurácia estatística aceitável para o sistema, de acordo com os objetivos a que se destina.
- **Seleção e coleta de dados:** considerando o público-alvo da solução de IA, é importante assegurar que os dados utilizados para treinamento: (i) sejam adequadamente representativos, completo e exatos; (ii) foram rotulados da forma correta; e (iii) tenham sido analisados quanto à ocorrência de riscos como *overfitting* ou *underfitting*.
- **Testes e validação:** durante essa etapa, recomenda-se realizar testes documentados para: (i) verificar a acurácia estatística global da solução, bem como sua eficácia em subgrupos populacionais relevantes, com base nos padrões mínimos definidos; (ii) identificar eventuais sinais de *overfitting* ou *underfitting*; e (iii) adotar medidas corretivas, como o retreinamento do sistema ou o ajuste de parâmetros, sempre que os resultados não atenderem aos critérios estabelecidos.

³⁵<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>

³⁶https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fico.org.uk%2Fmedia%2Fkr3mveig%2Fai_and_data_protection_risk_toolkit_v11.xlsx&wdOrigin=BROWSELINK

- **Implantação e monitoramento:** após o início da operação do sistema, recomenda-se: (i) avaliar a disponibilização de meios para que indivíduos afetados pelo sistema possam questionar os resultados da solução; (ii) implementar rotinas de monitoramento e testes periódicos para garantir a acurácia da estatística ao longo do tempo; e (iii) preservar cópias das versões anteriores da IAs que sejam de aprendizado contínuo, a fim de possibilitar o seu retorno caso as novas interações apresentem perda significativa do seu desempenho.

Em projetos envolvendo o uso experimental de IA, é recomendável que sejam incentivadas boas práticas que promovam desempenho seguro sem exigir, de forma indiscriminada, os mesmos níveis de robustez esperados de soluções aplicadas em contextos críticos. Por exemplo, testes realizados com impressões digitais sintéticas, geradas por modelos públicos, para validação de mecanismos de autenticação resistentes à fraude. Reconhecer a legitimidade de tais práticas – desde que sem finalidade comercial ou sem coleta persistente de dados de usuários – pode fomentar avanços relevantes em segurança digital, com baixos riscos associados ao tratamento de dados biométricos reais.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

O uso de reconhecimento facial não deve ser considerado adequado quando houver métodos igualmente eficazes e proporcionais para atingir o mesmo objetivo sem recorrer ao tratamento de dados biométricos — sobretudo nos casos em que tais alternativas forem consideravelmente menos invasivas e suficientes para cumprir a finalidade proposta. Em outras palavras, a tecnologia deve ser evitada sempre que existirem soluções capazes de oferecer um grau de identificação equivalente, ou ao menos adequado, frente aos riscos envolvidos.

No contexto educacional, por exemplo, empregar o reconhecimento facial para controle de frequência pode configurar uma forma desproporcional de monitoramento, com impactos negativos sobre o direito à educação. Em ambientes públicos, o uso dessa tecnologia sem justificativas claras e proporcionais pode ser interpretado como uma prática de vigilância em massa. Já em processos seletivos ou contratações, a análise de expressões faciais por meio de reconhecimento facial durante entrevistas representa risco real de discriminação, contribuindo para a reprodução de vieses algorítmicos e prejudicando a equidade no processo. Em situações como manifestações ou eventos políticos, a aplicação dessa tecnologia pode ser particularmente complexa, uma vez que pode ser utilizada para identificar e, eventualmente, perseguir manifestantes.

Quanto a tecnologias alternativas, há outras informações que podem complementar ou substituir o reconhecimento facial, dependendo da situação específica. A Autoridade de Proteção de Dados da Coreia do Sul (“PIPC”), por exemplo, em seu Guia sobre Dados Biométricos³⁷, aponta as seguintes alternativas:

- Para entrada em ambientes físicos ou uso de dispositivos, é possível recorrer a impressões digitais, bem como a cartões de acesso ou senhas robustas.

³⁷ <https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do#none>

- No caso de autenticação em aplicativos, é viável utilizar: (i) sistemas de resposta automática por telefone (em que o usuário recebe uma ligação e deve seguir determinadas instruções para validar sua identidade); ou (ii) códigos temporários e *tokens* enviados via SMS, e-mail ou por aplicativos autenticadores previamente cadastrados.

Outro recurso valioso na prevenção de fraudes é o uso de dados oriundos do setor de telecomunicações. Essas informações permitem, por exemplo, verificar se os dados de contato do usuário — como número de telefone — coincidem com os registros das operadoras, avaliar se a localização de determinada transação corresponde à localização real do dispositivo e identificar possíveis fraudes, como o *SIM Swap*. A ANATEL, por exemplo, destaca que instituições financeiras utilizam dados de telecomunicação “para prevenir fraudes no sistema financeiro, as prestadoras disponibilizam informações para os bancos, possibilitando que adotem providências preventivas relativas às movimentações financeiras atreladas ao número do celular envolvido em troca de chip”³⁸.

Eventual regulamentação também deve evitar uma abordagem excessivamente restritiva que comprometa o uso experimental de reconhecimento facial em ambientes controlados, como os laboratórios de pesquisa ou de prototipagem. Nesses contextos, o uso de modelos públicos de detecção facial, sem armazenamento de dados nem identificação de usuários, pode ser essencial para validar soluções técnicas voltadas à usabilidade, acessibilidade ou prevenção à fraude. A adoção de diretrizes específicas para os usos não comerciais e não identificáveis contribuirá para distinguir entre práticas de risco elevado e aplicações legítimas de baixo impacto, preservando a liberdade de pesquisa e o desenvolvimento tecnológico nacional.

Para que as organizações possam recorrer, sempre que adequado, a soluções alternativas ao reconhecimento facial — levando em consideração os riscos envolvidos —, é essencial que a ANPD atue na construção de um ambiente regulatório que favoreça a inovação, promovendo o desenvolvimento e a adoção de mecanismos eficazes e seguros. A falta de regulamentação que incentive a criação de alternativas ao tratamento de dados biométricos sensíveis pode acabar levando empresas a optarem pela biometria facial mesmo em contextos de alto risco, simplesmente por inexistirem opções viáveis e juridicamente seguras.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Conforme já destacado na resposta ao quesito nº 5, com fundamento nos entendimentos do ICO, da INAI e da Autoridade de Proteção de Dados da Coreia, indicamos a seguir as medidas de segurança consideradas essenciais para a proteção de dados biométricos:

- Controles de acesso aos dados;
- Realização de testes de penetração;
- Implementação de política de segurança da informação;

³⁸ <https://www.gov.br/anatel/pt-br/assuntos/dicas-contras-fraudes/golpes-atuais-mais-comuns>

- Criptografia dos dados pessoais, tanto em trânsito quanto em repouso;
- Realização de varredura (*scan*) de vulnerabilidades nos sistemas que tratam dados biométricos, com adoção de medidas corretivas;
- Registro em logs de todos os acessos aos dados biométricos;
- Armazenamento de dados biométricos de forma segregada de outras informações; e
- Quando houver contratação de fornecedor, realização de processo adequado de *due diligence*.

Com relação aos parâmetros mínimos que devem ser seguidos para identificar e monitorar os riscos de segurança relacionados à biometria facial, não há distinção relevante entre a metodologia aplicável a esse tipo de dado e aquela utilizada para riscos cibernéticos em geral. Nesse sentido, conforme estabelecido na norma ISO/IEC 27005:2023³⁹, os seguintes passos devem ser observados:

a) Estabelecimento de critérios de risco: consiste na definição, com base na tolerância ao risco da organização, dos parâmetros para a aceitação de riscos; e

b) Identificação dos riscos: inclui o mapeamento de: (i) ativos envolvidos; (ii) ameaças que possam incidir sobre tais ativos; (iii) controles de segurança já existentes; e (iv) vulnerabilidades identificadas. No contexto específico da biometria facial, é importante considerar os tipos de ataque mais comuns descritos no Guia do Centro de Cibersegurança Nacional do Reino Unido (“NCSC”)⁴⁰:

- **Ataques de apresentação:** técnica mais frequente em reconhecimento facial. Utiliza-se um artefato, como uma foto, para fraudar a validação da identidade.
- **Interceptação do resultado de sensores:** tentativa de interceptar ou modificar os dados captados pelo sensor, ou seja, *inputs* captados no mundo físico – como foto, vídeo ou quaisquer outros – para burlar o sistema ou prejudicar o seu funcionamento.
- **Subversão da integridade da inscrição:** inserir, nos registros de alguém, dados biométricos de outro indivíduo para fraudar a biometria facial.
- **Ataque de banco de dados:** alterar dados durante transmissão ou armazenamento.
- **Ameaça interna:** ações realizadas por profissionais que utilizam suas credenciais e seus acessos legítimos para executar ações criminosas.
- **Ataques aos sistemas de TI:** ataques típicos de segurança a sistemas de TI que sustentam a operação.
- **Ataques de negação de serviço:** ataques voltados à indisponibilização do sistema, podendo forçar a instituição a operar em redes alternativas e potencialmente menos seguras — motivo pelo qual a infraestrutura de contingência deve possuir padrão de segurança equivalente ao do sistema biométrico principal.

c) Analisar os riscos: identificar as potenciais consequências decorrentes da efetivação dos riscos e da probabilidade de sua ocorrência, definindo, por meio de ambos os elementos, o nível do risco.

d) Tomar decisão: com base nos critérios de risco definidos anteriormente, deve-se decidir se o risco é aceitável e, conforme o caso, escolher a estratégia apropriada: mitigação, retenção,

³⁹ <https://www.normas.com.br>

⁴⁰ <https://www.ncsc.gov.uk/collection/biometrics>

compartilhamento ou eliminação. Um plano de ação correspondente pode ser necessário a depender da estratégia de mitigação escolhida.

e) Monitoramento: os elementos que compuseram a análise de risco devem ser permanentemente observados, de modo que qualquer alteração — como o surgimento de uma nova ameaça — seja incorporada à avaliação de riscos de maneira tempestiva.

Considerando a natureza sensível e o alto potencial de impacto dos dados biométricos, é recomendável que se reconheça o uso de dados sintéticos gerados por modelos generativos de IA como medida complementar válida para mitigar riscos em testes e treinamentos, desde que utilizados de forma controlada e transparente.

No tocante ao primeiro questionamento, referente às boas práticas para assegurar que a limitação do uso de biometria facial não configure tratamento discriminatório, reiteramos os pontos já apresentadas no quesito nº 8.

Por fim, ressalta-se a recomendação feita pela Autoridade de Proteção de Dados Sul-Coreana (“PIPC”) ao afirmar que o tratamento de dados biométricos exige atenção redobrada devido ao seu caráter sensível, irreversível e altamente exposto a tentativas de fraude, como o uso de biometria forjada⁴¹. Esses ataques envolvem, por exemplo, impressões digitais em silicone, captura de fotos ou vídeos de rostos e íris de terceiros, gravações de voz ou *deepfakes* com alto nível de realismo. Assim, a PIPC afirma ser indispensável que os controladores adotem medidas técnicas e administrativas específicas para prevenir esse tipo de ataque.

Contudo, mesmo diante da adoção de melhores práticas, há situações em que fraudes cometidas por terceiros não podem ser integralmente prevenidas pelo controlador. Inclusive, a indústria de dispositivos móveis enfrenta riscos associados ao uso de biometria forjada, como impressões digitais em silicone, *deepfakes* de voz ou manipulações de imagem facial. Nesses casos, deve-se observar o art. 43, III, da LGPD, segundo o qual o controlador não pode ser responsabilizado quando provar que não foi o causador direto do dano — especialmente quando demonstrar que adotou todas as medidas razoáveis de segurança e mitigação dos riscos.

Dessa forma, a regulamentação deve estabelecer parâmetros mínimos para avaliação de risco e monitoramento contínuo, mas reconhecer os limites técnicos e operacionais de controle diante de ataques sofisticados. A lógica da responsabilização deve estar pautada no dever de diligência e proporcionalidade, promovendo a proteção dos titulares sem inviabilizar a inovação e o uso legítimo de dados biométricos.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

No que se refere ao primeiro questionamento, além das providências já descritas no item nº 8, consideramos essencial levar em conta a questão da acessibilidade da tecnologia empregada (como no caso de pessoas com deficiência visual, que podem enfrentar obstáculos relevantes ao

⁴¹ https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

utilizarem soluções desse tipo)⁴². Diante disso, é recomendável que as organizações reflitam sobre essas limitações e busquem implementar estratégias que reduzam tais barreiras. Sempre que for possível comprovar a existência de deficiência visual, podem ser adotadas, de forma excepcional, alternativas de autenticação, mesmo que não ofereçam o mesmo nível de segurança.

Quanto ao tratamento de dados fundamentado no consentimento, compreendemos que a recusa do titular em autorizar o uso de biometria pode acarretar a indisponibilidade de certas funcionalidades, desde que essas dependam, de forma efetiva, do uso de dados biométricos. Por exemplo:

- Se uma instituição financeira disponibiliza aos clientes a opção de autenticar transações por biometria ou senha, é legítimo deixar de oferecer o método biométrico àqueles que não consentirem com o tratamento dos dados.
- Uma rede de academias pode permitir o ingresso às suas instalações mediante reconhecimento facial ou senha vinculada ao número de matrícula⁴³; se o consentimento não for concedido, o acesso via biometria facial será inviabilizado.

Para garantir previsibilidade e segurança jurídica, é importante que se reconheça que, em certas funcionalidades tecnicamente estruturadas com base em autenticação biométrica, como acesso rápido a dispositivos ou ativação de serviços sensíveis, a recusa do consentimento poderá, sim, justificar a limitação proporcional da experiência do usuário. Tal reconhecimento é essencial para assegurar que o princípio do melhor interesse do titular não seja interpretado para inviabilizar, na prática, o uso legítimo de soluções seguras e eficientes, baseadas em biometria embarcada e protegidas por mecanismos de *opt-out* e informações claras.

É importante frisar que, no contexto em que o consentimento é a base legal adotada, a negativa do titular não pode resultar na limitação de acesso a funcionalidades ou serviços cuja operação não exija, de fato, o tratamento de dados biométricos.

Para as demais hipóteses, entende-se que a recusa do titular em fornecer sua biometria configura, na prática, o exercício do direito de oposição. Nesses casos, a restrição do acesso à funcionalidade, produto ou serviço que dependa da biometria será considerada legítima se ao menos uma das seguintes condições estiver presente: (i) a prestação da funcionalidade seja, na prática, inviável sem o tratamento de dados biométricos, conforme já mencionado no contexto do consentimento; ou (ii) os direitos e interesses protegidos que justificam o uso da biometria prevaleça sobre o direito do titular de se opor — ou seja, haja uma justificativa relevante que torne necessária a validação biométrica, como a tutela de um bem jurídico relevante⁴⁴.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Remetemos novamente às respostas já apresentadas nos quesitos nºs 2, 5, 8 e 11.

⁴² <https://www.vice.com/en/article/facial-recognition-apps-are-leaving-blind-people-behind/>

⁴³ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>

⁴⁴ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>

No que se refere aos mecanismos apropriados de proteção, além da indispensável análise dos riscos relacionados à segurança cibernética — conforme descrito no quesito nº 11 —, reforçamos a importância dos controles mencionados no quesito nº 8, os quais se baseiam em diretrizes emitidas por distintas autoridades de proteção de dados, como o ICO (Reino Unido), o INAI (México) e a Autoridade de Proteção de Dados sul-coreana.

Quanto às medidas de transparência, a exigência legal diz respeito ao fornecimento das informações previstas no artigo 9º da LGPD. A maneira mais adequada de apresentar essas informações, conforme destacado nos quesitos nºs 2 e 8 e com base nas orientações do ICO, dependerá de diversos elementos — como a finalidade da operação de tratamento, o tipo de vínculo com o titular e os dados envolvidos.

De forma resumida, quanto mais clara e previsível for a operação de tratamento em análise — levando em consideração também os padrões normalmente adotados pelo mercado —, menor será a necessidade de empregar mecanismos ativos de transparência para assegurar que as informações legais sejam efetivamente disponibilizadas ao titular.

Por fim, no que tange ao risco de discriminação, reiteramos as precauções já mencionadas no quesito nº 8, fundamentadas nas recomendações do ICO.

Além das práticas já mencionadas, devem ser considerados os diferentes níveis de maturidade e finalidade de soluções tecnológicas que usam dados biométricos. Em projetos experimentais ou de pesquisa aplicada, como o uso de sensores para rastreamento ocular, análise de marcha ou reconhecimento de tremores, eventuais dados coletados não visam a tomada de decisões individuais, tampouco resultam em perfilamento ou em segmentação de titulares. Nesses casos, exigências excessivas podem comprometer iniciativas de inovação com risco residual mínimo.

Assim, a abordagem baseada em risco e contexto permitirá distinguir tratamentos que exigem salvaguardas reforçadas daqueles voltados exclusivamente à pesquisa e ao desenvolvimento tecnológico. É essencial que a regulamentação permita que fabricantes de *hardware*, como os do setor de celulares, implementem estratégias de *privacy by design* ajustadas à sua atuação específica, distinguindo suas obrigações das de plataformas ou provedores de serviços online. A imposição de deveres uniformes pode comprometer a inovação e ignorar a diferença entre quem desenvolve o dispositivo e quem controla efetivamente os dados tratados em sua operação.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

No que se refere ao direito à informação, conforme já mencionado na resposta ao quesito nº 2, situações em que os titulares não possuem uma expectativa razoável quanto à coleta de seus dados biométricos, tampouco mantêm qualquer relação prévia com a empresa controladora, demandam um grau maior de esforço para o cumprimento do dever de transparência.

Esse dever pode ser satisfeito, por exemplo, por meio da instalação de sinalizações visuais em locais de fácil acesso e visibilidade, contendo explicações gerais sobre a atividade de tratamento

de dados, além da disponibilização de canais para obtenção de informações mais completas e para o exercício dos direitos previstos em lei. Da mesma forma, é possível empregar QR Codes fixados em suportes físicos — como paredes, totens ou telas — que direcionem os titulares ao Aviso de Privacidade da organização, a qual deve apresentar, de maneira clara, os elementos exigidos pela legislação aplicável.

Medidas semelhantes já foram objeto de análise por esta Autoridade Nacional, que as considerou adequadas ao dever de transparência, conforme registrado na Nota Técnica nº 29/2024/FIS/CGF/ANPD, item §6.1.4⁴⁵.

No contexto de cidades inteligentes e tecnologias embarcadas, é fundamental reconhecer que nem sempre será possível garantir a transparência tradicional por meio de vínculo direto entre controlador e titular. Para tais cenários, deve-se autorizar a adoção de mecanismos alternativos e escaláveis, como sinalizações visuais, QR Codes e acesso remoto a avisos de privacidade, que sejam razoáveis frente à tecnologia aplicada e ao tipo de interação com o usuário. Esse modelo é particularmente relevante para testes de detecção facial embarcada em dispositivos móveis, sem coleta persistente de dados, em que não há identificação do indivíduo nem geração de perfil, o que reforça a proporcionalidade do dever de transparência.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Para além das medidas de transparência já elucidadas nos quesitos anteriores, considerando as particularidades da tecnologia biométrica, a garantir de exercício dos direitos dos titulares é crucial.

Com relação ao direito de acesso, o ICO⁴⁶ observa que há limitações técnicas para disponibilizar os dados biométricos em sua forma bruta, pois normalmente se trata de representações numéricas complexas, que não são facilmente interpretáveis (“ilegíveis”). Por esse motivo, é possível substituir o fornecimento direto por um comunicado explicativo que:

- a) apresente a razão pela qual não é viável entregar o dado de forma direta;
- b) detalhe a natureza da informação biométrica em questão; e
- c) informe de que modo essa informação é armazenada pela organização.

É relevante ressaltar que isso não impede o compartilhamento de outros dados que estejam relacionados à validação biométrica do titular, como, por exemplo, seu identificador pessoal (CPF ou RG) ou, quando aplicável, as amostras biométricas originais utilizados para a criação dos *templates*.

Quanto ao direito de retificação, o ICO aponta que ele não se aplica à verificação probabilística entre a informação fornecida pelo titular e os registros existentes no banco de dados, uma vez

⁴⁵https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-29_2024.pdf

⁴⁶<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>

que esse processo tem base estatística⁴⁷. Todavia, esse direito poderá ser exercido se houver erro na vinculação entre o identificador do titular e seu *template* biométrico, ou ainda se houver uma modificação física significativa que exija a atualização do *template*, como uma cirurgia plástica.

Para que esse direito seja implementado de forma eficaz, é necessário que os *templates* biométricos possuam a característica de serem “revogáveis e renováveis” — ou seja, que possam ser atualizados sem manter relação técnica com os anteriores⁴⁸.

Com relação à revogação do consentimento, seu atendimento também depende da possibilidade de revogação do *template* biométrico, o que significa que ele deve ser passível de cancelamento.

No entanto, é preciso enfatizar que revogar o consentimento não implica, obrigatoriamente, eliminar o histórico das autenticações já realizadas. Isso porque podem existir finalidades legítimas e independentes do consentimento que justifiquem a conservação desses registros, como o atendimento a obrigações legais ou regulatórias, ou ainda a necessidade de manter os registros para auditorias ou segurança.

No caso de soluções tecnológicas baseadas em biometria embarcada, é igualmente importante assegurar que os *templates* gerados possam ser revogados e substituídos a qualquer tempo, sem gerar vínculo técnico irreversível com registros anteriores. Tal arquitetura técnica é essencial para permitir a efetiva revogação do consentimento e a renovação da biometria, garantindo autodeterminação informativa e segurança operacional. Além disso, ao tratar de sistemas que operam com IA embarcada ou com modelos pré-treinados por terceiros, deve-se esclarecer que a responsabilidade do usuário legítimo de tais modelos deverá se limitar à sua esfera de controle, em especial quando não há participação no pré-treinamento ou na coleta dos dados originais. A ausência de delimitação pode gerar insegurança jurídica desproporcional e desestimular o uso responsável de IA no país.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

Conforme já reconhecido pela ANPD por meio do Enunciado CD/ANPD nº 1/2023⁴⁹, o tratamento de dados pessoais de crianças e adolescentes pode se apoiar em qualquer uma das bases legais previstas no artigo 11 da LGPD, desde que seja garantido o respeito ao princípio do melhor interesse do menor.

Desse modo, uma vez observados os critérios legais de enquadramento e demonstrado que a finalidade do tratamento está alinhada com os interesses da criança ou do adolescente, será

⁴⁷<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>

⁴⁸ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

⁴⁹<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf>

possível fundamentar o tratamento de dados biométricos desses titulares em qualquer uma das hipóteses autorizadas pelo referido artigo da Lei.

No tocante à transparência e à participação dos pais ou responsáveis, ainda que a legislação britânica (*Protection of Freedoms Act 2012*) adote abordagem distinta — exigindo o consentimento parental para o tratamento de dados biométricos de menores —, as diretrizes presentes no manual do governo do Reino Unido⁵⁰ podem ser consideradas como parâmetro complementar, desde que devidamente adaptadas à realidade normativa brasileira.

Nesse sentido, além da inclusão do tratamento de dados biométricos no aviso de privacidade da organização, recomenda-se, sempre que possível:

- A realização de comunicação específica e formal aos pais ou responsáveis legais, contendo informações objetivas sobre a operação de tratamento, seus propósitos e fundamentos legais;
- A disponibilização de canais de atendimento para o esclarecimento de dúvidas e o exercício de direitos dos titulares;
- Quando aplicável, a oferta de meios para que os responsáveis se oponham ao tratamento, com orientações visíveis e de fácil compreensão sobre como exercer essa prerrogativa.

A análise do melhor interesse da criança, por sua vez, deve ser feita caso a caso, considerando, entre outros aspectos:

- O bem jurídico protegido, especialmente o interesse do menor, de forma a permitir uma avaliação da proporcionalidade entre a finalidade pretendida e o nível de interferência na privacidade do titular;
- A viabilidade de adotar alternativas menos invasivas que possam alcançar os mesmos objetivos com desempenho semelhante;
- A instabilidade de certas características biométricas em crianças e adolescentes, como, por exemplo, a alteração significativa dos traços faciais durante a puberdade — o que pode comprometer tratamentos que demandem a conservação de dados por longos períodos⁵¹.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

No que diz respeito às bases legais aplicáveis e à necessidade de participação informada de pais ou responsáveis, são pertinentes as considerações já expostas no tópico anterior. Em resumo:

- **Sobre as hipóteses legais:** conforme estabelecido pela ANPD por meio do Enunciado CD/ANPD nº 1/2023, o tratamento de dados pessoais de crianças e adolescentes pode ser fundamentado em qualquer uma das bases legais previstas no art. 11 da LGPD, desde que, em todos os casos, seja priorizado o melhor interesse do menor. Dessa forma, é possível a utilização de dados biométricos de crianças e adolescentes, desde que a base legal adotada esteja devidamente justificada e a atividade de tratamento seja conduzida com foco na proteção dos seus direitos e interesses.

⁵⁰ https://assets.publishing.service.gov.uk/media/62d7d76c8fa8f50c012d14df/Biometrics_Guidance_July_2022.pdf

⁵¹ https://quno.org/sites/default/files/resources/QUNO_Briefing%20Paper_Biometric%20data%20of%20CPACTO_SE_P2020.pdf

- **Quanto à prestação de informações:** além da disponibilização das informações exigidas por lei no Aviso de Privacidade da organização, recomenda-se, sempre que viável, a comunicação direta e formal aos pais ou responsáveis legais. Essa comunicação deve apresentar, de maneira objetiva, os principais aspectos do tratamento realizado e os canais disponíveis para o exercício dos direitos dos titulares.

Ainda nesse contexto, é relevante que se incentive a adoção de boas práticas já consolidadas em ambientes de pesquisa, como a dissociação entre dados biométricos e identificadores pessoais, o uso de técnicas de anonimização desde a origem e o acesso restrito às equipes diretamente envolvidas nos projetos. Essas medidas demonstram que é possível compatibilizar a proteção de direitos de crianças e adolescentes com a continuidade de iniciativas científicas inovadoras e eticamente conduzidas.

Por fim, no que se refere à adoção de medidas de segurança, aplicam-se as orientações previamente descritas nos quesitos nºs 5 e 11.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

A implementação de métodos para verificar a idade deve levar em conta: (a) o cenário específico em que tal verificação ocorre; (b) o nível de precisão da tecnologia utilizada; e (c) a presença de alternativas menos invasivas que sejam igualmente eficazes em alcançar o objetivo pretendido.

i) Contexto de verificação da faixa etária

A avaliação do contexto é fundamental para determinar se a coleta de dados biométricos é compatível com o princípio da necessidade e com a proteção do melhor interesse da criança ou do adolescente. De acordo com as diretrizes do ICO⁵², o método escolhido para verificar a idade deve ser proporcional aos riscos que o serviço prestado e o respectivo tratamento de dados podem representar aos menores.

Por exemplo, quando se trata de acesso a jogos eletrônicos ou a plataformas com conteúdo adulto — ou que exponham crianças e adolescentes a riscos digitais como a interação com pessoas desconhecidas e potencialmente perigosas — o uso de biometria facial pode ser considerado apropriado e em consonância com a proteção dos interesses do menor. Em contrapartida, para situações de menor sensibilidade, como o envio de boletins informativos, uma simples autodeclaração pode ser considerada suficiente.

ii) Acuracidade da tecnologia adotada

Outro ponto que merece atenção é o grau de exatidão da ferramenta tecnológica adotada. Soluções de estimativa de idade com base em características biométricas tendem a apresentar margens de erro mais elevadas^{53 54}. Por isso, a combinação de análise documental

⁵² <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/3-age-assurance-methods/>

⁵³ [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA\(2023\)739350_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf)

⁵⁴ <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>

(documentoscopia) com a verificação da correspondência entre o indivíduo e o documento apresentado pode oferecer maior confiabilidade.

iii) Meios alternativos menos intrusivos

Também deve ser considerada a possibilidade de adotar soluções alternativas que, embora menos intrusivas, apresentem nível de confiabilidade equivalente — ou minimamente suficiente em relação ao risco de acesso indevido por parte de menores. Exemplos de métodos alternativos incluem^{55 56}:

- Autodeclaração da idade, por meio do preenchimento da data de nascimento pelo próprio usuário;
- Validação por cartão de crédito, com realização de transação simbólica (como R\$ 0,01) para confirmar a titularidade e idade;
- Análise comportamental, inferindo a idade a partir do padrão de navegação, tipo de conteúdo acessado e outras informações contextuais;
- Verificação presencial de documentos, em ambiente físico, antes da liberação de acesso;
- Obtenção de consentimento dos responsáveis legais, desde que a identidade e autoridade desses responsáveis possam ser verificadas com segurança.

Em relação à verificação de idade por meio de biometria facial, é essencial que a regulamentação estabeleça critérios proporcionais ao risco do serviço oferecido, evitando assim a imposição de soluções excessivamente intrusivas em situações de baixo risco e impacto. Além disso, devem ser reconhecidos os avanços tecnológicos na adoção de técnicas híbridas, como a própria análise de documentos combinada com detecção facial em tempo real sem armazenamento, as quais conciliam maior precisão com menor exposição de dados. Em ambientes de alto risco, o uso de soluções com essa arquitetura pode representar medida tecnicamente adequada e compatível com o melhor interesse do menor, desde que complementada por salvaguardas apropriadas e possibilidade de controle pelos responsáveis legais.

Em síntese, o uso da biometria facial como ferramenta para verificação etária requer análise criteriosa em cada situação, sempre à luz do princípio do melhor interesse da criança e do adolescente, levando em consideração os riscos envolvidos e os impactos potenciais do tratamento de dados biométricos.

Atenciosamente,

Samsung

Pamella Kim | Marina Almeida

VLK Advogados

Caio Lima | Giovanna Milanese | Ingrid Soares | Alana Dalcin

⁵⁵ [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA\(2023\)739350_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf)

⁵⁶ <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>

Brasília, 02 de julho de 2025

À

**Coordenação-Geral de Normatização da
Autoridade Nacional de Proteção de Dados (ANPD)**

Ref.: Contribuições da Associação Brasileira de Anunciantes – ABA à TPS de Dados Sensíveis – Dados Biométricos

Prezados (as) Senhores (as),

Este documento tem como objetivo apresentar à Coordenação-Geral de Normatização da ANPD informações complementares e mais detalhadas às contribuições da Associação Brasileira de Anunciantes – **ABA** – submetidas na Plataforma Participa + Brasil a respeito da Tomada de Subsídios para a elaboração de materiais orientativos e regulamentos acerca do tratamento de dados biométricos, relevante assunto que tem se tornado cada vez mais urgente face à evolução de soluções digitais.

REPRESENTATIVIDADE DA ABA

A **ABA – Associação Brasileira de Anunciantes**, entidade sem fins lucrativos atuante há mais de 65 anos no mercado, posiciona-se publicamente contra toda comunicação publicitária enganosa ou abusiva, atuando ativamente para conscientizar anunciantes e agências contra representações que possam gerar qualquer tipo de discriminação. Na qualidade, ainda, de uma das fundadoras do CONAR (Conselho Nacional de Autorregulamentação Publicitária) e por ser filiada à **WFA** (*World Federation of Advertisers*) e membro de seu **Executive Committee** – entidade que congrega associações de anunciantes de 60 países – a **ABA** atua ativamente para conscientizar anunciantes contra quaisquer práticas que possam implicar desrespeito à legislação e à autorregulamentação existentes ou abuso ao consumidor.

ABA está igualmente atenta e preocupada com o uso equilibrado de novas tecnologias no contexto da publicidade digital, o que pode englobar a utilização de dados biométricos como forma de provisão e personalização de serviços, mecanismos de autenticação e segurança, e insumo para o desenvolvimento de novos sistemas computacionais.

A **ABA** compreende que o uso de dados biométricos por ferramentas de inteligência artificial no contexto da publicidade digital deve observar critérios de necessidade, proporcionalidade e transparência, de modo a garantir que sua aplicação esteja alinhada ao melhor interesse do consumidor, à ética na comunicação e ao respeito às normas de proteção de dados, inclusive no tocante a públicos sensíveis como crianças e adolescentes. Nesse contexto, a **ABA** apresenta, a seguir, os eixos centrais que orientam sua contribuição.

CONTRIBUIÇÕES DA ABA

BLOCO I DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) classifica os dados biométricos como dados pessoais sensíveis (art. 5º, II), mas não define de forma precisa os critérios para essa caracterização. Nesse contexto, é útil observar parâmetros internacionais, em especial o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), cujo artigo 4(14) define dados biométricos como “dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a sua identificação única”.

Essa definição é aprofundada pelo Information Commissioner's Office (ICO) do Reino Unido, que estabelece três critérios cumulativos para a qualificação de um dado como biométrico:

- **Natureza do dado:** o dado deve se referir a características físicas (como distância entre os olhos), fisiológicas (como padrão da íris) ou comportamentais (como modo de andar ou padrão de digitação) de uma pessoa natural;
- **Tratamento técnico específico:** é necessário que o dado seja submetido a um processo técnico que extraia um identificador único da pessoa. Desse modo, uma simples fotografia de uma pessoa, ainda que possa caracterizar um dado pessoal, não equivale a um dado biométrico caso não seja submetida a técnicas específicas para extração de

padrões da imagem que permitam a obtenção de uma identidade digital única a partir de outra imagem.

- Finalidade de identificação: o dado deve ser processado com a finalidade de permitir ou confirmar a identificação única do indivíduo.

Outros critérios que poderiam conferir maior segurança jurídica e nível de certeza ao regulado:

- Avaliar o grau de permanência e estabilidade do dado, dado que características biométricas geralmente são relativamente estáveis ao longo do tempo, como a íris ou impressões digitais.
- Maior potencial de permitir a reidentificação a partir do cruzamento de famílias de dados pessoais anonimizados de diferentes naturezas.
- Emprego do dado para reconhecimento automático de indivíduos.
- Grau de exclusividade das relações estatísticas extraídas a partir do dado em relação a um único sujeito.

A adoção de critérios objetivos como esses pela ANPD contribuiria para maior segurança jurídica e coerência interpretativa à aplicação da LGPD no que diz respeito ao tratamento de dados biométricos.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Para assegurar o cumprimento do princípio da transparência (art. 6º, VI, LGPD), os controladores que realizam tratamento de dados biométricos devem adotar práticas que garantam ao titular informações claras, completas e acessíveis **antes ou no momento** da coleta dos dados.

As orientações do ICO, a esse propósito, são muito instrutivas.¹ Segundo a autoridade britânica de proteção de dados, dentre os elementos mínimos que devem ser comunicados (antes e/ou durante a coleta) para que se cumpra o princípio da transparência estão: os canais de contato do controlador; as finalidades específicas do tratamento; a base legal correspondente e, quando for o caso, a explicitação do interesse legítimo invocado; os dados que serão efetivamente coletados; os destinatários ou categorias de destinatários com os quais os dados poderão ser

¹ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>

compartilhados; e, se aplicável, a existência de transferências internacionais para empresas ou organizações estrangeiras.

Além disso, devem ser informados os prazos de retenção dos dados biométricos ou, caso não seja possível especificá-los, os critérios utilizados para definição desse período. O controlador deve também esclarecer quais são os direitos assegurados aos titulares nos termos da LGPD, inclusive a possibilidade de revogação do consentimento e de apresentação de reclamação à autoridade supervisora, bem como informar, quando pertinente, se há obrigação legal ou contratual para o fornecimento dos dados pessoais.

O ICO também destaca que as informações prestadas devem ser redigidas de forma concisa, transparente, acessível e em linguagem clara e simples, respeitando a capacidade de compreensão do público-alvo e reduzindo a assimetria informacional entre controlador e titular. Não há uma única forma prescrita para a disponibilização dessas informações, devendo a escolha do meio levar em conta as especificidades do contexto de tratamento.

Em ambientes físicos, por exemplo, recomenda-se o uso de folhetos informativos, códigos QR posicionados antes da entrada em locais monitorados, orientações prestadas por funcionários treinados, além de recursos visuais ou sonoros acessíveis. Já em ambientes digitais, as boas práticas incluem o uso de notificações em camadas (*layered notices*), painéis de controle (dashboards) com explicações sobre os tratamentos realizados, e avisos no momento da coleta (*“just-in-time notices”*), que contextualizam de forma direta e imediata o uso pretendido dos dados.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A biometria comportamental, como reconhecimento de voz, padrões de digitação e rastreamento ocular, traz desafios específicos à proteção de dados pessoais. A União Europeia² tem reconhecido que esse tipo de dado pode viabilizar violações graves à privacidade dos titulares, especialmente quando utilizado para finalidades além daquelas para as quais o consentimento foi inicialmente fornecido. Isso ocorre porque, diferentemente da biometria tradicional — que visa a identificação inequívoca de um indivíduo com base em características físicas estáveis —, os dados biométricos comportamentais permitem a realização de inferências biométricas, ou seja, a extração de informações preditivas sobre o comportamento, os

² [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/697131/IPOL_BRI\(2021\)697131_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/697131/IPOL_BRI(2021)697131_EN.pdf)

sentimentos e os pensamentos dos titulares. Trata-se, portanto, de espécie de profilização que depende de mecanismos muito mais pervasivos de monitoramento do indivíduo, e que é fundada em dados que podem revelar aspectos subjetivos e íntimos da personalidade, frequentemente sem que o titular tenha plena ciência ou tenha consentido com esse tipo de uso.

Apesar desses riscos, não há, até o momento, diferenciação regulatória expressa entre biometria tradicional e comportamental nas principais jurisdições. Assim, entende-se que o tratamento desses dados deve observar rigorosamente os princípios da LGPD, com destaque para os princípios da qualidade dos dados — que impõe a adoção de medidas para garantir a exatidão, relevância e atualização dos dados coletados — e da segurança, que exige a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, perdas e outros incidentes.

Adicionalmente, recomenda-se que controladores que utilizem biometria comportamental adotem medidas reforçadas de transparência, como explicitação das inferências possíveis, revisão periódica das finalidades do tratamento, e análise de proporcionalidade quanto à real necessidade de coleta desse tipo de dado. Em casos de tratamento contínuo ou preditivo, a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) pode ser uma boa prática para documentar os riscos envolvidos e as salvaguardas aplicadas.

Embora as disposições gerais da LGPD e as boas práticas de governança e segurança sejam atualmente suficientes como marco jurídico, é recomendável que a ANPD acompanhe a evolução técnica e comercial da biometria comportamental, avaliando, no futuro, a necessidade de normativos específicos para garantir a proteção adequada aos titulares frente a essa tecnologia emergente.

BLOCO II

HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Como indicado na pergunta, à luz da LGPD, para que o consentimento no tratamento de dados biométricos seja válido ele deve ser livre, específico, destacado, informado e inequívoco. Esse é um assunto fundamental, pois a aparente liberdade de decisão do titular por consentir ou não com o tratamento de seus dados por vezes é insuficiente para garantir que seu consentimento

seja de fato livre, informado e inequívoco, eis que por vezes o contexto no qual está inserido e a falta de alternativas pode **condicionar o titular ao consentimento**, mesmo que aquela não fosse sua primeira opção.

Nesse contexto, digno de nota são as diretrizes do ICO³, do Reino Unido, que oferecem boas práticas que podem ser utilizadas como referência para garantir tais condições:

- É essencial que haja transparência plena quanto às finalidades do tratamento, às bases legais envolvidas, ao compartilhamento de dados e aos direitos do titular.
- Além disso, o titular deve ter autonomia real para recusar ou revogar o consentimento a qualquer momento, de maneira simples e sem sofrer qualquer forma de prejuízo.
- Para que a escolha seja genuinamente livre, é fundamental oferecer uma alternativa funcional e adequada àqueles que optem por não consentir. A ausência dessa alternativa – exceto em hipóteses de impossibilidade técnica em que o dado biométrico seja imprescindível à execução do serviço – compromete a validade do consentimento.
- O consentimento deve ser específico, ou seja, atrelado a finalidades determinadas e informadas previamente. Qualquer alteração nas finalidades ou nas operações de tratamento requer novo consentimento. Também deve ser inequívoco, manifestado por meio de ação afirmativa clara (*opt-in*), como: assinatura de formulário; clique em botão de aceite em ambiente digital; seleção ativa de opções em dashboards de preferências; ou resposta expressa a e-mail solicitando consentimento. O silêncio do titular, caixas pré-marcadas, *opt-outs* ou a aceitação genérica de termos de uso não satisfazem esse requisito.
 - Importante destacar que a oferta de contrapartida financeira pode comprometer a liberdade do consentimento, ao induzir a manifestação de vontade por razões econômicas. No Brasil, esse entendimento foi acolhido pela ANPD no caso Tools for Humanity, no qual a Autoridade entendeu que a coleta de dados biométricos de íris, ainda que respaldada por consentimento formal, não atendia ao requisito de liberdade, uma vez que envolvia pagamento ao titular, criando assim um vício de vontade.
- Por fim, como mencionado, o consentimento não deve ser utilizado como base legal quando não for possível oferecer uma escolha genuína ao titular.⁴ Isso se aplica a contextos em que: (i) o dado seria tratado mesmo sem o consentimento (e.g., com

³ Tradução nossa. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/#whatotherspecial>.

⁴ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/#:-:text=Consent%20will%20not%20usually%20be,is%20not%20considered%20freely%20given.>

base em contrato ou interesse público); (ii) o consentimento é exigido como pré-condição para acesso a produtos ou serviços; ou (iii) há desequilíbrio de poder entre controlador e titular, como ocorre em relações entre empregador e empregado ou entre autoridades públicas e cidadãos. Nessas hipóteses, a utilização do consentimento como base legal pode ser inadequada e ilusória.

A ANPD, ao regular o tema, pode detalhar diretrizes específicas para o uso legítimo do consentimento no contexto da biometria, de modo a assegurar proteção efetiva aos direitos fundamentais dos titulares.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A aplicação da hipótese legal de tratamento de dados pessoais sensíveis prevista no art. 11, II, “g” da LGPD — referente à “garantia da prevenção à fraude e à segurança do titular” — exige o atendimento rigoroso aos princípios da necessidade, da proporcionalidade e da finalidade específica,⁵ sobretudo quando envolvido o uso de dados biométricos.

Quanto à *necessidade*, é imprescindível que o controlador demonstre, de forma documentada, que o uso de dados biométricos é indispensável para alcançar um nível de segurança que não poderia ser razoavelmente obtido por meios menos intrusivos. A utilização de biometria deve ser justificada a partir da análise de risco concreta da operação, sendo necessário mostrar por que alternativas como senhas fortes, autenticação de múltiplos fatores (MFA) baseadas em posse (tokens, celulares) ou conhecimento (senhas), ou ainda verificações por outros canais (SMS, e-mail), seriam insuficientes. A mera conveniência operacional ou redução de custos não satisfazem esse critério.

No que se refere à *proporcionalidade*, a tecnologia biométrica empregada deve ser adequada e proporcional ao risco que se pretende mitigar. A adoção, por exemplo, de reconhecimento facial contínuo para autenticação em um aplicativo de baixo risco — que sequer realiza transações financeiras — seria claramente desproporcional. Medidas excessivas, além de

⁵ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>.

desnecessárias, podem estabelecer precedentes para a normalização de formas ainda mais invasivas de coleta de dados, *em desrespeito à autodeterminação informativa*.

Já no tocante à *finalidade específica*, é fundamental que os dados biométricos coletados sob a justificativa de prevenção à fraude sejam utilizados exclusivamente para este fim, dentro do contexto estritamente relacionado à autenticação, segurança da conta e prevenção de acessos indevidos. A reutilização desses dados para fins secundários, como marketing, personalização de conteúdo ou *analytics*, deve ser expressamente vedada.

A experiência regulatória comparada oferece bons parâmetros. No Reino Unido, por exemplo, a Data Protection Act reconhece a prevenção à fraude como uma das hipóteses de legítimo interesse público substancial para o tratamento de dados biométricos. Nesses casos, é exigido que o controlador comprove que o tratamento é eficaz para prevenir ou detectar ilícitos e que não existem meios menos intrusivos para alcançar o mesmo objetivo.

Para mitigar os riscos associados ao uso dessa base legal, recomenda-se a adoção das seguintes salvaguardas:

- (i) elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), documentando a avaliação de risco, as alternativas consideradas, a justificativa da escolha biométrica e as medidas de mitigação adotadas;
- (ii) implementação de Tecnologias de Privacidade (Privacy-Enhancing Technologies – PETs), como armazenamento descentralizado dos dados biométricos (localmente no dispositivo do titular), uso de chaves criptográficas em posse exclusiva do usuário; ou verificação biométrica por meio de "sinal de autorização" (sem envio do dado biométrico bruto ao servidor);
- (iii) Adoção de criptografia de ponta a ponta, segregação de bases de dados, controle rigoroso de acesso, anonimização ou pseudonimização quando possível, e planos específicos de resposta a incidentes envolvendo dados biométricos; e
- (iv) Transparência ativa com os titulares, que devem ser claramente informados sobre a utilização de seus dados biométricos para fins de prevenção à fraude, sobre o funcionamento da tecnologia, e sobre as garantias implementadas.

Tais salvaguardas estão alinhadas com diretrizes da EDPB⁶ (European Data Protection Board) e da CNIL⁷ (Comissão Nacional de Informática e Liberdades, da França), e reforçam a compatibilização entre segurança e proteção de direitos fundamentais. A ANPD, ao

⁶ https://www.edpb.europa.eu/system/files/2024-05/edpb_opinion_202411_facialrecognitionairports_en.pdf

⁷ https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_ven_0.pdf

regulamentar o tema, poderá consolidar esses critérios como condição para o uso legítimo da base legal de prevenção à fraude no tratamento de dados biométricos.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

O tratamento de dados biométricos com base no art. 11, II, “a” da LGPD — que autoriza o tratamento de dados sensíveis quando necessário para o cumprimento de obrigação legal ou regulatória pelo controlador — deve observar uma série de critérios para assegurar que esse fundamento seja aplicado de forma legítima, proporcional e de acordo com os direitos dos titulares.

Conforme orientações do ICO,⁸ a aplicação dessa base legal é válida quando atendidos aos seguintes **requisitos**:

- A obrigação legal que justifica o tratamento deve estar prevista em norma interna do ordenamento jurídico.
- A aplicação da norma deve ser previsível aos indivíduos, ou seja, os titulares devem ser capazes de antecipar, de modo razoável, que seus dados poderão ser tratados nesse contexto.
- A obrigação deve ser identificável de maneira clara, seja por meio da menção expressa ao dispositivo legal aplicável, seja por referência inequívoca a fontes oficiais (como portais governamentais, normas infralegais ou diretrizes regulatórias setoriais).
- O tratamento biométrico deve ser necessário e proporcional ao cumprimento da obrigação legal ou regulatória, sendo inadequada a aplicação dessa base legal se houver outro meio razoável e menos intrusivo de atender à norma em questão.

A adoção dessa hipótese legal por órgãos públicos ou entidades sujeitas a deveres regulatórios deve vir acompanhada de salvaguardas robustas, que assegurem a proteção dos direitos fundamentais dos titulares. Dentre elas, destacam-se:

- **Minimização de dados:** devem ser coletados apenas os dados biométricos estritamente necessários ao cumprimento da obrigação legal.

⁸ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legal-obligation/>

- **Limitação de finalidade:** os dados coletados não devem ser utilizados para outros propósitos além daqueles expressamente vinculados à norma legal que embasa o tratamento, sendo vedada sua reutilização para fins secundários não compatíveis.
- **Limitação do período de retenção:** os dados devem ser armazenados apenas pelo tempo necessário para o cumprimento da obrigação, sendo excluídos após o atingimento dessa finalidade.
- **Segurança desde a concepção e por padrão (*privacy by design and by default*):** exige-se a aplicação de medidas técnicas e organizacionais adequadas, como técnicas de criptografia, segregação de bases de dados, controle de acesso restrito e mecanismos de rastreabilidade.
- **Transparência ativa:** os titulares devem ser claramente informados sobre o tratamento de seus dados, com destaque para a base legal utilizada, a norma aplicável, a finalidade do tratamento e os direitos disponíveis.

A utilização dessa hipótese legal por entes estatais demanda ainda uma postura reforçada de responsabilização e prestação de contas (*accountability*), inclusive com a adoção, sempre que pertinente, de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), especialmente quando o tratamento envolver tecnologias biométricas altamente invasivas, como reconhecimento facial em espaços públicos.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Nos termos do art. 11, II, “c”, da LGPD, o tratamento de dados sensíveis, como os biométricos, é autorizado para fins de realização de estudos por órgãos de pesquisa, desde que respeitados os princípios da legislação e, sempre que possível, com a utilização de dados anonimizados. A anonimização, quando efetiva e irreversível, retira o dado da categoria de dado pessoal nos termos do art. 5º, III, da LGPD. No entanto, para que essa exclusão de aplicabilidade seja válida, é necessário garantir que a técnica de anonimização seja robusta e não possa ser revertida mediante cruzamento com outras bases de dados ou uso de inferências externas.

O European Data Protection Board (EDPB)⁹ publicou estudo em que examina os limites do tratamento de dados para fins de pesquisa científica, reconhecendo que a anonimização,

⁹ https://www.edpb.europa.eu/system/files/2022-01/legalstudy_on_the_appropriate_safeguards_89.1.pdf

embora desejável, não é absoluta e que a possibilidade de reidentificação por meio de cruzamento de bases é um risco real que deve ser mitigado por meio de salvaguardas técnicas e organizacionais.

Além disso, no contexto europeu, o art. 89(1) do GDPR impõe, como salvaguardas obrigatórias, o respeito ao princípio da **minimização de dados** (isto é, a coleta e uso apenas dos dados estritamente necessários ao objetivo da pesquisa) e a **pseudonimização**, como técnica adicional de proteção, especialmente quando a anonimização plena não é possível. Um exemplo é a substituição do template biométrico por um código criptografado, o que permite reduzir riscos sem comprometer a integridade da pesquisa.

Outrossim, diversas jurisdições europeias adotam salvaguardas específicas. A França, por exemplo, pode exigir o consentimento expresso do titular ou a autorização prévia da autoridade competente. Na Alemanha, exige-se a elaboração de um plano de proteção de dados, bem como o fracionamento e armazenamento separado de conjuntos de dados que, combinados, poderiam levar à reidentificação. Outros países requerem a realização de uma avaliação de impacto (DPIA) específica, para documentar os riscos e as estratégias de mitigação adotadas.

No Reino Unido, a norma técnica ISO/IEC 24745,¹⁰ oferece diretrizes fundamentais para a segurança de dados biométricos, que poderiam ser adotadas ou recomendadas pela ANPD. Elas incluem:

- Irreversibilidade do dado (template), que não pode ser revertido para reconstruir a aparência da pessoa.
- Desvinculação do dado para que o template não possa ser correlacionado com outras bases ou reutilizado em diferentes sistemas para identificação cruzada.
- Revogabilidade e renovação do dado, de modo que o template possa ser substituído sem nova coleta biométrica, o que reduz os impactos em caso de incidente.

Dessa forma, mesmo em contextos de pesquisa científica, em que há forte interesse público e incentivo à produção de conhecimento, é imprescindível que o tratamento de dados biométricos — ainda que anonimizados — observe um padrão elevado de governança, segurança e prestação de contas.

BLOCO III

TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

¹⁰ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

O uso de tecnologias de reconhecimento facial, mesmo quando respaldado por uma das hipóteses legais previstas na LGPD, demanda um grau elevado de cautela, transparência e responsabilidade por parte do controlador. Como se trata de uma modalidade de tratamento automatizado de dados biométricos sensíveis, com forte potencial de impacto sobre direitos fundamentais, sua utilização deve observar com rigor os princípios da necessidade, da proporcionalidade, da transparência e da não discriminação.

Aplicam-se aqui as mesmas exigências normativas já estabelecidas para outras formas de tratamento de dados biométricos. **Assim, na ausência de consentimento válido, é preciso demonstrar que não há meio menos intrusivo capaz de atingir a finalidade pretendida, sendo o reconhecimento facial a única alternativa tecnicamente viável.** Já nos casos em que o tratamento se baseia no consentimento, como dito, este deve ser livre, informado, destacado, específico e inequívoco — o que pressupõe, entre outros aspectos, **a oferta de alternativa equivalente para os que optarem por não consentir, salvo nas raras hipóteses de impossibilidade técnica.** A simples conveniência operacional ou o apelo à inovação tecnológica não bastam para justificar a adoção dessa tecnologia.

Além disso, é essencial que sejam adotadas boas práticas de transparência e segurança da informação, informando de forma clara aos titulares como a tecnologia funciona, qual a finalidade do reconhecimento facial, qual a base legal adotada, quem terá acesso aos dados coletados, por quanto tempo eles serão armazenados e como podem ser excluídos. Deve ser assegurada também a possibilidade de revisão humana de decisões automatizadas, sempre que aplicável.

No entanto, os riscos envolvidos na aplicação dessa tecnologia transcendem a lógica individual de proteção de dados. Estudos nacionais e internacionais demonstram que algoritmos de reconhecimento facial frequentemente apresentam maior taxa de erro para pessoas negras, mulheres, crianças, idosos e pessoas trans, **gerando discriminações estruturais**, especialmente quando aplicados em contextos de segurança pública, controle de acesso e vigilância em massa. Nesses casos, **o impacto sobre grupos vulnerabilizados pode se traduzir em violações sistemáticas de direitos fundamentais**, como liberdade de locomoção, presunção de inocência, privacidade e igualdade.

Diante desse cenário, recomenda-se a implementação de salvaguardas técnicas, jurídicas e institucionais específicas, entre as quais se destacam:

- Avaliação prévia de impacto à proteção de dados pessoais (RIPD), especialmente em projetos que envolvam uso em larga escala ou em espaços públicos.
- Auditorias algorítmicas independentes, com foco em viés, acurácia e impactos discriminatórios, com divulgação dos resultados sempre que possível.
- Proibição do uso da tecnologia em determinadas finalidades de alto risco, como vigilância generalizada, profilagem automatizada ou abordagens policiais com base em probabilidade de comportamento futuro.
- Obrigação de *accountability* reforçada, com relatórios periódicos de governança e documentação das decisões que justificaram a escolha da tecnologia.
- Supervisão externa por órgãos de controle e participação social, especialmente em contratos públicos e parcerias com empresas privadas que utilizam esse tipo de solução.
- Adoção de medidas de mitigação técnica, como uso de modelos treinados com conjuntos de dados representativos da diversidade demográfica, exclusão de armazenamento permanente dos dados biométricos e utilização de sistemas descentralizados ou locais, sempre que possível.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Para garantir a eficácia e confiabilidade dos sistemas de reconhecimento facial (FRT), é essencial que eles sejam desenvolvidos com base no princípio da proteção de dados desde a concepção (*privacy by design*), incorporando salvaguardas técnicas e organizacionais desde as fases iniciais do projeto.

O EDPB¹¹ classifica as principais técnicas de mitigação de viés e aumento de acurácia em três categorias complementares:

¹¹ https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf. p. 8 e ss. Tradução nossa.

1. **Pré-processamento:** modificação dos dados de treinamento para reduzir viés de origem histórica, de mensuração ou de representação, evitando associações indesejadas entre variáveis sensíveis (como raça ou gênero) e os resultados.
2. **Durante o processamento:** ajustes no próprio processo de treinamento do modelo, como alteração da função-objetivo ou inclusão de restrições de otimização para minimizar o viés e reduzir erros sistemáticos.
3. **Pós-processamento:** aplicação de correções estatísticas aos resultados já obtidos, com uso de métricas como taxas de erro por grupo, margem de confiança ou ajuste de decisão conforme contexto de uso.

Essas técnicas são fundamentais para mitigar falsos positivos e negativos, que podem gerar impactos graves sobre os titulares, especialmente em contextos de controle de acesso, segurança ou concessão de benefícios.

Além das salvaguardas algorítmicas, é indispensável que o sistema assegure ao titular o **direito** à revisão humana sempre que a decisão automatizada puder produzir efeitos relevantes — como bloqueio de acesso, recusa de serviço ou penalidades automáticas. Essa revisão deve ser:

- **Tempestiva:** com prazos razoáveis, definidos em políticas internas;
- **Real:** realizada por pessoa qualificada, com poder de modificar a decisão;
- **Acessível:** com canais claros, visíveis e funcionais para acionamento pelo titular.

O design e a governança de sistemas de reconhecimento facial devem ainda incluir monitoramento contínuo de performance, documentação de testes por grupo demográfico, e, quando aplicável, auditorias independentes.

A ANPD poderá definir requisitos mínimos para garantir a confiabilidade e a auditabilidade desses sistemas, especialmente em contextos de uso público ou em aplicações que afetem direitos fundamentais.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Não existem restrições absolutas de tecnologias de reconhecimento facial que sirvam de exemplo para o Brasil. Contudo, existem algumas tendências relevantes no campo internacional: na Europa, por exemplo, conforme ilustra o documento “*Guidelines 05/2022 on*

*the use of facial recognition technology in the area of law enforcement*¹², a utilização de tecnologias de reconhecimento facial na segurança pública para vigilância em massa tem sido cada vez menos recomendada – sendo, inclusive, proibida em muitos países –, diante do risco de que o perfilamento leve a discriminação, bem como do inúmeros dilemas éticos que dizem respeito a essa prática, como a dificuldade de informar devidamente o titular do dado ou de, se for o caso, obter o seu consentimento.

Em atenção ao princípio da necessidade e da proporcionalidade, existem alternativas ao reconhecimento facial que garantem relativa segurança, como a utilização de verificação em dois fatores, *token* em posse exclusiva do titular, senhas e afins, a depender do contexto (como numa operação bancária ou para entrada em espaços restritos).

¹² https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

BLOCO IV

SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Diante da natureza sensível e imutável dos dados biométricos, o comprometimento desses dados — como no caso de vazamentos, clonagens ou uso indevido — pode gerar prejuízos severos e irreversíveis, como o roubo de identidade. Por isso, a proteção desses dados exige medidas técnicas e administrativas robustas, baseadas em análise de risco contextualizada e na adoção de padrões de segurança contínuos e verificáveis.

A análise de risco deve considerar: (i) as circunstâncias específicas do tratamento; (ii) a gravidade do dano potencial em caso de incidente; e (iii) os vetores mais prováveis de ataque, incluindo falhas humanas, vulnerabilidades técnicas e ameaças internas.

Entre as medidas de segurança indispensáveis, o ICO¹³ destaca:

- Testes regulares e revisão contínua das medidas de segurança adotadas;
- Criptografia forte para proteger os dados biométricos em trânsito e em repouso;
- Controle físico de acesso aos locais onde se armazenam os bancos de dados e servidores;
- Avaliação sistemática de vulnerabilidades.

No caso específico de dados biométricos, recomenda-se a adoção de tecnologias de aprimoramento da privacidade (Biometric PETs). A norma ISO/IEC 24745 estabelece três atributos de segurança essenciais:

- Irreversibilidade do dado (template), que não pode ser revertido para reconstruir a aparência da pessoa.
- Desvinculação do dado para que o template não possa ser correlacionado com outras bases ou reutilizado em diferentes sistemas para identificação cruzada.
- Revogabilidade e renovação do dado, de modo que o template possa ser substituído sem nova coleta biométrica, o que reduz os impactos em caso de incidente.

¹³ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

Outra boa prática é a verificação no dispositivo (on-device verification), que reduz o risco de exposição, uma vez que o template é gerado e armazenado apenas no dispositivo do titular, e apenas um token criptografado é transmitido ao servidor.

Assim, para garantir a conformidade com a LGPD, a ANPD pode exigir:

- Adoção de medidas preventivas baseadas nos princípios da minimização e limitação de armazenamento, tratando apenas o mínimo necessário e armazenando os dados pelo menor tempo possível;
- Testes periódicos de segurança, inclusive com simulações de ataque (como testes de penetração e auditorias externas);
- Revisão periódica da análise de risco e dos controles de segurança associados a sistemas biométricos, documentados por meio de Relatórios de Impacto (RIPD) e planos de resposta a incidentes.

Dado o alto risco associado ao tratamento de dados biométricos, essas medidas devem ser vistas como patamar mínimo de conformidade, especialmente em setores sensíveis como finanças, saúde, transporte, segurança pública e educação.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

A utilização de dados biométricos em serviços não essenciais, especialmente quando fundamentada no consentimento, deve ser guiada pelos princípios da proporcionalidade, não discriminação e autonomia do titular. Como se trata de dados sensíveis e imutáveis, os titulares devem ter a opção real de recusar seu fornecimento sem prejuízo desproporcional ou tratamento desfavorável.

Para evitar discriminação injusta, recomenda-se como boa prática a oferta de alternativa funcionalmente equivalente à biometria. Por exemplo, no lugar de leitura de impressão digital, pode-se utilizar senhas combinadas com tokens ou dispositivos de uso exclusivo do titular. Essa abordagem é especialmente importante para garantir acessibilidade, evitando a exclusão de pessoas que, por razões físicas ou técnicas, não podem utilizar soluções biométricas.

O tratamento biométrico deve ser estritamente proporcional ao fim pretendido. Em uma plataforma de e-commerce, por exemplo, a navegação, a realização de compras e o pagamento não podem depender exclusivamente de autenticação biométrica. Essa funcionalidade pode ser oferecida como opção para facilitar o acesso, mas jamais como pré-condição de uso.

De forma geral, a negativa do titular ao fornecimento de dados biométricos não pode resultar em restrição de acesso ao serviço ou produto, salvo quando o tratamento for efetivamente necessário à execução do contrato, hipótese que exige comprovação objetiva dessa indispensabilidade.

Segundo o ICO,¹⁴ do Reino Unido, quando o acesso a um serviço estiver condicionado ao fornecimento de dados biométricos, o consentimento não será considerado válido se não houver real liberdade de escolha. Nestes casos, a base legal mais apropriada pode ser a execução do contrato, desde que o uso da biometria seja indispensável à funcionalidade em questão. O consentimento, por sua vez, só deverá ser exigido quando houver previsão normativa específica, como ocorre, por exemplo, nas situações reguladas pelas normas britânicas de comunicações eletrônicas (PECR).

Portanto, é essencial que o tratamento biométrico em serviços facultativos seja opcional, claramente informado, e baseado em alternativas não discriminatórias, com salvaguardas que assegurem tratamento isonômico e respeito à autodeterminação informativa.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Para garantir a proteção eficaz dos dados biométricos, os controladores devem adotar boas práticas específicas, alinhadas aos princípios da LGPD e aos padrões internacionais de governança em proteção de dados sensíveis. Como esses dados são altamente identificáveis, imutáveis e de uso crescente em sistemas automatizados, sua coleta e uso exigem níveis elevados de cautela, responsabilidade e transparência.

Em primeiro lugar, o tratamento deve observar rigorosamente os princípios da necessidade e proporcionalidade: os dados só devem ser coletados se não houver outra forma menos invasiva de atingir a finalidade pretendida, e o tipo de biometria utilizada deve ser compatível com o nível

¹⁴ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>

de risco e sensibilidade da operação. A finalidade deve ser específica e claramente informada ao titular, sendo vedada a reutilização dos dados para fins secundários não compatíveis.

No plano técnico, é essencial que os sistemas adotem medidas de segurança desde a concepção e por padrão (privacy by design e by default), o que inclui a aplicação de:

- Tecnologias de privacidade para dados biométricos (B-PETs), como templates irreversíveis, desvinculados e revogáveis;
- Criptografia forte, controle de acesso rigoroso e segregação de dados;
- Verificação local (on-device) sempre que possível, para evitar exposição excessiva dos dados.

No aspecto organizacional, os controladores devem garantir:

- Transparência ativa, com informações claras e acessíveis sobre como os dados biométricos são coletados, utilizados e protegidos;
- Auditorias e testes regulares, inclusive com foco na detecção e mitigação de vieses discriminatórios nos sistemas biométricos;
- Revisão humana de decisões automatizadas baseadas em biometria, especialmente quando tais decisões impactam o acesso a direitos ou serviços;
- Treinamento de equipes técnicas e jurídicas para evitar usos abusivos ou excessivos da tecnologia.

A prevenção da discriminação ilícita ou abusiva exige atenção especial a sistemas automatizados, como os de reconhecimento facial ou verificação comportamental, que historicamente têm apresentado desempenho desigual entre grupos sociais. A aplicação de testes de acurácia segmentada, avaliação prévia de impacto (RIPD) e supervisão contínua são elementos-chave para evitar efeitos discriminatórios não intencionais.

Por fim, os dados biométricos devem ser armazenados apenas pelo tempo estritamente necessário, em conformidade com o princípio da limitação de armazenamento, sendo descartados ou anonimizados de forma segura ao final de sua finalidade.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle

sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

O tratamento contínuo e massivo de dados biométricos em espaços públicos — como em projetos de cidades inteligentes, eventos de grande porte e monitoramento urbano — impõe desafios concretos à efetivação da autodeterminação informativa dos titulares. Nesses contextos, o exercício dos direitos previstos na LGPD não pode ser comprometido pela escala da coleta, pela ausência de interação direta entre controlador e titular, ou pela alegada impossibilidade de obtenção de consentimento.

Para garantir que os titulares sejam devidamente informados e possam exercer seus direitos, os controladores devem adotar medidas de transparência ativa, adaptadas ao ambiente físico e digital. Essas medidas incluem:

- Sinalização clara e acessível nos pontos de entrada e circulação (como cartazes, painéis visuais e avisos sonoros);
- Disponibilização de QR Codes, folhetos explicativos ou materiais informativos nos locais monitorados;
- Colaboradores treinados para esclarecer dúvidas;
- Páginas web ou plataformas digitais com informações completas, preferencialmente acessíveis antes da chegada ao local (como no ato de compra de ingressos).

Essas informações devem incluir a finalidade do tratamento, os dados coletados, a base legal aplicada, os direitos dos titulares (como acesso, retificação, oposição ou eliminação), bem como os canais para exercício desses direitos.

Além da transparência, o respeito à autodeterminação informativa exige o cumprimento rigoroso dos princípios da necessidade e da proporcionalidade. Isso significa que a coleta biométrica deve ser limitada ao estritamente necessário, justificada por objetivos legítimos, e empregada apenas quando não houver meio menos intrusivo para atingir a finalidade desejada.

Casos de uso por autoridades públicas, especialmente para fins de segurança pública ou law enforcement, merecem atenção redobrada. O uso de reconhecimento facial para vigilância generalizada, por exemplo, tem sido objeto de críticas de entidades como o EDPB¹⁵, em razão dos riscos de perfilamento discriminatório e violação da privacidade em massa. Nessas situações, o consentimento individual pode ser inviável, o que reforça a necessidade de fundamentar o tratamento em base legal compatível (como interesse público) e de realizar avaliações prévias de impacto à proteção de dados (RIPD).

¹⁵ https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

A coleta massiva de dados biométricos, por sua natureza, demanda ainda:

- Limitação do tempo de retenção, com exclusão automática dos dados assim que a finalidade for atingida ou expirado o prazo necessário;
- Medidas robustas de segurança da informação, para evitar vazamentos ou usos indevidos;
- Supervisão por órgãos de controle independentes, com transparência sobre os critérios de uso e mecanismos de auditoria.

BLOCO V

DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

O respeito aos direitos dos titulares em contextos de tratamento automatizado de dados biométricos exige a adoção de práticas específicas de transparência, controle e responsabilização, especialmente diante da opacidade que sistemas algorítmicos podem gerar.

Em primeiro lugar, deve-se assegurar que o direito à informação clara seja respeitado de forma ativa. Isso significa apresentar os avisos de privacidade em linguagem acessível, estruturados em camadas e no momento da coleta, especialmente quando o titular interage com sistemas automatizados, como aplicativos, sites ou totens. A interface deve exibir os avisos de maneira proeminente antes da ativação do sensor biométrico, permitindo a tomada de decisão consciente.

O titular deve ser claramente informado sobre:

- Quais dados biométricos serão coletados;
- A finalidade específica do tratamento;
- A base legal adotada;
- O tempo de retenção;
- E quais são os seus direitos, inclusive com links ou comandos para exercício imediato desses direitos.

No que diz respeito ao direito de acesso e correção, o controlador deve disponibilizar canais acessíveis e funcionais para que o titular possa visualizar os dados coletados e solicitar, por

exemplo, a releitura biométrica ou recalibração do template (como uma nova captura de face ou impressão digital).

Já quanto ao direito de revogação do consentimento, deve-se garantir que o ato de revogar seja tão simples quanto o de consentir. Recomenda-se que o sistema disponha de um botão ou comando claramente identificado, como “desativar login por biometria” ou “revogar consentimento”, garantindo que o titular possa exercer sua vontade de forma intuitiva e sem barreiras técnicas.

Em casos de decisões automatizadas com efeitos relevantes — como o bloqueio de conta ou a negação de acesso a determinado espaço —, o titular deve ser informado sobre essa possibilidade e ter assegurado o direito à revisão humana qualificada, em prazo razoável, por profissional com autoridade para revisar e eventualmente alterar a decisão.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O tratamento de dados biométricos de crianças e adolescentes exige um grau ainda mais elevado de proteção, em razão tanto da natureza sensível desses dados quanto da condição peculiar de desenvolvimento dos titulares. Nos termos do art. 14 da LGPD, o tratamento de dados de menores deve sempre observar o princípio do melhor interesse, sendo este o critério interpretativo central para avaliar a legitimidade de qualquer operação.

As hipóteses legais de tratamento previstas na LGPD são, em tese, aplicáveis — como o consentimento dos pais ou responsáveis, o cumprimento de obrigação legal ou regulatória, ou a proteção da vida ou da incolumidade física do titular. No entanto, em qualquer dessas hipóteses, é indispensável respeitar os princípios da necessidade, proporcionalidade, finalidade específica, transparência, minimização dos dados e segurança.

O caso analisado pela autoridade de proteção de dados da Polônia,¹⁶ sob a vigência do GDPR, oferece importante precedente. Em uma escola, dados biométricos de alunos — no caso, impressões digitais — foram coletados para controle de acesso à cantina. Embora a escola obtivesse o consentimento prévio e expresso dos pais, a autoridade concluiu que o tratamento

¹⁶ https://www.edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en

era desnecessário e, portanto, ilegal. Isso porque havia meios menos invasivos, como o uso de carteiras de identificação, e alunos cujos responsáveis não consentiram eram submetidos a constrangimento — tendo de aguardar ao final da fila, o que configurou tratamento discriminatório indireto.

Esse exemplo evidencia que o consentimento, ainda que formalmente obtido, não legitima o tratamento quando este não for necessário ou proporcional ao fim pretendido. A simples conveniência administrativa não justifica o uso de tecnologias invasivas em relação a menores. Portanto, para garantir o respeito ao melhor interesse da criança e do adolescente, os agentes de tratamento devem:

- Obter consentimento específico, expresso e destacado dos pais ou responsáveis, preferencialmente por escrito e com linguagem acessível;
- Avaliar se o tratamento é estritamente necessário e não pode ser substituído por alternativa menos intrusiva;
- Garantir igualdade de acesso aos serviços independentemente da opção dos pais pelo uso da biometria;
- Aplicar medidas de segurança e retenção mínima, com exclusão dos dados ao final da finalidade ou do vínculo contratual;
- Adotar práticas reforçadas de transparência ativa, inclusive com canais de contato específicos para os responsáveis legais.

A ANPD poderá estabelecer diretrizes específicas para ambientes educacionais e recreativos, reforçando que, no caso de menores, a proteção da privacidade não é apenas um direito individual, mas também um dever coletivo de cuidado.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

O tratamento de dados biométricos de crianças e adolescentes, por envolver tanto dados sensíveis quanto titulares em condição peculiar de desenvolvimento, exige o cumprimento rigoroso da LGPD, com especial atenção ao princípio do melhor interesse do menor (art. 14) e aos princípios gerais aplicáveis ao tratamento de dados sensíveis.

As hipóteses legais admissíveis incluem, entre outras, o consentimento específico e informado dos pais ou responsáveis legais, o cumprimento de obrigação legal ou regulatória, e a proteção da vida ou da incolumidade física do titular. Independentemente da base legal adotada, o tratamento deve observar os princípios da necessidade, proporcionalidade, finalidade específica, minimização dos dados, transparência e segurança da informação.

Para garantir a participação informada dos pais ou responsáveis, é necessário:

- Obter consentimento expresso, específico e destacado, preferencialmente por escrito, com linguagem clara e acessível;
- Fornecer informações completas sobre os dados coletados, a finalidade do tratamento, o tempo de retenção, os direitos dos titulares e os canais de comunicação;
- Assegurar que nenhum prejuízo ou discriminação indireta recaia sobre o menor caso os pais optem por não consentir com o uso da biometria.

Do ponto de vista técnico e organizacional, devem ser implementadas medidas eficazes para prevenir abusos, vazamentos e acessos não autorizados. Dentre elas, destacam-se:

- Criptografia de ponta a ponta para dados em trânsito e em repouso;
- Armazenamento descentralizado ou local, quando possível, com uso de tokens controlados pelos responsáveis;
- Controle de acesso rigoroso às instalações físicas e aos sistemas digitais que armazenam dados biométricos;
- Registro e rastreabilidade de acessos;
- Elaboração de Relatório de Impacto à Proteção de Dados (RIPD) em contextos de maior risco;
- Treinamento de pessoal envolvido no tratamento, inclusive em ambientes escolares ou recreativos.

Essas medidas devem ser reforçadas por governança contínua e prestação de contas, especialmente quando o tratamento envolver terceiros contratados, como empresas de tecnologia educacional ou prestadoras de serviços em ambientes com presença infantil.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

A utilização de dados biométricos para verificação ou estimação de idade em plataformas digitais acessadas por crianças e adolescentes requer especial atenção aos princípios da necessidade, proporcionalidade e, sobretudo, ao melhor interesse do menor, conforme previsto

no art. 14 da LGPD. As autoridades europeias — como o EDPB¹⁷ e o ICO¹⁸ — já se manifestaram sobre esse tema, oferecendo diretrizes que podem inspirar boas práticas no Brasil.

Para o EDPB, é essencial avaliar se a verificação de idade por dados biométricos é realmente necessária para o tipo de serviço prestado. O uso dessa tecnologia não será proporcional se aplicado de forma indiscriminada a todos os usuários, inclusive em serviços sem conteúdo sensível ou risco associado. O Comitê recomenda que as organizações realizem:

- Uma Avaliação de Impacto sobre os Direitos da Criança (CRIA), quando o serviço representar riscos ao público infantojuvenil (como exposição a conteúdo nocivo ou interação com adultos); ou
- Uma Avaliação de Impacto à Proteção de Dados (DPIA), documentando os riscos e as salvaguardas aplicadas.

O EDPB também reforça a importância de fornecer métodos alternativos de verificação, evitando discriminação contra usuários sem acesso a meios tecnológicos ou documentos oficiais. Em caso de decisões automatizadas com efeitos significativos, como bloqueio de acesso à plataforma, devem ser previstos mecanismos de revisão humana e de correção de dados.

A transparência também é fundamental. As informações sobre o tratamento dos dados devem ser comunicadas de forma clara e apropriada à idade da criança, nos termos dos artigos 13 e 14 do GDPR, incluindo:

- A finalidade da verificação;
- As categorias de dados utilizadas;
- O tempo de retenção;
- A existência de decisões automatizadas;
- A possibilidade de exercício dos direitos dos titulares (acesso, correção, oposição etc.).

O ICO, por sua vez, destaca que a adoção de biometria para fins de *age assurance* deve seguir os princípios de legalidade, justiça, transparência, limitação de propósito, minimização, precisão, segurança, limitação de armazenamento e accountability. Antes de implementar essa tecnologia, o controlador deve:

- Avaliar os riscos específicos da plataforma para crianças;
- Justificar a necessidade da verificação de idade;
- Escolher o método mais proporcional e menos intrusivo possível.

¹⁷ https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_en

¹⁸ <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/6-expectations-for-age-assurance-and-data-protection-compliance/>

Na perspectiva da LGPD, a adoção desse tipo de verificação só será legítima se observadas as seguintes condições:

- Base legal adequada, com destaque para o consentimento dos pais ou responsáveis, nos termos do art. 14, §1º, ou outro fundamento cabível em contexto regulatório;
- Avaliação de necessidade e proporcionalidade, considerando se há meios alternativos viáveis e menos invasivos;
- Uso exclusivo para a finalidade declarada, com exclusão imediata dos dados após a verificação, se possível;
- Garantia de que o titular ou seu responsável poderá revisar decisões, corrigir imprecisões e revogar o tratamento com facilidade.

A ANPD poderá considerar a elaboração de diretrizes específicas sobre mecanismos de verificação de idade biométrica, especialmente em serviços digitais voltados ou acessíveis a crianças e adolescentes, assegurando a proteção de seus direitos e a compatibilidade com os princípios da LGPD.

* * *

Cordialmente,



Sandra Martinelli

CEO da ABA e Membro do *Executive Committee* da WFA

CONTRIBUIÇÃO ABCD – ASSOCIAÇÃO BRASILEIRA DE CRÉDITO DIGITAL

Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos

Assunto: Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos

Prazo: 1.8.2025

Protocolo: Espaço Opine Aqui, dentro da plataforma Participe+Brasil e no e-mail: normatizacao@anpd.gov.br

RESUMO (texto da ANPD)

O uso de dados biométricos teve um crescimento nos últimos anos, com potencial impacto nos direitos fundamentais. Se, por um lado, o tratamento desses dados pode ampliar a segurança e auxiliar a prevenção de fraudes; por outro lado, também são ampliados os riscos sobre os titulares, a exemplo de impactos negativos decorrentes de erros dos sistemas utilizados e de efeitos discriminatórios sobre grupos vulneráveis.

Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) incluiu, no item 5 da Agenda Regulatória para o biênio de 2025/2026, uma iniciativa para analisar a necessidade de intervenção regulatória sobre o tema, seja mediante regulamentação ou documento de caráter orientativo.

Os dados biométricos, caracterizados como dados pessoais sensíveis pela LGPD, demandam um tratamento rigoroso devido aos riscos que representam para a privacidade e os direitos dos titulares. A ANPD, em seu papel de regulamentar e fiscalizar o cumprimento da LGPD, busca aprofundar a compreensão sobre o uso dessas tecnologias no cenário brasileiro e nas situações destacadas no art. 3º da Lei.

Esta Tomada de Subsídios tem como objetivo coletar informações, evidências e perspectivas de diversos setores da sociedade sobre o tratamento de dados biométricos, visando a elaboração de materiais orientativos ou regulamentos que promovam a proteção de dados pessoais e a inovação responsável. As contribuições serão divididas em blocos temáticos, abordando hipóteses legais para o tratamento de dados biométricos, reconhecimento facial e aplicação de tecnologias emergentes e inovadoras, governança e boas práticas e direitos dos titulares e grupos vulneráveis.

BLOCO I - DEFINIÇÕES E PRINCÍPIOS (texto da ANPD)

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados Pessoais (LGPD),

especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo “dados biométricos”, mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos - que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Para caracterizar um dado como biométrico nos termos da LGPD, é necessário que ele se refira a características físicas, fisiológicas ou comportamentais únicas de uma pessoa natural, como impressões digitais, íris, geometria da face, voz, entre outros. No entanto, tais características só serão consideradas dados biométricos quando forem tecnicamente tratadas com a finalidade de identificar ou autenticar um indivíduo de forma inequívoca. Assim, o simples armazenamento de uma foto ou gravação de voz não configura, por si só, um dado biométrico: é imprescindível o uso de tecnologia para extrair, medir ou analisar essas características com propósito de identificar a pessoa física.

Além disso, devem ser observados critérios objetivos como a singularidade da característica (exclusiva de cada pessoa), sua mensurabilidade por meios tecnológicos, a relativa permanência no tempo e sua capacidade de promover identificação segura. O dado biométrico, portanto, resulta da conjugação entre a natureza da informação, o método técnico utilizado para tratá-la e a finalidade de identificação individual.

A confiabilidade da tecnologia utilizada também influencia diretamente a qualificação do dado, uma vez que o nível de precisão do sistema pode determinar o grau de sensibilidade e risco envolvido. A LGPD exige, portanto, uma análise contextual que considere a intenção,

o meio técnico e o resultado identificador do tratamento para enquadrar determinado dado como biométrico.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Os controladores já possuem a obrigação de garantir informações claras aos titulares de dados sobre o tratamento de seus dados pessoais, conforme disposto no artigo 9º da LGPD. No cenário em que ocorre o tratamento de dados pessoais biométricos, sugerimos como práticas de transparência ativa a serem consideradas como boas práticas:

- (i) Inserir, em suas políticas de privacidade, uma seção específica com informações sobre o tratamento de dados biométricos, contendo os dados coletados e as suas respectivas finalidades;
- (ii) Inserir, no momento da coleta de dados de entrada (e.g., face, impressão digital, íris), aviso sobre o tratamento de dados biométricos. O aviso pode ser realizado através de pop-up ou banner, por exemplo;
- (iii) Disponibilizar um canal específico para que os titulares de dados possam se comunicar com o controlador, nos casos em que houver questionamentos sobre o tratamento de dados biométricos e para gerenciamento do consentimento do titular sempre que essa for a base legal utilizada para justificar o tratamento.

A forma pela qual os controladores devem garantir a transparência do tratamento de dados biométricos, no entanto, pode variar a depender do agente de tratamento, da forma de comunicação entre o agente de tratamento e o titular dos dados e da finalidade do tratamento, de modo que o formato da comunicação não deveria ser pré-estabelecido.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A biometria comportamental — como padrões de digitação, entonação da voz, movimento ocular ou forma de uso de dispositivos — deve ser tratada com o mesmo rigor que a biometria tradicional — como impressão digital, íris, face -, desde que utilizada com a finalidade de identificação ou autenticação de indivíduos. Ambas se enquadram como dados pessoais sensíveis nos termos da LGPD, devendo observar os mesmos requisitos legais. No entanto, a biometria comportamental apresenta particularidades relevantes: pode ser coletada de forma passiva e contínua, muitas vezes sem o conhecimento direto do

titular, o que demanda uma postura proativa de transparência por parte dos agentes de tratamento. Isso inclui avisos claros sobre a coleta, as finalidades envolvidas, e — quando aplicável — a coleta do consentimento.

BLOCO II – HIPÓTESES LEGAIS (texto da ANPD)

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

O consentimento não deve ser considerado a base legal adequada para o tratamento de dados biométricos em todos os casos, especialmente quando esse tratamento for obrigatório para todos os titulares, sem possibilidade real de escolha. Em situações como a prevenção de fraudes no setor financeiro, por exemplo, a utilização de dados biométricos é fundamental para garantir a segurança e a verificação eficaz da identidade dos usuários.

Permitir que o titular opte por não fornecer esses dados poderia comprometer a finalidade legítima do tratamento e criar riscos operacionais. Nesses casos, o uso de outras bases legais — como o cumprimento de obrigação legal ou regulatória ou a prevenção à fraude — é mais apropriado, estando em conformidade com os princípios da necessidade e da segurança previstos na LGPD, especialmente no art. 49.

Quando o consentimento for a base legal escolhida, ele deve ser obtido de forma clara e transparente, conforme exigido pela LGPD: deve ser informado, específico e uma

manifestação inequívoca da vontade do titular. Isso implica apresentar, de forma acessível, quais dados biométricos estão sendo tratados, com que finalidade e oferecer a possibilidade de o titular consentir de forma consciente.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A aplicação da base legal de “prevenção à fraude” (art. 11, II, “g”, da LGPD) ao tratamento de dados biométricos deve considerar a existência de risco concreto de fraude que justifique o uso da biometria como medida eficaz de mitigação. Não se exige prova absoluta da indispensabilidade, mas é recomendável que o controlador possa demonstrar sua utilidade no contexto de tratamento.

O uso deve ser limitado a finalidades específicas, como identificação e autenticação, evitando extensões indevidas, como marketing. Sempre que possível, recomenda-se o uso de representações vetoriais (templates) e medidas como pseudonimização, autenticação local e controle de acesso.

A elaboração de um RIPD pode ser útil para documentar riscos e salvaguardas. A biometria pode compor estratégias de autenticação multifator, e alternativas razoáveis devem ser consideradas para quem não desejar fornecê-la. Transparência, revisão periódica e prevenção de vieses completam o conjunto de boas práticas.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Nos casos de tratamento de dados biométricos com base em obrigação legal (art. 11, II, “a”, da LGPD), é essencial que haja norma específica que justifique a coleta, com finalidade legítima e claramente definida. O uso deve ser proporcional e limitado ao necessário, preferindo-se representações vetoriais em vez de imagens brutas.

No setor financeiro, normas como a Circular 3.978/2020, Resolução 85/2021 (BCB) e Resolução CVM 50/2021 já regulam o uso de biometria para autenticação e prevenção à lavagem de dinheiro, com padrões técnicos e de segurança específicos.

Mesmo em tratamentos obrigatórios, devem ser adotadas salvaguardas como RIPD, controle de acesso, políticas de retenção e transparência sobre direitos dos titulares. A conformidade com a LGPD e com a regulação setorial é fundamental para garantir a legitimidade do tratamento.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Sem contribuição, considerando que a presente pergunta trata especificamente de estudos realizados por órgãos de pesquisa, a pergunta foge do escopo de atuação da ABCD.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS (texto da ANPD)

A utilização das tecnologias de reconhecimento facial (Facial Recognition Technologies, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento.

Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando

há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Para garantir que o uso de tecnologias de reconhecimento facial observe os princípios da LGPD, é necessário que o controlador:

- (i) Adote medidas para garantir a transparência sobre o tratamento aos titulares de dados, informando sobre a coleta de dados biométricos e finalidade do tratamento;
- (ii) Realize uma análise sobre possíveis outras formas de autenticação da identidade do titular, para verificar se há medidas menos invasivas, mas que garantam o mesmo nível de acurácia e eficiência;
- (iii) Identifique o tipo de dado de entrada necessário para atingir o propósito esperado, sem a coleta de dados excessivos (por exemplo, coleta de diversos dados de entrada para a geração de dados biométricos, quando a finalidade pode ser alcançada mediante o uso de um único tipo de dado de entrada); e
- (iv) Evite armazenar imagens brutas (por exemplo, fotos completas de rosto) se apenas representações vetoriais ou templates são suficientes para o reconhecimento.

Além disso, para evitar a discriminação ilícita ou abusiva, faz-se necessário que as tecnologias de reconhecimento facial possuam acesso amplo a conjuntos de dados relevantes e diversificados (e.g., raça, gênero, etnia) que permitam à tecnologia aprender representações robustas de diferentes grupos sociais e contextos, reduzindo riscos de discriminação e aumentando sua eficácia normativa e social.

Com informações limitadas, o sistema de reconhecimento facial potencialmente falhará ao inferir padrões e tenderá a reforçar vieses existentes (exacerbando desigualdades). A inclusão de critérios éticos na curadoria e uso das bases de treinamento é fundamental para garantir que a tecnologia opere de forma justa, responsável e alinhada aos direitos fundamentais.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Para garantir maior eficácia e confiabilidade, os sistemas de reconhecimento facial devem ser estruturados a partir de acesso amplo a conjuntos de dados relevantes e diversificados (e.g., raça, gênero, etnia) que permitam à tecnologia aprender representações robustas de diferentes grupos sociais e contextos, reduzindo riscos de discriminação e aumentando sua eficácia normativa e social. Com informações limitadas, o sistema de reconhecimento facial potencialmente falhará ao inferir padrões e tenderá a reforçar vieses existentes (exacerbando desigualdades) (referências de estudos: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf) e <https://open-research-europe.ec.europa.eu/articles/2-126>).

Para evitar e corrigir falhas identificadas nos sistemas de reconhecimento facial, os controladores devem implementar mecanismos como: (i) realização testes antes da utilização dos sistemas; (ii) realização de auditoria nos resultados; (iii) monitoramento contínuo dos resultados e das informações inseridas para treinamento dos sistemas; (iv) avaliação de fornecedores previamente à contratação; (v) adoção de proteções contratuais em relação aos fornecedores dos sistemas de reconhecimento facial; (vi) permitir o envio de feedbacks dos próprios usuários quanto aos sistemas utilizados.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Sim, é possível identificar contextos em que o uso de tecnologias de reconhecimento facial não é recomendado, mesmo reconhecendo sua utilidade para segurança e prevenção à fraude — especialmente no setor financeiro. A recomendação de restrição aplica-se, sobretudo, a usos sem finalidade legítima clara, com impactos desproporcionais à privacidade dos titulares, como em monitoramento massivo e contínuo de espaços públicos sem transparência ou base legal específica. Nesses casos, o reconhecimento facial pode gerar discriminação algorítmica, limitar liberdades individuais e ser inadequado à luz do princípio da necessidade, inclusive segundo entendimentos da própria ANPD.

No entanto, no contexto bancário e financeiro, o uso de reconhecimento facial pode ser altamente eficaz e proporcional, desde que voltado a finalidades legítimas e específicas — como autenticação segura de usuários, prevenção à fraude e atendimento a obrigações regulatórias (e.g., KYC). Para garantir o equilíbrio entre segurança e proteção de dados,

instituições financeiras devem avaliar o uso da tecnologia com base em RIPDs, adotar mecanismos de minimização (como uso de templates em vez de imagens brutas), e implementar salvaguardas como autenticação local (on-device), controle de acesso e criptografia forte. Ainda assim, é recomendável que, sempre que viável, sejam consideradas soluções complementares ou alternativas menos invasivas, como autenticação multifator, tokens, biometria comportamental ou QR Codes dinâmicos — tecnologias que, combinadas, permitem alto grau de segurança com menor impacto à privacidade.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS (texto da ANPD)

O tratamento de dados biométricos exige uma abordagem cautelosa e estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos.

Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes.

Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados.

Com base nisso, questiona-se:

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas

indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Diante dos riscos associados a eventuais violações de dados biométricos, como roubo de identidade e reidentificação indevida, é fundamental a adoção de medidas técnicas que garantam a segurança do tratamento desses dados sensíveis.

Entre as principais estão: criptografia em trânsito e em repouso, uso de templates biométricos em vez de imagens brutas, pseudonimização ou anonimização sempre que possível, controle rigoroso de acesso, gerenciamento seguro de chaves, firewalls e sistemas de detecção e prevenção de intrusos (IDS/IPS), além da realização periódica de testes de segurança, como pentests e varreduras de vulnerabilidade. Também se recomenda o monitoramento constante da performance dos sistemas biométricos — incluindo a detecção de vieses — e a coleta apenas dos dados estritamente necessários à finalidade pretendida.

Do ponto de vista administrativo, é essencial implementar políticas internas claras sobre o uso de dados biométricos, treinar regularmente os colaboradores, manter plano de resposta a incidentes atualizado, controlar acessos e revisar contratos com cláusulas específicas de proteção de dados. Além disso, devem ser realizadas avaliações de impacto à proteção de dados (RIPD), mantidos registros das operações de tratamento (ROPA), monitorados logs e atividades relevantes, e gerida adequadamente a cadeia de fornecedores. A combinação dessas medidas permite mitigar riscos, garantir conformidade com a LGPD e assegurar a proteção efetiva dos direitos dos titulares.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Eventual limitação de acesso a funcionalidades por não realização de autenticação biométrica é fundamental no contexto da sociedade brasileira, na qual a fraude é constante e cada dia mais elaborada, e principalmente para a atuação no sistema financeiro.

Para avaliar que tal limitação não configure discriminação ilícita ou abusiva, os controladores devem avaliar: (i) a essencialidade da funcionalidade; (ii) a criticidade do uso da funcionalidade; e (iii) os riscos relacionados à falta de autenticação biométrica para o uso da funcionalidade em questão. Em se verificando um risco relevante do uso de determinadas funcionalidades – sejam elas essenciais ou não – o uso de tecnologias de

identificação biométrica deveria ser suportado, desde que adotadas medidas de segurança adequadas.

Conforme já apresentado em questões anteriores, o tratamento de dados biométricos pode ser indispensável para uma determinada finalidade, como no caso de obrigações legais que determinem a necessidade de coleta e tratamento desses dados. Sempre que o tratamento de dados biométrico for indispensável para o acesso a uma funcionalidade, a base legal para justificar tal tratamento não será o consentimento. Ou seja, o consentimento só poderia ser utilizado como base legal para tratar dados biométricos quando o usuário puder, de fato, optar por não consentir com o tratamento.

Especificamente para os casos em que a base legal para tratar dados biométricos é o consentimento, seria justificável restringir o uso de funcionalidades caso o titular não dê o seu consentimento caso o acesso à funcionalidade sem a verificação biométrica permita riscos elevados, como acesso a informações altamente sensíveis, risco de fraude ou nos casos de pagamentos de alto valor, transferências financeiras em valores relevantes, assinatura eletrônica de documentos, entre outras.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

As boas práticas a serem adotadas pelos controladores especificamente no tratamento de dados biométricos devem incluir: (i) identificar o tipo de dado de entrada necessário para atingir o propósito esperado, sem a coleta de dados excessivos (por exemplo, coleta de diversos dados de entrada para a geração de dados biométricos, quando a finalidade pode ser alcançada mediante o uso de um único tipo de dado de entrada); (ii) evitar armazenar imagens brutas (por exemplo, fotos completas de rosto) se apenas representações vetoriais ou templates são suficientes para o reconhecimento; (iii) realizar testes e monitorar a performance de tecnologias de análise de dados biométricos; (iv) implementar controles internos de acesso e de retenção dos dados tratados; e (v) preencher um RIPD referente ao tratamento de dados biométricos.

Como forma de garantir transparência, os controladores devem fornecer informações claras aos titulares sobre o tratamento de seus dados biométricos, através de uma política de privacidade, por exemplo, sendo que as informações podem ser reforçadas no momento da coleta dos dados de entrada (facial, digital, voz, íris).

Conforme já destacado em outras respostas, para evitar a discriminação é necessário que se garanta acesso amplo a conjuntos de dados relevantes e diversificados (e.g., raça, gênero, etnia) que permitam à tecnologia aprender representações robustas de diferentes grupos sociais e contextos, aumentando sua eficácia normativa e social. Com informações

limitadas, sistemas de reconhecimento facial, por exemplo, potencialmente falharão ao inferir padrões e tenderão a reforçar vieses existentes (exacerbando desigualdades) (referências de estudos: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf) e <https://open-research-europe.ec.europa.eu/articles/2-126>).

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

O respeito à autodeterminação informativa do titular seria garantido pelos controladores através da disponibilização de informações relacionadas ao tratamento de dados biométricos e a partir da disponibilização de canais de comunicação aos titulares.

Para garantir a transparência os controladores devem adotar as medidas razoáveis, que estejam a seu alcance, para que as informações sobre o tratamento alcancem os titulares, como informações nos locais nos quais o tratamento ocorre ou nos quais os dados de entrada são coletados.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas

que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Para garantir o respeito aos direitos dos titulares, os controladores devem:

- (i) Assegurar a existência de um canal de comunicação acessível aos titulares, para que solicitações de exercício de direitos possam ser realizadas;
- (ii) Fornecer informações aos titulares de dados a respeito do tratamento, informando quando o tratamento de dados biométricos for realizado de forma automatizada;
- (iii) Na medida em que a base legal utilizada para o tratamento de dados biométricos for o consentimento, garantir que o titular reconheça o seu direito de revogação do consentimento, informando sobre as consequências de eventual revogação;
- (iv) Implementar mecanismos para a revisão de decisões tomadas unicamente com base em tratamento automatizado; e
- (v) Implementar processos internos para o atendimento da solicitação de titulares.

No entanto, conforme já discutido pelo Information Commissioner's Office (ICO) no *Biometric data guidance: Biometric recognition*, é importante destacar que pode haver limitações no exercício de direitos no contexto do tratamento de dados biométricos. Isso porque os vetores ou modelos gerados a partir do tratamento de dados de entrada, que permitem a identificação biométrica podem conter segredos de negócio e configurar propriedade intelectual de uma empresa. Como muito bem pontuado pelo ICO (disponível aqui: [biometric-data-guidance-biometric-recognition-all-1-0-3.pdf](#)):

“Ao mesmo tempo, podem existir algumas questões práticas ao fornecer a alguém uma cópia de seus dados biométricos.

Isso ocorre porque os dados biométricos provavelmente consistem em saídas matemáticas complexas em um formato específico (e muitas vezes proprietário) legível por máquina. Dados biométricos nesse formato não são “legíveis” por pessoas e, por design, podem nem mesmo ser legíveis por outros sistemas de reconhecimento biométrico.

O formato dos dados biométricos também pode significar que não seja possível fornecer as informações em outros formatos (ou seja, em papel ou mesmo em um formato eletrônico comumente utilizado).

Responder a solicitações de acesso do titular não exige que você traduza ou decifre as informações em sua totalidade.”

Dessa forma, as limitações existentes à tradução ou disponibilização de dados biométricos devem ser consideradas por esta r. Autoridade, em vista das excepcionalidades técnicas e tecnológicas aplicadas aos dados biométricos.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

No contexto do mercado financeiro, no qual a abertura de contas de menores de idade não emancipados está diretamente relacionada à representação dos responsáveis legais, conforme orientação do Banco Central do Brasil (disponível aqui: <https://www.bcb.gov.br/meubc/faqs/p/o-menor-de-idade-pode-ser-titular-de-conta>), a garantia da participação informada dos responsáveis pode ser obtida através do fornecimento de informações claras aos responsáveis sobre a necessidade do tratamento de dados biométricos do menor.

Ressalta-se o fato de que para as atividades relacionadas ao mercado financeiro, o uso de biometria para a validação da identidade do titular é considerado uma boa-prática para garantir a prevenção à fraude.

Com relação às hipóteses legais, nos termos do Enunciado CD/ANPD n° 1/2022, o tratamento de dados biométricos de crianças e adolescentes poderia ser fundamentado em qualquer uma das bases legais previstas no art. 11 da LGPD, desde que o melhor interesse da criança ou do adolescente seja observado.

Para assegurar o alinhamento ao princípio do melhor interesse, conforme previsto no art. 14 da LGPD e no Estatuto da Criança e do Adolescente, é necessário que o uso da biometria seja justificado por uma finalidade legítima, necessária e proporcional, evitando-se a coleta excessiva ou desnecessária de dados.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Nos termos do Enunciado CD/ANPD n° 1/2022, o tratamento de dados biométricos de crianças e adolescentes poderia ser fundamentado em qualquer uma das bases legais previstas no art. 11 da LGPD, desde que o melhor interesse da criança ou do adolescente seja observado.

Para garantir a participação dos pais, o controlador deve fornecer informações claras sobre o tratamento de dados, conforme disposto na Questão 2, bem como fornecer um canal de comunicação através do qual os responsáveis legais possam entrar em contato com o controlador a respeito do tratamento dos dados do menor.

Com relação à adoção de medidas técnicas e organizacionais para garantir a proteção dos dados, os controladores devem implementar procedimentos e políticas como: limitar o uso dos dados biométricos de menores à finalidade estritamente necessária, controle de acesso, adoção de firewalls e antivírus, realização de testes de penetração e treinamentos periódicos com seus colaboradores.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Os métodos de verificação de idade têm sido constantemente discutidos, uma vez que a eficiência de diversos métodos é questionada. A possibilidade de realização de verificação etária através de biometria é um avanço significativo da tecnologia, principalmente em se tratando do mercado financeiro, um ambiente no qual o combate à fraude deve ser ininterrupto.

Nesse sentido, ressalta-se a relevância das ferramentas de verificação de identidade através de dados biométricos, que podem, inclusive, reduzir ou eliminar o acesso indevido de menores em plataformas digitais.

O tratamento dos dados deve observar os princípios da LGPD, com a garantia de transparência, a existência de uma finalidade determinada e legítima, bem como a minimização dos dados pessoais. Além disso, deve ser observado o melhor interesse do menor, análise que deverá ser realizada pelos controladores através da elaboração de um RIPD.

Para garantir a observância do princípio da necessidade, deve-se avaliar a eficiência do método de verificação etária em relação a métodos alternativos, além de restringir os dados coletados apenas àqueles necessários. Por exemplo, caso a biometria possa ser realizada através da facial, não haveria necessidade de coleta da facial + digital. Por fim, o sistema utilizado deve garantir que a biometria não seja retida por mais tempo do que o necessário, observadas obrigações legais e regulatórias do controlador de manter os dados.

Blocos Temáticos	ID	Questões	Respostas	Número de Caracteres (limite de 300 caracteres)	Comentários adicionais
Definições e Princípios	1	Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?	Critérios objetivos a serem observados: (i) natureza do dado (dados físicos, fisiológicos ou comportamentais); (ii) uso de tecnologia específica para o tratamento; e (iii) finalidade específica (dado coletado com a intenção de identificação ou autenticação única do titular).	275	1. Relação com características físicas, fisiológicas ou comportamentais O dado deve se referir a elementos únicos do corpo ou do comportamento de uma pessoa natural — como impressão digital, iris, rosto, voz, forma de andar ou digitar. Isso é destacado pelo Art. 4(14) da GDPR e pela orientação do ICO (https://ico.org.uk/our-organisations/about-our-approach-to-regulation/data-protection/biometric-data/). 2. Processamento técnico específico Não basta o dado bruto e é necessário que haja tratamento técnico específico (como algoritmos de reconhecimento facial ou análise de voz), que extraia vetores ou padrões biométricos a partir desses dados. Por exemplo, uma foto é um dado pessoal comum, mas se for tratada por um sistema de reconhecimento facial, torna-se dado biométrico. 3. Finalidade de identificação ou autenticação O dado só é considerado biométrico sensível quando a finalidade do tratamento for identificar ou autenticar unicamente o titular. A própria LGPD, a GDPR e o ICO são categóricos: a intenção do tratamento define a sensibilidade do dado. Ou seja, a finalidade é um elemento definidor da natureza sensível do dado.
	2	Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?	Devem ser informados, de forma clara e prévia, origem do dado, finalidades específicas, prazo de retenção, compartilhamento, medidas de segurança, direitos e canais de contato. Avisos internos e externos devem ser destacados, com sinalização em coletas automatizadas.	267	As medidas de transparência devem ser alinhadas às exigências da legislação de proteção de dados pessoais e em recomendações emitidas pela ANPD.
	3	De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deve ser tratada em comparação à biometria tradicional (digital, iris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, diferentemente especial observância aos princípios da qualidade dos dados e da segurança?	A biometria comportamental é menos precisa, mas também menos intrusiva e pode servir como apoio seguro à identificação. Por isso, não exige mais restrições que a biometria tradicional, mas sim tratamento proporcional ao risco, com foco em qualidade dos dados e prevenção de erros.	260	A biometria comportamental, embora menos precisa e mais suscetível a variações contextuais, pode funcionar como mecanismo complementar e menos intrusivo de autenticação. Justamente por sua menor precisão, seu uso isolado impõe riscos como falhas de autenticação e negativas indevidas de acesso, o que exige atenção aos princípios da qualidade dos dados e da prevenção. No entanto, diferentemente da biometria tradicional, que é altamente identificável e imutável, a biometria comportamental pode representar uma solução proporcional e segura, desde que adotada com transparência, em conjunto com outras camadas de verificação e com mecanismos de correção de erro. Assim, não se justifica uma regulamentação mais restritiva sobre a biometria comportamental em relação à tradicional, mas sim uma abordagem baseada em risco real e contexto de uso, incentivando seu uso como ferramenta de apoio à identificação.
	4	Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?	Deve ser ofertado opção real de aceitar ou de recusar, sem condicionamento ou coerção imposta ao titular. Não deve ser usado se houver base legal mais adequada ao caso concreto, especialmente quando houver desequilíbrio de poder ou impossibilidade de fornecimento de consentimento válido pelo titular.	269	O consentimento para o tratamento de dados biométricos deve ser livre, informado, específico, destacado e inequívoco, com opção real de recusa e alternativa viável. No entanto, o consentimento não deve prevalecer sobre outras bases legais. Quando outra base legal for mais adequada ao caso concreto, ela deve ser priorizada, garantindo maior proteção ao titular e mais segurança jurídica ao controlador. O uso do consentimento é inadequado em contextos com desequilíbrio de poder, ausência de transparência ou quando não for possível assegurar sua real voluntariedade.
	5	Quais critérios devem ser observados para a adequada aplicação da hipótese legal de garantia da prevenção à fraude? (art. 11, II, “f”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a serviços bancários e financeiros, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?	É necessário pesar pela proporcionalidade ao bem jurídico tutelado, como a segurança e a integridade dos titulares. Para avaliar a adequação, considere a finalidade e o benefício gerado com o tratamento. É possível a combinação com outros métodos, como análise de documentos, como salvaguarda.	265	A aplicação da hipótese legal de prevenção à fraude exige que o uso da biometria seja proporcional ao risco envolvido e ao bem jurídico tutelado, como a segurança patrimonial e a integridade do titular. Deve-se observar a legalidade da atividade, a adoção da medida e a estrita necessidade da coleta do dado biométrico. Para compatibilizar o princípio da necessidade, recomenda-se adotar abordagens graduais, como o uso combinado de biometria com outros métodos (ex.: análise documental ou autenticação multifator), evitando a coleta excessiva. Salvaguardas como avaliação de impacto, medidas de segurança, revisão periódica da eficácia do método e garantia de alternativas viáveis ao titular são fundamentais para mitigar riscos e proteger os direitos fundamentais.
Hipóteses Legais	6	Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observados nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando a mitigação de riscos e a garantia de direitos dos titulares?	O critério deve ser se restringir à finalidade específica abrangida pela determinação legal ou regulatória. Salvaguardas a serem observadas: transparência ativa, medidas técnicas como controle de acesso e criptografia, e políticas de governança que assegurem a proteção dos direitos dos titulares.	267	Entre os critérios e salvaguardas exigidos, destacam-se: (i) finalidade legítima e específica, claramente vinculada à obrigação legal; (ii) transparência ativa, com aviso prévio aos titulares sobre a coleta e o uso dos dados; (iii) medidas técnicas e organizacionais robustas, como controle de acesso, criptografia e registros de acesso (logs); (iv) anonimização sempre que possível e compatível com a finalidade do tratamento; (v) governança estruturada em proteção de dados, com políticas e controles internos.
	7	Quais os limites do tratamento de dados biométricos para a realização de estudos por motivos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nestes casos?	O tratamento deve ocorrer dentro do âmbito, com finalidade legítima, em ambiente seguro e mediante anonimização ou pseudonimização. Devem ser adotados controles de acesso, segregação de bases e rastreabilidade das operações, bem como restrições contínuas quanto ao uso e compartilhamento dos dados.	269	Portanto, mesmo em contextos de exceção, os princípios da proteção de dados permanecem como parâmetros mínimos para mitigar riscos e garantir a proporcionalidade e a legitimidade do tratamento. O tratamento de dados biométricos para fins de pesquisa deve observar os limites do art. 13 da LGPD. Mesmo com a anonimização, é obrigatório que os dados: (i) sejam tratados exclusivamente dentro do âmbito de pesquisa; (ii) tenham uso restrito à finalidade específica e legítima do estudo; (iii) sejam mantidos em ambiente controlado e seguro; e (iv) passem por processos de anonimização ou pseudonimização sempre que possível. Além disso, a divulgação dos resultados não pode, sob nenhuma hipótese, revelar dados pessoais.
	8	Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?	Para garantir o uso ético do reconhecimento facial, é preciso diversidade no banco de dados, testes de viés, validação do algoritmo, opções acessíveis, informação clara ao titular, avaliação de riscos, treinamento de equipes e orientações da ANPD dos padrões de segurança e transparência aplicáveis.	269	Como salvaguardas adicionais diante do risco de reidentificação pelo cruzamento de bases, devem ser adotadas medidas como: segregação e controle rigoroso de acesso aos dados, restrições contínuas quanto ao uso e compartilhamento, rastreabilidade das operações de tratamento e aplicação de padrões éticos e técnicos de segurança da informação. A responsabilidade pela integridade e proteção dos dados recai integralmente sobre o órgão de pesquisa, sendo vedada sua transferência a terceiros. Para garantir que o uso de tecnologias de reconhecimento facial, mesmo com base legal, respeite os princípios da necessidade, proporcionalidade, transparência e não discriminação, é essencial: (i) Práticas e salvaguardas técnicas, como: - Diversidade no banco de dados de treinamento, evitando vieses algorítmicos e garantindo representatividade de diferentes grupos sociais. - Testes, principalmente em sistemas usados para prevenção à fraude. - Alternativas de desempenho do algoritmo, com foco em taxa de erro e impacto sobre grupos vulneráveis. - Treinamentos acessíveis, como sessões ou fóruns, para pessoas com deficiência digital ou que não possam fornecer biometria. (ii) Salvaguardas jurídicas e institucionais, como: - Informação clara e acessível ao titular, detalhando finalidade, base legal, retenção e direitos. - Avaliação de impacto à privacidade de dados, quando houver alto risco, como uso em locais públicos ou situações de poder assimétrico. - Treinamento ético de equipes técnicas, conscientizando desenvolvedores sobre riscos de discriminação e violação de direitos. - Supervisão contínua da ANPD, com padrões de transparência, segurança e possibilidade de auditoria. Sistemas de reconhecimento facial devem ser projetados com base no princípio da Privacy by Design, adotando algoritmos precisos e treinados com bases de dados diversas em idade, etnia e gênero, sob padrões técnicos adequados (ex.: normas ISO). É essencial garantir boas condições ambientais (como iluminação e qualidade da imagem), uso de dados de teste de segurança e segurança no processamento (criptografia e controle de acesso).
	9	Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para compensar temporariamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?	Devem usar algoritmos precisos sob padrões técnicos adequados (ex.: ISO), treinados com bases diversas e atualizadas, garantir segurança no processamento, boas qualidade de imagem e controle ambiental. Devem prever revisão humana, canais de correção e medidas para reduzir erros e proteger titulares.	268	Para minimizar erros como falsos positivos e negativos, é necessário implementar: (i) monitoramento contínuo da acurácia do sistema; (ii) mecanismos de revisão humana; (iii) canais acessíveis para que titulares relatem falhas; e (iv) atualizações periódicas do sistema. Quando houver decisões automatizadas com base no reconhecimento facial, devem ser garantidos o direito à intervenção humana, a transparência sobre os critérios adotados e avaliações de impacto para prevenir riscos aos direitos dos titulares. O uso de reconhecimento facial é considerado mais intrusivo e deve ser empregado apenas em situações de alto risco de discriminação e vigilância massiva. (i) controle de presença em escolas e ambientes de trabalho, quando as alternativas menos invasivas; (ii) identificação de perfis para marketing, por ser excessivamente intrusivo.
	10	É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma ética, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?	Não é recomendado em identificação remota em tempo real, com câmeras ou idiosos, para marketing ou para tomada de decisão automatizada, por poder ser intrusivo ou discriminatório. Alternativas de identificação com menor impacto à privacidade são crachás, vídeo comum ou autenticação multifator.	267	Alternativas incluem vídeo convencional, autenticação multifator e cartões de identificação. No entanto, em certos contextos, como os enfrentados pela Latam, a biometria pode ser mais eficaz e precisa para autenticação, especialmente quando outras soluções não garantem segurança ou acessibilidade adequadas. Nessas situações, o uso da biometria pode ser legítimo, desde que proporcional, transparente e com salvaguardas para mitigar seus impactos.
Tecnologias de reconhecimento facial (FRTS) e aplicação de tecnologias emergentes e inovadoras no tratamento de dados biométricos	11	Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de risco e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?	Verificações de acurácia e vulnerabilidades (auditorias, testes de intrusão e risco), revisão contínua das medidas de segurança, uso de criptografia, controle de acesso, intervenção humana qualificada e monitoramento de aspectos legais e éticos no uso da tecnologia.	265	Diante do alto risco associado à violação de dados biométricos, como roubo de identidade, devem ser adotadas medidas técnicas e administrativas indispensáveis, como: criptografia forte, controle rigoroso de acesso, revisão periódica das medidas de segurança, auditorias independentes, testes de intrusão e detecção de vulnerabilidades. É fundamental prever a intervenção humana qualificada, política de resposta a incidentes, bem como o monitoramento contínuo das implicações legais e éticas da tecnologia.
	12	Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?	Boas práticas são: proporcionalidade ao risco, especialmente quanto à proteção contra fraudes e acesso a dados sensíveis, com transparência na justificativa sobre a finalidade de uso e a necessidade da biometria, medidas testadas para evitar discriminação ou exclusão indevida.	277	Além disso, é necessário estabelecer parâmetros mínimos de avaliação e gestão de riscos, como: definição de métricas de impacto e probabilidade de falhas, análises periódicas de risco, registro das operações de tratamento, e revisão de políticas conforme o ciclo de vida dos dados. Essas ações asseguram conformidade com a LGPD e proteção integral aos dados sensíveis. Em serviços não essenciais, a exigência de biometria deve ser proporcional ao risco envolvido, especialmente quanto à proteção contra fraudes e acesso a dados sensíveis. Boas práticas incluem: (i) avaliação do impacto da negativa do titular, garantindo que haja meios alternativos de acesso sempre que possível; (ii) oferta clara e transparente de informações sobre a finalidade e a necessidade da biometria; (iii) garantia de que a recusa não resulte em discriminação ou exclusão indevida; e (iv) aplicação de salvaguardas como segurança técnica e controle de acesso.
	13	Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?	Boas práticas incluem uso de bases diversas e atualizadas, testes regulares de acurácia e viés, criptografia, controle de acesso, transparência sobre finalidades e riscos, limitação do uso ao necessário, revisão ética (humana) contínua e canais acessíveis para contestação e correção de erros.	263	Em linha com as considerações feitas às questões 8 e 9.
	14	Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos — como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?	Controladores podem garantir transparência com placas informando o uso de câmeras com reconhecimento facial e QR Code para acesso a informações adicionais, como finalidade do tratamento (ex.: segurança pública), identidade do controlador, canal de contato e direitos dos titulares.	260	Medidas concretas aplicáveis neste cenário dizem respeito ao fornecimento ativo de mecanismos de transparência para que os titulares informados possam exercer seus direitos e sua autodeterminação informativa. Nesse contexto, cita-se como exemplo: - placas que informem o uso de câmeras com reconhecimento facial - estratégias com QR Code para acesso a informações adicionais, como finalidade do tratamento, identidade do controlador, canal de contato e direitos dos titulares.
	15	De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?	Por meio de medidas de transparência como aviso de privacidade acessível no ponto de coleta, por opções facilitadas de recadastramento com duplo fator de autenticação em comunicações e por canal claro para revogação do consentimento ou opção no próprio ponto de controle de acesso e comunicações.	269	A interação com o titular mostra-se como meio mais relevante para poder informá-lo e engajá-lo sobre o exercício de seus direitos em relação ao tratamento de dados biométricos, especialmente em contextos de tratamentos automatizados.
Direitos dos titulares e grupos vulneráveis	16	Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio da melhor interesse, nos termos do art. 14 da LGPD?	A participação dos pais deve ser garantida por comunicado específico em linguagem clara sobre a finalidade da biometria. Deve ser avaliado meios menos invasivos e assegurar o melhor interesse do menor, prevalecendo os casos de uso benéfico ao titular para a identificação precisa (ex.: segurança).	265	O princípio do melhor interesse do menor é invocado nesses casos, considerando que o tratamento de dados de crianças não será vedado mais demandado que o controlador avaliar e pondera sobre o o tratamento pretendido impacta os direitos e liberdades fundamentais da criança e do adolescente, incluindo o que tange à participação parental. Por esta razão, as medidas citadas, considerando o ambiente escolar e de espaços recreativos, focam em um lado no envolvimento informado para participação dos pais, e de outro na ponderação a ser feita pelo controlador para avaliar o melhor interesse da criança e do adolescente.
	17	Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?	O tratamento é admissível quando alinhado ao melhor interesse da criança. Deve haver participação informada dos responsáveis por meio de avisos de privacidade e comunicações claras. É essencial adotar criptografia, controle de acesso, logs, auditorias contínuas, RIPO e treinamento.	263	Em linha com as considerações feitas à questão 16, o melhor interesse é o norte a ser seguido, inclusive respaldado por posicionamento da ANPD em sua Enunciado COAPND Nº 01/2023. Adicionalmente, as medidas abordadas focam em aspectos alinhados aos princípios da LGPD, como transparência (aviso de privacidade e comunicações claras), segurança e prevenção (criptografia, controle de acesso) e responsabilização e prestação de contas (logs, auditorias contínuas, RIPO e treinamento).
	18	Em casos de verificação ou estimativa de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?	Medidas de verificação de idade não devem ser excessivas, demandando análise de proporcionalidade. Para compatibilizar com o melhor interesse do menor, é preciso minimizar o uso dos dados coletados, limitar o prazo de retenção com sua eliminação após verificação, e conduzir RIPO para avaliar impactos.	265	As técnicas empregadas para verificação de idade devem ser minimamente invasivas, sendo proporcional em relação ao risco do tratamento de dados pessoais. Assim, o tratamento relativo à verificação de idade não deve implicar em usos secundários, sendo recomendável a exclusão dos dados coletados durante este processo assim que o nível adequado de confiança quanto à idade do usuário for atingido. Substituído, neste momento de verificação, independentemente do método escolhido, é importante reforçar a necessidade de ser transparente com o usuário sobre como sua idade está sendo verificada.



Brasília, 01 de agosto de 2025.

À

Autoridade Nacional de Proteção de Dados – ANPD

Coordenação-Geral de Normatização

Assunto: Contribuições da Associação Brasileira de Emissoras de Rádio e Televisão (ABERT)

Referência: Tomada de Subsídios – Dados Pessoais Sensíveis: Dados Biométricos

CONSIDERAÇÕES INICIAIS

Fundada em 27 de novembro de 1962, a Associação Brasileira de Emissoras de Rádio e Televisão - ABERT é uma sociedade civil sem fins econômicos, de duração indeterminada, constituída por empresas de radiodifusão autorizadas a funcionar no País. Tem como principal objetivo a defesa da liberdade de expressão, em todas as suas formas, bem como dos interesses das emissoras de radiodifusão, suas prerrogativas como executoras de serviços de interesse público, assim como seus direitos e garantias.

Neste contexto, a ABERT gostaria de contribuir para a Tomada de Subsídios¹ sobre o tratamento de dados biométricos, conforme respostas a seguir.

CONTRIBUIÇÕES DA ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO - ABERT

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

¹ Disponível em

<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-tratamento-de-dados-biometricos>.





A ABERT considera essencial que a definição de dado *biométrico*, conforme prevista na Lei Geral de Proteção de Dados Pessoais ("LGPD") deva se apoiar em critérios objetivos, claros e restritos, que estejam em conformidade com o artigo 5º, inciso II, da LGPD, ou seja, vinculado a uma pessoa natural. Essa clareza conceitual é fundamental para assegurar a proteção dos titulares e, ao mesmo tempo, garantir segurança jurídica às empresas, aos órgãos públicos e às demais organizações que lidam com esse tipo de dado em suas atividades cotidianas.

Nesse sentido, com base no artigo 5º, inciso II, da LGPD, a ABERT entende que, à luz do Regulamento Geral sobre a Proteção de Dados (GDPR) europeu, bem como o entendimento do *Information Commissioner's Office* (ICO) britânico, da Autoridade de Proteção de Dados holandesa (*Autoriteit Persoonsgegevens*) e do *National Institute of Standards and Technology* (NIST) estadunidense, três condições cumulativas devem estar presentes para que determinada informação seja classificada como dado biométrico:

I. Natureza do Dado

Trata-se de elementos individuais que podem fundamentar a qualificação como dado biométrico, sendo normalmente identificados por características físicas, fisiológicas ou comportamentais que tendem a ser imutáveis e que pertencem ou identificam inequivocamente determinada pessoa natural.

Assim, estaríamos diante de atributos únicos e inerentes a um indivíduo, como impressões digitais, padrões faciais, íris, modo de caminhar ou dinâmica de digitação. Contudo, esses elementos somente serão considerados biométricos quando possibilitarem a identificação unívoca de uma pessoa natural, especialmente com o uso de tecnologias apropriadas, como é o caso da técnica de biometria. Tal conceito encontra-se em consonância com a definição de dado biométrico prevista no artigo 4º, inciso 14², do GDPR bem como com o entendimento do ICO, que reconhece como dados

² Article 4(14), General Data Protection Regulation – GDPR: “‘Biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.”



biométricos tanto características físicas imutáveis quanto padrões comportamentais quantificáveis, desde que utilizados para fins de identificação pessoal³.

Isso posto, devemos ainda considerar que, assim como nem toda informação relativa a um indivíduo será considerada um dado pessoal, como nos casos de dados anonimizados, de forma que não há possibilidade de associação direta ou indireta a um indivíduo (art. 5º, III e XI c/c art. 12, LGPD), nem toda característica física, fisiológica ou comportamental deverá ser enquadrada como um dado biométrico. De forma análoga, a partir de exemplo disponibilizado pelo ICO⁴, é possível constatar que *nem toda informação genética constitui dado genético (portanto, dado sensível); uma amostra genética em si não é um dado pessoal até que você a analise para produzir alguns dados; e dados de análise genética só são dados pessoais (e, portanto, dados genéticos) se você puder vinculá-los a um indivíduo identificável*.

Portanto, resta claro que, ainda que se esteja diante de informações de características que, a princípio, possam constituir um dado biométrico, caso essas mesmas informações não sejam processadas por meios adequados, com uso de biometria, com a finalidade específica de identificação de indivíduo, elas não serão consideradas dados biométricos, como veremos detalhadamente a seguir. Indo além, caso essas mesmas informações não possam ser vinculadas a um indivíduo, sequer serão consideradas dados pessoais e, por sua vez, seu processamento não se estaria sujeito ao regime disposto na LGPD.

II. Propósito do Meio e Método de Processamento

Trata-se do papel das soluções tecnológicas específicas empregadas para que se possa concluir pela caracterização de dados como biométricos.

As características físicas, fisiológicas ou comportamentais apenas adquirem natureza biométrica quando submetidas a tratamento por meio de tecnologias específicas que se valem da técnica de biometria, tais como algoritmos de reconhecimento facial, sistemas

³ Disponível em

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/#scd4>

⁴ Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/#scd4>

de autenticação vocal ou *softwares* de análise de padrões comportamentais, a fim de identificar uma pessoa natural.

A biometria, assim como exposto por esta r. ANPD⁵, é a *“análise técnica realizada por meios matemáticos e estatísticos”* dessas características de cada indivíduo. O NIST⁶ define como a *“mensuração automatizada de característica física ou traço comportamental pessoal usado para reconhecer a identidade, ou verificar a identidade”*.

Em outras palavras, trata-se de técnica de individualização de pessoas naturais, reconhecendo suas características únicas, a partir de uma leitura matemática das métricas atribuídas a cada pessoa, por meio de análise comparativa, a fim de buscar exatas correspondências, que possam, enfim, identificar, individualizar e expressamente distinguir os indivíduos entre si. Sobre esse aspecto, é importante ressaltar que, por se tratar de uma leitura matemática, será realizada por algoritmos no formato de números e códigos. Portanto, a biometria não será realizada por mera análise comparativa ao olho humano, por exemplo, entre as características físicas identificadas em uma fotografia de documento de identificação civil e uma pessoa. Assim, a técnica em nada se aproxima de uma simples observação humana de que *“aquela pessoa se parece com a pessoa da fotografia”*.

Os propósitos que justificam a utilização dessas tecnologias são os mais variados, como exemplificado no próprio documento “Radar Tecnológico: Biometria e Reconhecimento Facial” desta r. ANPD⁷: *“controle de fronteiras e aeroportos, segurança pública, sistema de saúde, transações financeiras e pagamentos, marketing e experiência do cliente e controle de acesso”*.

A Autoridade holandesa⁸ assim dispõe: a caracterização como dados biométricos tem como pressuposto *“um tratamento técnico específico”*, pelo qual os dados são

⁵ Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf>

⁶ Disponível em: <https://csrc.nist.gov/glossary/term/biometrics#:~:text=Definitions%3A,claimed%20identity%2C%20of%20an%20applicant>

⁷ Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf>

⁸ Disponível em: <https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/rules-for-the-use-of-biometrics>

analisados e, posteriormente, comparados com uma determinada referência/modelo. Por essa razão, é extremamente relevante o critério do meio que é utilizado para o processamento desses dados, assim como a forma, o modo pelo qual essas tecnologias específicas realizam esse processamento. Nesse sentido, ainda que características físicas, fisiológicas ou comportamentais possam ser processadas, caso o meio, o instrumento ao qual elas serão submetidas não apresente condições tecnológicas específicas suficientemente adequadas para o emprego da técnica de biometria – ou tenha sido premeditadamente desenhado dessa forma – e, por consequência, não sejam a eles atrelados os propósitos e a finalidade de identificação unívoca de um indivíduo, não se deve considerar essas características como dados biométricos. Isso, principalmente, porque, nesses casos, não estaremos diante da realização de uma análise e comparação matemática a partir de prévia referência estabelecida, por meio da conversão das informações em um *template*.

O NIST⁹, por sua vez, corrobora esse entendimento, ao afirmar que o meio empregado deve ter como característica fundamental o propósito de reconhecer os indivíduos de forma automatizada, por meio de uma medição e análise estatística desses dados para a autenticação e verificação das características do corpo humano. Não sendo reconhecida essa característica fundamental, não estaremos diante de um processamento de dado biométrico.

A título de exemplo – já consagrado na literatura de referência –, uma fotografia não constitui, por si só, um dado biométrico, ainda que permita a identificação de determinadas características físicas de uma pessoa. Porém, essa mesma fotografia, pode assumir essa classificação quando processada por meios que se valham de tecnologias específicas de processamento, associadas à técnica de biometria, que poderão realizar a comparação matemática a *template* existente, a fim de identificar inequivocamente pessoas naturais.

O próprio ICO destaca essa diferenciação, esclarecendo que o processamento técnico voltado à identificação é que transforma uma característica em dado biométrico¹⁰.

⁹ Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf>

¹⁰ Disponível em <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/>

Outro exemplo prático encontramos quando diante de câmeras de monitoramento instaladas em entradas de condomínios. Ainda que a câmera possa registrar o deslocamento de transeuntes e, evidentemente, algumas de suas características físicas, caso essas câmeras e o sistema envolvidos no processamento das informações captadas não possuam os recursos técnicos adequados para a realização de uma leitura biométrica desses indivíduos, ou, ainda, tenham sido arquitetados para que não atendam a esse propósito – evitando, por exemplo, a criação de *templates* voltados à identificação –, as imagens registradas não serão consideradas, em qualquer medida, dados biométricos, ainda mais, se considerada ausência de específica finalidade de identificação inequívoca de pessoa natural.

III. Finalidade do Agente

Trata-se da identificação individualizada e inequívoca como critério para classificação de um dado como biométrico.

O elemento determinante consiste na intenção de uso ou no resultado prático alcançado, que deve objetivar a identificação, autenticação ou rastreamento individualizado de uma pessoa natural. É assim como se manifesta, por exemplo, a Autoridade holandesa¹¹: uma informação somente poderá se enquadrar como dado biométrico, caso utilizada para fins de identificação de titulares de dados. A técnica da biometria, portanto, é intrinsecamente orientada a estabelecer e confirmar a identidade de um titular.

Esta própria r. ANPD¹² elenca algumas das principais finalidades da técnica biométrica: *detecção (descobrir e localizar faces nas imagens e vídeos), identificação (quem é a pessoa da imagem?) e verificação (a pessoal existe ou está cadastrada?)*. Mais ainda, todos os propósitos elencados no documento “Radar Tecnológico: Biometria e Reconhecimento Facial” desta r. ANPD¹³ envolvem a identificação de indivíduos como componente fundamental. Afinal, para as finalidades de “*controle de fronteiras e aeroportos, segurança pública, sistema de saúde, transações financeiras e pagamentos,*

¹¹ Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>

¹² Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf>

¹³ Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf>

marketing e experiência do cliente e controle de acesso”, a identificação do indivíduo é indissociável do objetivo final.

No contexto europeu, por exemplo, o AI Act¹⁴ indica que a identificação biométrica apresenta como objetivo a *“verificação da identidade de uma pessoa, comparando os dados biométricos dessa pessoa com dados biométricos de pessoas armazenados numa base de dados de referência”*.

Por outro lado, quando a informação é empregada exclusivamente para fins estatísticos ou analíticos, sem ter por finalidade a individualização e identificação inequívoca do titular, não se enquadra na categoria de dado pessoal, tampouco dado biométrico.

Neste contexto, é igualmente importante evitar interpretações que ampliem de forma excessiva o conceito de dado biométrico e, conseqüentemente, extrapolem os critérios definidos na própria LGPD. A adoção de interpretações demasiadamente amplas pode resultar em insegurança jurídica, dificultando o cumprimento da norma por parte das organizações que tratam dados de forma responsável. A clareza e objetividade na definição são fundamentais para garantir previsibilidade regulatória e permitir que os agentes de tratamento compreendam com precisão quando estarão sujeitos às obrigações específicas aplicáveis ao tratamento de dados biométricos.

Por exemplo, a evolução das tecnologias de inteligência artificial generativa exige uma interpretação cuidadosa e tecnicamente precisa dos conceitos de dados pessoais e biométricos. Isso se torna particularmente relevante diante da proliferação de sistemas capazes de gerar vozes e rostos sintéticos com notável realismo, incluindo aqueles que, em certa medida, tentam se aproximar de uma replicação de características de pessoas específicas, ainda que, em uma análise matemática e estatística, não representem idênticas cópias.

É importante compreender que conteúdos gerados por IA (sejam conteúdos sonoros ou audiovisuais que simulam e reconstituem vozes, rostos ou outras características aparentemente humanas) poderão não constituir dados biométricos para fins da LGPD, GDPR ou legislações similares, mesmo quando originalmente baseados em pessoas reais. Tal enquadramento sobrevém em função de três fatores fundamentais:

¹⁴ Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689

- a) **Ruptura do vínculo identificador:** quando uma IA gera conteúdos sonoros ou audiovisuais que simulam e reconstituem uma voz ou face, mesmo que treinada com dados de uma pessoa específica (como no caso de clonagem vocal de atores falecidos), o *output* resultante pode ser – e geralmente é – uma criação sintética totalmente nova, de modo que a própria informação que servirá de subsídio para o treinamento desta IA, não será, por si só, considerada um dado biométrico, vez que sobre ela não terá sido aplicada técnica de biometria – leia-se, por “biometria”, a mensuração voltada à identificação de pessoas. Tal processo de geração introduz uma camada de abstração e transformação que rompe a conexão direta necessária para caracterizar um dado biométrico. O resultado é uma representação artificial que, embora possa lembrar características humanas, não mantém a unicidade biológica que define dados biométricos. Como exposto, essa representação artificial não corresponderá à exata reprodução matemática de métricas de um indivíduo, de forma que sequer poderia ser utilizada para fins de identificação.
- b) **Ausência de mensurabilidade biológica direta:** dados biométricos, conforme definidos no artigo 5º, inciso II, da LGPD, pressupõem características físicas, fisiológicas ou comportamentais mensuráveis de uma pessoa natural. Conteúdos sintéticos gerados por IA são construções matemáticas, derivadas de análises estatísticas e probabilísticas - sequências de pixels ou ondas sonoras artificialmente produzidas por algoritmos, portanto, sem qualquer correspondência exata a métricas de características de indivíduos. Não há medição de características biológicas reais; há apenas a simulação computacional de padrões que tentam se aproximar de características humanas.
- c) **Impossibilidade de identificação reversa confiável:** um verdadeiro dado biométrico permite a identificação inequívoca de seu titular. Vozes e rostos gerados por IA, mesmo quando inspirados em pessoas reais, não possibilitam essa identificação reversa com a absoluta certeza necessária para caracterizá-los como dados biométricos. A natureza probabilística e combinatória dos modelos generativos introduz variações e elementos sintéticos que tornam impossível estabelecer uma correspondência unívoca com qualquer pessoa natural.

Esta interpretação tem implicações práticas significativas: permite o desenvolvimento responsável de tecnologias de IA para dublagem póstuma, assistentes virtuais com



vozes naturais, e outras aplicações benéficas, sem criar obrigações regulatórias desproporcionais. Importante ressaltar que isso não isenta os desenvolvedores de outras responsabilidades legais, como direitos de imagem, propriedade intelectual ou uso indevido de direitos da personalidade.

Portanto, a **caracterização de dados biométricos deve observar critérios técnicos objetivos que considerem (i) a natureza e origem dos dados, (ii) o meio de processamento empregado e, principalmente, (iii) sua finalidade.** Considerar apenas a aparência superficial, interpretando conteúdos sintéticos como dados biométricos representaria uma expansão injustificada do escopo regulatório, criando barreiras desnecessárias à inovação sem proporcionar proteção adicional significativa aos titulares de dados, uma vez que não há titular de dados identificável em conteúdos puramente sintéticos.

Por fim, é relevante reforçar que dados biométricos não devem ser considerados, por natureza, de alto risco. O grau de risco associado ao tratamento desses dados depende diretamente de variáveis como o contexto de uso, a finalidade do tratamento, a escala da operação e as medidas de segurança adotadas.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

A ABERT entende que o princípio da transparência é um dos pilares centrais da proteção de dados pessoais. Assim, os controladores de dados pessoais, independentemente de tratarem dados biométricos, devem adotar as melhores práticas de transparência ativa.

Nesse sentido, a ABERT entende não haver a necessidade de se inaugurar uma espécie de “nova categoria” de práticas de transparência ativa específicas para o tratamento de dados biométricos, uma vez que os mesmos princípios e exigências já se aplicam a qualquer tipo de tratamento de dado pessoal.

Assim, como em qualquer cenário, controladores de dados pessoais, tratem ou não dados biométricos, devem adotar medidas de transparência adequadas, tais como:



- 1) Comunicação clara por meio dos canais institucionais estabelecidos, utilizando políticas de privacidade, comunicados ou outros instrumentos informativos já integrados à rotina comunicacional da organização com seus titulares de dados;
- 2) Utilização de linguagem acessível, garantindo a efetiva compreensão das informações sem gerar encargos desproporcionais na produção de materiais diferenciados; e
- 3) Utilização da estrutura de atendimento existente para suporte aos titulares, assegurando a identificação do Encarregado de Proteção de Dados (DPO).

A ABERT ressalta, ainda, ser fundamental que a regulamentação não imponha obrigações rígidas quanto aos meios ou formatos de comunicação, mas sim assegure margem de escolha para que os agentes de tratamento possam adotar as soluções mais adequadas ao seu perfil, às suas atividades e à sua base de titulares.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Diante das semelhanças entre a biometria tradicional e a biometria comportamental, a ABERT entende, em princípio, não haver qualquer distinção entre as duas modalidades.

Os requisitos para que um dado seja considerado biométrico são apresentados na resposta à questão 01 desta Tomada de Subsídios. Nesse sentido, é importante demarcar que nem toda análise comportamental implicará em tratamento de dados biométricos comportamentais. Perfilamentos e perfilizações de consumo, incluindo os que busquem antever e prever reações quando dissociados da finalidade de identificação pessoal, não consistem em tratamento de dados biométricos comportamentais.

Necessária essa distinção, pois a atividade de perfilamento consiste na análise de padrões de comportamento de grupos de indivíduos com o objetivo de prever prováveis

reações, a partir de informações agregadas e estatísticas, sem qualquer identificação individualizada. Veja-se, portanto, que, neste caso, pelo menos um dos três principais requisitos para que uma informação seja considerada biométrica não está presente: a finalidade de identificação única e inequívoca do titular.

Como mencionado, dados biométricos comportamentais consistem em características únicas e individualizadas relacionadas ao comportamento de uma pessoa, utilizados com a finalidade de identificar aquele indivíduo de forma única e inequívoca. Já a criação e interpretação de perfis com base em atributos comportamentais (como hábitos de compra, navegação e interações digitais) permite a manutenção de uma comunicação mais eficiente e a antevisão de possíveis comportamentos de um grupo de pessoas, sem a necessária identificação individual de cada um desses titulares.

Assim, o agrupamento ou clusterização de pessoas a partir de informações sobre seu comportamento; ou, ainda, com vistas à predição de seu comportamento, inclusive de consumo, não configura análise individualizada, podendo sequer envolver dados de natureza pessoal (biométricos ou não).

Em breve exemplo prático: no caso do falecimento de um grande ídolo da música, o perfilamento capaz de detectar que aqueles mais ativos em suas redes sociais, exibindo certo padrão comportamental, estão mais propensos a consumir conteúdos específicos do cantor falecido não envolve qualquer tipo de tratamento de dado pessoal, muito menos de qualquer análise de biometria comportamental.

Em síntese, diante de todo o exposto, considerando que a finalidade de identificação é essencial para o enquadramento de informações como dados biométricos e com fulcro na LGPD e demais normas internacionais, os padrões e perfis comportamentais, não voltados à identificação forma única e inequívoca um indivíduo, não consistem em dados biométricos comportamentais. Isso porque a simples inferência de padrões estatísticos não deve ser considerada, por si só, tratamento de dados biométricos. Cabe, evidentemente, de toda sorte, ao agente de tratamento garantir os limites do perfilamento estatístico, sem vinculação direta à identidade pessoal, e com observância aos princípios e disposição da LGPD e regulamentação desta r. ANPD.

BLOCO II - HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

O consentimento é uma das bases legais possíveis para o tratamento de dados sensíveis, conforme previsto nos artigos 5º, inciso XII, e 8º da LGPD, e deve atender aos requisitos legais de forma clara, livre e informada.

No entanto, há situações em que o uso do consentimento pode não ser a opção mais eficaz, por exemplo, em contextos que envolvem medidas de prevenção a fraudes ou segurança da informação, onde sua exigência poderia comprometer a efetividade do tratamento ou inviabilizar respostas rápidas a riscos concretos. Assim, o consentimento não deve ser interpretado como requisito universal ou obrigatório para o tratamento de dados biométricos, sob pena de inviabilizar operações legítimas e fundamentais para a proteção de interesses públicos e privados.

Por isso, é essencial que os controladores tenham liberdade para avaliar, com base nas especificidades de sua atividade, qual a base legal mais adequada ao caso concreto. A escolha deve sempre observar os princípios da LGPD, como necessidade, finalidade e adequação, e estar devidamente registrada em processos internos de governança e conformidade.

Além disso, a ABERT aproveita a oportunidade para reforçar que a LGPD, acertadamente, com intuito de preservar a liberdade de expressão, de imprensa e de criação artística, excetua do seu escopo a atividade jornalística e artística (art. 4º, inciso II, alínea a). É dizer, o tratamento de dados pessoais, sejam biométricos ou não, para a produção de conteúdo com fins exclusivamente artísticos e jornalísticos, não estarão sujeitos ao regramento previsto na LGPD, tornando dispensável, inclusive, o consentimento do seu titular. A saber:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
(...)

II - realizado para fins exclusivamente:



a) jornalístico e artísticos; ou (grifo nosso)

A proteção da imagem e privacidade dos indivíduos, nessas hipóteses, ficam por conta, primeiramente, da Constituição Federal, que resguarda tais direitos fundamentais (art. 5º, X da CF/88), assim como por outras leis ordinárias, como o Código Civil (art. 20). Deste modo, o uso indevido de dados pessoais, como o abuso ou violação de direitos da personalidade, inclusive com fins artísticos e jornalísticos, é passível de responsabilização civil.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de "garantia da prevenção à fraude" (art. 11, II, "g", LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

SEM CONTRIBUIÇÃO.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o "cumprimento de obrigação legal ou regulatória" (art. 11, II, "a", LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

SEM CONTRIBUIÇÃO.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, "c", LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

SEM CONTRIBUIÇÃO.



BLOCO III - TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

SEM CONTRIBUIÇÃO.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

SEM CONTRIBUIÇÃO.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

SEM CONTRIBUIÇÃO.

BLOCO IV - SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros

mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

SEM CONTRIBUIÇÃO.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

SEM CONTRIBUIÇÃO.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

SEM CONTRIBUIÇÃO.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos -- como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

SEM CONTRIBUIÇÃO.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

SEM CONTRIBUIÇÃO.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

SEM CONTRIBUIÇÃO.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

SEM CONTRIBUIÇÃO.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

SEM CONTRIBUIÇÃO.

Segurança

Legal

Abese

01 AGOSTO 2025

BIOMETRIA e+

DADOS PESSOAIS SENSÍVEIS



www.abese.org.br



Olá,

Bem-vindo ao [MUNDO ABESE](#), um mundo onde as PESSOAS SE CONECTAM, SE INFORMAM E CRESCEM JUNTAS, porque JUNTOS SOMOS MAIS.

VOCÊ está acessando edição especial do [SEGURANÇA LEGAL ABESE](#), exclusivo sobre os [BIOMETRIA e+](#), [DADOS PESSOAIS SENSÍVEIS](#) a fim de tratar de aspectos relevantes para contribuir com a AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD).

Esperamos supere sua expectativa e que agregue valor ao mercado concorrencial da segurança eletrônica. Sucesso e ótima LEITURA.

ABESE. **SEGURANÇA É A NOSSA UNIÃO.**

SELMA MIGLIORI
Presidente

SUMÁRIO

1. INTRODUÇÃO	5
2. DAS PRIMEIRAS CONTRIBUIÇÕES DA ABESE	7
2.1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?	8
2.2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?	8
2.3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?	9
2.4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?	9
2.5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?	10
2.6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?	10
2.7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?	11
2.8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos	

sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos? 12

2.9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado? 12

2.10.É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?..... 13

2.11.Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis? 13

2.12.Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades? 14

2.13.Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários? 15

2.14.Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência? 15

2.15.De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos? 16

2.16.Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD? 17

2.17.Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos? 17



2.18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse? 18

3. NÚMEROS DA ABESE..... 19

4. CONCLUSÃO DE SUGESTÕES DE PROVIDÊNCIAS..... 20

1. INTRODUÇÃO

Em meio à acirradas discussões sobre Inteligência Artificial (IA), eis que nos deparamos com mais esse desafio, o tratamento adequado dos dados biométricos, assunto de vital importância para o mercado representado pela ABESE – ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SISTEMAS ELETRÔNICOS DE SEGURANÇA.

Fundada há 30 (trinta) anos com atuação ininterrupta desde então, a ABESE representa toda a cadeia da segurança eletrônica¹ e tem elevado interesse e responsabilidade quanto a este debate.

Apenas para ilustrar, na EXPOSEC² deste ano (2025), maior feira de segurança privada da América Latina e uma das realizações que a ABESE tem maior orgulho, foi publicada a *"Pesquisa Panorama 2024 e Perspectiva 2025"*, que revelou números impactantes que convém trazer aqui, como o número de câmeras vendidas somente no ano de 2024 – mais de 155 mil -, e o percentual de produtos fabricados com IA embarcada, sendo da ordem de 64,3%.

Estamos falando de ferramentas utilizadas inclusive para tratamento de dados pessoais sensíveis, dados biométricos.

É notório o crescimento acelerado das tecnologias de identificação biométrica, voltadas para o reconhecimento facial, impressões digitais, íris e padrões comportamentais, o que tem gerado discussões e significativas mudanças na forma como a sociedade interage com sistemas de segurança, autenticação e controle de acesso.

Essas tecnologias têm se tornado vitais para ampliar a eficiência, segurança e confiabilidade dos serviços prestados pelo Poder Público e pela iniciativa privada, e é natural que suscitem

¹ **Nota:** A ABESE é uma organização empresarial de fins não econômicos com atuação em âmbito nacional e que representa os interesses do setor de segurança eletrônica desde a indústria, desenvolvedores de softwares e hardwares, distribuidores, e prestadores de serviços diversos como controle de acesso e portaria remota, rastreamento de numerários, bens e valores, drones, videomonitoramento, serviços de instalação de sistemas, manutenção preventiva e corretiva, projetos de segurança eletrônica, dentre outros serviços relacionados.

² <https://exposec.tmp.br/>

preocupações em determinadas hipóteses, sobre privacidade, discriminação, excesso ou até riscos à autodeterminação informativa.

Nesse contexto, a iniciativa da Autoridade Nacional de Proteção de Dados (ANPD) de abrir uma Tomada de Subsídios sobre o tratamento de dados biométricos é oportuna, necessária e digna de aplausos.

Para a ABESE, a construção de orientações regulatórias claras e equilibradas exige escuta ativa da sociedade e a colaboração efetiva de que possa e queira somar. A transparência do processo e a participação democrática reforçam o compromisso com uma regulação técnica, proporcional e legítima.

Todavia, é fundamental consignar que este é um tema que tende a demandar tempo dada sua sensibilidade, para que que no afã de ajustarmos questões tão delicadas não criemos embargos ou desmedidas punições que se traduzam em barreiras desmotivadoras para o progresso de nossas tecnologias e desenvolvimento de nosso País.

Diante da relevância e complexidade do tema, apresentamos nossas primeiras³ contribuições aos 18 eixos propostos nesta Tomada de Subsídios, com a meta de colaborar para um ambiente regulatório que seja ao mesmo tempo protetivo, inovador e seguro. visando promover a segurança pública e privada, a inovação tecnológica, e a proteção dos direitos dos titulares, em conformidade com a LGPD. **Ótima leitura.**

³ **Nota:** Como sinalizado, cremos que o tema demandará ampla e profundas discussões ainda, e a ABESE se coloca como canal de consultas e como parceria para agregar valor ao importante papel da ANPD.

2. DAS PRIMEIRAS CONTRIBUIÇÕES DA ABESE

De fato, o uso de dados biométricos teve relevante crescimento nos últimos tempos, com potencial impacto nos direitos humanos, mas com profundos avanços e benefícios para a sociedade.

Justamente por essa razão é que essa discussão deve ser promovida com a devida cautela e profundidade, com a consciência de que ainda há muito o que amadurecer.

Para ilustrar, há elevado número de projetos de lei em tramite no Congresso Nacional para tratar de IA⁴ e que impacta diretamente na presente discussão.

Pertinente às tecnologias de identificação biométrica, de igual modo, há outra enxurrada de propostas estabelecendo seu uso, pelo Poder Público em diversas situações para otimização de recursos. A prova de vida do INSS por biometria facial⁵ é um exemplo disso.

⁴ [Projeto de Lei nº 21/2020](#) - Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Iniciativa do Deputado Federal Eduardo Bismark (PDT/CE). | [Projeto de Lei nº 5051/2019](#) - Regulamenta o uso de Inteligência Artificial no Brasil. Iniciativa do Senador Styvenson Valentim (PODEMOS/RN). | [Projeto de Lei nº 5691/2019](#) - Institui a Política Nacional de Inteligência Artificial, com o objetivo de estimular a formação de um ambiente favorável ao desenvolvimento de tecnologias em Inteligência Artificial. Iniciativa do Senador Styvenson Valentim (PODEMOS/RN). | [Projeto de Lei nº 2338/2023](#)⁴ - Dispõe sobre o uso da Inteligência Artificial de iniciativa do Senador Rodrigo Pacheco. | [Projeto de Lei nº 3592/2023](#) - Estabelece diretrizes para o uso de imagens e áudios de pessoas falecidas por meio de inteligência artificial (IA), com o intuito de preservar a dignidade, a privacidade e os direitos dos indivíduos mesmo após sua morte. Iniciativa do Senador Rodrigo Cunha (PODEMOS/AL). | [Projeto de Lei nº 872/2021](#) - Dispõe sobre os marcos éticos e as diretrizes que fundamentam o desenvolvimento e o uso da Inteligência Artificial no Brasil. Iniciativa do Senador Veneziano Vital do Rêgo (MDB/PB). | [Projeto de Lei nº 266/2024](#) - Dispõe sobre o uso de sistemas de inteligência artificial para auxiliar a atuação de médicos, advogados e juízes de iniciativa do Senador Veneziano Vital do Rêgo (MDB/PB). | [Projeto de Lei nº 210/2024](#) - Dispõe sobre os princípios para uso da tecnologia de inteligência artificial no Brasil, de iniciativa do Senador Marcos do Val (PODEMOS/ES). | [Projeto de Lei nº 146/2024](#) - Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena para os crimes contra a honra e hipótese qualificada para o crime de falsa identidade, para quando houver a utilização de tecnologia de inteligência artificial para alterar a imagem de pessoa ou de som humano, de iniciativa do Senador Chico Rodrigues (PSB/RR). | [Projeto de Lei nº 145/2024](#) - Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para regular o uso de ferramentas de inteligência artificial para fins publicitários e coibir a publicidade enganosa com uso dessas ferramentas, de iniciativa do Senador Chico Rodrigues (PSB/RR)

⁵ <https://www.camara.leg.br/radio/programas/minuto-da-economia/733773-prova-de-vida-por-biometria-facial/> - Prova de vida por biometria facial

Em verdade, são diversas as hipóteses de aplicação no dia a dia como o acesso a contas bancárias e outros sistemas por meio de smartphones e que a sociedade se adaptou de forma positiva.

Portanto, ainda que o uso dessas tecnologias represente riscos e desafios, não podemos ignorar que o contrário representaria riscos ainda maiores além de representar retrocesso.

Partindo para os eixos definidos na Tomada de Subsídio, a seguir, na forma de **Perguntas & Respostas**, eis as primeiras contribuições para **uma conversa que a ABESE considera que está só começando**, o que é importantíssimo ficar registrado uma vez que nossa base de discussão está em transformação constante e cada vez mais célere e dinâmica.

2.1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Para a ABESE os dados biométricos se traduzem na identificação única do indivíduo, logo, é preciso observar se há captura automatizada de características físicas fisiológicas ou, possivelmente, comportamentais, afinal, diferente dos dados pessoais comuns como uma senha de um banco, por exemplo, os dados biométricos não podem ser modificados sendo este o traço determinante para o maior rigor no seu tratamento.

2.2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Numa primeira análise, a ABESE entende que os controladores devem adotar e disponibilizar previamente informações visíveis e acessíveis sobre suas políticas de privacidade, devendo constar capítulo específico sobre o tratamento de dados pessoais sensíveis.

A forma de acesso pode ser diversa como placas, sites e apps, através de um QR-CODE, visando inclusive evitar dispêndio de elevados recursos desnecessariamente.

- 2.3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Além da elevada importância e complexidade, a pergunta revela em si parte da resposta no sentido de que os dados biométricos demandarão, ao menos em alguns aspectos, tratamentos distintos conforme o tipo de dado biométrico.

Em linhas gerais, é preciso obedecer à minimização de dados, bem como observar riscos específicos de reidentificação e monitoramento não autorizado. O refinamento e distinções de tratamento demandará estudo aprofundado das tecnologias e possibilidades de gestão.

- 2.4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Eis providência desafiadora. Para a ABESE, é preciso traçar um roteiro que possa ser padronizado e sistematizado para atender a estes passos ao tempo de evidenciar sua aplicação pela segurança das partes relacionadas, sobretudo dos responsáveis pelo tratamento dos dados (controladores e operadores).

Quanto aos contextos que tratam do consentimento, no âmbito da segurança eletrônica, vertical dos serviços de Portaria Remota, há grande controvérsia quanto a exigibilidade ou não destes dados biométricos implementados para fins de segurança de um condomínio.

A aplicação normalmente é deliberada em assembleia condominial, e a recusa de um usuário tem potencial de comprometer a segurança de todos. O consentimento nesse contexto vulnerabiliza toda uma operação de segurança, em detrimento da coletividade do condomínio de modo que a ABESE considera que a base legal que autoriza o tratamento dos dados é o

legítimo interesse aliado ao cumprimento do contrato, sem prejuízo do titular dos dados requerer a exclusão de seus dados biométricos mediante alternativa de acesso ao local.

2.5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Por um lado, a hipótese legal de “prevenção à fraude” está relacionada à análise de risco concreto à segurança do sistema ou do patrimônio, para demonstrar que o uso de dados biométricos é proporcional e necessário frente a alternativas menos invasivas. Por outro, as partes podem desejar se valer do seu uso.

A compatibilização com o princípio da necessidade ocorre pela adoção de medidas de minimização dos dados, coleta específica à finalidade, e limitação temporal do armazenamento. Para mitigação dos riscos, a criptografia forte, autenticação multifator, segregação de acesso, registro de logs de auditoria e relatórios de impacto podem ser o caminho.

2.6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Nos casos em que o tratamento de dados biométricos se fundamenta no “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD), é prudente que o controlador comprove a existência de norma expressa que exija ou autorize tal tratamento, como boa prática.

A finalidade deve ser específica, legítima e documentada, com coleta restrita ao mínimo necessário. Entidades públicas devem observar os princípios da legalidade, proporcionalidade, transparência e eficiência, com publicação de Relatório de Impacto à Proteção de Dados (RIPD) sempre que aplicável.

Como salvaguardas adicionais, recomenda-se a adoção de controles de acesso, registros de operações, eventualmente auditorias internas, anonimização sempre que possível, e mecanismos para exercício dos direitos dos titulares.

Essas medidas reforçam a segurança jurídica e a proteção à autodeterminação informativa, mas é importante ponderar, ainda, para o fator recursos. Uma preocupação do mercado que a ABESE reputa legítima é um emaranhado de normas que represente desmedida burocracia que eleva o chamado custo Brasil⁶.

2.7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Sabemos que mesmo quando há anonimização, o tratamento de dados biométricos para fins de pesquisa (art. 11, II, “c”, LGPD) exige cautela redobrada devido ao alto risco de reidentificação por cruzamento de bases. O tratamento deve estar limitado a finalidades científicas, estatísticas ou relevantes para interesse público, vedada sua reutilização para fins distintos. Os dados devem ser efetivamente anonimizados com técnicas robustas e atualizadas, e o processo documentado. Como salvaguardas, recomenda-se: comitê de ética, controle de acesso restrito, termos de confidencialidade, segregação de dados, auditoria independente e avaliação contínua do risco de reidentificação. Sempre que possível, adotar pseudonimização adicional e eliminar

⁶ <https://custobrasil.org.br/abrir-um-negocio/> | Nota: No Brasil, já enfrentamos uma série de desafios desde a abertura do negócio até horas trabalho para atender obrigações burocráticas, em prejuízo da produtividade e, conseqüentemente, da capacidade competitiva.

os dados ao final da pesquisa. Tais medidas preservam os direitos dos titulares e a integridade da pesquisa.

2.8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Eis mais um ponto desafiador, e é importante reconhecer que nenhuma tecnologia é infalível. Em linhas gerais, a coleta deve ser limitada à finalidade específica e com base legítima, como segurança ou prevenção à fraude. A transparência deve ser assegurada com informações claras ao titular e canal para exercício de direitos.

Como salvaguardas, o desenvolvimento de treinamentos de algoritmos com bases diversas para evitar viés discriminatório, auditoria contínua de desempenho, relatórios de impacto, criptografia, trilhas de auditoria e segregação de acesso, nos parecem ser caminhos para este fim.

Políticas internas e códigos de conduta devem regular o uso e corrigir desvios. O uso responsável dessas tecnologias fortalece a segurança e a confiança no setor da segurança eletrônica.

2.9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Para elevar a eficácia e confiabilidade desde a concepção, os sistemas de reconhecimento facial devem ser desenvolvidos com base em princípios de *privacy by design* e *by default*, adotando

algoritmos treinados com bases de dados diversas e atualizadas, que evitem viés e aumentem a conformidade.

É essencial a realização de testes periódicos de performance, com monitoramento de taxas de falsos positivos e negativos, além da calibração contínua dos sistemas. Mecanismos de correção devem incluir validação humana em decisões críticas, registros detalhados de acesso (logs), e canais de contestação acessíveis aos titulares.

No setor de segurança eletrônica, tem havido significativa evolução, inclusive na aplicação dessas tecnologias em locais de aglomeração de pessoas, esta sim área mais sensível para sua aplicação.

2.10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

A ABESE não tem certeza sobre este ponto que merece mais pesquisa e estudo.

2.11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Diante do alto risco associado aos dados biométricos, é indispensável adotar medidas técnicas como criptografia forte em trânsito e repouso, autenticação multifator, controle segmentado de acessos, logs imutáveis, backups protegidos e testes regulares de intrusão.

Administrativamente, a empresa deve implementar política de segurança da informação, plano de resposta a incidentes, avaliação de impacto à proteção de dados (DPIA) e governança com

papéis bem definidos. O monitoramento contínuo, auditorias internas e a revisão periódica dos riscos são essenciais para manter a conformidade com a LGPD.

No setor de segurança eletrônica, onde o tratamento é constante e sensível, essas práticas devem ser integradas ao ciclo de vida dos sistemas, com foco na prevenção de vazamentos e na responsabilização.

2.12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Esta é uma questão relativa, porque ainda que não se trate de serviço essencial a opção pode ser pelo uso do dado biométrico em razão de praticidade, ou até maior segurança operacional, como ocorre no mercado da segurança eletrônica.

Em todo caso, é possível garantir ao titular dos dados meios alternativos de acesso, como senhas, QR Codes ou cartões. Para evitar discriminação, a recusa ao fornecimento dos dados não pode implicar exclusão total do serviço, salvo se a funcionalidade for tecnicamente inviável sem a biometria — o que deve ser justificado de forma proporcional e documentada.

A transparência exige aviso prévio sobre os impactos da negativa, com linguagem acessível. No setor de segurança eletrônica, isso significa respeitar o direito de escolha dos usuários em condomínios ou empresas, sem comprometer a segurança coletiva. A adoção de alternativas e o registro das escolhas do titular são boas práticas indispensáveis.

2.13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Boas práticas para o tratamento de dados biométricos exigem medidas como a adoção de política específica de proteção a dados sensíveis, mapeamento de riscos, minimização de dados, definição clara da base legal, criptografia, controle de acesso com autenticação forte, e revisão periódica de segurança.

A transparência deve ser garantida com aviso prévio ao titular, linguagem clara, política de privacidade acessível e canal direto com o encarregado de dados.

Para evitar discriminação, é essencial validar os algoritmos usados, garantir diversidade nas bases de treinamento e permitir revisão humana nas decisões automatizadas. No setor da segurança eletrônica, essas práticas asseguram a confiança do usuário, a efetividade da tecnologia e o alinhamento com os princípios da LGPD.

2.14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

Eis mais um grande desafio que confronta o interesse coletivo versus direitos individuais.

Numa primeira análise, entendemos que para respeitar a autodeterminação informativa em contextos de tratamento massivo e contínuo, como *smart cities* que, aliás, a ABESE contribui, e monitoramento em locais públicos, os controladores podem adotar medidas como sinalização clara sobre o uso de biometria, disponibilização de políticas de privacidade em locais visíveis

(físicos e digitais), criação de portais de informação com canais para exercício de direitos, e uso de tecnologia que permita anonimização ou pseudonimização.

O tratamento deve ter base legal adequada, com avaliação de impacto e supervisão de autoridade pública, quando necessário. Em situações de difícil transparência, é fundamental reforçar a governança de dados, garantindo que o titular tenha meios de compreender e questionar o uso de suas informações.

2.15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Em um cenário ideal, os agentes de tratamento devem garantir os direitos dos titulares com políticas de privacidade claras e acessíveis, canais de atendimento eficazes e mecanismos digitais que permitam consulta, correção e revogação do consentimento de forma simples, quando essa for a base.

Em tratamento automatizado de dados biométricos, é essencial oferecer revisão humana de decisões, registros de tratamento, e transparência quanto às finalidades e impactos. A comunicação deve usar linguagem compreensível e estar disponível em múltiplos meios (apps, sites, portarias).

Todavia, é fundamental ressaltar as barreiras que existem atualmente para oferecer aos titulares mecanismos digitais para essas consultas atualmente. A exemplo da massa de empresas constituídas no Brasil, o universo da segurança eletrônica é composto predominantemente, por empresas de menor porte, com dificuldades para essa adaptação. Mesmo as grandes carecem de soluções para dar efetividade a tais comandos, daí um dos motivos da ponderação.

2.16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O tratamento de dados biométricos de crianças e adolescentes exige rigor extremo, dado seu caráter sensível. A participação informada dos pais ou responsáveis deve ser garantida por meio de consentimento explícito, livre, informado e inequívoco, preferencialmente por escrito, antes do início do tratamento.

Legalmente, o tratamento é admissível quando necessário para cumprir obrigação legal ou regulatória, para a execução de políticas públicas previstas em lei, ou com o consentimento dos responsáveis, conforme art. 14 da LGPD.

2.17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

O tratamento de dados biométricos de crianças e adolescentes é admissível nas hipóteses previstas no art. 14 da LGPD: com consentimento específico dos pais ou responsáveis, para cumprimento de obrigação legal ou regulatória, para proteção da vida ou da incolumidade física do titular ou de terceiros, ou para execução de políticas públicas.

Para garantir a participação informada dos responsáveis, deve-se obter consentimento claro, prévio, informado e documentado, com linguagem acessível. Além disso, as empresas devem implementar medidas técnicas (criptografia, controle de acesso, anonimização) e organizacionais (treinamento, políticas internas, auditorias) para prevenir abusos, vazamentos e acessos não autorizados, assegurando a segurança, a privacidade e o respeito ao princípio do melhor interesse do menor.

2.18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Entendemos que o tratamento de dados biométricos para verificação ou estimação de idade de crianças e adolescentes em plataformas digitais deve observar os princípios da necessidade e do melhor interesse, limitando a coleta ao mínimo indispensável para a finalidade específica.

Em todo caso, a plataforma deve garantir que o uso dos dados não exponha a criança ou adolescente a riscos ou discriminações, respeitando direitos fundamentais e legislação aplicável, em especial o art. 14 da LGPD, que prioriza a proteção integral do menor.

No mercado da segurança eletrônica essa não é uma questão comum, o que impõe maior reflexão junto ao mercado que lida com dados de menores, lembrando que o foco é a segurança.

3. NÚMEROS DA ABESE

Classificação	Mercado	Indireto	Notas Explicativas ⁷
Empresas	+33 mil	-	Indústrias, desenvolvedores de softwares, hardwares e prestadores de serviços
Faturamento	+14 bi	-	Faturamento ano de 2024
Empregos	1,5 mi	3,5 mi	Milhões de empregos diretos e indiretos gerados
Crescimento	16,1%	-	Crescimento no ano de 2024
Projeção 2025	18,6%	-	Estimativa de crescimento médio para este ano
Câmeras vendidas	+155 mil	-	Somente no ano de 2024
Produtos com IA	64,3%	-	
Desenvolvedores	18,5%	-	Crescimento de desenvolvedores de softwares em 2024

A pesquisa revela, ainda, que os desenvolvedores de Softwares devem contratar funcionários das áreas: comercial; administrativo; **suporte técnico**; marketing; **IA**; **DPO**.

⁷ **Nota:** Dados da Pesquisa Panorama 2024 e Perspectivas de 2025 do Mercado da Segurança Eletrônica.

4. CONCLUSÃO DE SUGESTÕES DE PROVIDÊNCIAS

Como pudemos ver, a maior parte das questões levantadas demandam aprofundadas análises sob diferentes pontos de vista, jurídico, tecnológico, operacional, em termos de usabilidade, enfim.

Para melhor dimensionar as preocupações da ABESE, relembramos aqui que há alguns poucos anos, em uma das edições da EXPOSEC – feira que é realizada já há quase 3 (três) décadas –, a ABESE promoveu concurso de startups criando ilha na feira para projetar as selecionadas para o mercado brasileiro e internacional.

Dentre as startups escolhidas, uma oferecia solução para aplicação da LGPD, porém, na prática, estava distante de pacificar o tema e sanar essa que é uma grande dor para o mercado da segurança eletrônica e para todos os setores.

Até os dias atuais as ferramentas disponíveis carecem de muita evolução, o que poderá mudar com o desenvolvimento e maturidade da IA.

A ABESE reafirma seu compromisso com a segurança, a proteção de dados e o desenvolvimento tecnológico seguro e responsável. O setor de segurança eletrônica é essencial à proteção de pessoas e patrimônio e precisa de um ambiente regulatório claro, seguro e favorável à inovação.

Estamos à disposição para contribuir tecnicamente com a ANPD e a sociedade nesse sentido, mas é preciso muita ponderação para que não acabemos engessando processos e impondo desmedidas obrigações.

A ABESE está convicta que a ANPD e partes relacionadas não medirão esforços para promover estudos aprofundados, ponderados para construção de regras adequadas e equilibradas, e conta com isso. Sem mais, permanecemos à disposição através do e-mail juridico@abese.org.br, desejando SUCESSO nesse grande desafio.



LGPD

SELMA MIGLIORI

Presidente

ABESE

JOSÉ LÁZARO DE SÁ

OAB/SP nº 305.166

#ABESE. SEGURANÇA É A NOSSA UNIÃO.

BIOMETRIA e+

DADOS PESSOAIS
SENSÍVEIS

SELMA MIGLIORI

Presidente

JOSÉ LÁZARO DE SÁ

Coordenação, redação e
conteúdo



SIGA-NOS NAS REDES SOCIAIS



São Paulo, 1 de agosto de 2025

À

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Via e-mail: normatizacao@anpd.gov.br

Via Plataforma + Brasil

Ref.: Tomada de Subsídios sobre o Tratamento de Dados Biométricos

Prezados,

A **Associação Brasileira de Instituições de Pagamentos ("ABIPAG")**, inscrita no CNPJ/MF sob o nº 26.425.404/0001-10, vem, respeitosamente, perante esta Autoridade Nacional de Proteção de Dados ("ANPD") e em complemento às sugestões realizadas na plataforma Participa + Brasil, apresentar sua manifestação com contribuições para a regulação do tratamento de dados biométricos.

A ABIPAG é uma associação setorial do mercado de meios de pagamento eletrônicos, formada por instituições de pagamento e instituições financeiras. Nesse sentido, suas contribuições buscam conciliar a proteção dos direitos dos titulares com a necessidade de inovação e segurança no setor, essencial para a economia do país, oferecendo uma perspectiva prática sobre a aplicação da tecnologia biométrica.

I – SUMÁRIO EXECUTIVO

O setor de pagamentos no Brasil opera sob uma sólida estrutura de regulação setorial promovida pelo Banco Central do Brasil, que zela pela segurança e estabilidade do Sistema de Pagamentos Brasileiro. Esta estrutura inclui nuances relacionadas à Segurança Cibernética, conforme estabelecidas pela Resolução BCB nº 85/2021, que já orienta as instituições na implementação de importantes controles de segurança e governança de dados. Nesse contexto, em que os dados biométricos são uma ferramenta valiosa para a autenticação de usuários e prevenção a fraudes, a ABIPAG acredita que a futura disciplina da ANPD sobre o tema pode se beneficiar ao dialogar com este arcabouço setorial, promovendo um alinhamento que fortaleça a proteção dos titulares e que aproveite os mecanismos de segurança já consolidados no setor.

Dentre as respostas às perguntas formuladas na Tomada de Subsídios, a ABIPAG ressalta a importância de 3 itens:

- **Critérios para o Uso da Biometria na Prevenção à Fraude:** o desafio em torno do uso de dados biométricos para a garantia da prevenção à fraude reside na necessidade de estabelecer critérios claros para a aplicação da hipótese legal do art. 11, II, “g”, da LGPD, de modo a compatibilizar a segurança de operações, especialmente no setor financeiro, com os direitos fundamentais dos titulares. Nesse sentido, a ABIPAG entende que o uso de dados biométricos para essa finalidade exige uma justificativa definida e contextual, por meio da qual o agente de tratamento possa demonstrar o risco de fraude existente e a indispensabilidade da biometria para mitigá-lo, especificando o bem jurídico que se busca proteger. A aplicação dessa hipótese deveria ser orientada pelos princípios da necessidade e da minimização, limitando o tratamento à identificação e autenticação do titular. Como salvaguardas essenciais, recomenda-se a elaboração de Relatório de Impacto à Proteção de Dados, a garantia de transparência aos titulares sobre a coleta e suas finalidades, a realização de auditorias sistêmicas e a adoção de tecnologias como padrões criptográficos robustos e pseudonimização.
- **Parâmetros para o Tratamento em Cumprimento de Obrigação Legal:** a questão central é definir os parâmetros e as salvaguardas a serem observados pelos controladores ao tratarem dados biométricos para o cumprimento de obrigação legal ou regulatória (art. 11, II, “a”, LGPD), visando mitigar riscos e assegurar os direitos dos titulares. A ABIPAG entende que o tratamento de dados biométricos sob essa hipótese deve ser pautado pelos critérios de necessidade, proporcionalidade e legalidade, com a sua finalidade vinculada ao cumprimento da obrigação em questão. Como salvaguardas mandatórias, sugere-se a transparência sobre as informações do tratamento, a elaboração de Relatório de Impacto à Proteção de Dados e a adoção de um programa de governança que contemple medidas técnicas e administrativas em todo o ciclo de vida dos dados.
- **Medidas de Segurança Técnicas e Administrativas Indispensáveis:** dado o impacto de uma violação de dados biométricos, como o roubo de identidade, o desafio deste tema consiste em determinar quais medidas de segurança devem ser consideradas indispensáveis para mitigar tais riscos. A ABIPAG entende ser fundamental a implementação de um arcabouço de segurança. No campo técnico, é importante que haja aplicação de criptografia forte para os dados em trânsito e em repouso, utilização de *templates* biométricos em vez das imagens brutas, controles de acesso com autenticação multifator (MFA) e monitoramento contínuo por meio de testes de intrusão e varreduras de vulnerabilidades. Como medidas organizacionais e de governança, recomenda-se o desenvolvimento de políticas internas sobre o tratamento de dados biométricos, a elaboração de Relatórios de Impacto à Proteção de Dados, a implementação de um plano de resposta a incidentes e a condução de processos de avaliação prévia de fornecedores.

A seguir, a ABIPAG detalha suas contribuições e posicionamentos para cada um dos blocos e itens apresentados na Tomada de Subsídios.

II – RESPOSTAS AOS ITENS DA TOMADA DE SUBSÍDIOS

Bloco I – Definições e Princípios

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

R: a caracterização de um dado como biométrico, assim como estabelecido pelo GDPR, deve considerar as características físicas, biológicas e comportamentais de uma pessoa natural. Considerando que biometria se configura como uma “análise, realizada por meios matemáticos e estatísticos, das características físicas ou comportamentais de um indivíduo”¹, tais características só serão efetivamente consideradas como dados biométricos se forem processadas por uma tecnologia específica com a finalidade de identificar ou autenticar um indivíduo de maneira inequívoca. Assim, a caracterização de um dado como biométrico depende da combinação entre a sua origem (uma característica humana), o processamento tecnológico aplicado e o objetivo de individualizar uma pessoa.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

R: conforme estabelece o art. 9º da LGPD, os agentes de tratamento têm o dever de fornecer informações claras e de fácil acesso aos titulares a respeito do tratamento de seus dados pessoais. No âmbito dessa obrigação, os agentes de tratamento podem abrir uma seção específica em suas políticas e avisos de privacidade relacionada ao tratamento dos dados biométricos, indicando as respectivas finalidades para tanto.

Não obstante, é fundamental que os avisos e as políticas de privacidade sejam elaborados e publicados levando em conta a experiência do titular. Para isso, o documento deve utilizar uma linguagem acessível e adequada à faixa etária do seu público, garantindo que a informação seja compreendida com clareza.

Além disso, nas hipóteses em que o consentimento do titular for a base legal adequada para o respectivo tratamento, os formulários de coleta de consentimento, no mesmo sentido, devem indicar as informações necessárias para que o titular compreenda o tratamento e

¹ Radar Tecnológico: Biometria e Reconhecimento Facial. ANPD, 2024. p.12

possa fornecer seu consentimento sem vícios, como, por exemplo, quais dados biométricos serão coletados, para quais finalidades, dentre outras informações tal como exigidas pela LGPD.

- 3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?**

R: como premissa inicial, tanto a biometria comportamental quanto a biometria tradicional devem ser tratadas com altos níveis de segurança e proteção, considerando que são classificadas como dados sensíveis e, portanto, as medidas legais devem ser devidamente observadas. No entanto, a coleta da biometria comportamental, apesar de ser uma técnica menos invasiva do que a da biometria tradicional, demanda requisitos específicos, uma vez que pode ser coletada de maneira passiva, mesmo sem a ciência do titular, bem como pode ser alterada a depender de diversos fatores.

Para mitigar tais riscos, propõe-se que os sistemas adotem um conjunto de medidas técnicas, como criptografia de ponta a ponta, pseudonimização, controles de acesso, auditoria algorítmica e adoção de padrões de segurança reconhecidos pelo mercado, minimização dos dados e a adoção do *Privacy by Design*.

Bloco II – Hipóteses Legais

- 4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?**

R: quando o consentimento for a base legal para o tratamento dos dados, é fundamental que ele seja obtido em conformidade com as exigências da LGPD. A garantia principal é que o consentimento jamais deve ser presumido, mas, sim, concedido por meio de uma manifestação de vontade ativa, livre e inequívoca por parte do titular. Para ser válido nesse contexto, o consentimento precisa ser informado, específico para uma finalidade legítima e apresentado de forma destacada e acessível. Na prática, isso implica o dever de informar claramente ao titular quais dados estão sendo tratados e com qual propósito. A ausência da observância dos requisitos para a coleta do consentimento pode implicar em sua invalidação, uma vez que este pode ser considerado nulo. Em certas ocasiões, como, por exemplo, em procedimentos para garantir a tutela da saúde e/ou para prevenção a fraudes,

a utilização do consentimento não parece ser a melhor base legal a ser utilizada. Isso porque basear o tratamento na possibilidade de o titular fornecer ou não seus dados podem comprometer a finalidade do tratamento.

- 5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?**

R: o uso de dados biométricos para prevenção à fraude requer uma justificativa definida e contextualizada, de modo que o agente de tratamento consiga demonstrar a existência do risco de fraude e a indispensabilidade do uso da biometria para mitigá-lo. Para tanto, o bem jurídico a ser protegido deve ser devidamente especificado. A utilização de dados biométricos para prevenção à fraude deve considerar os princípios de necessidade e minimização, de forma que o tratamento deve ser limitado à identificação e autenticação do titular. Dentre as salvaguardas para garantir a segurança dos dados tratados, destacamos: (i) elaboração de um Relatório de Impacto à Proteção de Dados, (ii) transparência aos titulares sobre a coleta de referidos dados e respectivas finalidades; (iii) auditorias e avaliações sistêmicas; (iv) criptografia robusta, tal como o padrão AES-256 e pseudonimização.

- 6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?**

R: o tratamento de dados biométricos para cumprimento de obrigação legal ou regulatória pelo controlador deve se basear nos critérios de necessidade, proporcionalidade e, evidentemente, da legalidade, cuja finalidade deve ser vinculada ao cumprimento da obrigação legal ou regulatória. Dentre as salvaguardas, destacamos (i) transparência com relação às informações sobre o tratamento, (ii) elaboração de Relatório de Impacto à Proteção de Dados; e (iii) adoção de medidas técnicas e administrativas, com governança em todo o ciclo.

- 7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização**

dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

R: não aplicável, considerando o escopo de atuação da ABIPAG.

Bloco III – Tecnologias De Reconhecimento Facial (Frts) E Aplicação De Tecnologias Emergentes E Inovadoras No Tratamento De Dados Biométricos

- 8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?**

R: sendo uma técnica naturalmente invasiva, a utilização de reconhecimento facial deve ser realizada quando outra tecnologia não for suficiente para atingir a finalidade pretendida com o tratamento. Para que os princípios da LGPD sejam observados, os agentes de tratamento devem adotar salvaguardas técnicas, administrativas e institucionais para garantir a proteção dos dados que serão tratados, bem como a integridade do titular. As salvaguardas incluem pseudonimização, criptografia, políticas claras para garantir transparência aos titulares, fiscalização de vieses algorítmicos e governança robusta. No mais, para evitar resultados discriminatórios, é importante que as tecnologias de reconhecimento facial sejam treinadas com bases de dados diversificadas, que reflitam as diversas raças e etnias da população. A ausência dessa diversificação pode levar a vieses nos resultados das análises.

- 9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?**

R: para garantir a eficácia, a confiabilidade e, principalmente, para mitigar riscos de discriminação, os sistemas de reconhecimento facial devem ser projetados e mantidos por meio de um ciclo de vida que integre aspectos técnicos e de governança. Para tanto, esse ciclo de vida deve ser projetado a partir de uma base de dados diversificada, com uma pluralidade de rostos, expressões, iluminação e imagens de qualidade. Além disso, as melhores práticas de arquitetura para os modelos de reconhecimento facial devem ser

empregadas. Revisão humana periódica para monitoramento das respostas do algoritmo testes e auditorias contínuas também são medidas para mitigar eventuais falhas dessas tecnologias.

No mais, o processo anterior à utilização das tecnologias de reconhecimento facial é crucial. Por isso, os agentes de tratamento devem realizar uma avaliação cautelosa dos fornecedores antes da contratação, com procedimentos de *due diligence*, e a previsão de canais de contato que facilitem a comunicação com tais fornecedores para a correção tempestiva das falhas.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

R: a utilização de tecnologias de reconhecimento facial deve ser precedida de uma análise da finalidade, do contexto e da proporcionalidade da medida. O uso dessas tecnologias não é recomendado em situações sem uma finalidade legítima e específica, ou quando envolve um impacto desproporcional à privacidade e aos direitos fundamentais, como é o caso de vigilância em massa de espaços públicos. O uso dessas tecnologias em hospitais e escolas também deve ser cuidadosamente analisado, uma vez que envolve titulares de dados em situação de vulnerabilidade. Contudo, no contexto específico do mercado de meios de pagamento, a ABIPAG ressalta que os casos de uso são frequentemente essenciais para a prevenção a fraudes e segurança das operações, não identificando, a princípio, a dispensabilidade da tecnologia para essas finalidades críticas. Como medida de mitigação, é recomendável que os agentes de tratamento (i) elaborem um Relatório de Impacto à Proteção de Dados, de forma a avaliar a proporcionalidade do uso da tecnologia e os impactos às liberdades individuais; (ii) adotem mecanismos de minimização de dados; e (iii) implementem medidas de segurança complementares, como criptografia, tokens e biometria comportamental, priorizando segurança e menor impacto à privacidade.

Bloco IV - Segurança, Governança E Boas Práticas

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

R: dentre as medidas técnicas, podemos listar: (i) criptografia forte, tanto aos dados em trânsito quanto aos em repouso, (ii) utilização de *templates* biométricos em vez das imagens brutas, (iii) controles de acesso com a implementação de MFA, (iv) monitoramento constante de riscos e testes de segurança, como *pentests* e varreduras de vulnerabilidades. Como medidas organizacionais e de governança apropriadas, recomenda-se: (i) desenvolvimento de políticas e procedimentos internos sobre o tratamento de dados biométricos, (ii) atualização dos registros de operações de tratamento (RoPA) para as novas finalidades que demandem a coleta de dados biométricos, (iii) elaboração de Relatório de Impacto à Proteção de Dados, (iv) treinamento e conscientização de colaboradores, (v) atualização e implementação de um plano de resposta a incidentes, e (vi) procedimentos para avaliação prévia de fornecedores relacionados à segurança da informação e proteção de dados.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

R: em serviços não essenciais, a utilização da biometria deve ser justificada por uma finalidade legítima e critérios de razoabilidade previamente definidos, especialmente em cenários de alto risco. Nessas ocasiões, a recusa do titular em fornecer sua biometria deve ser analisada com base no risco. Em eventuais recusas ou situações externas, o controlador deve oferecer alternativas que garantam nível mínimo de segurança para garantir o acesso, como tokens, senhas únicas ou mesmo certificados digitais.

Importante destacar que a limitação de acesso a determinadas finalidades em decorrência da verificação da identidade do titular, por si só, não configura prática discriminatória ou abusiva. Para corroborar a decisão de limitar ou não o acesso, os controladores devem fundamentar a decisão em uma análise que considere a essencialidade da função, a criticidade de seu uso e os perigos associados a um acesso sem a verificação biométrica. Se a análise concluir que o acesso sem biometria acarreta riscos elevados, como em transações financeiras ou acesso a informações sensíveis, a exigência da verificação biométrica para aquela funcionalidade específica é uma medida de segurança justificável.

Além disso, quando a biometria for indispensável para a segurança da operação ou para o cumprimento de uma obrigação legal, o consentimento do titular não será necessário para legitimar o tratamento.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

R: conforme já destacado em outras respostas, medidas de segurança devem ser implementadas em todo o ciclo de vida do tratamento de dados biométricos. Dentre as medidas de segurança que podem ser implementadas, destacamos: (i) análise prévia, que justifique a necessidade e razoabilidade do tratamento de dados biométricos e posterior elaboração de um Relatório de Impacto à Proteção de Dados, (ii) implementar medidas de minimização durante a coleta dos dados, como, por exemplo, selecionar apenas os dados de entrada estritamente necessários para o atingimento da finalidade, bem como utilizar *templates* ao invés de dados brutos, (iii) implementar políticas para controle de acesso, retenção dos dados, criptografia e expurgo de dados, (iv) fornecer informações claras e acessíveis aos titulares sobre o tratamento dos dados, (v) realizar testes e monitoramento contínuo nos sistemas .

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

R: a transparência é fundamental para preservar a autodeterminação informativa dos titulares. Assim, mesmo na ocorrência de eventos de tratamento massivo de dados, os controladores devem informar aos titulares, através de avisos claros, portais públicos ou outros veículos de comunicação, que seus dados pessoais serão coletados. Além disso, garantir a transparência também implica a disponibilização de canais de comunicação acessíveis, por meio dos quais os titulares possam tirar dúvidas, obter mais detalhes e exercer seus direitos.

Bloco IV – Direitos dos Titulares e Grupos Vulneráveis

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

R: para garantir respeito aos direitos dos titulares, os agentes de tratamento devem prover informação clara, acessível e de fácil compreensão. Além disso, a disponibilização de canais de comunicação direta com os titulares é essencial para o correto atendimento aos direitos dos titulares. Tais canais devem possibilitar que os titulares questionem sobre a existência de decisões automatizadas e revoguem seu consentimento quando este for a base legal utilizada para amparar o tratamento.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

R: o tratamento de dados biométricos de crianças e adolescentes é uma atividade que exige cuidados específicos, sendo sempre pautada pelo princípio fundamental do melhor interesse do menor. Conforme o Enunciado 1 da ANPD, o tratamento não se limita ao consentimento parental específico e pode se basear em outras hipóteses legais claras do artigo 11 da LGPD, como o cumprimento de obrigação legal ou a garantia da prevenção à fraude, desde que a escolha sempre vise proteger a criança ou o adolescente. No contexto financeiro, por exemplo, em que a abertura de contas para menores não emancipados depende da representação de seus responsáveis legais e a biometria é considerada uma boa prática de segurança, a aplicação dessa tecnologia é admissível. Para que isso ocorra de forma legítima, é essencial garantir a participação informada dos responsáveis, oferecendo-lhes explicações transparentes sobre porque o uso dos dados biométricos do menor é uma medida necessária e proporcional para a finalidade pretendida.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

R: o tratamento de dados biométricos de crianças e adolescentes deve ser sempre guiado pelo princípio do melhor interesse do menor e, nos termos do Enunciado nº1 da ANPD, o tratamento não se restringe apenas ao consentimento parental específico, uma vez que pode ser amparado em outras bases legais do artigo 11 da LGPD. Para que os pais ou responsáveis legais possam participar, o controlador deve fornecer as informações pertinentes sobre o tratamento, além de disponibilizar um canal de contato para que os pais possam contatar o controlador. Em complemento, os controladores devem implementar medidas de segurança robustas, como criptografia, *templates*, controles de acesso, *firewalls* e antivírus, além de elaborar políticas internas e Relatório de Impacto à Proteção de Dados.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

R: a operação de um sistema de verificação de idade precisa estar alinhada aos pilares da LGPD, o que inclui transparência, um propósito determinado e a minimização dos dados. Acima de tudo, deve prevalecer o melhor interesse do menor, exigindo que o controlador documente sua análise de risco e necessidade de Relatório de Impacto à Proteção de Dados (RIPD).

A observância do princípio da necessidade implica comparar a eficácia da biometria com métodos alternativos e restringir a coleta de dados ao essencial. Por exemplo, não se deve coletar a impressão digital se a análise facial já cumpre o objetivo pretendido. Adicionalmente, o sistema deve garantir que os dados biométricos não sejam retidos além do tempo estritamente necessário, respeitando-se sempre as obrigações legais ou regulatórias de manutenção de dados que recaiam sobre o controlador.



São Paulo, 31 de julho de 2025.

Diretoria de Normatização da Autoridade Nacional de Proteção de Dados - ANPD

Ref.: Tomada de Subsídios sobre dados biométricos

Venho, em nome da **Associação Brasileira de Planos de Saúde - ABRAMGE** e da **Associação Brasileira de Planos Odontológicos - SINOG**, na figura de sua Encarregada de Proteção de Dados, parabenizar esta autoridade pela excelente condução do tema por intermédio de estudo preliminar, possibilitando à sociedade a participação na construção e maturação da cultura de proteção de dados no Brasil, e também pela importância dada ao tema, a ponto de deliberarem pela aprovação de concessão de prazo adicional para participação social.

Importante reforçar que sinalizamos, tempestivamente na página “Participa + Brasil” voltada à recepção de contribuições à consulta pública, que encaminharíamos nossas contribuições via e-mail [REDACTED], em virtude da restrição de caracteres (300) dos campos destinados à consulta pública. De tal modo, o fazemos em obediência à orientação da própria ANPD, no item 2 “gostaria de deixar algum comentário ou sugestão adicional?”.

Cabe mencionar que o setor de saúde e odontologia suplementares, especialmente as associadas das entidades ABRAMGE e SINOG, acompanha de perto as atividades desta autoridade, sempre que possível contribuindo com as participações sociais propostas pela ANPD, com a ajuda das construções de diversos Grupos de Trabalho sobre o tema.

Deste modo, aproveitamos a oportunidade concedida para destacar os principais pontos de preocupação deste setor em relação ao estudo realizado, conforme expomos a seguir.

BLOCO I – DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Dados biométricos são informações únicas e mensuráveis do corpo ou do comportamento de uma pessoa natural, usadas para identificá-la ou autenticá-la. Nos moldes adotados pela GDPR, ele deve ser conceituado como um dado relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, identificada ou identificável, resultante de um tratamento técnico específico. Ademais, o dado biométrico deve permitir a identificação única de um indivíduo, seja por meio de características físicas (impressões digitais, reconhecimento

Associação Brasileira de Planos de Saúde – ABRAMGE
Associação Brasileira de Planos Odontológicos – SINOG



facial, íris), fisiológicas (padrões de voz) ou comportamentais (padrões de digitação, movimento ocular).

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Práticas de transparência ativa podem e devem ser exigidas dos controladores que tratam dados biométricos, antes mesmo da coleta dos dados, em especial por serem considerados dados pessoais sensíveis pela Lei Geral de Proteção de Dados (LGPD).

Sugestões de práticas de transparência ativa exigidas dos controladores:

A. Política de Privacidade Clara e Detalhada

As políticas de privacidade devem ser claras, abrangentes e de fácil acesso, detalhando todas as práticas de tratamento de dados biométricos, incluindo: Finalidade da coleta dos dados biométricos (por que estão sendo coletados); Forma e duração do tratamento (como serão usados, por quanto tempo); Base legal utilizada (ex.: consentimento, cumprimento de obrigação legal); Direitos dos titulares (acesso, correção, revogação do consentimento etc.); Informações sobre compartilhamento com terceiros, se houver.

B. Consentimento Livre, Informado, Específico e destacado

Quando a base legal for o **consentimento**, este deve ser claro e destacado; informar exatamente **o que está sendo coletado e para qual finalidade**. O titular deve ter opção de **negar sem prejuízo**, quando o consentimento for necessário.

C. Acesso facilitado aos dados:

Os titulares devem ter acesso fácil aos seus dados biométricos armazenados pelo controlador, podendo solicitar correções, atualizações ou remoção, quando necessário.

D. Avisos de Privacidade no Ponto de Coleta

Os avisos devem ser objetivos e visíveis, explicando a coleta, uso e quem é o controlador. Por sua vez, o controlador deve comunicar de forma transparente os riscos associados ao tratamento de dados biométricos.

E. Canal de Comunicação Acessível

Deve haver um canal claro (telefone, e-mail, site) para que o titular possa tirar dúvidas ou exercer seus direitos previstos na LGPD.

F. Registro das Operações de Tratamento

O controlador deve manter um registro interno (como um relatório de impacto à proteção de dados - RIPD), e parte disso pode ser compartilhada com os titulares quando solicitado.

G. Facilidade de Revogação do Consentimento

O titular deve poder revogar o consentimento de forma simples e gratuita, a qualquer momento, com orientações claras sobre como fazer isso.



A transparência ativa no tratamento de dados biométricos é fundamental para garantir a proteção dos direitos dos titulares e promover a confiança nas tecnologias biométricas.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A biometria comportamental deve ser tratada com a mesma atenção especial relativo aos princípios de qualidade de dados e segurança, da biometria fisiológica/tradicional.

A Lei Geral de Proteção de Dados classificou ambos tipos de biometria como dado pessoal sensível, o que significa que, ao menos em tese, o regime jurídico de proteção ao titular de dado é o mesmo, exigindo maior rigor em todas as fases do tratamento, desde a coleta até a eliminação.

Contudo, apesar de ausência de tratamento jurídico diverso a depender do tipo de biometria utilizada, no tocante à qualidade e a segurança dos dados biométricos comportamentais, pode-se considerar a adoção de obrigações adicionais caso o controlador opte pela adoção dessa modalidade.

A biometria comportamental analisa padrões de comportamento do titular de dados. Apesar de ser difícil a falsificação desses dados, pois requer a imitação do comportamento específico do usuário, esses padrões podem variar com o tempo ou com a condição física da pessoa.

Assim, por se tratar de dados mais dinâmicos, recomenda-se a adoção de transparência ativa ampliada, de modo a deixar claro ao titular a finalidade, os tipos de dados biométricos comportamentais que estão sendo coletados e a possibilidade de opt-out caso o dado seja modificado posteriormente à coleta.

BLOCO II – HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

O consentimento para dados biométricos, conforme a LGPD, deve ser livre, informado e inequívoco. Isso significa que o titular dos dados deve ter total ciência de como seus dados serão utilizados e poder consentir livremente, sem coação, e de forma clara. O consentimento também deve ser específico para a finalidade do uso dos dados biométricos.

Para que o consentimento seja livre é necessário que o titular tem condições de entender e querer, sem pressões de qualquer natureza, o tratamento de dados pessoais ao qual está sendo solicitado seu consentimento ou de seu representante legal.

Para que o consentimento seja inequívoco, deve resta evidenciado que o titular dos dados pessoais ou quem age em nome deste, realiza ato inequívoco e proativo de vontade, indicando a nítida intenção de querer que aquela situação que envolve o tratamento de dados pessoais efetivamente ocorra.

Por fim, para ser considerado informado, é necessário que o titular dos dados pessoais receba todas as informações relativas ao tratamento, para o qual será solicitado seu consentimento.



Essas informações podem ser, mas não se limitam a: Finalidade do tratamento; Duração e forma do tratamento; Dados pessoais tratados; Possibilidade de compartilhamento dos dados; Possibilidade e consequências da recusa em conceder o consentimento; direitos legalmente disponíveis para exercício, sobretudo o de revogação do consentimento; e Canais de contato para dúvidas e requisições.

Entretanto, no caso da Saúde e odontologia suplementar, consentimento possivelmente não será considerada a melhor base legal a ser utilizada, uma vez que a coleta de dados biométricos pelas operadoras visará melhor identificar o titular de tais dados para prevenir fraudes na utilização dos planos de saúde e planos odontológicos e assegurar a segurança do titular de modo a incidir a aplicação do artigo 11, II, g da LGPD.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Com a vigência das leis de proteção de dados pelo mundo, um dos valores mais comuns entre elas é de que o tratamento de dados deve contar com as informações estritamente necessárias, observando a proporcionalidade assim considerado o equilíbrio entre o que as informações podem gerar de conhecimento ao agente de tratamento e os interesses do titular, a menor intrusão na vida privada do titular, assim considerando não só a quantidade e qualidade dos dados como fator de conhecimento de aspectos íntimos do titular, mas também a forma menos intrusiva de tratar os seus dados, o que se coaduna com o princípio da adequação.

Entendemos que, exclusivamente, para os processos em que haja alta incidência de fraude, os direitos e liberdades fundamentais do titular podem ser equilibradas com o interesse do sistema da saúde suplementar em diminuir a incidência de fraude, sobretudo porque é interesse do titular que esse desafio se equalize, uma vez que a alta incidência de fraude impacta diretamente e financeiramente o beneficiário, uma vez que a mensalidade necessita de reajuste.

Critérios para a aplicação da hipótese de prevenção à fraude:

- Necessidade: O tratamento de dados biométricos deve ser estritamente necessário para a finalidade de prevenção à fraude, não podendo ser substituído por meios menos intrusivos.
- Proporcionalidade: A coleta e o tratamento devem ser proporcionais ao risco de fraude identificado, evitando a coleta excessiva de dados.
- Finalidade específica: A finalidade do tratamento deve ser claramente definida e comunicada ao titular dos dados, sendo imprescindível que a prevenção à fraude seja o objetivo principal.
- Segurança reforçada: Implementar medidas de segurança robustas para proteger os dados biométricos.
- Transparência: Informar de forma clara e precisa aos usuários sobre a coleta, o tratamento e a finalidade dos dados biométricos, bem como sobre as medidas de segurança implementadas.

Salvaguardas para mitigar riscos:

- Relatórios de impacto: Realizar Relatórios de Impacto à Proteção de Dados (RIPD) para avaliar os riscos do tratamento de dados biométricos e implementar medidas de mitigação.



- Criptografia e anonimização: Biometria deve ser armazenada em formatos protegidos e não imagens brutas.

- Registro das operações:

Manter um registro detalhado de todas as operações de tratamento de dados biométricos, incluindo a finalidade, os dados coletados e as medidas de segurança implementadas.

- Treinamento: Capacitar os colaboradores envolvidos no tratamento de dados biométricos sobre as boas práticas de proteção de dados e a legislação aplicável.

- Monitoramento: Monitorar continuamente o ambiente de tratamento de dados biométricos em busca de vulnerabilidades e ameaças.

- Revisão periódica: Realizar revisões periódicas das medidas de segurança e das políticas de proteção de dados para garantir sua efetividade.

Segmentação de acesso: Acesso aos dados biométricos deve ser limitado apenas a quem realmente precisa.

- Transparência ativa: Informar de forma clara e acessível como, por que e por quanto tempo os dados serão tratados.

- Prazo de retenção limitado: Excluir dados biométricos assim que a finalidade for alcançada (ex.: não guardar após a autenticação, quando possível).

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares? O tratamento de dados biométricos para cumprimento de obrigação legal ou regulatória deve atender, de igual forma, ao que foi exposto no questionamento 06.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

A utilização de dados biométricos para fins de pesquisa com base na base legal do art. 11, II, “c” da LGPD exige rigorosos cuidados para proteger os direitos e liberdades dos titulares. Mesmo com a anonimização, o risco de reidentificação não pode ser ignorado, especialmente quando ocorre o cruzamento de bases de dados.

Sendo assim, mesmo nos casos em que o tratamento seja feito de maneira anonimizada, é importante observar que o tratamento deve estar claramente vinculado à pesquisa e não pode ser desviado para outros fins.

Noutro ponto, a anonimização, neste caso, deve ser irreversível e qualquer tentativa de cruzamento de dados deve ser considerada inadequada. Em caso de a anonimização não ser considerada irreversível, o consentimento do titular pode ser necessário.

E, por fim, mesmo com a anonimização, só devem ser coletados os dados estritamente necessários para o objetivo da pesquisa. O uso de dados biométricos deve ser cuidadosamente ponderado, e os dados devem ser limitados àqueles que são imprescindíveis para alcançar os objetivos da pesquisa.



As salvaguardas a serem adotadas incluem: Garantia da irreversibilidade da anonimização; Adoção de medidas de segurança como criptografia, pseudonimização e auditorias; Controle rigoroso de acesso; transparência com os titulares; e a utilização de sistema com alto grau de proteção de segurança.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Mesmo amparado por uma base legal da LGPD, o uso do reconhecimento facial exige um esforço redobrado de conformidade e ética, pois envolve dados sensíveis. Sendo assim, a adoção de salvaguardas para a mitigação de risco é imprescindível. Destaca-se as principais:

- **Técnicas** - Avaliação de viés algorítmico; Minimização de dados; Controle de acesso restrito; Exclusão dos dados após atingida a finalidade; avaliação de risco à privacidade (por exemplo: Privacy by Design) para garantir que medidas técnicas adequadas de proteção estejam sendo adotadas, tais como requisitos mínimos de segurança da informação (por exemplo: Security by Design) e governança de dados/TI.
- **Jurídicas** - Realização prévio de Relatório de Impacto à Proteção de Dados; Política de privacidade clara e acessível, explicando o uso da tecnologia, inclusive com linguagem acessível e adaptada; Adoção de Mecanismo de opt-out ou oferecimento de método alternativo, sempre que possível, quando o titular escolher não ser identificado por biometria e adoção de bases legais bem fundamentadas.
- **Institucionais** - Treinamento de todos os envolvidos sobre os riscos da biometria e seus limites legais; realização de auditorias e revisões regulares; instituição de grupo multidisciplinar para revisar usos de alto impacto; canal de comunicação eficaz com titulares

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Os sistemas de reconhecimento facial devem ser projetados considerando a aplicação medidas e processos que visem garantir o desenvolvimento ético e seguro desde a sua concepção. Além disso, devem ser adotados altos padrões de governança no que tange a aplicação de controles sobre desenvolvimento e testes de funcionalidades, não somente no momento do desenvolvimento como na aplicação de melhorias contínuas. Devem também existir controles e



processos para identificação proativa de falhas e inconsistências geradas, visando a melhoria e garantia do tratamento ético e adequado dos dados pessoais.

A seguir, destaca-se alguns pontos essenciais para projetar sistemas eficazes, confiáveis e seguros, minimizando falsos positivos/negativos e corrigindo falhas de forma tempestiva, conforme exige a LGPD.

Para garantir eficácia e confiabilidade, desde a concepção, importante treinamento de modelos com dados representativos, ou seja, com bases de dados diversas e balanceadas em termos de gênero, raça, idade. Ademais, bases devem ser auditadas eticamente e legalmente, sem coleta abusiva.

Necessário ainda acurácia e validação técnica contínua, com avaliação de índices de erro (false match rate, false non-match rate) antes da implantação, bem como estabelecer limiares de confiança ajustáveis conforme a criticidade da operação.

Outro ponto importante, é a minimização e qualidade dos dados: coletar apenas o necessário para identificação; e evitar armazenamento permanente sempre que possível.

Por fim, a realização de teste contínuo em ambiente real, com a simulação de cenários diversos para testar a robustez; avaliar o desempenho antes do rollout em larga escala; e estabelecer feedback loop entre o sistema e os responsáveis pela supervisão humana.

Para corrigir falhas tempestivamente, pode-se destacar a supervisão humano das decisões automatizadas, como já previsto na LGPD; a existência de mecanismos de contestação acessíveis pelo titular; monitoramento em tempo real das decisões automatizadas; atualização e retreinamento dos modelos.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Um exemplo de situações onde o uso de tecnologia de reconhecimento facial pode não ser recomendado seria em alguns tipos de serviços em que a autenticação de acesso é necessária, mas os serviços ofertados não estejam diretamente atrelados à autenticação da identidade do indivíduo. Para esses serviços outros meios de autenticação podem ser avaliados, tais como tokens, duplo fator de autenticação.

Entretanto, para serviços que necessitam da garantia e validação automatizada da identidade do indivíduo, principalmente visando a proteção à fraude em sistemas de autenticação, como exemplo serviços de seguros e saúde, a utilização dessas tecnologias, observadas as adequadas salvaguardas técnicas e de segurança, tem se mostrado efetivas.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?



A Lei Geral de Proteção de Dados Pessoais (LGPD) exige medidas reforçadas de segurança e governança para tratar esses dados. Pode-se citar algumas medidas indispensáveis de segurança técnicas e administrativas e dos parâmetros mínimos de avaliação de riscos e monitoramento, conforme exigências da LGPD e boas práticas internacionais.

- **Medidas Técnicas:** criptografia de ponta a ponta; gestão segura de chaves; segregação de bases de dados; controle de acesso robusto; mecanismos de detecção de intrusão para identificar e bloquear tentativas de acesso não autorizado; backups criptografados

- **Medidas Administrativas e Organizacionais Essenciais:** Política de segurança da informação e proteção de dados sensíveis; capacitação contínua de colaboradores e operadores; avaliação de fornecedores; política de governança e responsabilização (accountability); plano de resposta a incidentes de dados sensíveis.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

A negativa ao fornecimento de dados biométricos pode justificar restrições proporcionais ao uso de certas funcionalidades em casos específicos, especialmente quando a biometria é o único meio eficaz para garantir a segurança do titular/organização bem como para assegurar a integridade do serviço.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

A proteção eficaz no tratamento de dados biométricos requer a integração de boas práticas técnicas, jurídicas e éticas, orientadas pelos seguintes pilares:

- A. Segurança reforçada – os dados são irrecuperáveis, portanto, a proteção deve ser máxima;
- B. Transparência e responsabilização – o titular deve entender claramente como seus dados são usados e ter controle sobre eles;
- C. Não discriminação e proporcionalidade – garantir que o uso da biometria não gere exclusão, viés ou coerção.

Ademais, mencionamos, na resposta da pergunta 11 as medidas a serem adotadas para mitigação de risco.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como



em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

Para garantir a autodeterminação informativa em contextos de tratamento contínuo e massivo de dados biométricos, os controladores devem adotar medidas concretas que assegurem transparência acessível e proativa; minimização da coleta e do armazenamento; e participação e controle efetivo do titular. Entre elas:

- A.** Transparência ativa e multilocal: Os controladores devem ser transparentes sobre como os dados biométricos são coletados, usados, armazenados e compartilhados, incluindo informações sobre a duração do tratamento e a identidade dos responsáveis. Quando possível, pode-se pensar no uso de tecnologias complementares de notificação, como QR codes, painéis digitais ou notificações em aplicativos.
- B.** Design ético e governança desde a concepção (Privacy by Design e by Default), garantindo que o sistema de monitoramento minimize a coleta de dados; permita o anonimato quando a finalidade não exigir identificação; uso de tecnologias menos invasivas; e implemente períodos curtos de retenção e descarte automático.
- C.** Canais acessíveis para o exercício dos direitos dos titulares: Criar meios digitais e físicos para que o titular possa solicitar informações sobre o tratamento; solicitar correção de dados incorretos ou incompletos; exercer o direito de oposição, quando aplicável; solicitar anonimização ou exclusão, nos termos legais.
- D.** Monitoramento e Avaliação Contínuos: Implementação das medidas de proteção deve ser continuamente monitorada e avaliada, com a realização de auditorias e avaliações de impacto à privacidade, para garantir a sua eficácia.
- E.** Revisão humana e controle de decisões automatizadas se o sistema utilizar decisões automatizadas baseadas em dados biométricos, bem como o direito de contestação pelo titular, conforme art. 20 da LGPD.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Garantir o respeito aos **direitos dos titulares** no tratamento de **dados biométricos**, especialmente em **contextos de tratamento automatizados**, exige dos **agentes de tratamento** uma atuação ativa, transparente e tecnicamente estruturada. Dentre as medidas que podem ser adotadas, menciona-se:

- A.** Política de privacidade específica para dados biométricos, com linguagem acessível;
- B.** Consentimento destacado e granular, com separação clara de finalidades, quando utilizada essa base legal;
- C.** Existência de um meio facilitado para acesso aos dados tratados e correção de dados incompletos, inexatos ou desatualizados.

Importante destacar, que em dados biométricos, muitas vezes **não há a possibilidade de correção do dado** em si, mas é possível corrigir **atribuições incorretas ou registros associados erroneamente**.



- D. Existência de Mecanismo simples e acessível de revogação no mesmo canal em que o consentimento foi obtido, quando for o caso, com a explicação prévia das consequências da revogação, de forma objetiva e transparente
- E. Explicitar na política de privacidade, avisos sobre a utilização de decisão automatizada;
- F. Existência de canal para contestação
- G. Existência de revisão humana tempestiva;
- H. Monitoramento e registro de falsos positivos/negativos, para fins de auditoria.
- I. Aplicações padrões avançados de governança em Privacidade e Segurança da Informação.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

A participação informada dos pais ou responsáveis no tratamento de dados pessoais — especialmente dados sensíveis como biométricos — de crianças e adolescentes é um princípio central da Lei Geral de Proteção de Dados Pessoais, que estabelece requisitos específicos para o tratamento de dados.

- A. Consentimento específico e destacado por pelo menos um dos pais ou responsável legal, quando necessário, com conteúdo em linguagem simples, acessível e adequada à compreensão. Deve ainda informar quais dados serão coletados, por que serão usados, com quem serão compartilhados e como serão armazenados.
- B. Política de Privacidade Infantil
- C. Mecanismo de verificação de identidade dos responsáveis
- D. Possibilidade de revogação de consentimento, quando for o caso, e acesso.

Entre as hipóteses legais possíveis pode-se mencionar: Consentimento explícito de um dos pais ou responsável legal (Art. 11, I); Obrigação legal ou regulatória (Art. 11, II, a); Execução de políticas públicas (Art. 11, II, b); Proteção da vida ou incolumidade física (Art.11, II, e) e Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (Art.11, II, g)

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

A resposta a esse questionamento encontra-se na pergunta 16.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Diante da vulnerabilidade destes titulares, não se recomenda a coleta de dados biométricos para verificação ou estimação de idade, uma vez que há outras formas de tratamento de dados a fim de confirmar tal informação.



Contribuições à Tomada de Subsídios ANPD: Dados Biométricos
Sistema ABRAMGE/SINAMGE/SINOG/UCA

Renovando os protestos de elevada estima e consideração, colocamo-nos à disposição para demais informações necessárias e despedimo-nos,


Deborah Cristina Couri
Advogada
OAB/DF nº 39.703

São Paulo, 01 de agosto de 2025

À

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Coordenação-Geral de Normatização

A/C: Sr Rodrigo Santana dos Santos

normatizacao@anpd.gov.br

Ref.: Contribuições da ABRANET à Tomada de Subsídios da ANPD, que aborda o tratamento de Dados Biométricos.

Prezados/as,

A **ASSOCIAÇÃO BRASILEIRA DE INTERNET - ABRANET**, entidade de classe de âmbito nacional que representa empresas de tecnologia da informação relacionadas à prestação de serviços nativos de Internet, entre as quais provedores de conectividade, acesso e conteúdo, plataformas, fintechs, paytechs e data centers, vem, respeitosamente, apresentar a ANPD suas contribuições a Tomada de Subsídios, que aborda o tratamento de Dados Biométricos.

Abaixo seguem as contribuições da Associação sobre o tema da Consulta, que, de forma geral, abordam os seguintes pontos:

- i. Entendemos que o critério objetivo de capacidade de identificação inequívoca auxilia na definição de dado pessoal sensível/biométrico e aplicabilidade das medidas de segurança compatíveis.
- ii. É necessário separar os padrões comportamentais que levam a identificação inequívoca dos usuários de análises de padrões comportamentais utilizados de maneira agregada para aferir métricas.
- iii. O consentimento não deve ser a hipótese legal quando a coleta de dados biométricos decorre de obrigação regulatória que busque prevenir fraudes e garantir segurança na autenticação do cadastro do usuário em seu aplicativo bancário.
- iv. A hipótese de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) deve vir acompanhada do teste de balanceamento que demonstre medidas de segurança capazes de mitigar riscos para o titular de dados pessoais.
- v. A coleta de dados biométricos deve ser informada ao titular de maneira clara e contextualizada sendo os mesmos cuidados necessários para possibilitar o exercício dos direitos dos titulares.
- vi. O reconhecimento facial se faz uma medida de segurança adequada para autenticar o usuário em aplicativos financeiros, e o avanço das tecnologias de reconhecimento contribuem para uma autenticação mais assertiva e segura.

- vii. As medidas de segurança devem incluir a utilização de criptografia forte para armazenar e transmitir dados biométricos.
- viii. É essencial que os controladores apliquem o princípio da necessidade identificando se a coleta de dados biométricos é o único meio possível de fornecer o acesso a determinado produto ou serviço.
- ix. É necessário que as tecnologias de reconhecimento facial sejam desenvolvidas e treinadas utilizando uma base de dados ampla que contemple as especificidades de cada usuário e suas características físicas considerando a diversidade de dados biométricos existente na população brasileira.
- x. A transparência ostensiva em pontos de coleta de dados biométricos se faz necessária para garantir ao titular a possibilidade de exercer o seu direito à autodeterminação informativa
- xi. Pais ou responsáveis devem ser claramente informados sobre a finalidade, a duração, e os destinatários dos dados biométricos, em linguagem acessível e inteligível, inclusive, para as crianças e adolescentes.

Sendo o que cumpria para o momento, a ABRANET coloca-se à disposição para qualquer colaboração que esta Casa venha a julgar necessária, apresentando seus protestos de elevada estima e consideração.

Atenciosamente,

ASSOCIAÇÃO BRASILEIRA DE INTERNET – ABRANET

Contribuição ABRANET | TS ANPD

Íntegra da Consulta [aqui](#).

Tratamento de Dados Pessoais Sensíveis – Dados Biométricos

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

Perguntas ANPD	Comentários ABRANET (Até 2.000 caracteres)
1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?	Entendemos que a definição de dados biométricos do GDPR deve ser usada como inspiração para a ANPD. O GDPR (considerando 51, art. 4º (14) e art. 9º (1)) define que os dados biométricos são dados capazes de levar a identificação inequívoca ou a autenticação de uma pessoa singular quando processados por meios técnicos específicos, eliminando as fotografias do escopo de dado biométrico quando distantes desse contexto de identificação do usuário. O critério objetivo de capacidade de identificação inequívoca auxilia na definição de dado pessoal sensível/biométrico e aplicabilidade das medidas de segurança compatíveis.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?	A Abranet entende que as práticas de transparência ativa para garantir que os titulares possuem informações claras sobre o tratamento podem envolver: (i) Avisos de privacidade no momento da coleta / <i>legal disclaimer</i> nos pontos de coleta ativa de dados biométricos; (ii) Identificação dos controladores para exercício de direitos dos titulares e (iii) Política de privacidade que elenque as medidas de segurança utilizadas no tratamento de dados biométricos.
3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?	A Abranet entende ser necessário separar os padrões comportamentais que levam a identificação inequívoca dos usuários de análises de padrões comportamentais utilizados de maneira agregada para aferir métricas, por exemplo, qualidade do atendimento dos usuários ou análise de movimentações financeiras com a finalidade de identificar comportamentos suspeitos e prevenir fraudes. Quando a biometria comportamental for utilizada para identificar um usuário de maneira inequívoca, as mesmas regras e cuidados devem ser observados.
BLOCO II – HIPÓTESES LEGAIS	
4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?	A Abranet entende que o consentimento não deve ser a hipótese legal quando a coleta de dados biométricos decorre de obrigação regulatória que busque prevenir fraudes e garantir segurança na autenticação do cadastro do usuário em seu aplicativo bancário.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?	Entendemos que a hipótese de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) deve vir acompanhada do teste de balanceamento que demonstre medidas de segurança capazes de mitigar riscos para o titular de dados pessoais. A segurança do usuário e a obrigação regulatória de prevenção à fraude estão em linha com o princípio da necessidade, finalidade e segurança e o controlador deve utilizar os dados coletados para a finalidade informada em sua política de privacidade possibilitando o exercício dos direitos dos titulares sempre que demandado. Além disso, como boa prática, pode ser utilizado: (i) Criptografia dos dados coletados; (ii) Autenticação Multi-Fator (<i>Multi-factor authentication</i> – MFA); (iii) Controle de acesso a sistemas e bases para necessidades específicas; (iv) Monitoramento e tratamento em caso de qualquer incidente identificado e (v) Registro de logs. Vale ressaltar que, diferente do cenário de monitoramento em zonas públicas muito debatido no contexto de tratamento de dados biométricos, o uso de biometria na autenticação em sistemas e aplicativos é uma forma segura, rápida e eficaz de autenticação do usuário que permite que ele acesse suas contas ao mesmo tempo que contribui para cumprimento de obrigação regulatória de prevenção a fraude, colaborando para a higidez do sistema financeiro.

	O tratamento de dados biométricos neste contexto previne o acesso indevido por terceiros e tem níveis de erro (falso positivo) mínimos, sendo as novas tecnologias amplamente desenvolvidas para a melhora desse fluxo um segundo fator que colabora para uma maior segurança do sistema e do titular enquanto usuário.
6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?	A coleta de dados biométricos deve ser informada ao titular de maneira clara e contextualizada sendo os mesmos cuidados necessários para possibilitar o exercício dos direitos dos titulares: (i) Avisos de privacidade no momento da coleta e <i>legal disclaimer</i> nos pontos de coleta ativa de dados biométricos; (ii) Identificação dos controladores para exercício de direitos dos titulares e (iii) Política de privacidade que elenque as medidas de segurança utilizadas no tratamento de dados biométricos.
7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?	A Abranet entende que em relação à pergunta 7, esclarecemos que a hipótese apresentada não se aplica ao nosso escopo, razão pela qual não temos elementos para uma contribuição adequada sobre os limites do tratamento de dados biométricos por órgãos de pesquisa, mesmo em contextos de anonimização e possíveis re-identificações, tampouco quanto às salvaguardas adicionais que poderiam ser implementadas nesses casos.
BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS	

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?	Entendemos que a metodologia <i>Privacy by Design</i> é essencial para identificar potenciais riscos no tratamento de dados biométricos e registrar as medidas de segurança capazes de mitigar riscos decorrentes do tratamento de tais dados pessoais. Além disso, deve-se certificar de que os sistemas de reconhecimento facial são treinados com dados diversos para evitar vieses, especialmente em relação à aspectos de cor e raça. Isso ajuda a garantir que a tecnologia funcione de forma equitativa para diferentes grupos de indivíduos, prevenindo discriminação.
9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?	Conforme exposto acima, através do <i>Privacy By Design</i>, deve-se buscar assegurar que os sistemas sejam desenvolvidos observando-se critérios como diversificação de dados de treinamento, ajustes algorítmicos, transparência e explicabilidade acerca do tratamento dos dados. Em suma, é crucial estar atento aos vieses incorporados nos algoritmos e adotar práticas que ajudem a mitigar esses vieses. Essa responsabilidade deve recair sobre os desenvolvedores dessa tecnologia cabendo aos utilizadores avaliar e arquivar os reports que demonstrem as diretrizes e bases utilizadas neste treinamento.
10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?	A Abranet entende que o reconhecimento facial é a medida de segurança adequada para autenticar o usuário em aplicativos financeiros, e o avanço das tecnologias de reconhecimento contribuem para uma autenticação mais assertiva e segura, a exemplo da técnica <i>liveness</i> que coleta a biometria do usuário por meio de movimentos da face, impedindo que fotografias estáticas sejam utilizadas por terceiros para burlar o sistema. A documentoscopia, por exemplo, é um meio alternativo de autenticação do usuário, mas a

	possibilidade de fraude de documento de identidade fragiliza a utilização deste meio de autenticação, sendo menos seguro para o usuário e para o sistema financeiro de maneira geral.
BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS	
11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?	Entendemos que a constante evolução das tecnologias de reconhecimento facial é imprescindível para garantir a segurança de sua utilização tanto para o usuário quanto para as empresas que dependem de tal meio de autenticação para validar o acesso aos seus produtos e serviços digitais. Os parâmetros mínimos já estão contidos na legislação, quais sejam: <i>Privacy by Design</i>, política de privacidade, <i>privacy notice</i> no ponto de coleta ativo de dados pessoais, elaboração de relatórios de impacto que registrem as medidas de segurança aplicadas e constantes testes para verificar ao longo do tempo a efetividade das medidas e o volume de falhas identificado. Nesse sentido, as medidas de segurança devem incluir a utilização de criptografia forte para armazenar e transmitir dados biométricos. Além disso, é fundamental adotar mecanismos avançados de autenticação multifator, restringir o acesso a dados sensíveis através de controles de acesso rigorosos e realizar auditorias regulares para identificar e corrigir possíveis vulnerabilidades.
12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o	A Abranet entende ser essencial que os controladores apliquem o princípio da necessidade identificando se a coleta de dados biométricos é o único meio possível de fornecer o acesso a determinado produto ou serviço. Por se tratar de dado pessoal sensível, caso o serviço não seja essencial e a coleta de dados

tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?	pessoais biométricos seja opcional, deve ser garantido ao usuário a utilização do produto ou serviço com forma diversa de autenticação.
13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?	Entendemos que para evitar discriminação ilícita e abusiva em face dos usuários é necessário que as tecnologias de reconhecimento facial sejam desenvolvidas e treinadas utilizando uma base de dados ampla que contemple as especificidades de cada usuário e suas características físicas considerando a diversidade de dados biométricos existente na população brasileira. Promover equidade e transparência na aplicação das tecnologias biométricas e monitorar seu impacto sobre diferentes grupos de indivíduos são passos essenciais para evitar discriminação ilícita e abusiva. Essa responsabilidade deve recair sobre os desenvolvedores dessa tecnologia cabendo aos utilizadores avaliar e arquivar os reports que demonstrem as diretrizes e bases utilizadas neste treinamento. Além disso, como boa prática, podem ser utilizadas pelos Controladores as seguintes medidas: (i) Criptografia dos dados coletados; (ii) Autenticação Multi-Fator (<i>Multi-factor authentication</i> – MFA); (iii) Controle de acesso a sistemas e bases para necessidades específicas; (iv) Monitoramento e tratamento em caso de qualquer incidente identificado e (v) Registro de logs.
14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de	A Abranet entende que a transparência ostensiva em pontos de coleta de dados biométricos se faz necessária para garantir ao titular a possibilidade de

dados biométricos – como em iniciativas de cidades inteligentes (<i>smart cities</i>), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?	exercer o seu direito à autodeterminação informativa entrando em contato com o Encarregado no canal também informado no aviso de privacidade.
BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS	
15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?	Entendemos que os avisos de privacidade em contexto, no ponto de coleta ativo de dados pessoais, são a forma de garantir que o titular está ciente de quais dados serão coletados e para quais finalidades bem como terceiros envolvidos no fluxo de compartilhamento de dados pessoais. Por meio do canal do Encarregado o usuário terá a oportunidade de exercer seus direitos previstos no art. 9º da LGPD, inclusive sobre decisões automatizadas, obrigação que não limita aos dados biométricos.
16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?	A Abranet entende ser importante que os pais ou responsáveis sejam claramente informados sobre a finalidade, a duração, e os destinatários dos dados biométricos, em linguagem acessível e inteligível, inclusive, para as crianças e adolescentes. O tratamento desses dados deve ocorrer sob hipóteses legais específicas, sempre prevalecendo o princípio do melhor interesse da criança ou adolescente. É necessário que se garanta a minimização de dados, além de implementar medidas de segurança rigorosas para proteger esses dados.

	As empresas devem também estabelecer um canal de comunicação aberto com os pais ou responsáveis para esclarecer dúvidas e fornecer informações adicionais sempre que necessário.
17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?	Entendemos que a autenticação dos usuários menores de idade em aplicativos digitais é tão importante quanto a de usuários maiores, sendo a biometria um meio seguro e eficaz de garantir a segurança do usuário para identificação inequívoca e prevenir fraudes que possam ocorrer. Por outro lado, o uso para verificação etária não parece adequado, pois traz mais riscos que benefícios. Assim, entendemos que as mesmas medidas de segurança devem ser aplicadas para garantir segurança e direitos dos titulares, conforme acima elencadas: (i) Criptografia dos dados coletados; (ii) Autenticação Multi-Fator (<i>Multi-factor authentication</i> – MFA); (iii) Controle de acesso a sistemas e bases para necessidades específicas; (iv) Monitoramento e tratamento em caso de qualquer incidente identificado; (v) Registro de logs; (vi) Avisos de privacidade no momento da coleta e <i>legal disclaimer</i> nos pontos de coleta ativa de dados biométricos;

	(vii) Identificação dos controladores para exercício de direitos dos titulares e (viii) Política de privacidade que elenque as medidas de segurança utilizadas no tratamento de dados biométricos.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Reconhecemos a utilidade e importância das tecnologias de reconhecimento facial disponíveis no mercado hoje, especialmente para identificação inequívoca de pessoa individual e outros usos já comuns. No entanto, entendemos que estas tecnologias ainda não estão aptas a identificar, com segurança e precisão, a idade de determinado usuário.

Isso porque a verificação de idade é significativamente mais complexa do que a identificação inequívoca ou outros usos já corriqueiros no mercado. O período da infância e adolescência atinge de forma diferente os indicadores faciais de cada jovem, especialmente durante a puberdade. Características etárias variam significativamente entre pessoas, etnias etc.

A leitura e validação biométrica também podem ser afetadas por variáveis externas, como condições de iluminação e qualidade dos dispositivos de captura, aumentando a margem de erro e potencialmente comprometendo a segurança dos dados.

Considerando que um falso positivo na verificação de idade pode limitar que pessoas acessem serviços legítimos e exerçam seus direitos, a verificação ou estimação de idade por meio do fornecimento de dados biométricos não é a ferramenta mais adequada.

Nesse sentido, há o risco de erro na estimativa, o que pode levar a situações de discriminação ou tratamento inadequado, bem como restrição de acesso a direitos. Além disso, a tentativa de deduzir a idade através de dados biométricos pode violar a privacidade dos indivíduos, gerando preocupações com a vigilância excessiva e uso indevido desses dados.

Para compatibilizar tal prática com o princípio da necessidade, é importante que se busque minimizar a coleta de dados àqueles estritamente necessários para verificar ou estimar a idade do usuário.

Entretanto, é importante que se frise que a verificação de idade poderá ser feita através de outros meios que prescindem do tratamento de dados pessoais sensíveis, como a documentoscopia, revelando que a leitura biométrica não seria o meio mais seguro de se essa finalidade.



CONTRIBUIÇÃO DO INSTITUTO ALANA

**TOMADA DE SUBSÍDIOS SOBRE DADOS BIOMÉTRICOS DA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS**

JULHO DE 2025

À Coordenadoria de Normatização da Autoridade Nacional de Proteção de Dados,

O Instituto Alana, organização da sociedade civil que atua na promoção e defesa dos direitos de crianças e adolescentes, apresenta sua contribuição à Tomada de Subsídios sobre Dados Biométricos, reiterando a importância de que o tratamento de dados pessoais biométricos de crianças e adolescentes seja compreendido, no âmbito regulatório mais abrangente, **como medida de exceção e de último recurso**.

A natureza sensível e imutável desses dados, aliada à condição peculiar de desenvolvimento dos titulares crianças e adolescentes, exige do Estado brasileiro o fortalecimento de salvaguardas normativas específicas, capazes de mitigar riscos e garantir o respeito ao melhor interesse da criança e sua proteção integral, fundamentos previstos no art. 227 da Constituição Federal, no Estatuto da Criança e do Adolescente (ECA), na Lei Geral de Proteção de Dados Pessoais (LGPD) e em tratados internacionais ratificados pelo Brasil.

A presente contribuição sistematiza os riscos jurídicos, técnicos e éticos associados a esse tratamento e propõe alternativas para a construção de caminhos futuros. O objetivo é colaborar com a consolidação de uma cultura de proteção de dados pessoais que tenha como premissa a proteção integral e prioritária da infância e da adolescência.

Além disso, o Instituto Alana reitera o apelo para que a ANPD priorize, de forma transparente e participativa, a edição de **diretrizes normativas específicas sobre o tratamento de dados pessoais de crianças e adolescentes**, conforme previsão expressa na Agenda Regulatória 2023–2024 e no Mapa de Temas Prioritários da Autoridade. A **construção de guias interpretativos e códigos de conduta apropriados à idade é urgente**, sobretudo diante da expansão do uso irrefletido de tecnologias em contextos educacionais e em espaços públicos.

Permanecemos à disposição para dialogar e aprofundar os pontos aqui apresentados.

Instituto Alana

Ana Claudia Cifali
Coordenadora Jurídica
OAB/RS nº 80.390

**Júlia Fernandes de
Mendonça**
Advogada
OAB/BA: 41.785

Maria Mello
Coordenadora do programa
Criança e Consumo

**João Francisco de Aguiar
Coelho**
Advogado
OAB/SP: 442.643

Samidy Ribeiro
Estagiária de Direito

Participa + Brasil - Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos

Prazo: 01/08/2025

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Resumo executivo para a Plataforma Participa + Brasil

A coleta e o tratamento de dados biométricos de crianças e adolescentes devem ser considerados como último recurso, especialmente quando associados a decisões automatizadas. Crianças são titulares plenos dos direitos da LGPD (art. 18) e gozam de

proteção reforçada (art. 14), que exige transparência ativa, qualificada e acessível, conforme §2ª e §6º. Produtos e sistemas devem adotar o “direito por design”, com interfaces adequadas à autonomia progressiva. Termos genéricos e práticas opacas são incompatíveis com o dever de informação. A experiência internacional mostra que ferramentas como o *Playful by Design* ajudam a equilibrar metas comerciais e direitos da criança. Por isso, seria importante consolidar diretrizes específicas sobre o tema, conforme previsto na agenda regulatória e o Mapa de Temas Prioritários da ANPD. O detalhamento completo encontra-se no documento enviado por e-mail.

Antes de adentrarmos às especificidades das perguntas, é importante destacar que a coleta e o tratamento de dados biométricos de crianças e adolescentes, para qualquer finalidade, devem ser compreendidos como **último recurso**, conforme será aprofundado nas respostas seguintes. Tal entendimento é ainda mais rigoroso quando se trata do uso de tecnologias baseadas em decisões automatizadas, dado o potencial de amplificação de assimetrias, riscos e impactos sobre sujeitos em condição peculiar de desenvolvimento biopsicossocial.

Considerando, contudo, que a Autoridade Nacional de Proteção de Dados (ANPD) abriu recentemente uma tomada de subsídios sobre “Inteligência Artificial e Revisão de Decisões Automatizadas”¹, compreendemos que o foco desta pergunta está centrado no exercício dos direitos dos titulares, especialmente daqueles juridicamente considerados vulneráveis, como é o caso de crianças e adolescentes.

É fundamental reiterar que crianças e adolescentes, enquanto sujeitos de direitos (art. 227 da Constituição Federal e art. 3º do ECA), são titulares de **todos os direitos previstos no art. 18 da LGPD**, além de gozarem de proteção normativa qualificada no art. 14 da mesma lei, o qual estabelece salvaguardas adicionais no tratamento de seus dados pessoais.

Destaca-se que o **princípio da transparência** (art. 6º, IV) ganha uma **qualificação e reforço normativo específico** quando aplicado a esse público. O §2º do art. 14 determina que, nos casos em que o tratamento se fundamente no consentimento, os controladores devem **manter pública a informação** sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos do titular. Já o §6º exige que tais informações sejam fornecidas de modo **simples, claro e acessível**, considerando as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais da criança ou adolescente, inclusive com **uso de recursos audiovisuais**, quando adequado.

¹ BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). ANPD apresenta resultados da Tomada de Subsídios sobre Tratamento Automatizado de Dados Pessoais. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apresenta-resultados-da-tomada-de-subsidios-sobre-tratamento-automatizado-de-dados-pessoais>. Acesso em: 23 jul. 2025.

Isso significa que, **se o produto, serviço ou sistema automatizado puder ser acessado ou impactar crianças e adolescentes**, ele deverá ser desde o início **projetado com medidas de transparência a partir dos direitos da criança por design²**, não sendo admissível a aplicação de cláusulas genéricas ou práticas opacas que impossibilitem a compreensão e o exercício de direitos por seus responsáveis legais, ou pelas próprias crianças, conforme sua autonomia progressiva.

(i) Exercício de direitos dos titulares crianças e adolescentes e seus direitos garantidos por design

Nesse sentido, **a orientação inicial no desenvolvimento de produtos digitais voltados ao público infantil deve partir dos direitos das crianças como premissa fundante do processo de design, e não como um elemento de adequação posterior a metas comerciais ou técnicas.**

Conforme apontado no recentíssimo artigo “Applying Children’s Rights to Digital Products: Exploring Competing Priorities in Design”³, essa inversão de preceitos exige que designers e tomadores de decisão tratem os direitos das crianças - como participação, desenvolvimento saudável e privacidade - como **parâmetros de design**, e não como obstáculos a serem mitigados. Tal perspectiva está alinhada aos princípios do design centrado na criança e ao dever de respeito ao superior interesse da criança (art. 227 da CF/88; art. 100 do ECA). Reverter a lógica usual em que as metas comerciais orientam o projeto e os direitos infantis são tratados como elementos acessórios, permite maior conformidade com os marcos normativos nacionais e internacionais, como a Convenção sobre os Direitos da Criança e o Comentário Geral nº 25 da ONU.

Para operacionalizar essa abordagem, ferramentas como o **Playful by Design (PbD)** mostram-se promissoras. O estudo mencionado demonstrou que o seu uso contribui para que designers **reconheçam tensões entre prioridades comerciais e princípios éticos**, e desenvolvam modos de equilibrá-las. Nesse sentido, os autores destacam que ferramentas como o PbD fornecem tanto uma **justificativa convincente (“compelling rationale”)** quanto **meios práticos** para implementar os direitos das crianças no design de produtos e serviços digitais. Sua adoção pode ser vista como uma **boa prática de governança ética e preventiva**, em

² Information Commissioner’s Office (ICO). Age appropriate design: a code of practice for online services. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>. Acesso em: 23 jul. 2025.

³ Pothong, K, Livingstone, S, Colvert, A & Pschetz, L 2024, Applying children’s rights to digital products: Exploring competing priorities in design. in *IDC '24: Proceedings of the 23rd annual ACM Interaction Design and Children Conference*. ACM, pp. 93-104. <https://doi.org/10.1145/3628516.3655789>

consonância com os princípios da LGPD (art. 6º, incisos II, VII e VIII) e com diretrizes internacionais de proteção de dados de crianças e adolescentes em ambientes digitais.

Nesse contexto, reforça-se respeitosamente **o apelo para que a Autoridade avance na construção de diretrizes específicas voltadas à proteção de crianças e adolescentes, alinhando-se a experiências internacionais que já implementaram códigos de design apropriado à idade e padrões de boas práticas para esse público.** Essa demanda, que vem sendo reiterada desde a primeira tomada de subsídios sobre o tema, em 2022, já integra a Agenda Regulatória da Autoridade para o biênio 2023–2024 e foi reconhecida no Mapa de Temas Prioritários do segundo semestre de 2024. Diante disso, solicita-se que a ANPD priorize esse processo de normatização, de forma transparente e participativa, garantindo que os direitos da infância e adolescência sejam devidamente protegidos no ambiente digital.

(ii) Transparência ativa, qualificada e acessível

O princípio da transparência é reiteradamente consagrado na LGPD - no art. 6º, inciso VI -, sendo detalhado pelos artigos 9º e 18, que estabelecem diretrizes para a garantia do livre acesso, tanto na sua dimensão ativa quanto passiva. Crianças e adolescentes, enquanto titulares de dados, gozam dos mesmos direitos que qualquer adulto. No entanto, **o art. 14 da LGPD, em seus §§ 2º e 6º, qualifica esse direito de transparência** ao reconhecer que, diante da sua condição peculiar de desenvolvimento, o tratamento de seus dados requer deveres adicionais por parte dos controladores.

O § 2º do art. 14 estabelece a obrigação de transparência ativa: **os controladores devem manter públicas, desde a concepção do produto ou serviço, as informações sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos** previstos no art. 18. Já o § 6º do mesmo artigo reforça que essas informações **devem ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do titular, e com o uso de recursos audiovisuais**, quando adequado.

Essa dupla exigência normativa — transparência ativa e qualificada — evidencia que termos de uso genéricos ou políticas de privacidade opacas são ineficazes e ilegais quando aplicados a crianças e adolescentes. Tal entendimento é reforçado pela Resolução CONANDA nº 245/2024 e pelo Comentário Geral nº 25, que, em seus artigos 13 e 16, exige comunicação adequada e transparente, bem como escuta significativa de crianças e adolescentes, respeitado seu grau de maturidade.

Ou seja, documentos jurídicos padronizados, como termos de uso genéricos e políticas de privacidade opacas, são insuficientes e ineficazes para esse público. A comunicação deve ser pensada a partir da perspectiva de adaptação a partir da autonomia progressiva.

Além da informação, é fundamental garantir o **direito de acesso aos dados tratados**, bem como a possibilidade de **retificação de dados incorretos** e de **revogação do consentimento a qualquer momento** (art. 18, incisos I, III e V da LGPD). No caso de crianças e adolescentes, tais prerrogativas devem ser implementadas de forma desburocratizada, intuitiva e segura, conforme previsto também no art. 14 da Resolução Conanda nº 245/2024 e no já mencionado art. 14 §6ª da LGPD. Isso implica:

- Adoção de **interfaces intuitivas** para solicitações de acesso, correção ou exclusão de dados, sem exigência de procedimentos excessivamente complexos;
- Implementação de **mecanismos auditáveis e rastreáveis** que permitam comprovar o exercício e o atendimento aos direitos dos titulares e seus responsáveis;
- No caso de tratamento com base no consentimento parental, deve-se assegurar a possibilidade de **revogação simples e sem ônus**, com consequências informadas e claras sobre a suspensão do tratamento.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

Resumo executivo para a Plataforma Participa + Brasil

O tratamento de dados biométricos de crianças e adolescentes só deve ocorrer em casos excepcionais, com base em avaliação robusta de necessidade, proporcionalidade e no melhor interesse da criança (art. 14 da LGPD). Isso exige a realização de avaliações de impacto específicas (CRIAs) e a priorização de meios menos invasivos. A coleta biométrica em escolas, por exemplo, não pode ser justificada por ganhos operacionais, como controle de frequência, sobretudo diante de alternativas adequadas. A Resolução

CONANDA nº 245/2024 reforça que tais práticas devem respeitar a privacidade e garantir o direito à informação e à oposição, conforme o grau de maturidade da criança. O consentimento parental, por si só, não basta. Tecnologias biométricas devem ser vetadas quando os riscos superam os benefícios. O detalhamento completo da resposta está no documento encaminhado por e-mail.

O ponto de partida para qualquer operação de tratamento de dados pessoais envolvendo crianças e adolescentes é a conformidade com o melhor interesse da criança, nos termos do art. 14 da LGPD. Importante destacar que este dispositivo, como reconhecido em diversas manifestações da própria ANPD, não deve ser compreendido apenas como um princípio abstrato, mas sim como um conceito jurídico tripartite, nos termos do Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU (2013)⁴, que o define como: (I) um direito substantivo da criança, que deve ser prioritariamente considerado em todas as ações que lhe digam respeito; (II) um princípio jurídico interpretativo, que orienta a leitura e aplicação das demais normas; (III) uma regra de procedimento, que impõe a realização de avaliações específicas e documentadas da compatibilidade de cada decisão com o melhor interesse.

Assim, não é possível justificar o tratamento de dados biométricos de crianças e adolescentes apenas com base em uma hipótese legal da LGPD, sem antes demonstrar de forma robusta que tal tratamento é necessário, proporcional, e orientado pelo melhor interesse da criança em um caso concreto.

Nesse sentido, é recomendável que os agentes de tratamento realizem avaliações documentadas de impacto sobre os direitos da criança e do adolescente (Child Rights Impact Assessments – CRIAs)⁵, conforme sugerido por organismos internacionais como a UNICEF⁶, a fim de mensurar riscos e benefícios do tratamento proposto. Caminho similar é também defendido por Sonia Livingstone em seu recente artigo “Child Rights Impact Assessment: A Policy Tool for aRights-Respecting Digital Environment”⁷

Isso porque os dados biométricos, na qualidade de dados pessoais sensíveis, possuem o potencial inerente de revelar características íntimas e imutáveis do

⁴ COMITÊ SOBRE OS DIREITOS DA CRIANÇA (CRC). Comentário Geral nº 14 (2013) sobre o direito da criança de ter seus melhores interesses considerados como prioridade (art. 3, §1). Disponível em: <https://www.refworld.org/legal/general/crc/2013/en/95780>. Acesso em: 23 jul. 2025.

⁵ 5Rights Foundation. Child Rights Impact Assessment (CRIA) Report. 2024. Disponível em: <https://5rightsfoundation.com/wp-content/uploads/2024/09/CRIA-Report.pdf>. Acesso em: 23 jul. 2025.

⁶ UNICEF UK. Child Rights Impact Assessment (CRIA): Template and Guidance for Local Authorities. Junho de 2022. Disponível em: https://www.unicef.org.uk/child-friendly-cities/wp-content/uploads/sites/3/2022/06/CRIA_June-2022.pdf. Acesso em: 23 jul. 2025.

⁷ Livingstone, S. and Pothong, K. (2025), Child Rights Impact Assessment: A Policy Tool for a Rights-Respecting Digital Environment. Policy & Internet, 17: e70008. <https://doi.org/10.1002/poi3.70008>

titular, expondo-o e colocando-o em posição de vulnerabilidade. Quando se trata de crianças e adolescentes — sujeitos que já são considerados juridicamente vulneráveis — o tratamento desses dados implica a intensificação de vulnerabilidades estruturais e contextuais preexistentes. Tal preocupação agrava-se diante do fato de que, ao contrário de credenciais substituíveis, como senhas, os dados biométricos são, via de regra, permanentes e não podem ser revogados ou modificados em caso de incidente de segurança, por exemplo.

Essa preocupação foi reconhecida pela própria Autoridade na Nota Técnica nº 5/2025/FIS/CGF/ANPD, elaborada no contexto da coleta de dados biométricos em estádios de futebol. O documento aponta riscos elevados à privacidade, à exclusão e à estigmatização de grupos vulneráveis, sobretudo quando o uso de tecnologias biométricas não está vinculado a finalidades legítimas, tampouco acompanhado de transparência, proporcionalidade e salvaguardas adequadas. A necessidade de atenção cuidadosa foi igualmente demonstrada no Radar Tecnológico nº 2: biometria e reconhecimento facial⁸ da Autoridade, o qual aponta que “o uso das tecnologias de biometria nas escolas suscita preocupação”.

Ainda na mencionada Nota Técnica, a Autoridade destaca expressamente a Resolução nº 245/2024 do Conselho Nacional dos Direitos da Criança e do Adolescente (CONANDA), que trata da proteção de dados pessoais de crianças e adolescentes no ambiente digital. Nos termos do art. 16 da Resolução, “qualquer tipo de mecanismo de vigilância e monitoramento digital de crianças e adolescentes, associado a ferramentas de automação e tratamento de dados pessoais, deve respeitar seu direito à privacidade e não deve ser utilizado de forma indiscriminada e injustificável”. O parágrafo único do mesmo artigo complementa ao estabelecer que, quando forem utilizados mecanismos de segurança, ainda que justificados pelo interesse superior da criança ou adolescente, devem ser priorizados os meios menos invasivos, e deve ser assegurado à criança ou adolescente o direito de conhecer o funcionamento da tecnologia e manifestar oposição, conforme seu grau de maturidade. Tais disposições normativas dialogam diretamente com os princípios da adequação e da necessidade previstos no art. 6º, II e III da LGPD, segundo os quais o tratamento deve se restringir ao mínimo necessário para a finalidade pretendida, de forma proporcional e justificada. Nunca é demais reiterar que o princípio da necessidade, no caso de crianças e adolescentes, é qualificado pelo §4º do artigo 14.

Transpondo essa análise para o contexto educacional, é necessário reconhecer que as mesmas premissas se aplicam com igual ou maior intensidade. A introdução de tecnologias biométricas em escolas e espaços recreativos não pode ser

⁸ Autoridade Nacional de Proteção de Dados (ANPD). *Radar Tecnológico: biometria e reconhecimento facial*. Brasília: ANPD, 2024. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf>. Acesso em: 23 jul. 2025.

naturalizada com base em supostas promessas de eficiência, como ganho de tempo no controle de frequência. Pelo contrário, a existência de alternativas menos invasivas torna o uso dessas tecnologias desnecessário e potencialmente violador de direitos fundamentais.

Dessa forma, exige-se que os responsáveis pelo tratamento de dados no ambiente educacional considerem alternativas que respeitem os princípios da necessidade e da proporcionalidade, garantindo, ao mesmo tempo, a proteção da privacidade e a segurança dos estudantes sem recorrer a meios excessivos, discriminatórios, desnecessários ou opacos. A incorporação das diretrizes da Resolução CONANDA nº 245/2024 é, portanto, essencial para assegurar a compatibilidade entre o uso de tecnologias e a proteção integral dos direitos da criança e do adolescente, conforme previsto na LGPD e no ECA.

O uso de tecnologias biométricas no ambiente escolar só pode ser pensando e fomentado sob a lógica da promoção de direitos fundamentais, como no caso do uso de tecnologias para acessibilidade de pessoas com deficiência ou neurodivergentes, a exemplo de tecnologias como o Blindtalk⁹. No entanto, ainda assim, cabe a ressalva de que as tecnologias biométricas hoje no mercado carecem de muitos aprimoramentos para serem verdadeiramente inclusivas¹⁰.

Sendo assim, a conformidade com o melhor interesse não se esgota em medidas de mitigação de riscos. É necessário também avaliar criticamente a proporcionalidade e a real necessidade da tecnologia adotada. No caso de sistemas biométricos aplicados em escolas ou ambientes recreativos, como os voltados à chamada automatizada, controle de presença ou segurança perimetral, é imprescindível questionar se os benefícios concretos compensam os riscos potencialmente irreversíveis à privacidade e ao bem-estar dos estudantes.

A esse respeito, destaca-se a contribuição de Eva Lievens, Law & Technology Associate Professor at Ghent University, para quem o princípio da precaução deve ser central na regulação de tecnologias aplicadas a crianças, pois “inverte a lógica e acrescenta importância à verificação de que a tecnologia traz, de fato, benefícios, ao invés de apenas provar que ela realmente causa ou pode causar danos no futuro”.¹¹

⁹ SBEB. Prêmio de Inovação em Engenharia Biomédica para o SUS transforma vidas e impulsiona a inovação na saúde pública. SBEB, 13 mar. 2025. Disponível em: <https://sbeb.org.br/premio-de-inovacao-em-engenharia-biomedica-para-o-sus-transforma-vidas-e-impulsiona-a-inovacao-na-saude-publica/>. Acesso em: 23 jul. 2025.

¹⁰ Ólafsdóttir, Berglind; Rathgeb, Christian; Kolberg, Jascha. A case study on the inclusiveness of biometric technologies for individuals with congenital disabilities. In: Proceedings of the 13th Nordic Conference on Human-Computer Interaction (NordiCHI '24), Uppsala, Sweden, 13–16 October 2024. New York: Association for Computing Machinery, 2024. p. 83. DOI: 10.1145/3679318.3685485.

¹¹ LIEVENS, Eva. Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children's rights. Nordic Journal of Human Rights, v.

Essa lógica foi recentemente adotada pela Relatora Especial da ONU para o Direito à Educação, em seu relatório “The Right to be Safe in Education”, que reconhece o uso de tecnologias biométricas e de reconhecimento facial como especialmente intrusivos, com impactos no bem-estar mental, na liberdade de expressão e na equidade escolar¹². O documento recomenda sua proibição em contextos educacionais, em linha com decisões adotadas por sistemas educacionais de países como Luxemburgo.

De igual maneira, no relatório “Artificial Intelligence in Education”¹³, a relatora reforça a preocupação com o uso crescente de tecnologias de reconhecimento facial baseadas em inteligência artificial nas escolas, destacando seu caráter intrusivo e os vieses recorrentes, especialmente contra estudantes negros e com deficiência. Ela destaca a ausência de escrutínio público, avaliações de impacto e marcos regulatórios adequados, como no caso do Paraná, no Brasil, onde o sistema foi implementado em mais de 1.500 escolas públicas sem estudos prévios de impacto em direitos humanos¹⁴. O relatório também aponta os riscos do uso de variações dessa tecnologia, como o e-proctoring em universidades da América Latina, implementado sem observância adequada das normas de proteção de dados. Diante desse cenário, a relatora volta a recomendar a proibição do uso de tecnologias de reconhecimento facial em instituições educacionais, em razão de seu potencial de vigilância massiva e ameaça à liberdade acadêmica.

Outro aspecto relevante é a proibição de condicionar o acesso ao direito fundamental à educação e outros direitos à cessão de dados biométricos. Condicionar a matrícula, o acesso à merenda ou à confirmação de presença ao fornecimento de dados biométricos não apenas viola a LGPD (arts. 14 e 18), como também pode representar tratamento discriminatório e desproporcional, incompatível com os parâmetros do ECA (art. 4º) e de tratados internacionais de direitos humanos, como a Convenção sobre os Direitos da Criança (arts. 3º e 19). Em verdade, essa é uma problemática ainda mais profunda que pode suscitar

39, n. 2, p. 128–145, 2021. Disponível em: <https://doi.org/10.1080/18918131.2021.1992951>. Acesso em: 23 jul. 2025. Disponível em: <https://biblio.ugent.be/publication/8732320>. Acesso em: 23 jul. 2025.

¹² SHAHEED, Farida. The right to be safe in education: report of the Special Rapporteur on the right to education. Genebra: Conselho de Direitos Humanos das Nações Unidas, 2025. Relatório (A/HRC/59/41). Disponível em:

<https://www.ohchr.org/en/documents/thematic-reports/ahrc5941-right-be-safe-education-report-special-rapporteur-right>. Acesso em: 23 jul. 2025.

¹³ SHAHEED, Farida. Artificial intelligence in education: Report of the Special Rapporteur on the right to education. United Nations General Assembly, Human Rights Council, 2024. (A/79/520). Disponível em:

<https://www.ohchr.org/en/documents/thematic-reports/ahrc79520-artificial-intelligence-education-report-special-rapporteur>. Acesso em: 31 jul. 2025.

¹⁴ INTERNET LAB. Surveillance technologies and education: mapping facial recognition policies in Brazil public schools – diagnosis and recommendation no. 8. 2023. Disponível em: <https://www.internetlab.org.br/en/research/surveillance-technologies-and-education-mapping-facial-recognition-policies-in-brazil-public-schools/>. Acesso em: 31 jul. 2025.

questionamentos à luz da justiça de dados¹⁵, que precisam ser debatidos no contexto nacional.

Portanto, antes de se discutir qual hipótese legal de tratamento seria aplicável (como o consentimento do responsável legal, cumprimento de obrigação legal ou regulatória, arts. 7º e 11 da LGPD), é imprescindível uma análise concreta, com base em evidências, da compatibilidade do tratamento com o melhor interesse da criança e adolescente. Essa análise deve incorporar os princípios da precaução, da minimização de dados e da não discriminação, e rejeitar o uso de tecnologias biométricas em contextos educativos quando os riscos superarem os benefícios comprovados.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Resumo executivo para a Plataforma Participa + Brasil

O tratamento de dados biométricos de crianças e adolescentes exige mais do que a indicação formal de base legal: deve estar ancorado no melhor interesse do titular, com avaliação prévia de impacto e salvaguardas robustas. A LGPD impõe um padrão mais elevado para dados sensíveis e titulares vulneráveis. Ainda que o consentimento parental (art. 14, §1º) seja juridicamente possível, ele não é suficiente sem transparência, linguagem acessível e real compreensão dos riscos. As hipóteses legais mais viáveis incluem: prevenção à fraude (art. 11, II, “g”) e proteção da vida (art. 11, II, “e”). Todas demandam demonstração de necessidade e proporcionalidade. É essencial garantir participação informada dos responsáveis (art. 14, §6º), escuta ativa da criança (Res. CONANDA nº 245/2024), e revisão contínua da tecnologia. O uso de biometria por conveniência ou utilitarismo é incompatível com a LGPD e a doutrina da proteção integral. O detalhamento completo da resposta está no documento encaminhado por e-mail.

Conforme apontado, a admissibilidade do tratamento de dados biométricos de crianças e adolescentes exige uma abordagem que vá além da mera identificação de hipóteses legais. Por se tratar de dados sensíveis e de titulares em situação de vulnerabilidade especial, é imperativo observar que a conformidade com o “melhor interesse” da criança e do adolescente (art. 14, LGPD) não é uma etapa secundária,

¹⁵ BIONI, Bruno; MESQUITA, Hana; MONAGREDA, Johanna K.; ZANATTA, Rafael. Construindo caminhos para a justiça de dados no Brasil: o papel das Defensorias Públicas na proteção de dados pessoais. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. 1. ed. ISBN 978-65-997956-0-2. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2022/06/ebook-defensorias-vf-.pdf>. Acesso em: 23 jul. 2025.

mas um fundamento antecedente e estruturante de qualquer operação de tratamento.

Desse modo, independentemente da base legal invocada, o tratamento de dados de crianças e adolescentes só será legítimo se **anteriormente compatibilizado com o melhor interesse do titular**, conforme a interpretação tripartite do Comentário Geral nº 14 da ONU (2013), já mencionada pela ANPD em documentos públicos e estudos técnicos. Trata-se de um requisito substancial, interpretativo e procedimental.

Após realizada e documentada a avaliação de impacto, então será possível avaliar a aplicabilidade das hipóteses legais do art. 11 da LGPD (dados sensíveis), sempre com a ressalva de que o tratamento de dados biométricos de crianças e adolescentes exige um padrão mais elevado de justificação, proporcionalidade e salvaguardas.

As hipóteses mais discutidas nesse contexto incluem:

(i) Consentimento específico e destacado do responsável legal (art. 11, I e art. 14, §1º, LGPD)

Embora juridicamente possível, essa hipótese exige cautela e atenção crítica. O consentimento parental não deve ser presumido como livre, informado e consciente, sobretudo em ambientes institucionais marcados por assimetrias de informação e ausência de cultura de proteção de dados no Brasil. Existe o risco de que o consentimento parental se torne meramente formal, sem que os responsáveis compreendam os riscos implicados no uso de tecnologias biométricas.

Portanto, mesmo quando o consentimento for utilizado, ele não exime o controlador da obrigação de demonstrar o alinhamento da operação ao melhor interesse da criança e da necessidade do tratamento, com a comprovação dos benefícios envolvidos. Nesse sentido, vale reiterar o artigo 14 da Resolução 245 do Conanda:

- Art. 14º: Sempre que o tratamento de dados pessoais de crianças e adolescentes for realizado com base no consentimento, deverá ser obtido de forma livre e prévia junto aos responsáveis, solicitado de forma específica e destacada, para finalidades específicas e, sempre que possível, junto à criança ou adolescente, observado seu grau de maturidade e compreensão sobre os efeitos do consentimento.

Como garantir a participação informada dos pais ou responsáveis?

A participação dos pais ou responsáveis deve atender aos **critérios formais e materiais de informação clara, acessível e adequada**, conforme os arts. 6º, VI, 9º e 14 §6º da LGPD. Isso implica que:

- **As informações sobre a natureza da tecnologia, os riscos envolvidos, as finalidades específicas e as consequências da não adesão sejam comunicadas de modo acessível e multiformato**, especialmente quando envolverem decisões automatizadas, biometria ou outras técnicas sensíveis. Isso inclui o uso de linguagem simples, recursos audiovisuais, traduções em Libras e formatos acessíveis a pessoas com deficiência;
- **O consentimento dos pais ou responsáveis seja livre, informado e inequívoco**, não podendo estar vinculado ao acesso a serviços essenciais como matrícula escolar, merenda, transporte ou segurança mínima — sob pena de descaracterizar o consentimento como base legítima (conforme art. 8º, §5º da LGPD e art. 14, §1º);
- **O direito de revogação do consentimento seja assegurado a qualquer tempo, de forma desburocratizada**, com garantia de que essa decisão não resultará em discriminação ou prejuízo ao desenvolvimento da criança ou adolescente;
- **Sejam criados mecanismos de escuta ativa das crianças e adolescentes, adequados ao seu grau de maturidade e compreensão**, em conformidade com o art. 16, parágrafo único, da Resolução CONANDA nº 245/2024, o que inclui metodologias participativas e respeitadas que considerem a opinião dos próprios titulares como parte do processo decisório sobre o uso de seus dados.

Essa hipótese poderia ser aplicada, por exemplo, no uso de tecnologias biométricas voltadas à acessibilidade de crianças e adolescentes com deficiência, como sistemas de reconhecimento facial para facilitar a comunicação de pessoas com deficiência intelectual ou motora severa.

Nesses casos, o consentimento específico e destacado dos responsáveis legais deve ser obtido mediante diálogo transparente, linguagem acessível e demonstração clara dos benefícios concretos à criança, sempre acompanhado de documentação que comprove a necessidade da tecnologia empregada e sua aderência ao melhor interesse do titular. Ainda assim, o uso da biometria deve ser precedido de avaliação de impacto, conter salvaguardas técnicas e organizacionais proporcionais, e ser revisto periodicamente quanto à sua eficácia e proporcionalidade.

(ii) Prevenção à fraude e segurança nos processos de identificação (art. 11, II, “g”)

Essa hipótese é frequentemente invocada para justificar o uso de biometria em sistemas de autenticação digital. Contudo, a LGPD estabelece um limite expresso: essa base legal é válida apenas “exceto no caso de prevalecerem direitos e liberdades fundamentais do titular”.

No caso de crianças e adolescentes, essa ressalva deve ser interpretada de maneira restritiva, especialmente porque o art. 14, §3º, determina que o tratamento de dados deve ser realizado com medidas específicas de proteção e não pode condicionar o acesso a serviços essenciais.

A aplicação dessa hipótese só seria admissível se demonstrado que a biometria é a única forma segura e proporcional de garantir a proteção e segurança do titular, e que os direitos fundamentais da criança estão devidamente salvaguardados.

(iii) Proteção da vida ou da incolumidade física do titular ou de terceiro (art. 11, II, “e”)

Embora raramente aplicável de forma genérica, essa hipótese poderia ser considerada em situações excepcionais, como contextos de emergência ou ameaças concretas à segurança física do titular. Ainda assim, sua aplicação deve observar estritamente o princípio da necessidade e da limitação temporal do tratamento, sob pena de violação dos direitos do titular.

Em resumo, a legalidade do tratamento de dados biométricos de crianças e adolescentes está condicionada não apenas à identificação formal de uma base legal válida, mas à demonstração concreta da compatibilidade da operação com o melhor interesse da criança, a realização de avaliações de impacto de riscos (RIPD’S) e específicas (CRIAs), e à adoção de medidas técnicas e organizacionais robustas. O uso de tecnologias biométricas com base em racionalidades utilitaristas ou conveniência administrativa, sem lastro em evidências e proporcionalidade, não atende aos padrões exigidos pela LGPD, pelo ECA e pelas normas internacionais de proteção à infância.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Resumo executivo para a Plataforma Participa + Brasil

A verificação ou estimação de idade por biometria só deve ser adotada como último recurso, após avaliação de impacto nos direitos da criança (CRIA) e demonstração de necessidade e proporcionalidade (art. 14, § 4 LGPD). Métodos como análise facial, digitação ou fala implicam riscos elevados à privacidade, acurácia e dignidade, especialmente para crianças negras, neuroatípicas ou com deficiências. É essencial distinguir verificação (alto grau de certeza) de estimativa etária (probabilística), priorizando soluções menos invasivas. Salvaguardas incluem: uso limitado e não retentivo de dados; transparência técnica; auditorias independentes; e participação infantojuvenil no design (Res. CONANDA nº 245/2024). Iniciativas como a EU Age Verification Solution demonstram a viabilidade de sistemas interoperáveis sem biometria. Exigir dados biométricos como condição de acesso viola frontalmente a LGPD. O detalhamento completo da resposta está no documento encaminhado por e-mail.

A implementação de mecanismos de verificação ou estimativa de idade por meio de dados biométricos deve ser utilizado como último recurso, especialmente em plataformas digitais e ambientes de jogos, pois exige rigorosa compatibilidade com os princípios da necessidade, da minimização e, sobretudo, com o melhor interesse da criança e do adolescente (art. 14, LGPD).

Antes da adoção de qualquer solução tecnológica que envolva a coleta ou análise de dados biométricos, é essencial distinguir os conceitos centrais relacionados à garantia etária (age assurance), conforme sistematizado pela 5Rights Foundation em seu relatório “But how do they know it’s a child?”¹⁶: (i) Garantia etária (Age Assurance): termo abrangente para diferentes soluções de verificação e estimativa de idade, com graus variados de certeza; (ii) Verificação etária (Age Verification): sistemas baseados em identificadores rígidos e verificáveis, que asseguram com alto grau de certeza a idade do usuário (ex: documentos oficiais, autenticação com base legal); (iii) Estimativa etária (Age Estimation): métodos que inferem idade com base em dados comportamentais, padrões de uso, análise de voz, rosto, digitação, entre outros. Não asseguram identidade ou idade precisa, mas oferecem uma aproximação probabilística.

Segundo esse mesmo relatório, muitas soluções de estimativa de idade, especialmente aquelas que utilizam características biométricas inferidas – como análise facial, dinâmica de digitação, padrões de fala, forma de caminhar ou interações com dispositivos móveis – implicam riscos elevados à privacidade e à dignidade de crianças e adolescentes. Esses métodos, além de opacos, possuem alta margem de erro, especialmente:

¹⁶5Rights Foundation. But How Do They Know It Is a Child? Age Assurance in the Digital World (Updated). 2021. Disponível em: <https://5rightsfoundation.com/resource/but-how-do-they-know-its-a-child/>. Acesso em: 31 jul. 2025

- Para crianças e adolescentes em faixas etárias próximas (ex. 12/13 ou 17/18 anos);
- Para crianças negras, dada a recorrente falta de representatividade dos bancos de dados usados para treinar os sistemas;
- Para crianças com deficiências craniofaciais ou expressões não padrão, sujeitas a erros de classificação ou exclusão;
- Quando há risco de perfis biométricos serem usados para finalidades secundárias, como monitoramento emocional, vigilância de comportamento ou construção de perfis.

Dessa forma, qualquer implementação dessas tecnologias deve ser submetida previamente a avaliações específicas de impacto nos direitos da criança (CRIAs) e limitada a situações em que não existam alternativas menos invasivas, como exige a Resolução CONANDA nº 245/2024, que veda o uso indiscriminado de ferramentas de vigilância e exige priorização de métodos menos invasivos.

É importante dizer que existem iniciativas em curso que demonstram ser possível desenvolver mecanismos de verificação etária que não demandam coleta de dados biométricos. Destaca-se, nesse sentido, o projeto “EU Age Verification Solution”¹⁷, que busca desenvolver uma solução interoperável para verificação de idade em toda a União Europeia, alinhada à Lei de Serviços Digitais da UE (DSA) e à futura Carteira de Identidade Digital Europeia (EUDI Wallet). A proposta visa garantir o acesso a serviços online com restrição etária sem necessidade de exposição excessiva de dados pessoais. A publicação mais recente da Biometric Update (julho/2025)¹⁸ destaca que os guias técnicos e o software piloto da iniciativa europeia já foram divulgados, com foco em transparência, interoperabilidade, auditoria externa e minimização da coleta de dados

Essas abordagens apontam caminhos concretos para superar o tecnossolucionismo e estimular o desenvolvimento de soluções éticas, voltadas à verificação de idade sem recorrer à biometria como primeiro recurso.

Para que soluções de verificação ou estimação de idade estejam em conformidade com os princípios da LGPD — especialmente no que se refere à proteção de

¹⁷ EUROPEAN COMMISSION. European Age Verification Solution. Bruxelas, 2025. Disponível em: <https://ageverification.dev>. Acesso em: 23 jul. 2025.

¹⁸ McCONVEY, Joel R. EU moves forward on age verification with release of guidelines, software. Biometric Update, 14 jul. 2025. Disponível em: <https://www.biometricupdate.com/202507/eu-moves-forward-on-age-verification-with-release-of-guidelines-software>. Acesso em: 23 jul. 2025.

crianças e adolescentes —, é necessário observar, cumulativamente, os seguintes critérios:

(i) Avaliação prévia de impacto – CRIA

Assim como toda pretensão de coleta de dados biométricos de crianças e adolescentes, deve-se realizar uma avaliação de impacto nos direitos da criança (Child Rights Impact Assessment – CRIA), como etapa antecedente e obrigatória. Essa avaliação deve examinar os riscos envolvidos, a existência de alternativas menos invasivas, a finalidade específica da solução proposta e sua proporcionalidade. É essencial que sejam considerados os impactos de curto, médio e longo prazo sobre o desenvolvimento e os direitos fundamentais da criança, à luz do princípio da precaução¹⁹. Existindo técnicas menos invasivas que possam cumprir a mesma finalidade, as mesmas devem ser adotadas no lugar da biometria.

(ii) Princípio da necessidade qualificado – § 4º do art. 14 da LGPD

O art. 14, § 4º da LGPD estabelece que não se pode condicionar o acesso de crianças a jogos, aplicativos ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Assim, qualquer mecanismo de verificação de idade deve ser desenhado de acordo com o princípio da minimização, restringindo-se ao mínimo indispensável. O uso de dados biométricos, por seu grau de sensibilidade, só pode ser considerado em situações absolutamente excepcionais, mediante justificativa robusta e demonstrada inviabilidade de métodos menos invasivos.

Caso isso não seja cumprido e esteja sendo condicionado o acesso a tais serviços à cessão de dados biométricos, estaremos diante de uma violação expressa à LGPD.

(iii) Salvaguardas técnicas e organizacionais específicas

Nos raros casos em que o uso de biometria seja considerado necessário, deverão ser implementadas medidas de segurança reforçadas, tais como:

- Uso de tecnologias do tipo “zero knowledge proof”, que permitam a verificação da idade sem acesso direto ao dado biométrico bruto;
- Arquiteturas que assegurem o apagamento automático dos dados biométricos após a verificação pontual, evitando retenções indevidas ou criação de bases centralizadas;
- Auditorias independentes e periódicas, com foco em acurácia, viés algorítmico e proporcionalidade do sistema;

¹⁹ LIEVENS, Eva. Growing up with digital technologies: how the precautionary principle might contribute to addressing potential serious harm to children’s rights. *Nordic Journal of Human Rights*, v. 39, n. 2, p. 128–145, 2021. Disponível em: <https://doi.org/10.1080/18918131.2021.1992951>. Acesso em: 23 jul. 2025.



- Transparência e explicabilidade técnica, por meio da publicação de relatórios acessíveis a pais, responsáveis e autoridades de supervisão;
- Inclusão significativa de crianças e adolescentes no processo de design e validação das soluções, respeitando seu grau de maturidade, nos termos do art. 16 da Resolução CONANDA nº 245/2024 e no Comentário Geral nº25.

Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem mais cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo “dados biométricos”, mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos - que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

R: Embora a Lei Geral de Proteção de Dados Pessoais não traga um conceito específico para dados biométricos, a referida norma os classifica como dados pessoais sensíveis (artigo 5º, II, LGPD).

No âmbito internacional, o Regulamento Geral sobre a Proteção de Dados da Europa (“GDPR”), apresenta o conceito de dados biométricos como os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural que permitam ou confirmem a identificação única dessa pessoa natural, nomeadamente imagens faciais ou dados datiloscópicos (artigo 4º, n.º 14, GDPR).

Por sua vez, a própria ANPD, em seu Guia de Biometria e Reconhecimento Facial, conceitua a biometria como a análise técnica, realizada por meios matemáticos e estatísticos, das características fisiológicas (tais como impressão digital, face, íris, geometria da mão, vascularização da mão, DNA e voz) ou comportamentais (voz, expressão facial, assinatura, modo de andar etc.) de um indivíduo. Quanto maior a quantidade de dados presentes na amostra biométrica provenientes de uma ou mais características, maior será a probabilidade de que ela tenha uma correspondência única, ou seja, a amostra apresentará maior qualidade para que a análise seja mais precisa e confiável.

Nesse sentido, pertinente esclarecer que a simples coleta de dados que podem revelar informações biométricas não pode ser considerada automaticamente uma atividade de tratamento de dados pessoais sensíveis. É necessária uma justificativa específica – de forma que somente dados utilizados para identificar ou autenticar titulares podem ser considerados biométricos. Além disso, se a informação não for operada por meio técnico que permita a identificação, não será considerada dado biométrico. Esse entendimento alinha-se ao sustentado pela autoridade de proteção de dados do Reino Unido (“ICO”), a qual afirma que os dados biométricos somente serão considerados dados sensíveis quando forem utilizados com a finalidade de identificar uma pessoa de forma única, de modo que a sua categorização dependerá da finalidade do tratamento.

No sentido acima exposto, conclui-se, portanto, que o mero tratamento de fotografias sem a utilização de técnicas específicas que permitam a identificação inequívoca ou a autenticação de uma pessoa natural não deve ser considerado sistematicamente como tratamento de dados pessoais sensíveis, no contexto do art. artigo 5º, II, da LGPD.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

R: As boas práticas de transparência devem balizar todo e qualquer tratamento de dados, independentemente do dado ser caracterizado como dado pessoal sensível, como é o caso do dado biométrico.

Dessa forma, medidas que garantam aos titulares, o acesso a informações claras e precisas acerca da realização do tratamento de dados, informando a finalidade dos respectivos tratamentos, mediante indicação de propósitos legítimos, específicos e explícitos, bem como a limitação do tratamento de dados de forma incompatível com as finalidades determinadas são referência de boas práticas no que tange à transparência, sendo que essas medidas fazem parte das disposições da LGPD e já são empregadas pelas empresas que realizam tratamento de dados pessoais.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

R: A biometria comportamental deve ser tratada à luz dos mesmos princípios e requisitos legais previstos na LGPD e aplicáveis ao tratamento de dados pessoais sensíveis, tal como já ocorre com a biometria tradicional. Isso inclui a observância dos princípios da finalidade, necessidade, qualidade de dados e segurança, bem como a exigência de base legal específica, nos termos do artigo 11 da LGPD.

Segundo a autoridade britânica de proteção de dados (“ICO”), a biometria comportamental refere-se a características biométricas relacionadas a aspectos como movimentos, gestos ou habilidades motoras, e pode incluir a caligrafia de uma pessoa, a forma como ela digita, seu modo de andar ou correr e os movimentos dos olhos. Por conta dessas características, sua adoção pode se mostrar mais adequada em determinados contextos, como nos casos de prevenção à fraude e autenticação contínua. Como já indicou o Grupo de Trabalho do Artigo 29 (“WP”), depoimentos publicados por fabricantes relatam que, ao implementar essa tecnologia, empresas do setor financeiro aumentaram as taxas de detecção de fraudes e passaram a oferecer um serviço mais ágil para a resolução de reivindicações legítimas.

O WP também comparou o uso da assinatura gráfica e da assinatura dinâmica para fins de prevenção a fraudes (anti-spoofing), sugerindo que a assinatura dinâmica poderia oferecer maior segurança, pois o processo de verificação também analisaria características dinâmicas, que são complexas e únicas ao estilo de escrita manual de cada indivíduo. A autoridade de proteção de dados de Singapura (“PDPC”) igualmente indicou utilizações desse tipo de biometria no contexto de aplicações voltadas à segurança.

Quanto à existência de “obrigações específicas”, é certo que a LGPD não estabeleceu requisitos ou obrigações específicas aplicáveis ao tratamento de dados biométricos comportamentais. Deve-se considerar, com isso, os contornos específicos – e não necessariamente obrigações adicionais – quanto à aplicação do princípio da qualidade dos dados (artigo 6º, V, LGPD) e da segurança (artigo 6º, VII, LGPD) no contexto da biometria comportamental, na medida em que esse tipo de dado envolve padrões dinâmicos e variáveis que podem se alterar com o decorrer do tempo (como voz, digitação e movimento ocular).

O WP sugere que, para assegurar a exatidão e a atualização dos dados pessoais, deve-se implementar mecanismos de revisão dos modelos de reconhecimento comportamental, evitando falhas como falsos positivos/negativos decorrentes da variabilidade natural do comportamento humano.

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

R: O tratamento de dados pessoais biométricos, à luz da LGPD, fundamenta -se nas bases legais previstas pela LGPD para dados pessoais sensíveis, no âmbito do art. 11 da LGPD.

Contudo, deve-se considerar que o consentimento nem sempre será a hipótese autorizativa mais adequada nesse cenário, razão pela qual o art. 11, em seu inciso II, traz outras hipóteses nas quais o tratamento do dado biométrico dispensa o consentimento.

Nesse sentido, destaca-se a alínea “g”, a qual prevê expressamente a dispensa do consentimento para garantia da prevenção à fraude em processos de identificação e autenticação de cadastro. Nota-se, portanto, que o referido tratamento tem por finalidade proteger a segurança do próprio titular do dado contra usos indevidos de sua identidade. Nesse mesmo contexto, a exigência do consentimento poderia inviabilizar mecanismos de segurança automatizados, como as autenticações por reconhecimento facial ou impressão digital, em claro prejuízo à segurança dos próprios titulares dos dados.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

R: A adequada aplicação da hipótese legal da garantia da prevenção à fraude pressupõe o atingimento de requisitos de segurança e da aplicação de princípios balizadores do tratamento de dados pessoais de forma geral, não apenas ao tratamento de dados sensíveis.

Na ótica de segurança, vislumbra-se a implementação de técnicas de proteção, tais como, medidas de rastreamento e monitoramento, controle de acesso, registro das operações de tratamento, medidas essas que as empresas já empregam no tratamento de dados pessoais e que mantêm uma melhoria contínua visando sempre ao emprego das melhores técnicas de segurança.

No que tange o princípio da necessidade, observam-se medidas que visem a utilização dos dados biométricos apenas de forma necessária para o atingimento da finalidade de proteção à fraude, atentando-se para a disponibilização de informação aos titulares acerca da finalidade do tratamento, de forma clara, precisa, e facilmente acessível, sendo que essas medidas fazem parte das disposições da LGPD e já são empregadas pelas empresas que realizam tratamento de dados pessoais.

Dessa forma, a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” prevista no artigo 11, II, “g” da LGPD, pressupõe a observância dos princípios da necessidade e finalidade e implementando boas práticas de governança e segurança da informação, com o objetivo de prover medidas de controle e rastreabilidade, bem como de proteção dos dados biométricos.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

R: No mesmo sentido do item anterior, entende-se que a adequada aplicação da hipótese legal do cumprimento de obrigação legal ou regulatória pressupõe o atingimento de requisitos de segurança e da aplicação de princípios balizadores do tratamento de dados pessoais de forma geral, não apenas ao tratamento de dados sensíveis.

Na ótica de segurança, vislumbra-se a implementação de técnicas de proteção, tais como, medidas de rastreamento e monitoramento, controle de acesso, registro das operações de tratamento, medidas essas que as empresas já empregam no tratamento de dados pessoais e que mantêm uma melhoria contínua visando sempre ao emprego das melhores técnicas de segurança.

No que tange o princípio da necessidade, observam-se medidas que visem à utilização dos dados biométricos apenas de forma necessária para o atingimento da finalidade, atentando-se para a disponibilização de informação aos titulares acerca da finalidade do tratamento, de forma clara, precisa e facilmente acessível, sendo que essas medidas fazem parte das disposições da LGPD e já são empregadas pelas empresas que realizam tratamento de dados pessoais.

Dessa forma, a adequada aplicação da hipótese legal de “cumprimento de obrigação legal ou regulatória” prevista no artigo 11, II, “a” da LGPD, pressupõe a observância dos princípios da necessidade e finalidade e implementando boas práticas de governança e segurança da informação, com o objetivo de prover medidas de controle e rastreabilidade, bem como de proteção dos dados biométricos.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

R: Nesse sentido, importante esclarecer que o dado anonimizado se caracteriza pelo dado que não é capaz de permitir a reidentificação posterior, ainda que aplicadas técnicas de cruzamento de bases de dados. Corrobora esse entendimento o conceito de dado anonimizado previsto no art. 5º, III da LGPD.

Diante desse cenário, em caso de uso de dados anonimizados, medidas técnicas de anonimização, bem como a aplicação de testes de robustez para validar se o dado está efetivamente anonimizado, conforme recomenda a ANPD em Guia de Boas Práticas de Anonimização e Pseudoanonimização, podem ser consideradas como salvaguardas para garantir a eficácia do processo de anonimização do dado.

Uma vez garantido o processo de anonimização, referido dado não é considerado como dado pessoal, em conformidade com o art. 12º da LGPD, tendo em vista que não é possível identificar o titular. Consequentemente, portanto, o dado deixa de figurar como dado sensível.

**BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE
TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS
BIOMÉTRICOS**

A utilização das tecnologias de reconhecimento facial (Facial Recognition Technologies, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento. Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

R: No que tange ao atingimento do princípio da necessidade e da proporcionalidade, tem-se como alternativa a análise da indispensabilidade do reconhecimento facial. Ou seja, avaliação se o reconhecimento facial é a forma mais adequada e, caso seja, medidas minimizem o uso irrestrito do reconhecimento.

Nessa ótica, ressalta-se que, para a finalidade de prevenção à fraude, o reconhecimento facial destaca-se como uma tecnologia de suma importância no contexto de proteção do titular. Ao usar dados biométricos únicos, a tecnologia mitiga consideravelmente a ocorrência de acessos indevidos, falsificações e usos fraudulentos de informações pessoais. O reconhecimento facial, portanto, é um recurso que fortalece mecanismos de autenticação, contribuindo significativamente para a proteção dos dados e integridade das operações.

Na ótica do princípio da transparência, é necessário garantir que o titular tenha ciência do tratamento de reconhecimento facial, disponibilizando informações acerca da finalidade deste reconhecimento.

No aspecto técnico, medidas de mitigação de vieses e testes de acurácia utilizando uma base ampla e diversificada contribuem para evitar situações de discriminação ilícita ou abusiva. Na visão jurídica, entende-se como mitigadores a correta identificação da base legal amparada pelo atingimento dos princípios acima observados. No que tange à visão institucional, as medidas de monitoramento, controle de acesso e rastreamento do tratamento dos dados, conforme já explicitado, visam contribuir com os riscos mapeados neste item.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

R: Os sistemas de reconhecimento facial devem ser projetados com base nos princípios de *privacy by design* e *privacy by default*, incorporando, desde a fase de concepção, medidas técnicas e organizacionais voltadas à precisão, segurança e mitigação de riscos.

A utilização de algoritmos robustos e continuamente testados em bases de dados diversificadas é essencial para reduzir a incidência de erros de identificação, como falsos positivos e falsos negativos, especialmente considerando a variabilidade de características demográficas.

Adicionalmente, destaca-se a implementação de mecanismos de monitoramento contínuo do desempenho do sistema e rotinas de atualização e revalidação dos modelos utilizados.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em

substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

R: Não se recomenda o uso de tecnologia de reconhecimento facial quando o tratamento de dados biométricos implicar riscos elevados à privacidade dos titulares sem justificativa proporcional ou base legal adequada.

Situações em que houver baixa previsibilidade aos indivíduos identificados e alto potencial de vigilância em massa, configurando riscos à liberdade individual, à autodeterminação informativa e à não discriminação ilícita ou abusiva.

Nesses casos, recomenda-se a adoção de medidas alternativas menos invasivas, tais como, autenticações multifator.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

O tratamento de dados biométricos exige uma abordagem cautelosa e estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos.

Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes.

Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados.

Com base nisso, questiona-se:

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

R: É de suma importância que os controladores do tratamento dos dados biométricos adotem medidas técnicas e administrativas robustas, entre as quais destacam-se:

- Programa de Segurança da Informação: implementação de medidas de segurança contra qualquer ameaça ao Tratamento dos Dados Pessoais;
- Gestão de Acesso: estabelecimento de padrões de controle sobre o Tratamento dos Dados Pessoais com responsabilidades definidas e gestão de acesso tanto de colaboradores quanto de prestadores de serviços, bem como o estabelecimento de mecanismos de autenticação de acesso aos Dados Pessoais;
- Relatório de Tratamento dos Dados Pessoais: manter o registro detalhado de todo o tratamento realizado, como informações quanto ao momento, a duração, a identidade do representante responsável pelo tratamento designado pelas partes e os dados pessoais tratados, inclusive quando tal tratamento é feito para cumprimento de obrigações legais ou determinações por parte de autoridades; e,
- Inviolabilidade dos Dados Pessoais: uso de soluções de gestão dos registros do Tratamento por meio de técnicas que garantam a inviolabilidade dos dados pessoais, como encriptação ou medidas de proteção equivalentes.
- Elaboração de Relatório de impacto DPIA/LIA, quando aplicável.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode

justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

R: Para evitar que a exigência de autenticação biométrica em serviços não essenciais configure discriminação ilícita ou prática abusiva, é fundamental que o tratamento desses dados observe os princípios da LGPD bem como esteja devidamente enquadramento em uma das bases legais autorizativas para o tratamento de dados pessoais, em especial, da necessidade, não discriminação e transparência, como todo e qualquer tratamento de dados pessoais deve observar.

Na situação em que o tratamento do dado biométrico é amparado no consentimento, o titular deve ter garantido o direito ao *opt-out*, de forma simples, acessível e sem que isso implique em restrições desproporcionais do serviço. A limitação de funcionalidades pode ser considerada legítima, entretanto, quando houver justificativa técnica concreta para sua implementação. Nessa ocasião, tal limitação deve ser previamente comunicada de forma clara e transparente.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

R: A proteção eficaz no tratamento de dados biométricos exige adoção de boas práticas voltadas à transparência, necessidade e mitigação de riscos discriminatórios. Entre essas práticas, destacam-se:

- Treinamento e Capacitação: oferecer treinamento específico quanto ao tema;
- Políticas e Procedimentos: reforçar as informações de forma detalhada sobre como deve ser realizado o tratamento de dados pessoais para essa categoria de dados;
- Relatório de Impacto à Proteção de Dados Pessoais (DPIA), quando aplicável.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

R: A proteção eficaz no tratamento de dados biométricos, especialmente no contexto do tratamento contínuo e massivo de dados biométricos, exige adoção de boas práticas voltadas à transparência, necessidade e mitigação de riscos discriminatórios. Entre essas práticas, destaca-se a implementação de comunicação de forma clara e acessível, por meio de materiais informativos e sinalizações que garantam ciência aos

titulares sobre o tratamento contínuo e massivo de dados biométricos, disponibilizando os meios aos quais o titular possa exercer seus direitos.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

R: Cumpre destacar que o direito à informação clara, o direito de acesso e à correção dos dados são direitos dos titulares que pressupõem todo e qualquer tratamento de dados pessoais, independentemente de o referido tratamento de dados pessoais estar ou não inserido no contexto de uma decisão tomada exclusivamente em tratamento automatizado de dados pessoais.

Nesse sentido, medidas de transparência, tais quais previsões claras e precisas em políticas de privacidade e divulgação de canais de atendimento são imprescindíveis para que o titular possa exercer seus direitos.

No que diz respeito à possibilidade de revogação, nos casos em que a base legal para o tratamento dos dados for o consentimento, o titular deve dispor de um canal de fácil acesso, viabilizando a revogação de forma simples, acessível e facilitada.

Por sua vez, conforme disposto na LGPD, o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

Dessa forma, enquanto requisito para a garantia e a aplicação do referido direito, é certo que a leitura do dispositivo deve considerar que a revisão ocorra apenas nos casos em que a decisão foi tomada unicamente de forma automatizada, bem como que os interesses dos titulares tenham sido afetados de forma ilícita ou abusiva e contrária à legislação.

Nesse sentido, importante destacar que a leitura e interpretação de referente direito do titular deve observar os requisitos dispostos no artigo 20 da LGPD, quais sejam: (i) decisão tomada unicamente com base em tratamento automatizado de dados pessoais; e (ii) decisão que afete os interesses do titular. Com efeito, esses requisitos devem ser observados em qualquer decisão automatizada, seja ela referente ao tratamento de dados biométricos ou qualquer outro tipo de dado.

Cumprido destacar ainda, que, no que tange ao conceito de decisão tomada unicamente com base em tratamento automatizado de dados pessoais, considera-se um processo de tomada de decisão que é totalmente automatizado e exclui qualquer influência humana no resultado. Um processo ainda pode ser considerado totalmente automatizado se um humano insere os dados a serem tratados e, então, a tomada de decisão é realizada por um sistema automatizado.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

R: As hipóteses legais de tratamento de dados biométricos decorrem do art. 11 da LGPD, mesmo quando os dados são de titularidade de crianças e adolescentes.

Isso porque, não obstante o art. 14 da LGPD, a ANPD, em seu Enunciado nº1/2023, dispõe:

“O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei”.

Quando a hipótese legal é o consentimento, este deve ser inequívoco e contemplar as finalidades para a qual o representante do titular concorda com o tratamento. O tratamento dos dados biométricos de crianças e adolescentes também pode ser amparado em outras bases legais que não o consentimento. Nesse cenário, é imprescindível que haja a devida transparência do tratamento e suas finalidades para os representantes do menor.

Por fim, o melhor interesse é o princípio orientador do tratamento de dados de menores, em conformidade com o art. 14 da LGPD. Portanto, para que seja factível o tratamento de dados biométricos de crianças e adolescentes, faz-se necessário avaliar se a atividade está atendendo ao melhor interesse daquele menor. Assim, por exemplo, faz-se necessária a observância da finalidade legítima do tratamento do dado biométrico com a proteção da criança e do adolescente, com isso atende-se ao princípio da proteção integral do menor.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

R: A hipótese de Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (Art. 11, II, “g”, LGPD). Quando a hipótese legal é o consentimento, este deve ser inequívoco e contemplar as finalidades para a qual o representante do titular concorda com o tratamento. O tratamento dos dados biométricos de crianças e adolescentes também pode ser amparado em outras bases legais que não o consentimento, especialmente considerando as disposições do Enunciado nº 1/2023 da ANPD. Nesse cenário, é imprescindível que haja a devida transparência do tratamento e suas finalidades para os representantes do menor.

Sobre as medidas técnicas e organizacionais, destacam-se as medidas de segurança relevantes para todo e qualquer tratamento de dados, independentemente do titular figurar como criança ou adolescentes, quais sejam: implementação de programas de Segurança da Informação, medidas de controle e gestão de acesso e, quando aplicável, elaboração de Relatório de Tratamento dos Dados Pessoais (DPIA).

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

R: Para compatibilizar a prática de verificação de idade com o princípio da necessidade, é essencial que a coleta de dados biométricos seja limitada ao mínimo necessário para atingir a finalidade pretendida, evitando excessos ou tratamentos desproporcionais. A biometria, por ser um dado sensível, deve ser utilizada apenas quando não houver outra forma menos invasiva de verificar a idade do usuário. Além disso, é fundamental garantir a transparência do processo, com informações claras e acessíveis aos pais ou responsáveis, incluindo a finalidade da coleta, os direitos dos titulares e os mecanismos disponíveis para exercer esses direitos.

O tratamento de dados biométricos para casos de verificação ou estimação de idade de crianças e adolescentes deve priorizar a proteção do menor, evitar riscos à sua dignidade, liberdade e segurança, de forma a se garantir o melhor interesse do menor.

OF-DG-025/2025

São Paulo, 29 de julho de 2025.

À

Autoridade Nacional de Proteção de Dados – ANPD

Coordenação-Geral de Normatização – Coordenação de Normatização 1

E-mail: normatizacao@anpd.gov.br**Ref.: Nota Técnica nº 17/2025/CON1/CGN/ANPD: Tomada de Subsídios: Dados Pessoais Sensíveis - Dados Biométricos**

A ANCORD – Associação Nacional das Corretoras e Distribuidoras de Títulos, Valores Mobiliários, Câmbio e Mercadorias, inscrita sob o CNPJ/MF sob o n. 43.452.531/0001-28 (“ANCORD”), associação que representa as corretoras e distribuidoras de valores mobiliários e corretoras de câmbio, vem, por meio desta, em atendimento à Consulta Pública para Tomada de Subsídios sobre o Tratamento de Dados Pessoais Biométricos, promovida pela Autoridade Nacional de Proteção de Dados (“ANPD”), apresentar suas contribuições.

Informamos que a ANCORD também submeteu manifestação por meio da plataforma Participa Mais Brasil. Este documento tem por objetivo complementar aquela manifestação, reunindo, de forma mais detalhada, as análises e sugestões das Associadas da ANCORD, com vistas a contribuir para o aprimoramento da regulamentação sobre o tema, conforme abaixo:

BLOCO I - DEFINIÇÕES E PRINCÍPIOS**1) Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?**

Para a caracterização de um dado como biométrico nos termos da LGPD, o critério objetivo fundamental é que ele se refira a uma característica física, fisiológica ou comportamental de uma pessoa natural identificada ou identificável, conforme disposto no art. 5º, inciso II da LGPD, de forma que seja possível tecnicamente identificar o titular associado a tais características a partir do tratamento realizado com a informação biométrica.

Adicionalmente, podem ser considerados critérios técnicos como: (i) unicidade, isto é, a capacidade de distinguir um indivíduo de todos os outros; (ii)

permanência, ou seja, estabilidade da característica ao longo do tempo; e (iii) universalidade, no sentido de que a característica esteja presente em todos os indivíduos, possibilitando sua aplicação generalizada em sistemas de identificação e autenticação.

Nesse sentido, recomenda-se que a regulamentação traga uma definição técnica clara de biometria que permita a identificação objetiva dos cenários em que há este tipo de tratamento, e evite confusões com possível tratamento de dados que, embora envolvam características físicas, fisiológicas ou comportamentais (a exemplo de imagens, capturas de vídeo, voz, etc.), não poderiam caracterizar a biometria devido à ausência de procedimentos técnicos que permitam associar essas características ao titular.

2) Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

As práticas de transparência ativa destacadas pelas Associadas são: (i) Apresentação clara da finalidade específica do tratamento, especialmente em hipóteses que não se baseiam no consentimento, como o uso da biometria para autenticação em sistemas eletrônicos; (ii) Indicação dos dados biométricos que serão coletados e sua respectiva finalidade;

Além da definição em Políticas quanto a Informação sobre o período de retenção dos dados, bem como sobre eventuais compartilhamentos com terceiros; Identificação do controlador e disponibilização de canal de contato com o encarregado pelo tratamento de dados pessoais; Publicação de Política de Privacidade atualizada, contendo as informações acima de forma compreensível ao titular; Esclarecimento quanto às consequências da recusa do titular em fornecer o dado biométrico; Garantia de que todas essas informações estejam acessíveis antes da coleta, de forma destacada, transparente e gratuita.

Além disso, quando o tratamento se basear em consentimento, este deve ser obtido de forma livre, informada, inequívoca e destacada, reforçando o compromisso com a autodeterminação informativa do titular.

3) De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular)

deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

As Associadas destacaram que é importante que tanto a biometria comportamental, quanto a tradicional, estejam submetidas aos mesmos princípios e diretrizes gerais da LGPD, assegurando previsibilidade regulatória e igualdade de tratamento no que se refere à proteção de dados pessoais.

Também devem ser implementados algoritmos de aprendizado adaptativo para maior precisão dos dados coletados; medidas técnicas capazes de assegurar a integridade e evitar vieses, bem como implantação de medidas de segurança robustas para minimizar falsificação ou simulação de características biométricas “spoofing”.

BLOCO II – HIPÓTESES LEGAIS

- 4) Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?**

As Associadas entendem que para garantir que o consentimento seja livre, específico, destacado, informado e inequívoco, é importante que sejam adotadas medidas de forma a garantir que (i) o titular obteve de forma transparente as informações necessárias em relação ao tratamento de dado biométrico que será realizado, em especial a sua finalidade específica de tratamento (a qual deverá ser bem delimitada, evitando tratamento posterior para finalidades incompatíveis com a finalidade original); (ii) que este aceite foi de fato dado de forma inequívoca pelo titular – como através do uso de *check-box* para *opt-in*, ou por meio de Termo de Consentimento; e (iii) que tal aceite seja apresentado como opção efetiva do titular (isto é, não constitua condição singular do titular para acesso a determinado produto, serviço, ambiente ou benefício, sem efetiva necessidade para tal, sendo que em tais casos, havendo real indispensabilidade do uso da biometria, poderia ser utilizada uma das hipóteses legais previstas no art. 11, II da LGPD).

DS


De forma a exemplificar, um titular poderia ser questionado por determinado controlador se gostaria de utilizar a sua biometria como um facilitador na autenticação para acesso a um determinado ambiente físico ou eletrônico. Quando a biometria é tratada neste caso como uma opção do titular, existindo formas alternativas de acesso aos ambientes que não envolvem este tratamento de dados, há consentimento inequívoco, na forma do art. 11, I da LGPD. No entanto, se a biometria é a única forma de acesso ao produto, serviço ou ambiente, o que pode ser muito bem fundamentado considerando situações como propensão à fraude, por exemplo, o consentimento pode não ser a hipótese legal mais apropriada, cabendo a avaliação pelo controlador das demais hipóteses do art. 11, II da LGPD.

Assim, o consentimento só deve ser utilizado quando houver real liberdade de escolha e inexistirem outras bases legais mais adequadas. Quando adotado, é fundamental garantir transparência, linguagem acessível, possibilidade de recusa com visibilidade clara das consequências, bem como registro da manifestação inequívoca da vontade do titular em permitir este tratamento de dados.

5) Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A aplicação da hipótese legal de “garantia da prevenção à fraude” para o tratamento de dados biométricos exige a observância rigorosa dos princípios da necessidade, proporcionalidade e finalidade. O uso da biometria deve ser indispensável para a segurança do processo, especialmente em sistemas eletrônicos, e ineficazmente substituível por métodos menos invasivos.

No contexto do setor financeiro, existe uma demanda adicional de segurança (a exemplo, combate de lavagem de dinheiro, prevenção à fraude, anticorrupção entre outros), e as instituições financeiras possuem regulamentações específicas para subsídio de prevenção a fraude. A biometria tem papel fundamental na autenticação de usuários e na mitigação de fraudes, sendo crucial para proteger tanto os titulares quanto as próprias instituições. A ausência de segurança jurídica quanto à coleta de dados biométricos pode comprometer a

integridade das operações e das transações, impactando negativamente a confiança no sistema.

Para compatibilizar com o princípio da necessidade, recomenda-se limitar o uso à finalidade de segurança, adotar autenticação multifator, e garantir transparência ao titular quanto à coleta e uso dos dados.

Como mitigadores, destacam-se: teste de balanceamento, política de retenção e descarte, monitoramento de falsos positivos e planos de resposta a incidentes. A biometria não deve ser aplicada de forma ampla e irrestrita, mas sim de maneira específica e tecnicamente fundamentada.

6) Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

O tratamento de dados biométricos deve estar expressamente previsto em norma legal ou regulatória vigente.

As Associadas destacam que, mesmo quando realizado por órgãos públicos, esse tratamento deve observar os princípios da LGPD, especialmente os da necessidade, minimização e segurança. Devem ser adotadas medidas de transparência, segurança da informação, informação clara ao titular e, quando cabível, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais. Os órgãos públicos devem manter padrões de segurança equivalentes aos do setor privado, para mitigar riscos e evitar danos em caso de incidentes de segurança.

Nos casos em que a transparência total não seja possível, como em investigações criminais ou situações com restrição de sigilo, é essencial que a regulamentação assegure a legitimidade da operação e o equilíbrio com os direitos dos titulares.

7) Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de

reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Deve-se observar a finalidade específica do estudo, tratando apenas os dados estritamente necessários, evitando coletas excessivas. É fundamental segregar os dados de pesquisa em relação a outros bancos de dados e restringir o acesso apenas a pessoas autorizadas, adotando técnicas robustas de anonimização sempre que possível. Além disso, as Associadas entendem ser imprescindível vedação expressa a reidentificação e o cruzamento de bases sem controle prévio e justificado, e sem a necessidade de um novo consentimento, exceto para uma finalidade distinta, garantindo que os dados permaneçam em ambiente seguro e com acesso controlado, conforme previsto no art. 13 da LGPD, e sob supervisão ética e científica das atividades de pesquisa.

Como salvaguardas adicionais, recomenda-se implementar uma política clara de eliminação dos dados ao término do estudo, definindo prazo máximo de manutenção dos dados, e se necessário, necessidade de renovação do consentimento, além da realização do monitoramento contínuo e auditorias periódicas do tratamento, formalizar termos de responsabilidade pelos pesquisadores e proibir a comercialização dos dados utilizados ou gerados.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

- 8) Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?**

É essencial garantir ao titular o acesso a informações claras sobre a real necessidade do uso da tecnologia, bem como a possibilidade de questionamento e correção em caso de falhas ou erros na identificação, evitando privações indevidas de acesso a produtos ou serviços.

DS


Para mitigar os riscos de discriminação ilícita ou abusiva, devem ser adotadas salvaguardas técnicas, jurídicas e institucionais, como a avaliação de impacto à proteção de dados pessoais, a adoção de mecanismos de anonimização sempre que possível, e o controle sistemático de viés nos sistemas utilizados. Também se recomenda o uso de algoritmos treinados com dados representativos de diferentes grupos sociais, incluindo diversidade de gênero, raça e etnia, a aplicação de métricas de conformidade contínuas, e a previsão de revisão humana.

9) Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Os sistemas devem ser desenvolvidos com testes contínuos, base de dados representativa e calibração. É importante incorporar, nos casos em que os interesses e liberdade do titular são afetados pelo reconhecimento facial, mecanismos de correção, como canais acessíveis para contestação por parte dos titulares e a possibilidade de revisão por pessoa humana, especialmente nos casos de decisões automatizadas. Auditorias internas periódicas e processos de correção ágeis também devem ser implementados, a fim de assegurar a integridade do sistema e mitigar os impactos negativos decorrentes de eventuais falhas de identificação.

10) É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Nestes casos, poderiam ser identificados contextos e situações em que o uso de tecnologias de reconhecimento facial não seja recomendado. As Associadas destacam alguns casos, como: situações que envolvam crianças e adolescentes; espaços de saúde; ambientes religiosos ou políticos, uma vez que, estes ambientes envolvem outros dados com características de dados sensíveis,

os quais podem levar a um cenário de discriminação, conforme os critérios e finalidades específicos e atendimento aos princípios da LGPD.

Como alternativa, as Associadas entendem que podem ser considerados o uso de autenticação multifator, biometria por dispositivo (impressões digitais) ou token físico.

Ainda, é essencial que o uso da tecnologia observe os princípios da necessidade e adequação, sendo avaliada a real sensibilidade do ambiente e os riscos envolvidos para os titulares, de modo a evitar sua exposição desnecessária e assegurar um tratamento proporcional, transparente e legítimo.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11) Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Entre as medidas técnicas, as Associadas destacam: criptografia dos dados, controle rigoroso de acesso, armazenamento seguro, registro e análise de logs, auditorias periódicas, além da implementação de plano de resposta a incidentes. Já do ponto de vista administrativo, é essencial a implantação de uma Política de Segurança da Informação, treinamentos periódicos para colaboradores e terceiros, análise de riscos de prestadores de serviços antes do início das atividades, além da existência de um plano de continuidade de negócios e monitoramento diário das operações.

Adicionalmente, devem ser exigidos das organizações parâmetros mínimos de avaliação de riscos contínua, incluindo a realização de Relatório de Impacto (nos termos do art. 38 da LGPD), garantindo a conformidade com os princípios da lei e a proteção integral desses dados sensíveis.

12) Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que

essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

É fundamental que a norma traga a definição de serviços não essenciais, para o uso da biometria e funcionalidades específicas de serviços não essenciais seja informado de forma clara ao titular, destacando seu caráter opcional sempre que o tratamento se basear no consentimento. Também é recomendável que sejam oferecidas alternativas viáveis de autenticação e que se justifique tecnicamente a adoção da biometria, evitando práticas que possam configurar discriminação ilícita ou abusiva.

A negativa do titular ao fornecimento de seus dados biométricos somente poderá justificar a restrição ao uso de determinadas funcionalidades quando estiver fundamentada a real necessidade da utilização da biometria para garantir maior segurança, prevenir fraudes ou assegurar a integridade da operação. Nesses casos, é essencial que o controlador informe claramente as finalidades do tratamento, as consequências da recusa e eventuais meios alternativos de acesso.

Além disso, é importante que os sistemas adotados garantam a eficácia da autenticação biométrica, com mecanismos que evitem vieses ou falhas que possam limitar de forma injustificada o acesso do titular. A coleta ou o uso excessivo da biometria deve ser evitado, privilegiando sempre o equilíbrio entre a segurança operacional e os direitos fundamentais do titular de dados.

13) Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Para garantir uma proteção eficaz no tratamento de dados biométricos, os controladores devem adotar boas práticas específicas como a coleta mínima de dados, com uso estritamente justificado, revisão periódica da real necessidade de manutenção dessas informações, e anonimização ou pseudonimização sempre que possível. A transparência é essencial.

DS


É igualmente importante a adoção de políticas internas claras, treinamentos regulares para equipes envolvidas no tratamento de dados sensíveis, canal de comunicação com os titulares e esteiras específicas para o atendimento de seus direitos.

Além disso, devem ser proibidas práticas de reidentificação indevida e adotados mecanismos robustos de prevenção à discriminação, como a supervisão contínua de vieses algorítmicos e mecanismos que permitam contestar e corrigir eventuais erros de identificação. Dessa forma, assegura-se que o uso de dados biométricos seja feito de maneira responsável, proporcional e respeitosa aos direitos fundamentais dos titulares.

14) Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

O entendimento das Associadas é de que os controladores devem adotar medidas que assegurem transparência, segurança e respeito aos direitos dos titulares. Isso inclui: (i) Informação clara e acessível, com sinalização visível e uso de canais digitais para informar o tratamento realizado e seus objetivos; (ii) Canais para exercício de direitos, como acesso, oposição e contestação de decisões automatizadas; (iii) Revisão humana em decisões automatizadas com impacto relevante, isto é, nos casos em que as decisões tomadas de forma automatizada podem impactar de forma efetiva em liberdades e direitos individuais do titular dos dados; (iv) Limitação da coleta ao mínimo necessário, respeitando os princípios da necessidade e proporcionalidade; e (v) Segurança técnica e administrativa adequada, incluindo anonimização, controle de acesso e políticas internas.

Dado o desafio de garantir consentimento individual nesses casos, é essencial que os controladores assumam responsabilidades claras e adotem práticas que equilibrem inovação, segurança e proteção de dados, com base em uma abordagem orientada a riscos.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

DS


15) De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Os agentes de tratamento devem garantir informações claras sobre o uso de dados biométricos por meio de Políticas de Privacidade acessíveis e canais adequados para o exercício dos direitos dos titulares, como acesso, correção e revogação do consentimento. É importante que haja mecanismos simples e eficazes para esses pedidos, com canais de atendimento de fácil acesso, e que aproveitem mecanismo já existentes como os canais de privacidade ou outros canais já administrados pelo controlador.

No tratamento automatizado, deve-se garantir revisão humana, permitir contestação e assegurar a transparência sobre a lógica envolvida na decisão. A revogação do consentimento deve ser viabilizada com clareza quanto às suas consequências, inclusive quanto à necessidade ou não de manter os dados para finalidades legítimas.

16) Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

A participação informada dos pais ou responsáveis deve ser garantida por meio de transparência prévia, com informações claras, acessíveis e adequadas à compreensão do público-alvo.

O tratamento de dados biométricos de crianças e adolescentes é admissível quando necessário para finalidades legítimas, como segurança ou acesso a serviços, desde que seja proporcional, justificado e limitado à coleta mínima indispensável. Deve estar alinhado ao princípio do melhor interesse da criança e do adolescente, o que exige a adoção de salvaguardas robustas, como medidas de

segurança reforçadas, restrição de acesso aos dados, avaliação de impacto e revisão periódica da real necessidade do tratamento.

17) Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

As Associadas entendem que o tratamento seria admissível em casos de proteção da criança, conforme previsão na LGPD. A participação informada dos pais ou responsáveis deve ser assegurada por meio de comunicação clara e acessível, com informações transparentes sobre a finalidade do tratamento conforme determinado em Políticas de Privacidade e aos princípios da LGPD.

Para evitar abusos, é necessário ter políticas claras, controle de acesso, anonimização, quando possível e auditorias periódicas para prevenir abusos e vazamentos. Essas medidas devem ser orientadas pelo princípio do melhor interesse da criança e do adolescente.

18) Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

A verificação ou estimação de idade por meio de dados biométricos só deve ser adotada quando estritamente necessária, observando o princípio da necessidade e do melhor interesse da criança ou do adolescente. Sempre que possível, devem ser priorizados métodos menos invasivos, como checagem documental, autodeclaração com responsabilização dos pais ou responsáveis, ou validação por terceiros confiáveis.

Caso o uso da biometria se justifique, é fundamental assegurar a transparência com os pais ou responsáveis, adotar medidas técnicas robustas de proteção dos dados, garantir a mínima retenção das informações, anonimização quando aplicável, impossibilidade de reutilização dos dados para outras finalidades, bem como supervisão contínua do tratamento.

^{DS}




Sem mais para o momento, a ANCORD permanece à disposição de V.Sas. para prestar os esclarecimentos adicionais que se fizerem necessários.

Atenciosamente,

DocuSigned by:
José David Martins Júnior
D9FC0CAB2E40466...

**ANCORD – Associação Nacional das Corretoras e Distribuidoras de Títulos,
Valores Mobiliários**

Relatório: Dicotomias no Direito e Proteção de Dados Pessoais – um olhar sobre a necessidade de proteção da pessoa idosa frente ao avanço no uso de dados biométricos em operações de crédito com tratamento automatizado

Autor: Raphael Gomes

Data: 01/08/2025

Sumário

Introdução	3
Da morosidade processo legislativo para regulamentar fatos sociais relevantes	3
Das consequências práticas da morosidade do processo legislativo	4
Da solução jurídica plausível	11

Introdução

Neste relatório abordar-se-á algumas dicotomias votadas ao estudo do direito e proteção de dados pessoais, com ênfase em princípios autônomos, e com conflitos aparentes, notadamente o da autodeterminação informativa frente ao da livre iniciativa.

Nas palavras da professora Maria Brochado o Direito é disciplina não disruptiva ou não voltada à revolução. Ou seja, entre os acontecimentos sociais considerados como relevantes e, portanto, alvo do processo de normatização, até a publicação no normativo que o regule há um longo e demorado caminho.

Da morosidade processo legislativo para regulamentar fatos sociais relevantes

Citemos a LGPD que, após extensos debates foi publicada em 2018 com vigência prevista apenas para agosto de 2020, e as sanções passaram a valer apenas em agosto de 2021. Nesse ambiente foi promulgada a EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022 assegurando, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais, aperfeiçoando o conceito de proteção da dados em formato eletrônico e colocando nele o status de direito fundamental.

Abordemos também a regulação de ilícito e contemplemos que o código penal de 1940 foi alterado em 2021, com vistas a contemplar a chamada fraude eletrônica.

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de um a cinco anos

Fraude eletrônica

§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021).

Observemos que o legislador tornou mais gravosa a pena de um delito, quando esse é cometido por meios eletrônicos, com o intuito de desestimular ou coibir o numeroso número de tentativas criminosas que passaram a ocorrer com o advento das tecnologias de processamento de transações online.

Para além dos casos em que o número de crimes incentiva a atuação do legislador, podemos contemplar exemplos em que a grande comoção provocada por apenas um caso já motiva a mobilização imediata em torno do tema, provocando a atuação do parlamento, com o intuito de regular o fato social.

Dentre alguns outros casos que poderiam ser mencionados, citemos que em meado de 2022 um anestesista Giovanni Quintella Bezerra, flagrado estuprando um mulher que passava por

uma cesariana no Hospital da Mulher, em São João de Meriti, na Baixada Fluminense. Em 2025, decorridos três anos, foi publicada uma lei que estabelece que Mulheres submetidas à sedação em serviços de saúde terão direito a um acompanhante, conforme estabelece a Lei 25.401, de 2025, publicada no Diário Oficial de Minas Gerais nesta terça-feira (29/7).

Podemos constatar que o Direito por vezes é muito lento para regular fatos sociais de extrema relevância e por vez é um pouco mais célere.

Retomando o aumento da pena do crime de estelionato, quando cometido por meios eletrônicos, pode se dizer que a intenção do legislador em incrementar o tempo de encarceramento seria a de coibir os possíveis criminosos de praticá-lo. Essa medida não se mostrou efetiva, tendo em vista o aumento significativo no número de crimes nas modalidades tentadas e consumadas.

Nesse diapasão, compete ao Estado engendrar novas medidas, uma vez que a caracterização desse delito e aumento da pena de reclusão não foi suficiente.

Voltando a exemplificar a lentidão do Estado (do Direito) para regular fatos sociais relevantes, contemplemos o PL 2131/2007 da Câmara dos Deputados, o qual se propôs a tornar obrigatória a homologação em cartório de todo contrato de empréstimo consignado a ser efetuado por aposentado ou pensionista do INSS. Apenas em 2023 (decorridos 16 anos) houve um encaminhamento meramente procedimental (vide <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=369205>). Enquanto isso, milhões de aposentados sofreram fraudes em empréstimos tratados de maneira automatizada, sem a necessidade de revisão humana.

Em uma nova iniciativa do Senado, pode ser vista outra tentativa de normatizar a temática. O PL 74/2023 que dispõe sobre a obrigatoriedade da assinatura física das pessoas idosas em contratos de operação de crédito firmados por meio eletrônico ou telefônico e propõe a exigência de que contratos de empréstimos que sejam feitos por idosos tenham assinatura em papel, mesmo que a contratação seja digital ou por telefone. O objetivo seria de proteger aposentados e pensionistas de fraudes e garantir que o idoso esteja plenamente informado sobre o contrato (<https://www25.senado.leg.br/web/atividade/materias/-/materia/155732>).

Das consequências práticas da morosidade do processo legislativo

Percebe-se assim que não há consenso capaz de promover a proteção devida aos idosos mais vulneráveis a esse tipo de crime. Em 2024 60% dos idosos no Brasil eram analfabetos ou de baixa escolaridade. O dado é alarmante porque essa parcela é o dobro da média nacional (de 30%). Fonte: Agência Câmara de Notícias.

Também aqui há uma certa dicotomia: uma vasta população que não teve o direito de acesso à educação tendo a sua dignidade afrontada, frente ao avanço tecnológico e uso criminoso de dados pessoais biométricos, colocando-os como alvos de operações de crédito

não consentidas, ou consentidas mediante fraudes. Segundo a Cybersecurity Ventures, os crimes cibernéticos custarão ao mundo cerca de US\$ 10,5 trilhões anualmente até 2025. Uma pesquisa realizada pelo MIT em 2020 mostrou que sistemas de reconhecimento facial apresentavam taxas de erro significativamente mais altas ao identificar pessoas de diferentes etnias, com taxas de erro de até 35% para mulheres de pele escura, em comparação com menos de 1% para homens de pele clara. Fonte: Valor econômico.

Das questões práticas envolvendo as disposições LGPD.

Como boa iniciativa para aprofundar os debates sobre a necessidade de aprofundamento dos debates sobre proteção de dados a Autoridade Nacional de Proteção de Dados (ANPD) incluiu, no item 5 da Agenda Regulatória para o biênio de 2025/2026, uma iniciativa para analisar a necessidade de intervenção regulatória sobre o tema, seja mediante regulamentação ou documento de caráter orientativo.

A ANPD chamou atenção para o fato de que uso de dados biométricos teve um crescimento nos últimos anos, com potencial impacto nos direitos fundamentais. Se, por um lado, o tratamento desses dados pode ampliar a segurança e auxiliar a prevenção de fraudes; por outro lado, também são ampliados os riscos sobre os titulares, a exemplo de impactos negativos decorrentes de erros dos sistemas utilizados e de efeitos discriminatórios sobre grupos vulneráveis. Os dados biométricos, caracterizados como dados pessoais sensíveis pela LGPD, demandam um tratamento rigoroso devido aos riscos que representam para a privacidade e os direitos dos titulares. A ANPD, em seu papel de regulamentar e fiscalizar o cumprimento da LGPD, busca aprofundar a compreensão sobre o uso dessas tecnologias no cenário brasileiro e nas situações destacadas no art. 3º da Lei.

Nesse ambiente, a mencionada autoridade elencou 18 perguntas. Este relatório se prestará a discorrer sobre algumas delas, apontando lacunas legislativas e promovendo o debate sobre eventuais soluções. O quesito número dois da tomada de subsídios questionou quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados. Já a pergunta de número quatro provoca reflexões de como seria possível garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD e em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados

Nesse ponto, é necessário salientar que, embora possa existir uma política de transparência adequada e um eventual processo de autenticação do titular não tenha apresentado falha técnica, nem sempre é possível comprovar de forma inequívoca que o consentimento foi livre. Exemplifiquemos com base em casos reais de pessoas idosas de baixa escolaridade sendo induzidas por meio fraudulento a realizar uma operação financeira, a qual não faria se não fosse coagida. Como agravante e para além dessas situações, soma-se a possibilidade de fraude a sistemas de autenticação facial. É possível constatar que, tendo em vista que os

mecanismos de autenticação podem ser burlados, o consentimento nunca gozará de presunção absoluta de veracidade.

Adentrando nessas peculiaridades, com vista a reduzir o número de fraudes no sistema financeiro e garantir que realmente seja atendido o princípio da autodeterminação informativa, um fato que deveria ser melhor delineado pela regulamentação é a possibilidade de titular de dados antecipar o não consentimento para tratamento de seus dados biométricos para fins de processamento de operações de crédito sem revisão humana, ou sem sua confirmação de modo presencial. É possível concluir que sem a implementação dessa antecipação de negativa de consentimento para tratamento de dados biométricos, o princípio da autodeterminação não estaria plenamente disponível ao titular. Esse quesito será explorado em outros pontos desse questionário.

A ANPD também apontou questionamentos sobre quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos, de que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras e quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais.

Também nestes quesitos, é importante destacar que por mais que haja robustez nas implementações técnicas de segurança, sempre haverá possibilidade de fraude. À medida que a biometria facial se populariza, as tentativas de golpes digitais também avançam. Os fraudadores usam imagens montadas, edição de vídeos em movimento, fotos com fundo falso, deepfake, que são redes neurais capazes de gerar faces aleatórias bem convincentes, para tentar se passar por outra pessoa. Mesmo consolidada as melhores práticas em segurança, sempre haverá a probabilidade de que agentes de contrainteligência burlam os sistemas de autenticação.

Somente a efetiva promoção da autodeterminação informativa, no sentido de o titular poder antecipar o não consentimento de tratamento de seus dados biométricos em sistemas de decisão automatizados e a vedação de operações de crédito por meios automatizados quando o beneficiário é pessoa idosa de baixa escolaridade poderiam mitigar os efeitos devastadores que as pessoas têm sofrido quando vítimas de operações fraudulentas.

Cumprir destacar com relação ao quesito da transparência que, mesmo existindo políticas bem elaboradas e publicadas, além da possibilidade de fraudes ou sistemas que burlam a autenticação de dados biométricos processados eletronicamente, existem grupos que estão sujeitos a serem induzidos a autenticação por meio fraudulento. Nesse contexto, como medidas adicionais, o controlador deve engendrar formas de garantir a licitude das operações, com destaque para aquelas que são notoriamente suspeitas. O Estado também pode agir no sentido de regulamentar, potencializar e dar pleno atendimento ao princípio da autodeterminação informativa. A LGPD dispõe que a revogação pode ocorrer a qualquer

tempo, mas a legislação ainda não prevê o registro de não consentimento prévio a operações de crédito tomadas sem revisão humana.

No quesito número nove foi questionado como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos e quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado.

Retomando a análise da necessidade da existência de revisão humana, é necessário ponderar que podem existir situações em que essa revisão seria imperativa. Tomemos o exemplo de uma pessoa idosa, analfabeta ou semianalfabeta, que supostamente solicita uma operação de crédito por meio de dispositivo móvel. Podem ocorrer casos em que a pessoa acabou de se cadastrar, fez contrato um empréstimo, considerando ainda sua baixa escolaridade e seu histórico de pouca destreza ao manipular dispositivos eletrônicos, e em seguida de uma transação financeira totalmente suspeita. Ademais, tem-se alguns agravantes que ocorrem no Brasil, que é o país em que mais sofre com tentativas de golpes e telemarketing invasivo, que tem uma numerosa população idosa de baixa escolaridade, a qual tem sofrido atualmente consequências severas das atividades criminosas (fraude a autenticação ou estelionato).

O que se pode vislumbrar no caso específico da população idosa de baixa escolaridade brasileira é o Estado se furtando do dever assegurar o gozo dos direitos fundamentais inerentes à pessoa idosa (conforme LEI No 10.741, DE 1º DE OUTUBRO DE 2003), e o sistema bancário não conseguindo reduzir de modo significativo a ocorrência das fraudes.

Há, por conseguinte, falha do Estado no quesito regulamentação, investigação e persecução penal, falha do sistema bancário no quesito detecção de fraudes, e quem sofre as consequências mais dramáticas é a população idosa vulnerável, que o Estado deveria proteger, notadamente por já haver falhado no passado com esses indivíduos não provendo uma educação de qualidade no passado.

Também foi questionado na tomada de subsídios se seria possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado e quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares

Em resposta a esses apontamentos poderia ser dito que não é recomendável que uma pessoa idosa analfabeta ou de baixa escolaridade tenha seus dados biométricos utilizados de forma automatizada para fins de concessão de crédito sem que haja uma revisão humana.

O Estado brasileiro, além de no passado não promover o acesso ao sistema de educação para esse grupo vulnerável, falha mais uma vez ao não determinar medidas efetivas no combate a fraudes e uso indevidos de dados biométricos mediante fraudes. Diversas

reportagens de diversas fontes poderiam ser citadas, mas pode se dizer que em linhas gerais a tragédia envolve milhões de pessoas.

É inconcebível que o Estado não tome providências com uma situação que está ocorrendo massivamente contra uma população idosa, vulnerável e de baixa escolaridade.

Avaliemos uma situação típica por etapas:

Um idoso faz um cadastro ou abertura de relacionamento recente em instituição financeira;

Usa sistema de autenticação por reconhecimento biométrico;

Contrata uma operação de crédito tramitado de modo automatizado (sem intervenção humana)

Faz uma movimentação atípica de recursos financeiros, muitas das vezes tendo como beneficiários sujeitos de localidades que ficam razoavelmente longe do tomador do empréstimo ou que não recebem habitualmente valores expressivos ou que não se dedicam a nenhuma atividade empresarial já consolidada em que se possa presumir a licitude do negócio jurídico.

Avaliando-se as etapas genéricas de um crime nos moldes do que foi exposto acima, constatar a caracterização de uma fraude não seria uma tarefa complexa. Mesmo assim, em caso semelhantes, nem o sistema bancário, nem o Estado está conseguindo prevenir esses ilícitos, desembocando-se em uma situação dramática para a população idosa de baixa escolaridade brasileira.

Dois pontos devem ficar claros:

1 - A necessidade gritante de possibilitar, dando pleno significado ao princípio da autodeterminação, a antecipação do não consentimento para operações automatizada, uma vez que a LGPD que o consentimento pode ser revogado, ou seja, negado, a qualquer tempo.

2 - A necessidade de se vedar operações de crédito por meios exclusivamente na modalidade automatizada aos idosos e/ou analfabetos.

Houve ainda na tomada de subsídios de solicitação de análise sobre que contextos a negativa do titular ao fornecimento de seus dados biométricos e como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos

Merece atenção o fato contrário ao exposto no questionário, no sentido de não haver previsto na legislação a possibilidade, consoante princípio da autodeterminação informativa, de o titular poder antecipar, notadamente junto ao Sistema Financeiro Nacional, o não consentimento ao tratamento de dados biométricos para fins de movimentações financeiras ou contratações de crédito.

De forma específica, a autodeterminação informativa é um dos fundamentos da LGPD (art. 2º, II) e implica que o titular deve ter o poder de decidir sobre o uso de seus dados pessoais, inclusive biométricos, mesmo em ambientes públicos ou automatizados. Repise a afirmação que esse fundamento nunca será pleno enquanto o titular não ter o direito de antecipar por meio de plataforma segura e centralizada o direito de antecipar a não anuência para tratamento de dados biométricos. Esta aplicabilidade já está disponível, por exemplo, para proteger o uso de um CPF contra a inclusão indesejada em empresas e demais sociedades, em todo o território nacional de forma gratuita (<https://www.gov.br/pt-br/servicos/impedir-permitir-participacao-do-meu-cpf-no-cadastro-nacional-de-pessoas-juridicas-cnpj>). Essa opção pode ser tida como um modelo a ser seguido para fortalecer e prever/criar outros casos em que o titular possa exercer o direito de autodeterminação informativa (negativa antecipada de consentimento), notadamente no que toca as operações de crédito.

O STF, ao reconhecer a autodeterminação informativa como direito fundamental autônomo (ADIn 6393), reforçou que o controle sobre os próprios dados deve ser garantido mesmo em contextos emergenciais ou de interesse público. Ponderemos que até em situações emergências, em tese, o princípio da autodeterminação informativa foi definido como sendo direito fundamental, mas na prática o titulares brasileiros ainda não gozam da prerrogativa de exercê-lo a qualquer tempo, no casos de querer antecipar o não consentimento (tal como já é feito para bloquear abertura de empresas com um determinado CPF, mas ainda não é feito no sistema bancário, no sentido de titular poder definir que seus dados para fins de contratação de operações de crédito tenham sempre passar por revisão humana ou confirmação presencial em caixas eletrônicos, por exemplo).

Por fim, no escopo deste relatório, foi sugerida pela tomada de subsídio uma análise de que formas os agentes de tratamento poderiam garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos. Em resposta a este tópico, cumpre destacar que a garantia o respeito aos titulares não é de competência exclusiva do agente de tratamento, embora esse possa contribuir de maneira significativa. Mesmo que somada a eventuais medidas de mitigação de riscos tomadas pelo controlador, tampouco a publicação das informações de maneira clara e ostensiva teria o condão de garantir o respeito aos direitos dos titulares, notadamente quando se tratar de operação fraudulenta, seja por meios técnicos capazes de burlar os sistemas de autenticação, seja por meio de estelionato, em que sempre estão presentes os métodos ardilosos.

Três fatores agravam o cenário exposto: o desenvolvimento constante de técnicas que visam burlar os sistemas de autenticação, a quantidade de criminosos e o número de idosos de baixa escolaridade, além dos analfabetos.

A únicas medidas que teriam impacto relevante e positivo em um curto prazo seriam as seguintes:

1 - Dar direito ao pleno gozo do princípio da autodeterminação aos titulares, permitindo a antecipação do não consentimento para operações automatizadas usando dados biométricos, uma vez que a própria LGPD reza que o consentimento pode ser revogado a qualquer tempo.

2 - Vedar operações de crédito por meios exclusivamente na modalidade automatizada aos idosos de baixa escolaridade ou analfabetos.

Para mais, na situação fática atual, principalmente no sistema bancário, há algumas afrontas às disposições da LGPD. Avaliemos as hipóteses de tratamento na referida lei, que, em tese, poderiam respaldar o tratamento para fins de operações de crédito, destacando os incisos I, V, IX e X e os parágrafos 4º e 5º.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

Art. 8º, § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

Avaliando novamente a situação típica de uma fraude por etapas:

Um idoso faz um cadastro ou abertura de relacionamento recente em instituição financeira;

Usa sistema de autenticação por reconhecimento biométrico;

Contrata uma operação de crédito tramitado de modo automatizado (sem intervenção humana);

Faz uma movimentação atípica de recursos financeiros, muitas das vezes tendo como beneficiários sujeitos de localidades que ficam razoavelmente longe do tomador do empréstimo ou que não recebem habitualmente valores expressivos ou que não se dedicam

a nenhuma atividade empresarial já consolidada e em que se possa presumir a licitude do negócio jurídico.

Conforme artigo 8, parágrafo 2º, conjugando-se o inciso um do artigo 7º seria possível o controlador comprovar a o consentimento do titular apenas com o log da autenticação, uma vez que caberia esse o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei? Do ponto de vista prático, muito idosos que são vítimas de fraude não conseguem reverter a operação e não têm recursos financeiros para buscar auxílio jurídico ou sabem que poderiam procurar a defensoria pública. Para além, caso as defensorias públicas fossem provocadas a agir em milhares de processos, a situação ficaria quase que insustentável.

Analizando outro dispositivo, o parágrafo 4 do artigo 8, o consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. Uma autorização de concessão de crédito para pessoa idosa ou analfabeta ou de baixa escolaridade em um dispositivo móvel recém cadastrada poderia ser considerada, como regra, uma autorização genérica e, portanto, nula.

Avaliando-se um extrato do parágrafo 5º da LGPD tem-se que o consentimento pode ser revogado a qualquer momento, grifo nosso, mediante manifestação expressa do titular, por procedimento gratuito e facilitado. É possível constatar que o titular deveria, notadamente no Sistema Financeiro Nacional, sob pena de sofrer severos prejuízos financeiros e morais, ter o direito de registrar não consentimento para que seus dados fossem tratados por decisões automatizada por meio de dados biométricos, sem a necessidade de intervenção humana. O Estado ainda não proveu meios de o titular ter o direito à revogação antecipada, assim digamos, do consentimento, presumindo-se legítima toda e qualquer operação em que os sistemas de autenticação não falhem ou mesmo aquelas operações consolidadas mediante estelionato. Pode-se concluir que o parágrafo 5º do artigo 8 da LGPD vigora, mas não é aplicável em situações reais que causam impacto significativo na vida dos titulares.

Dado que os sistemas bancários de detecção de fraudes não estão conseguindo proteger as operações de crédito fraudulentas contra pessoas idosa vulneráveis, caberia ao Estado promover regulamentos que visem reduzir os números de fraudes, potencializando o princípio da autodeterminação informativa e vedando operações de crédito presumidamente indevidas.

Posto em tela o número alarmante de idosos vulneráveis vítimas de fraude em empréstimos, seria imperativo ao Estado delinear as situações em que o consentimento deve ser tratado de forma que a revisão humana seja obrigatória por parte do controlador, notadamente quando se tratar de pessoa idosa de baixa escolaridade.

Da solução jurídica plausível

Diante do exposto, um projeto de lei em teor semelhante ao abaixo descrito poderia reduzir significativamente o número de tentativas e consequentemente o número de fraudes

consumada contra essa parcela tão carente da população brasileira, que são os idosos de baixa renda e baixa escolaridade.

Projeto de Lei xxxx/2025

Art. xx - O titular dos dados pessoais tem direito a registrar no sistema financeiro nacional ou aplicação de governamental própria a opção ter o tratamento de seus dados para fins de operação de crédito na modalidade exclusivamente presencial, ou eletrônica seguida de confirmação biométrica em caixas eletrônicos.

I - O registro da opção mencionada no caput deverá disponibilizado nos aplicativos e agências bancárias.

II - A revogação de opção pelo mencionada poderá ser feita somente de modo presencial.

III - No caso da opção de operação seguida de confirmação biométrica em caixas eletrônicos, este canal deve disponibilizar informações sobre os riscos de fraude nas operações de crédito. Fica vedado o uso de operações de crédito na modalidade exclusivamente eletrônica por pessoas analfabetas.



Opice

BLUM

Opice Blum Bruno Advogados

São Paulo, 28 de junho de 2025

À Autoridade Nacional de Proteção de Dados ("ANPD")**Setor: Coordenação-Geral de Normatização**Por e-mail: normatizacao@anpd.gov.br**Ref.: Material complementar às contribuições da Binance na Tomada de Subsídios: Dados pessoais sensíveis – dados biométricos.**

Prezados(as),

A **Binance**, por meio desta, encaminha o **RELATÓRIO COMPLEMENTAR** às suas contribuições à **Tomada de Subsídios: Dados pessoais sensíveis – dados biométricos** ("Tomada de Subsídios"), nos termos do quanto segue.

1. Introdução

A Binance é a maior corretora de criptomoedas do mundo, atendendo a 235 milhões de usuários registrados em mais de 180 países. Como plataforma global de ativos digitais, atua em um setor fortemente exposto a riscos de fraude e com alto volume de transações digitais. Esse cenário se torna ainda mais desafiador diante da crescente sofisticação dos esquemas criminosos, muitos dos quais já utilizam inteligência artificial para viabilizar fraudes em larga escala — que, entre 2022 e 2024, movimentaram aproximadamente US\$ 79,1 bilhões (cerca de R\$ 429,4 bilhões) no setor¹.

Diante desse contexto, a Binance tem se posicionado como referência internacional em segurança digital, com investimentos contínuos em tecnologia avançada, sistemas de prevenção à fraude e cooperação ativa com autoridades e órgãos reguladores. Ao adotar padrões rigorosos de verificação, detecção e resposta a ameaças, a empresa

¹ De acordo com estudo recente, o crescimento de 245% no número total de fraudes está relacionado a "deepfake", que é uma técnica que permite alterar uma foto com ajuda da IA. Com isso, os criminosos conseguem criar identidades virtuais para estabelecer contas fictícias e obter acesso não autorizado a outras contas. Disponível em: <https://g1.globo.com/economia/noticia/2024/06/27/estudo-fraudes-criptomoedas.ghtml>. Acesso em 25/06/2025.

tem contribuído para estabelecer um novo patamar de segurança no mercado global de criptoativos².

Uma das estratégias de segurança adotadas pela Binance consiste na aplicação de um conjunto de práticas rigorosas durante o processo de registro de novos usuários, com o objetivo de garantir a autenticidade da identidade apresentada e prevenir fraudes — especialmente em um ambiente digital de alto risco.

A título de exemplo, cita-se: (i) a implementação do recurso de *liveness check* para autenticação, que analisa os movimentos faciais do usuário para confirmar que se trata de uma pessoa real e não de uma imagem estática, gravação ou outra forma de tentativa de fraude; (ii) a correspondência facial (*face matching*) para confirmação de identidade, comparando a selfie capturada durante o cadastro e a fotografia presente no documento de identidade fornecido; (iii) uso de dados de movimento (*motion data*) coletados a partir dos sensores dos dispositivos móveis, como acelerômetro e giroscópio, para identificar padrões comportamentais suspeitos, como registros realizados de forma automatizada, sem movimentação natural do usuário; e (iv) a verificação contra cadastros duplicados, por meio da comparação da imagem facial recém-coletada com uma base interna de selfies já registradas, de forma a identificar tentativas de abertura de múltiplas contas com diferentes documentos, mas com a mesma biometria facial.

Assim como a adoção destas medidas está inserida no contexto de segurança, a Binance implementa medidas rigorosas de proteção dos dados coletados para estes fins, como a segregação das bases de dados, controles de acesso restritos, anonimização e criptografia dos dados biométricos, evitando seu acesso não autorizado e mitigando riscos em caso de incidente de segurança.

Diante deste cenário, o presente Relatório Complementar tem como objetivo aprofundar as contribuições da Binance à Tomada de Subsídios, trazendo uma perspectiva prática do setor de criptoativos e contribuindo para a construção de uma regulação equilibrada, que promova a inovação responsável e a proteção efetiva dos direitos dos titulares.

2. Contribuições adicionais à Tomada de Subsídios

² A Binance ajudou a evitar perdas de US\$ 4,2 bilhões para usuários, protegendo cerca de 2,8 milhões de pessoas contra agentes maliciosos. Disponível em: <https://exame.com/invest/onde-investir/binance-modelo-global-resposta-ataques-virtuais/>. Acesso em: 25/06/2025.

A Binance solicita que a ANPD considere as informações adicionais apresentadas abaixo, que consistem em informações complementares às contribuições da Binance na Tomada de Subsídios, tendo em vista a limitação de caracteres imposta pela Plataforma Participa + Brasil.

Destaca-se que as contribuições adicionais são direcionadas às perguntas que guardam relação direta com as operações da Binance enquanto corretora de criptoativos, como amparo na realidade prática deste mercado para permitir a melhor compreensão da contribuição submetida via plataforma.

Pergunta 1: Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Para fins da Lei Geral de Proteção de Dados Pessoais ("LGPD"), a caracterização de um dado como biométrico deve observar critérios objetivos já consolidados na legislação brasileira, bem como em normativas internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia ("GDPR") e as diretrizes do Information Commissioner's Office ("ICO") do Reino Unido. Esses critérios são os seguintes:

(a) Relação com características físicas, fisiológicas ou comportamentais do titular

O dado deve derivar de características únicas do corpo ou do comportamento de uma pessoa natural, tais como impressão digital, íris, voz, estrutura facial, padrões de movimento (por exemplo, a técnica de *liveness check* e *motion data* atualmente aplicadas pela Binance), forma de andar ou digitar. Essas características são inerentes ao indivíduo e geralmente imutáveis ou de difícil replicação.

(b) Processamento técnico específico

Não basta a coleta de uma característica bruta — como uma imagem ou som. É necessário que o dado seja submetido a um tratamento técnico específico, por exemplo, por meio de algoritmos ou sistemas automatizados, que extraiam padrões biométricos, vetores de identificação ou modelos matemáticos únicos. Assim, uma simples fotografia não é, por si só, um dado biométrico, mas passa a sê-lo quando processada por tecnologias de reconhecimento facial.

(c) Finalidade de identificação ou autenticação do titular

Para que o dado seja considerado biométrico sensível, a finalidade do tratamento deve ser a identificação ou autenticação individualizada da pessoa natural. Ou seja, o dado é utilizado para verificar a identidade do titular, de forma única e direta, como condição para acesso a serviços ou confirmação de legitimidade em um processo. Nesse sentido, a própria LGPD, o GDPR e o ICO são categóricos: a intenção do tratamento define a sensibilidade do dado. Ou seja, a finalidade é um elemento definidor da natureza sensível do dado.

[Pergunta 2 Deixada intencionalmente em branco]

Pergunta 3: De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A biometria comportamental, embora seja mais suscetível a variações contextuais e ambientais, pode funcionar como mecanismo complementar e menos intrusivo de autenticação. Por exemplo, para detecção de movimento e presença, relevantes em contextos de prevenção à fraude.

É válido pontuar que seu uso isolado poderia impor riscos de precisão, como falhas de autenticação e negativas indevidas de acesso, porém são elementos mitigáveis com medidas de avaliação de qualidade dos dados, imagem e ambiente.

Diferentemente da biometria tradicional, que é altamente identificável e imutável, a biometria comportamental pode representar uma solução proporcional e segura, desde que adotada com transparência, em conjunto com outras camadas de verificação e com mecanismos de correção de erro. Assim, não se justifica uma regulação mais restritiva sobre a biometria comportamental em relação à tradicional, mas sim uma abordagem baseada em risco real e contexto de uso, incentivando seu uso como ferramenta de apoio à identificação.

Pergunta 4: Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

O consentimento para o tratamento de dados biométricos deve ser livre, informado, específico, destacado e inequívoco, com opção real de recusa e alternativa viável. No entanto, o consentimento não deve prevalecer sobre outras bases legais. Quando outra base legal for mais adequada ao caso concreto (por exemplo, a base legal de prevenção à fraude estabelecida no art. 11, II, "g" da LGPD), ela deve ser priorizada, garantindo maior proteção ao titular e mais segurança jurídica ao controlador. O uso do consentimento é inadequado em contextos com desequilíbrio de poder, ausência de transparência ou quando não for possível assegurar sua real voluntariedade.

Pergunta 5: *Quais critérios devem ser observados para a adequada aplicação da hipótese legal de "garantia da prevenção à fraude" (art. 11, II, "g", LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?*

A aplicação da hipótese legal de prevenção à fraude exige que o uso da biometria seja proporcional ao risco envolvido e ao bem jurídico tutelado, como a segurança patrimonial e a integridade do titular. Como principal critério para sua aplicabilidade, está a adequação do tratamento a partir da finalidade pretendida, considerando nos objetivos de validação, autenticação, segurança e, especialmente, de prevenção à fraude.

Nesse cenário, de forma aderente a tais objetivos, destaca-se a compatibilidade no que tange à necessidade de tratamento de dados biométricos em suas aplicações no setor financeiro, bancário e de também de ativos virtuais, na medida em que correspondem a controles eficientes contra fraudes e de verificação de identidade, segurança das transações, validação dos dados.

Por fim, como salvaguardas, recomenda-se adotar abordagens graduais, como o uso combinado de biometria com outros métodos (ex.: análise documental ou autenticação multifator), evitando a coleta excessiva. Salvaguardas como avaliação de impacto, medidas de segurança, revisão periódica da eficácia do método e garantia de alternativas viáveis ao titular são fundamentais para mitigar riscos e proteger os direitos fundamentais.

Pergunta 6: *Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o "cumprimento de obrigação legal ou regulatória" (art. 11, II, "a",*

LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

O uso de dados biométricos por prestadores de serviços de ativos virtuais (VASPs) como a Binance, embora ainda não regulamentado de forma específica no Brasil, pode ser analisado à luz de normas já vigentes no setor financeiro tradicional, que estabelecem parâmetros técnicos, jurídicos e operacionais aplicáveis ao tratamento de dados sensíveis, com destaque para a autenticação e verificação de identidade em ambientes digitais.

Normas como a Circular BCB nº 3.978/2020³, a Resolução BCB nº 85/2021⁴ e a Resolução CVM nº 50/2021⁵ impõem exigências como:

- avaliação de risco do uso de novas tecnologias (incluindo biometria);
- exigência de identificação formal e qualificação de clientes antes do início do relacionamento;
- medidas de segurança cibernética, criptografia e controles de acesso para proteção de dados sensíveis; e
- adoção de procedimentos de verificação proporcionais ao nível de risco.

Tais obrigações, embora direcionadas a instituições financeiras, servem como referência legítima para VASPs, dada a similaridade funcional entre os setores e o nível de exposição a fraudes. Além disso, a Recomendação nº 10 do GAFI reconhece expressamente o uso de biometria como boa prática em procedimentos de diligência reforçada, o que se aplica especialmente a prestadores que atuam globalmente ou em contextos de alto risco.

Embora os VASPs ainda não tenham sido especificamente regulamentados, já existem algumas regras que antecipam essa abordagem e preveem obrigações de conformidade específicas para entidades desta natureza. Um exemplo é a Lei nº 9.613/98, que trata da prevenção de crimes de Lavagem de Dinheiro. Os VASPs estão incluídos na lista de entidades abrangidas por essa lei e já são obrigados a identificar seus usuários e manter seus cadastros atualizados.

³ Art. 3º, I, "b"; Art. 10, §1º, III; Arts. 13–16; Art. 23.

⁴ Art. 2º, §1º, III; Art. 3º, III; Art. 3º, V, "b".

⁵ Art. 7º, I, "a"; Art. 11; Art. 12; Art. 17, II.

Portanto, mesmo quando o tratamento de dados biométricos não decorre diretamente de uma obrigação legal vinculante, a adoção de normas setoriais reconhecidas como boas práticas, especialmente aquelas aplicáveis ao setor financeiro e aos VASPs, deve ser considerada para fins de aplicação da base legal prevista no art. 11, II, "a", da LGPD (cumprimento de obrigação legal ou regulatória).

Isso porque tais normas – como a Circular BCB nº 3.978/2020, a Resolução BCB nº 85/2021, a Resolução CVM nº 50/2021 e as recomendações internacionais do GAFI – não contradizem os princípios da LGPD e incorporam salvaguardas fundamentais para mitigar riscos aos titulares, como proporcionalidade, transparência, segurança da informação e finalidade legítima.

Dessa forma, ainda que essas regras não sejam obrigatórias para os VASPs em sentido estrito, sua adoção voluntária e consistente com os princípios da LGPD reforça a legitimidade do tratamento de dados biométricos e contribui para um padrão regulatório harmônico, baseado na proteção de dados e na inovação responsável.

[Pergunta 7 Deixada intencionalmente em branco]

Pergunta 8: Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Para garantir que o uso de tecnologias de reconhecimento facial, ainda que fundado em base legal, esteja em conformidade com os princípios da necessidade, proporcionalidade, transparência e não discriminação previstos na LGPD, é fundamental a adoção de salvaguardas técnicas, jurídicas e institucionais robustas, com abordagem integrada de cibersegurança, proteção de dados e ética algorítmica.

(a) Salvaguardas técnicas e de segurança da informação, como:

- coleta limitada de dados, estritamente necessária à finalidade declarada, com restrições ao reuso;
- criptografia dos dados biométricos tanto em repouso quanto em trânsito, além de autenticação forte e controle de acesso baseado em função (*role-based access*);

- registro detalhado (logs) de todas as atividades de tratamento, garantindo rastreabilidade e responsabilização;
-
- adoção de técnicas contra vieses em relação à diversidade no banco de dados considerado;
- validação periódica do desempenho dos sistemas, inclusive com testes de robustez em contextos de fraude ou manipulação de resultados;
- alternativas acessíveis, como senhas ou tokens, para titulares que não possam ou não desejem fornecer dados biométricos;
- anonimização ou pseudonimização dos dados, sempre que possível e compatível com a finalidade do tratamento; e
- monitoramento contínuo, sistemas de detecção de intrusão, proteção de *endpoints* e resposta a incidentes voltada a sistemas que processam biometria facial.

(b) Salvaguardas jurídicas e institucionais:

- informação clara, acessível e destacada aos titulares, especificando finalidade, base legal, critérios de retenção e direitos assegurados;
- avaliação de impacto à proteção de dados (RIPD) quando houver alto risco, como uso em locais públicos ou situações de poder assimétrico;
- treinamento ético de equipes técnicas, conscientizando desenvolvedores sobre riscos de discriminação e violação de direitos; e
- supervisão contínua da ANPD, com padrões de transparência, segurança e possibilidade de auditoria.

Esse conjunto de medidas pode não apenas mitigar riscos técnicos e jurídicos, mas também promover a confiança e a legitimidade do uso da biometria facial, especialmente em ambientes digitais de alto risco, como o setor financeiro e plataformas que operam com ativos virtuais.

Pergunta 9: Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Sistemas de reconhecimento facial devem ser projetados com base no princípio do *Privacy by Design*, adotando algoritmos precisos e treinados com bases de dados

diversas em etnia, idade e gênero, sob padrões técnicos adequados (ex.: normas ISO). É essencial garantir boas condições ambientais (como iluminação e qualidade da imagem), uso de dados de alta qualidade, e segurança no processamento (criptografia e controle de acesso).

Do ponto de vista de cibersegurança, o desempenho eficiente e confiável desses sistemas depende de:

- uso de dados de alta qualidade, obtidos em boas condições ambientais, com iluminação e resolução adequadas;
- criptografia e armazenamento seguro dos dados faciais, a fim de garantir sua integridade e prevenir adulterações que possam comprometer a acurácia do sistema; e
- controles de acesso rigorosos, com autenticação multifator e segregação de funções, limitando o acesso apenas a pessoal autorizado.

Para minimizar erros como falsos positivos e falsos negativos, é indispensável a implementação de medidas complementares, como:

- monitoramento contínuo da acurácia e do desempenho do sistema;
- testes adversariais periódicos para identificar vulnerabilidades exploráveis por agentes maliciosos;
- detecção em tempo real de anomalias, que possam indicar falhas operacionais ou ataques que impactem a performance;
- mecanismos de intervenção humana (human-in-the-loop), permitindo revisão e correção manual de correspondências duvidosas ou sinalizadas; e
- atualizações regulares dos algoritmos e da base de dados de treinamento, para manter a efetividade e minimizar vieses.

Além disso, é fundamental que haja:

- canais acessíveis e eficazes para que os titulares relatem falhas ou inconsistências no sistema;
- transparência sobre os critérios utilizados em decisões automatizadas, com disponibilização de logs de auditoria imutáveis que permitam a rastreabilidade de erros e análises forenses em caso de incidentes; e
- planos de resposta a incidentes específicos para erros de identificação biométrica, assegurando investigação rápida, correção e comunicação ao titular e às autoridades, quando aplicável.

Quando houver decisões automatizadas com base no reconhecimento facial, devem ser considerados registros que permitam transparência sobre os critérios adotados e avaliações de impacto para prevenir riscos aos direitos dos titulares.

A combinação desses requisitos técnicos, organizacionais e normativos fortalece a confiabilidade, legitimidade e responsabilidade no uso da biometria facial, promovendo uma aplicação ética e segura dessa tecnologia em conformidade com os princípios da LGPD e das melhores práticas globais de cibersegurança e governança algorítmica.

Pergunta 10: É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

O uso de tecnologias de reconhecimento facial (*Facial Recognition Technology* - FRT) deve ser cuidadosamente avaliado, especialmente em contextos em que há riscos elevados à privacidade, à liberdade individual e à não discriminação. A aplicação indiscriminada dessa tecnologia pode entrar em conflito direto com os princípios da necessidade, proporcionalidade e transparência, previstos na LGPD.

Em particular, o uso de FRT não é recomendado nas seguintes situações:

- identificação remota em tempo real em espaços públicos, pelo alto risco de discriminação e efeitos inibidores sobre o comportamento social;
- ambientes sensíveis, como hospitais, escolas, instituições religiosas ou locais de assistência social, onde a confidencialidade deve ser priorizada e o FRT pode ser excessivamente intrusivo;
- cenários com alto risco de discriminação algorítmica, nos quais sistemas de FRT possam apresentar viés, levando à identificação incorreta ou impacto desproporcional sobre determinados grupos demográficos; e
- tratamento de dados de crianças e grupos vulneráveis, dada a proteção legal mais rigorosa e os riscos éticos implicados.

Nesses contextos, o FRT pode resultar em violações de privacidade, identificações incorretas, exposição indevida a riscos de segurança e reforço de desigualdades estruturais.

Para garantir a segurança e autenticação de forma menos invasiva, é recomendável considerar soluções tecnológicas alternativas, tais como:

- autenticação baseada em tokens físicos ou digitais, como cartões inteligentes, crachás com RFID ou autenticação multifator por dispositivos móveis;
- biometria comportamental, como análise de padrões de digitação ou uso de dispositivos, que apresenta menor impacto à privacidade;
- credenciais tradicionais, como senhas ou PINs associados a tokens físicos, que oferecem segurança com risco reduzido à privacidade; e
- sistemas de detecção de anomalias, que monitoram eventos suspeitos sem realizar identificação direta dos indivíduos.

A adoção dessas alternativas deve ser priorizada sempre que oferecerem um nível de segurança adequado, promovendo a proteção de dados pessoais com menor interferência nos direitos e liberdades dos titulares.

Pergunta 11: Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Dado o impacto significativo que uma violação de dados biométricos pode causar — como roubo de identidade, discriminação e exposição indevida —, é indispensável que as organizações adotem medidas de segurança técnicas e administrativas robustas, em alinhamento com os princípios da LGPD.

Do ponto de vista técnico, recomenda-se a criptografia dos dados biométricos tanto em repouso quanto em trânsito, segregação de bases de dados que contenham dados biométricos das demais, controles de acesso rigorosos baseados em funções e autenticação multifator, além do armazenamento seguro dos templates biométricos em ambientes segregados. A minimização de dados e, quando possível, a pseudonimização, também são práticas importantes para reduzir a exposição dos titulares. É essencial realizar testes regulares de segurança, como avaliações de vulnerabilidade e testes de intrusão, bem como dispor de um plano de resposta a incidentes específico para violações envolvendo biometria.

Administrativamente, é fundamental promover treinamentos contínuos sobre proteção de dados para as equipes envolvidas, implementar políticas internas claras sobre o tratamento e retenção dos dados biométricos, garantir que fornecedores e terceiros estejam em conformidade com a LGPD e manter documentação detalhada para fins de responsabilização e auditoria.

No que se refere à avaliação de riscos e monitoramento, deve-se exigir a elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) antes da adoção de sistemas biométricos, além de monitoramento contínuo dos acessos e detecção de comportamentos anômalos. Auditorias periódicas são necessárias para verificar a conformidade com os requisitos legais e de segurança. Por fim, é imprescindível que as organizações tenham procedimentos prontos para notificar a ANPD e os titulares afetados de forma célere e transparente, conforme determina o art. 48 da LGPD.

A combinação dessas medidas contribui para a mitigação dos riscos associados ao tratamento de dados biométricos, promovendo a proteção integral dos titulares e a conformidade efetiva com a legislação vigente.

3. Conclusão

Por fim, a Binance reafirma seu compromisso com a proteção dos dados pessoais, especialmente os dados biométricos, reconhecendo sua sensibilidade e os riscos associados ao seu tratamento. Como líder global no setor de criptoativos, a empresa entende que a adoção de práticas seguras, transparentes e proporcionais é essencial para garantir a confiança dos usuários e a integridade do ecossistema digital.

Nesse sentido, a Binance se coloca à disposição para contribuir ativamente na construção de marcos regulatórios sólidos e pertinentes, que conciliem a segurança dos titulares de dados pessoais com a inovação tecnológica e o bom funcionamento do mercado de criptoativos. Acreditamos que a colaboração entre o setor privado, os reguladores e a sociedade são fundamentais para o desenvolvimento de soluções equilibradas, que fortaleçam tanto a proteção de direitos quanto a eficiência e a resiliência do sistema financeiro digital.

Atenciosamente,

OPICE BLUM BRUNO
ADVOGADOS ASSOCIADOS

Brasília, 01 de agosto de 2025.

CONTRIBUIÇÃO BRASSCOM | TOMADA DE SUBSÍDIOS: DADOS PESSOAIS SENSÍVEIS - DADOS BIOMÉTRICOS

ENTIDADE DESTINATÁRIA: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

SUMÁRIO EXECUTIVO

A Lei Geral de Proteção de Dados Pessoais (LGPD) classifica o dado biométrico como dado pessoal sensível, mas não fornece uma definição expressa sobre o que o caracteriza. Referências internacionais, como o GDPR europeu, são importantes fontes de hermenêutica para tal.

Segundo referências internacionais, a identificação de um dado como biométrico exige, cumulativamente, três critérios objetivos:

1. Referência a características físicas, fisiológicas ou comportamentais de uma pessoa natural (ex: voz, impressões digitais, traços faciais);
2. Tratamento técnico específico, com extração, codificação ou conversão dessas características;
3. Finalidade de identificação ou autenticação individual do titular.

Dessa forma, imagens, vídeos, áudios ou dados similares não deveriam ser automaticamente considerados biométricos — apenas se forem tratados de maneira técnica e específica, com finalidade de identificação única. Tecnologias que apenas detectam atributos ou rastreiam usuários de forma anonimizada, como fingerprinting de dispositivos, não se enquadrariam como tratamento de dados sensíveis, exceto quando associadas à identificação pessoal.

A própria ANPD, no Guia sobre Biometria e Reconhecimento Facial, adota entendimento semelhante, alinhado a órgãos como o European Data Protection Board (EDPB) e a Information Commissioner's Office (ICO) do Reino Unido: a categorização como dado sensível depende da finalidade do tratamento e do uso de técnicas que permitam a identificação única do titular.

A imutabilidade relativa, embora não seja critério obrigatório, é um indicativo importante: características como impressão digital ou estrutura facial são mais estáveis que padrões comportamentais, como marcha ou assinatura, que podem variar por contexto.

A biometria comportamental, portanto, não deve ser equiparada à biometria tradicional de forma automática, pois sua confiabilidade e estabilidade são distintas. A aplicação de

Brasscom - Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias Digitais
Rua: Gomes de Carvalho, nº 1629 – Vila Olímpia – SP – CEP: 04547-006 -Caixa Postal: 112147
SHN, Qd. 1, Bl. A, Edifício Le Quartier, Sala 1514 Brasília/DF

uma abordagem excessivamente ampla comprometeria a segurança jurídica e inviabilizaria o uso legítimo e de baixo risco de tecnologias inovadoras, inclusive em áreas sensíveis como saúde, pesquisa e prevenção a fraudes.

Entende-se que a ANPD deveria adotar abordagem técnica e cautelosa, alinhada às boas práticas internacionais, para evitar interpretações excessivamente amplas que comprometam a segurança jurídica e o uso responsável de tecnologias. O reconhecimento de um dado como biométrico deve depender da combinação entre as características intrínsecas, a técnica aplicada e a finalidade do tratamento, garantindo o equilíbrio entre proteção de dados e inovação.

A transparência no tratamento de dados biométricos deve considerar o contexto específico da operação de tratamento, conforme orientações do Information Commissioner's Office (ICO), do Reino Unido. Não há uma fórmula única, sendo necessário ponderar variáveis como o caso de uso, o tipo de relação com o titular e a natureza dos dados tratados. Quanto mais previsível e consolidado o tratamento (como no caso de verificação biométrica em serviços de telefonia), menor a exigência por medidas ativas, bastando mecanismos usuais de aviso, como cláusulas contratuais, QR Codes e informações no ponto de atendimento.

Apesar disso, boas práticas de transparência devem sempre ser observadas, mesmo quando os dados não forem sensíveis, incluindo a explicitação de finalidades específicas, legítimas e compatíveis com os propósitos declarados.

Além disso, vale destacar que a LGPD prevê múltiplas bases legais igualmente válidas para o tratamento de dados pessoais, inclusive os sensíveis, como os biométricos. A escolha da base mais adequada depende do contexto e da finalidade do tratamento, não havendo hierarquia entre elas.

O consentimento pode ser utilizado para o tratamento de dados biométricos, desde que atenda aos requisitos legais de ser livre, informado, inequívoco, específico e destacado. A LGPD não proíbe o condicionamento do serviço à coleta de dados, desde que:

- haja transparência sobre a necessidade do tratamento; e
- não haja desvantagens desproporcionais ou discriminatórias ao titular.

Essa interpretação se alinha ao princípio da autodeterminação informativa, conferindo ao titular o direito de escolher com quais serviços e práticas de tratamento deseja se relacionar, especialmente em um mercado digital competitivo e plural. Assim, o consentimento pode ser considerado válido mesmo que sua recusa implique na indisponibilidade do serviço, desde que este não seja essencial ou obrigatório.

No entanto, o consentimento não será sempre a base legal mais adequada — ou sequer válida —, especialmente em situações onde:

- não há alternativa técnica viável ao uso da biometria;

- há risco de fraude em caso de flexibilização;
- ou a biometria é condição necessária à prestação do serviço (como em pesquisas específicas).

Nesses casos, a LGPD prevê, no art. 11, II, "g", a base legal da prevenção à fraude, que dispensa o consentimento quando o tratamento biométrico é necessário para processos de identificação e autenticação.

Esse fundamento legal reflete uma ponderação entre o direito à privacidade e o interesse coletivo na segurança e estabilidade das relações digitais e econômicas. No Brasil, o elevado número de fraudes — como os 1,24 milhão de tentativas registradas só em janeiro de 2025 — demonstra a relevância prática dessa base, que viabiliza o uso de tecnologias biométricas para proteger tanto os titulares quanto o ecossistema digital.

Comparado ao GDPR europeu, a LGPD é mais avançada por reconhecer expressamente a prevenção à fraude como base legal autônoma. A ausência dessa previsão na Europa tem gerado entraves jurídicos e operacionais para empresas que lidam com autenticação biométrica em ambientes privados.

A base legal da prevenção à fraude deve ser reconhecida como legítima, necessária e proporcional ao tratamento de dados biométricos em diversos contextos, inclusive como alternativa válida ao consentimento. A flexibilidade normativa da LGPD, aliada a salvaguardas técnicas e organizacionais, assegura um equilíbrio entre proteção de direitos, segurança pública e inovação econômica.

No contexto do desenvolvimento e aperfeiçoamento de sistemas de IA, o uso de dados biométricos para o treinamento de modelos voltados à detecção e prevenção de vieses discriminatórios configura medida essencial para a efetividade dos deveres constitucionais e legais de promoção da igualdade. Ao possibilitar que os sistemas reconheçam, mensurem e corrijam distorções decorrentes de recortes raciais, de gênero, idade ou deficiência, o uso técnico e controlado desses dados serve diretamente ao objetivo de evitar tratamentos injustos ou excludentes por parte de sistemas baseados em IA e atendem o interesse público de combate à discriminação.

Esse uso encontra fundamento jurídico sólido na Constituição Federal (arts. 3º, IV e 5º, caput) e em legislações como o Estatuto da Igualdade Racial e o Estatuto da Pessoa com Deficiência, que impõem obrigações específicas para mitigação de desigualdades estruturais. Nessa perspectiva, o tratamento de dados biométricos pode ser legitimamente enquadrado na base legal do art. 11, II, "a" da LGPD — cumprimento de obrigação legal ou regulatória.

O tratamento de dados biométricos de crianças e adolescentes está sujeito a uma análise concreta e contextualizada do princípio do melhor interesse do menor, conforme o art. 14 da LGPD, o ECA e o Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU. Tal avaliação deve ponderar o interesse do menor em conjunto com outros direitos

fundamentais, assegurando margem de atuação para que o controlador demonstre, caso a caso, a legitimidade do tratamento.

De acordo com o Enunciado nº 1/2023 da ANPD, o tratamento pode se basear em qualquer das hipóteses legais previstas nos arts. 7º e 11 da LGPD, desde que respeitado o melhor interesse da criança ou adolescente. Quando adotado o consentimento, ele deve ser inequívoco, informado e transparente para os representantes legais.

Ainda, o cumprimento do princípio da necessidade exige a utilização estritamente limitada aos dados indispensáveis à finalidade legítima. Exemplo internacional relevante é o caso polonês sobre uso de biometria em escolas, no qual o tribunal reconheceu a validade do consentimento e a proporcionalidade do uso, reformando decisão anterior da autoridade de proteção de dados.

Diante do alto potencial lesivo decorrente de eventuais violações de dados biométricos, como o roubo de identidade, é indispensável a adoção de medidas técnicas e administrativas robustas para mitigar esses riscos. O setor de tecnologia tem atuado proativamente nesse sentido, incorporando mecanismos avançados de segurança da informação — como criptografia, segmentação de bases, anonimização, controle de acesso e rastreabilidade — desde as fases iniciais do desenvolvimento de produtos e sistemas. Além disso, muitas empresas já implementam práticas sofisticadas de privacy by design e by default, realizando o tratamento de dados biométricos de forma parametrizada, com o objetivo de identificar padrões ou calibrar sistemas, sem que haja identificação ou reidentificação de uma pessoa natural, o que reduz significativamente os riscos à privacidade.

Para garantir a conformidade com a LGPD, é essencial que as organizações adotem parâmetros mínimos de avaliação contínua de riscos, por meio de relatórios de impacto à proteção de dados (RIPDs) e monitoramento de possíveis vieses ou falhas de segurança. A definição de políticas internas claras, a capacitação de equipes e a governança ativa sobre o ciclo de vida dos dados também são medidas fundamentais para assegurar o tratamento responsável e proporcional desses dados sensíveis. Esse conjunto de ações, já amplamente adotado por empresas do setor, demonstra que é possível conjugar inovação tecnológica com proteção integral dos titulares de dados.

O uso de dados biométricos anonimizados, por sua vez, quando submetido a testes de robustez e medidas técnicas eficazes, deixa de configurar dado pessoal nos termos do art. 12 da LGPD. Isso viabiliza seu uso para fins como treinamento e calibração de modelos de IA, sem que haja necessidade de aplicação das restrições previstas para dados pessoais sensíveis.

BLOCO I - Princípio do melhor interesse

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados

Pessoais (LGPD), especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo “dados biométricos”, mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos - que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) não fornece uma definição expressa do que se entende por “dado biométrico”, limitando-se a incluí-lo como uma das espécies de dado pessoal sensível (art. 5º, II). Diante dessa lacuna conceitual, a adequada interpretação do que constitui dado biométrico exige a conjugação dos critérios previstos na própria LGPD com referências internacionais consolidadas, especialmente o Regulamento Geral sobre a Proteção de Dados (GDPR), bem como posicionamentos de autoridades de proteção de dados estrangeiras e entidades especializadas.

De início, é imprescindível considerar que, nos termos da LGPD, apenas se considera dado pessoal aquele que permite identificar ou tornar identificável uma pessoa natural. Esse critério é fundamental: características corporais ou comportamentais somente serão tratadas como dados pessoais sensíveis quando estiverem associadas, direta ou indiretamente, à identidade do titular.

Nesse sentido, o GDPR, em seu artigo 4º, n.º 14, define dado biométrico como o resultado de um “tratamento técnico específico” aplicado a características físicas, fisiológicas ou comportamentais de um indivíduo com o propósito de

permitir ou confirmar sua identificação única. O considerando 51 reforça que imagens brutas, como fotografias ou vídeos, não são, por si só, dados biométricos, salvo se forem processadas tecnicamente para fins de identificação.

Esse entendimento é corroborado pelo European Data Protection Board (EDPB), que esclarece que o simples registro de imagens não configura, por si só, o tratamento de dados pessoais sensíveis. Isso só ocorre quando essas imagens passam por algoritmos ou técnicas que extraem medidas biométricas — como vetores faciais ou mapas dactiloscópicos — e os utilizam com a finalidade de identificar ou autenticar indivíduos.

Autoridades nacionais europeias têm adotado critérios semelhantes. A Autoridade de Proteção de Dados do Reino Unido (ICO), por exemplo, sustenta que dados biométricos devem (i) referir-se a características físicas, fisiológicas ou comportamentais, (ii) ser objeto de tratamento técnico específico, e (iii) ter como finalidade permitir a identificação única de uma pessoa. A autoridade holandesa segue linha semelhante, dado biométrico é o que (i) diz respeito a características pessoais geralmente permanentes; (ii) resulta de tratamento técnico que compara medidas a uma referência; e (iii) tem como propósito estabelecer ou confirmar a identidade de alguém.

Com base no entendimento da Autoridade de Proteção de Dados do México (INAI), e do art. 16 ter da Lei de Proteção de Dados Chilena, consideram-se dados biométricos aqueles que, cumulativamente, atendem aos seguintes requisitos:

- a) estejam relacionados a características físicas, fisiológicas, comportamentais ou traços de personalidade de um titular de dados; e
- b) resultem de um tratamento específico (em regra, uma forma de medição), cuja finalidade seja identificar, de maneira única, o titular.

Dessa forma, imagens captadas em vídeo, fotografias, gravações de voz ou dados semelhantes não devem ser, isoladamente, considerados dados biométricos. Apenas o resultado do tratamento específico dessas informações que objetive identificar unicamente indivíduos pode ser considerado um dado biométrico.

Além disso, o Future of Privacy Forum (FPF) propõe uma taxonomia útil para distinguir os diferentes usos de dados corporais. A entidade divide esses usos em cinco categorias: detecção, caracterização, rastreamento único e persistente, verificação (1:1) e identificação (1:N). De acordo com essa tipologia, somente as duas últimas envolvem tratamento com capacidade efetiva de

identificação única e, portanto, se enquadram claramente como dados pessoais sensíveis.

Diante disso, é possível extrair três critérios objetivos que devem ser cumulativamente observados para que determinado dado possa ser considerado biométrico à luz da LGPD:

1. Referência a características físicas, fisiológicas ou comportamentais inerentes a uma pessoa natural (por exemplo: impressões digitais, traços faciais, voz, marcha);
2. Submissão a tratamento técnico específico, mediante uso de tecnologias que extraiam, codifiquem ou convertam essas características em medições ou templates;
3. Finalidade de identificação ou autenticação individual, ou seja, o uso do dado com o propósito de permitir ou confirmar quem é o titular.

Logo, não basta que uma tecnologia capture características do corpo humano para que esteja automaticamente tratando dados pessoais sensíveis. A identificação (ou identificabilidade) do titular é elemento indispensável. Tecnologias que apenas detectam presença, inferem atributos sem identificação ou realizam rastreamento anonimizado não devem ser enquadradas, por si só, como tratamento de dados pessoais sensíveis. A técnica de *fingerprinting*, por exemplo, envolve a coleta de várias características de um dispositivo ou navegador, como sistema operacional, versão do navegador, idioma, resolução da tela, plugins instalados e outros detalhes, criando uma "impressão digital" única que pode ser usada para identificar o dispositivo, e não características inerentes ao corpo ou ao comportamento individual da pessoa natural. Ainda que possa, em determinados contextos, contribuir para a singularização de um usuário, a informação extraída refere-se ao dispositivo e não ao titular, o que afasta a natureza biométrica da informação tratada.

O uso dessa técnica em contextos legítimos de prevenção à fraude e segurança da informação, especialmente quando anonimizada ou pseudonimizada, não objetiva a identificação direta do indivíduo, mas sim a detecção de padrões suspeitos de comportamento digital, sendo, portanto, desproporcional o enquadramento como dado sensível. Tal interpretação ampliada poderia comprometer a eficácia de medidas de segurança amplamente utilizadas pelo setor, além de distorcer o equilíbrio normativo proposto pela LGPD entre proteção de dados e inovação tecnológica.

A própria ANPD, em seu Guia de Biometria e Reconhecimento Facial, conceitua a biometria como a análise técnica, realizada por meios matemáticos e estatísticos, das características fisiológicas (tais como impressão digital, face, íris, geometria da mão, vascularização da mão, DNA e voz) ou comportamentais (voz, expressão facial, assinatura, modo de andar etc.) de um indivíduo. Quanto maior a quantidade de dados presentes na amostra biométrica provenientes de uma ou mais características, maior será a probabilidade de que ela tenha uma correspondência única, ou seja, a amostra apresentará maior qualidade para que a análise seja mais precisa e confiável.

Nesse sentido, pertinente esclarecer que a simples coleta de dados que podem revelar informações biométricas não pode ser considerada automaticamente uma atividade de tratamento de dados pessoais sensíveis. É necessária uma justificativa específica, de forma que somente dados utilizados para identificar ou autenticar titulares podem ser considerados biométricos. Além disso, se a informação não for operada por meio técnico que permita a identificação, não será considerada dado biométrico. Esse entendimento alinha-se ao sustentado pela autoridade de proteção de dados do Reino Unido ("ICO"), a qual afirma que os dados biométricos somente serão considerados dados sensíveis quando forem utilizados com a finalidade de identificar uma pessoa de forma única, de modo que a sua categorização dependerá da finalidade do tratamento. Conclui-se, portanto, que o mero tratamento de fotografias, sem a aplicação de técnicas específicas capazes de permitir a identificação inequívoca ou a autenticação de uma pessoa natural, não deve ser considerado, de forma sistemática, como tratamento de dados pessoais sensíveis nos termos do art. 5º, II, da LGPD.

Portanto, sugere-se que a ANPD adote uma abordagem criteriosa e tecnicamente orientada, alinhando-se às boas práticas internacionais, reconhecendo que o conceito de dado biométrico não deve ser aplicado de forma ampla ou imprecisa, mas apenas quando estiverem presentes os três critérios mencionados. Tal postura é essencial para garantir segurança jurídica, evitar distorções interpretativas e permitir o uso responsável de tecnologias que operam com dados corporais, mas que não necessariamente expõem os titulares a riscos relevantes de identificação.

No contexto de empresas que atuam como operadoras, como é o caso de empresas que disponibilizam sistemas com funcionalidades de autenticação biométrica a outras empresas, é essencial reconhecer que a caracterização do dado como dado pessoal sensível dependerá da forma como o controlador irá definir o tratamento. A empresa operadora, embora seja responsável por garantir padrões técnicos e de segurança da informação, não define a finalidade, base legal ou escopo do tratamento. Assim, é necessário que a regulamentação da ANPD reconheça que a análise da sensibilidade dos dados deve considerar o

papel desempenhado pelo operador que o enquadramento como dado biométrico requer a combinação da técnica aplicada com a finalidade determinada pelo controlador.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Conforme a Autoridade de Dados do Reino Unido (ICO), não existe metodologia única aplicável a todos os casos sobre como a transparência pode ser garantida, incluindo medidas ativas a serem adotadas pelos controladores. A forma mais eficiente de transparecer o uso de dados biométricos ao titular deverá ponderar fatores, como: i) o caso de uso; ii) a natureza de relacionamento com o titular; e iii) os dados envolvidos na atividade de tratamento.

Nesse sentido, quanto mais óbvia a atividade de tratamento em análise, considerando as práticas habituais de mercado e a natureza do relacionamento com o titular, menor a exigência de práticas ativas de transparência.

Quando o tratamento de dados pessoais ocorre no contexto da validação da identidade do titular, durante a contratação ou utilização de produto ou serviço — por exemplo, a verificação biométrica no processo de contratação ou portabilidade de plano de telefonia. Trata-se de prática consolidada no mercado, em que a coleta de dados biométricos é clara e previsível para o titular, inclusive devido à: (i) existência de regulamentações que requerem que empresas de telefonia adotem mecanismos de prevenção a fraudes, como o art. 65-M, da Resolução ANATEL 738/2020; e (ii) o fato de que fraudes no acesso às linhas de telefone dos usuários podem servir de ponto de partida para a realização de novas práticas criminosas, incluindo a obtenção de contas de e-mail, a estes vinculadas enquanto mecanismos de recuperação de senhas, e, a partir destas, contas de diversos serviços em que o titular está inscrito. Nesses casos, o fornecimento do Aviso de Privacidade ao longo da jornada do usuário, nos termos de seu contrato de prestação de serviço ou, no caso de atendimento presencial, por meio de QR Codes disponibilizados em telas, cartazes ou materiais similares dentro do local físico, ou mesmo breve explicação pelo atendente, é suficiente para assegurar o atendimento do dever de transparência.

De qualquer forma, as boas práticas de transparência devem balizar todo e qualquer tratamento de dados, independentemente do dado ser caracterizado como dado pessoal sensível, como é o caso do dado biométrico. Dessa forma, medidas que garantam, aos titulares, o acesso de informações claras e precisas acerca da realização do tratamento de dados, informando a finalidade dos

respectivos tratamentos, mediante indicação de propósitos legítimos, específicos e explícitos, bem como a limitação do tratamento de dados de forma incompatível com as finalidades determinadas são referência de boas práticas no que tange à transparência.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Como abordado na resposta nº 1, a LGPD não apresenta definição específica para “dado biométrico”, limitando-se a classificá-lo como uma categoria de dado pessoal sensível. Nesse contexto, a caracterização de um dado como biométrico exige uma análise baseada em critérios objetivos que levem em conta a finalidade e a forma de tratamento do dado. De acordo com a própria LGPD, um dado só será considerado pessoal se puder tornar o titular identificado ou identificável. Essa premissa é essencial para o enquadramento dos dados biométricos, pois apenas informações capazes de individualizar o titular podem ser qualificadas como tal.

Dessa forma, dados que possam conter características biométricas, sejam elas imagens captadas em vídeo, fotografias ou gravações de voz, não devem ser, isoladamente, considerados dados biométricos ou mesmo dados pessoais sensíveis, nos termos da LGPD. Se uma fotografia, por exemplo, for empregada para treinar um modelo de IA com o objetivo de aprimorar funcionalidades gerais — como detecção de objetos, identificação de padrões de métrica facial, ou classificação de imagens — sem a intenção de identificar ou autenticar uma pessoa natural de forma individualizada, não há que se falar em tratamento de dado pessoal sensível.

A interpretação conforme a LGPD deve se apoiar na finalidade específica e concreta do tratamento, conforme preceitua o princípio da necessidade (art. 6º, III) e da finalidade (art. 6º, I). A mera possibilidade teórica de que um dado possa vir a ser utilizado para identificação não é suficiente para que se imponha, de forma automática, o regime jurídico mais rigoroso aplicável aos dados sensíveis. Essa interpretação extensiva — e, portanto, desproporcional — comprometeria a segurança jurídica e inviabilizaria aplicações legítimas e de baixo risco da IA, inclusive em setores como pesquisa, saúde, educação e prevenção de fraudes.

Além disso, a Brasscom entende que a biometria comportamental não deve ser automaticamente equiparada à biometria tradicional apenas por estar vinculada

ao corpo humano. Dessa forma, enquanto a biometria tradicional se baseia em características físicas relativamente estáveis e imutáveis (como digitais, íris ou estrutura facial), a biometria comportamental envolve padrões que podem variar significativamente conforme o contexto. Por exemplo, a forma de caminhar de uma pessoa pode se modificar se ela sofrer uma lesão, passar por treinamento militar ou envelhecer. O mesmo se aplica a padrões de digitação, ritmo de voz ou movimento ocular. Tais variabilidades impactam diretamente a exatidão e confiabilidade desses dados, e devem ser levadas em conta na aplicação dos princípios da qualidade e da segurança.

Para suprir a ausência de definição legal no Brasil, o conceito adotado pelo Regulamento Europeu de Proteção de Dados (GDPR) serve como importante referência. Segundo o art. 4.14 do GDPR, dado biométrico é o resultado de tratamento técnico específico aplicado a características físicas, fisiológicas ou comportamentais de uma pessoa natural, com o objetivo de permitir ou confirmar sua identificação única.

O Information Commissioner's Office (ICO), autoridade britânica de proteção de dados, reforça essa definição ao estabelecer que apenas são considerados dados biométricos os que:

- (i) se referem a características físicas, fisiológicas ou comportamentais;
- (ii) foram submetidos a tratamento técnico específico, como extração e codificação; e
- (iii) têm como finalidade identificar ou autenticar uma pessoa de forma única.

Aplicando esses critérios aos dados biométricos comportamentais, como dinâmica de digitação, assinatura manuscrita, padrão de marcha ou entonação vocal, conclui-se que a mera coleta ou análise desses comportamentos não é suficiente para que se caracterizem como dados biométricos. Conforme o ICO, apenas quando essas informações são submetidas a algoritmos que as codificam em formatos técnicos específicos — como vetores ou templates — para fins de identificação ou autenticação individual, é que se poderá falar em dados pessoais sensíveis.

Outro elemento importante para essa análise é o conceito de imutabilidade relativa, abordado pelo European Parliamentary Research Service (EPRS). Segundo o estudo, o termo "biométrico" pressupõe certo grau de permanência: trata-se de características que o indivíduo não pode modificar voluntariamente, como o rosto ou a impressão digital. Por isso, técnicas que analisam gestos, assinatura, voz ou marcha — apesar de envolverem comportamento — podem ser consideradas biométricas, pois se baseiam em padrões corporais relativamente constantes. Em contrapartida, comportamentos voluntários e

amplamente modificáveis, como preferências de navegação, hábitos de consumo ou conteúdo de comunicação, não se enquadram como dados biométricos, por não refletirem uma característica física ou comportamental estável e intrínseca ao corpo da pessoa.

Diante disso, para que um dado comportamental seja considerado dado pessoal sensível nos termos da LGPD, é necessário que preencha três requisitos cumulativos:

1. Referência a uma característica física, fisiológica ou comportamental do indivíduo;
2. Tratamento técnico específico, com extração, conversão ou codificação por meio de algoritmos;
3. Finalidade de identificação ou autenticação única do titular, permitindo sua distinção individual em sistemas de verificação (1:1) ou identificação (1:N).

A presença de imutabilidade relativa serve como indicativo complementar relevante, embora não exclusivo, para a classificação do dado como biométrico.

Em síntese, a simples natureza comportamental do dado não é suficiente para enquadrá-lo automaticamente como dado pessoal sensível. É imprescindível avaliar o modo de tratamento técnico e a finalidade de uso. Essa abordagem evita uma interpretação excessivamente ampla e desproporcional da categoria de dados biométricos, e assegura um equilíbrio entre proteção de direitos e inovação tecnológica, em consonância com os princípios da LGPD.

Nos casos em que a biometria comportamental é utilizada por meio de soluções de autenticação embarcadas em softwares comercializados, é fundamental que a categorização do dado como biométrico considere a finalidade determinada pelo controlador. O operador pode realizar o tratamento técnico (como extração, processamento e codificação), mas não necessariamente define o propósito do uso, tampouco se os dados tratados serão utilizados para identificação única ou apenas como fator comportamental complementar.

BLOCO II – HIPÓTESES LEGAIS

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Antes de se responder de maneira direta, cumpre lembrar que existem diversas bases legais previstas na LGPD, e a mais apropriada dependerá do contexto específico, não havendo nenhum tipo de hierarquização entre elas, isto é, todas as hipóteses previstas são igualmente válidas e podem ser utilizadas sem haver a necessidade de se priorizar uma em detrimento de outras.

Para que o consentimento para o tratamento de dados biométricos seja considerado livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD, é fundamental que o titular tenha clareza sobre a finalidade do tratamento, compreenda suas implicações e possa manifestar sua vontade de forma autônoma, sem coerção ou engano.

A exigência de que o consentimento seja livre não implica, necessariamente, a ausência de qualquer condicionamento. O que a LGPD veda é a coação, a ausência de transparência ou a imposição de desvantagens excessivas ao titular. A simples oferta de um serviço vinculada ao tratamento de dados pessoais — inclusive biométricos — não invalida, por si só, o consentimento. A simples oferta de um serviço em troca do consentimento não o invalida, desde que:

- Haja transparência quanto à necessidade dos dados para a prestação do serviço; e

- O titular não seja compelido a consentir sob pena de sofrer desvantagens desproporcionais ou discriminatórias.

Importante reconhecer que o titular de dados pessoais detém a liberdade de determinar quais serviços deseja utilizar, podendo consentir ou não com o tratamento de seus dados, com base nas informações claras e suficientes que lhe forem apresentadas pelos agentes de tratamento. Tal premissa é a essência do princípio da autodeterminação informativa que norteia a estrutura de proteção de dados pessoais no Brasil. O ecossistema digital, caracterizado por elevada dinamicidade, competitividade e pluralidade de soluções, confere ao titular meios concretos para exercer essa autodeterminação informativa, optando por serviços que melhor se alinhem às suas preferências e expectativas. Assim, o consentimento pode ser livre, mesmo quando sua negativa resulte na indisponibilidade de determinado serviço, desde que não se trate de serviço essencial ou de acesso obrigatório.

Diante da relevância do consentimento como base legal no tratamento de dados pessoais sensíveis, é fundamental que a ANPD reconheça, em suas orientações e interpretações normativas, as nuances e particularidades envolvidas na aferição do consentimento livre, especialmente no contexto da economia digital. Tal reconhecimento é essencial para evitar abordagens excessivamente restritivas que possam comprometer a viabilidade jurídica e econômica de modelos de negócio legítimos, amplamente utilizados na oferta de serviços digitais. Ao considerar a liberdade do titular em escolher, com base em informações claras, quais serviços deseja utilizar e com quais práticas de tratamento de dados concorda, a ANPD contribuirá para a consolidação de um ambiente regulatório equilibrado, que simultaneamente protege os direitos dos titulares e garante a sustentabilidade da inovação e da competitividade no ambiente digital brasileiro.

De fato, há casos em que o consentimento não será a base legal mais adequada - e mesmo a efetivamente correta - para o tratamento de dados pessoais sensíveis, razão pela qual o art. 11, em seu inciso II, traz outras hipóteses nas quais o tratamento do dado biométrico dispensa o consentimento. Nesse sentido, destaca-se a alínea "g", a qual prevê expressamente a dispensa do consentimento para garantia da prevenção à fraude em processos de identificação e autenticação de cadastro. Nota-se, portanto, que o referido tratamento tem por finalidade proteger a segurança do próprio titular do dado contra usos indevidos de sua identidade. Nesse mesmo contexto, a exigência do consentimento poderia inviabilizar mecanismos de segurança automatizados, como as autenticações por reconhecimento facial ou impressão digital.

O consentimento não será a base legal adequada nas situações em que os requisitos de validade não podem ser satisfeitos, tipicamente isso transcorrerá em situações como quando não for viável oferecer alternativa à biometria facial ao titular de dados. **Por exemplo, em processos de prevenção a fraudes, nos quais eventual opção poderia facilitar a atuação de fraudadores, ou nos casos em que a biometria é essencial para a prestação do serviço ou funcionamento do produto.** Essa hipótese admite exceção quando não houver outra base legal aplicável e a ausência de consentimento tornar inviável o prosseguimento do tratamento biométrico - nesses casos, o prejuízo decorrente da negativa do titular é consequência necessária da própria impossibilidade de realizar a atividade. Por exemplo, se o titular deseja participar (com ou sem remuneração) de pesquisa conduzida por ente privado com fins lucrativos que envolva o uso de dados biométricos, a continuidade da participação estará legitimamente condicionada à oferta do consentimento, já que o tratamento dos dados é imprescindível para a execução da pesquisa.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A utilização de dados biométricos com a finalidade de prevenção à fraude deve ser analisada à luz da LGPD a partir de uma ponderação entre os direitos fundamentais à privacidade e à proteção de dados, de um lado, e o interesse coletivo na segurança, na estabilidade econômica e na prevenção de ilícitos, de outro. Trata-se de uma típica aplicação do princípio da proporcionalidade, que exige a verificação da adequação, necessidade e proporcionalidade em sentido estrito da medida. No contexto brasileiro, marcado por altos índices de fraudes bancárias, golpes digitais e uso indevido de identidades falsas, o tratamento de dados biométricos para fins de autenticação representa, muitas vezes, a medida mais segura, eficaz e menos invasiva disponível para proteger os usuários e o sistema financeiro como um todo - contexto que faz com que a base legal de prevenção à fraude seja extremamente relevante.

Vale mencionar que, de acordo com a Serasa, somente em janeiro de 2025, foram registradas 1,24 milhão de tentativas de fraude no Brasil, um aumento de 41,6% em relação ao ano anterior – o equivalente a uma tentativa de golpe a

cada 2,2 segundos. Dados da Serasa Experian mostram que em 2024 as tentativas de fraude contra bancos e cartões cresceram 10,4% em relação a 2023, representando 53,4% de todas as fraudes registradas no ano. Se não tivessem sido evitadas, graças ao uso de mecanismos de autenticação de usuário, essas fraudes poderiam ter causado um prejuízo estimado em R\$ 51,6 bilhões.

Sendo assim, a base legal da prevenção à fraude, prevista expressamente no art. 11, II, "g", da LGPD, reflete esse equilíbrio e representa um avanço normativo em comparação ao GDPR europeu, que não contempla essa hipótese de forma específica. A ausência dessa base legal na legislação europeia tem gerado dificuldades práticas, levando empresas a depender de hipóteses frágeis como o consentimento — que, em muitos casos, não se revela uma base jurídica adequada, especialmente quando há desequilíbrio entre controlador e titular ou impossibilidade de negativa real. A própria EDPB (European Data Protection Board) já reconheceu os obstáculos criados por essa lacuna normativa para o uso de biometria em contextos privados de prevenção à fraude.

No Brasil, o reconhecimento legal da prevenção à fraude como hipótese legítima para o tratamento de dados sensíveis deve ser interpretado como uma expressão dos princípios constitucionais da segurança jurídica e da ordem econômica (CF, art. 170), além de compatível com o princípio da necessidade previsto na LGPD. A utilização da biometria, desde que acompanhada de salvaguardas técnicas e organizacionais adequadas — como minimização de dados, medidas de segurança robustas, governança e avaliação de impacto —, é não apenas proporcional, mas socialmente desejável. Além de proteger o titular, a biometria pode atuar como mecanismo de inclusão digital e potencializar o exercício de direitos fundamentais por parte dos titulares, permitindo o acesso seguro a serviços essenciais, por exemplo.

Portanto, diante da realidade nacional e da necessidade de proteção contra ameaças sistêmicas, o tratamento de dados biométricos para fins de prevenção à fraude deve ser reconhecido como legítimo, necessário e proporcional, dentro de uma leitura equilibrada da LGPD que assegure tanto os direitos individuais quanto a segurança das relações sociais e econômicas.

Conforme Guia sobre o Legítimo Interesse da ANPD, os requisitos para o enquadramento do tratamento de dados biométricos na base legal de "prevenção à fraude" são semelhantes aos aplicáveis ao legítimo interesse. Nesse sentido, são aplicáveis os mesmos critérios do Teste de Balanceamento para enquadramento no "legítimo interesse", ressalvada a proibição de tratamento de dados pessoais sensíveis.

Isso não implica dizer que a realização prévia de Teste de Balanceamento (“LIA”) seja medida obrigatória para garantir a licitude da atividade, pois inexistente obrigação legal nesse sentido. Assim, o Teste de Balanceamento auxilia a organização a demonstrar o enquadramento na base legal, mas sua ausência, por si só, não implica em ilicitude da atividade de tratamento – o que requererá demonstração concreta de ausência de atendimento dos requisitos mínimos.

Assim, o Teste de Balanceamento auxilia a organização a demonstrar o enquadramento na base legal, mas sua ausência, por si só, não implica em ilicitude da atividade de tratamento – o que requererá demonstração concreta de ausência de atendimento dos requisitos mínimos.

No setor de telecomunicações, por exemplo, o uso de dados biométricos é, em regra, legítimo com base no art. 11, II, “g”, da LGPD. Essa prática encontra respaldo nas condutas usualmente adotadas pelo mercado e se justifica não apenas pela prevenção a fraudes no acesso aos serviços de telecomunicações, mas também pela necessidade de proteger a segurança de diversos serviços da sociedade da informação acessados por esses canais.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

No contexto do desenvolvimento e aperfeiçoamento de sistemas de IA, o uso de dados biométricos para o treinamento de modelos voltados à detecção e prevenção de vieses discriminatórios configura medida essencial para a efetividade dos deveres constitucionais e legais de promoção da igualdade. Ao possibilitar que os sistemas reconheçam, mensurem e corrijam distorções decorrentes de recortes raciais, de gênero, idade ou deficiência, o uso técnico e controlado desses dados serve diretamente ao objetivo de evitar tratamentos injustos ou excludentes por parte de sistemas baseados em IA e atendem o interesse público de combate à discriminação.

Tal prática encontra respaldo normativo na Constituição Federal, que consagra o princípio da igualdade (art. 5º, caput) e impõe como objetivo fundamental da República Federativa do Brasil a promoção do bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (art. 3º, IV). Do mesmo modo, diversas normas infraconstitucionais — como o Estatuto da Igualdade Racial (Lei nº 12.288/2010) e o Estatuto da Pessoa com Deficiência (Lei nº 13.146/2015) — impõem obrigações concretas ao poder

público e aos entes privados para adotar medidas que previnam e combatam a discriminação estrutural em diferentes esferas da vida social.

Nesse cenário, o tratamento de dados biométricos com a finalidade de garantir que modelos de IA se comportem de forma ética e não discriminatória deve ser interpretado como um instrumento de cumprimento de obrigação legal ou regulatória, em consonância com os princípios da finalidade, da boa-fé, da responsabilidade e da prestação de contas previstos na LGPD.

No mesmo sentido do item anterior, entende-se que a adequada aplicação da hipótese legal do cumprimento de obrigação legal ou regulatória pressupõe o atingimento de requisitos de segurança e da aplicação de princípios balizadores do tratamento de dados pessoais de forma geral, não apenas ao tratamento de dados sensíveis. Na ótica de segurança, vislumbra-se a implementação de técnicas de proteção, tais quais medidas de rastreamento e monitoramento, controle de acesso, registro das operações de tratamento.

No que tange o princípio da necessidade, observam-se medidas que visem à utilização dos dados biométricos apenas de forma estritamente necessária para o atingimento da finalidade, atentando-se para a disponibilização de informação aos titulares acerca da finalidade do tratamento, de forma clara, precisa e facilmente acessível. Dessa forma, a adequada aplicação da hipótese legal de "cumprimento de obrigação legal ou regulatória" prevista no artigo 11, II, "a" da LGPD, pressupõe a observância dos princípios da necessidade e finalidade e implementando boas práticas de governança e segurança da informação, com o objetivo de prover medidas de controle e rastreabilidade, bem como de proteção dos dados biométricos.

Em relação às salvaguardas a serem adotadas para mitigação de riscos, entendemos que devem ser as mesmas aplicáveis aos agentes de tratamento que utilizam a base legal de "prevenção à fraude". Isso porque as medidas de proteção de dados devem ser proporcionais aos riscos envolvidos, independentemente da base legal utilizada para justificar o tratamento. Assim, os controles e as salvaguardas adequados para mitigar os riscos decorrentes do uso de dados biométricos permanecem os mesmos, seja a base legal "prevenção à fraude", "cumprimento de obrigação legal" ou outra prevista na LGPD.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, "c", LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais

salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Nesse sentido, é importante esclarecer que o dado anonimizado se caracteriza pelo dado que não é capaz de permitir da reidentificação posterior. Corrobora esse entendimento o conceito de dado anonimizado previsto no art. 5º, III da LGPD. Diante desse cenário, em caso de uso de dados anonimizados, medidas técnicas de anonimização, bem como a aplicação de testes de robustez para validar se o dado está efetivamente anonimizado, conforme recomenda a ANPD em Guia de Boas Práticas de Anonimização e Pseudoanonimização, podem ser consideradas como salvaguardas para garantir a eficácia do processo de anonimização do dado. Uma vez garantido o processo de anonimização, referido dado não é considerado como dado pessoal, em conformidade com o art. 12º da LGPD, tendo em vista que não é possível identificar o titular. Consequentemente, portanto, o dado deixa de figurar como dado pessoal.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

A utilização das tecnologias de reconhecimento facial (Facial Recognition Technologies, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento.

Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

É importante reconhecer que, em determinados contextos, como a prevenção à fraude no sistema financeiro ou em serviços digitais, o uso de tecnologias de reconhecimento facial pode ser não apenas legítimo, mas essencial para proteger direitos de usuários e garantir a integridade das operações. Nesses casos, o reconhecimento facial pode ser a única ferramenta viável para evitar fraudes de identidade e acessos indevidos, desde que seu uso seja proporcional à gravidade do risco e cercado de salvaguardas adequadas.

Ainda assim, a proteção contra riscos à privacidade e à dignidade dos titulares permanece central. O princípio da necessidade exige que o uso dessa tecnologia se restrinja ao mínimo indispensável para atingir a finalidade de prevenção à fraude, sem derivações para outras finalidades não autorizadas. Já a proporcionalidade demanda uma avaliação clara de que os benefícios, especialmente em termos de interesse coletivo na segurança, na estabilidade econômica e na prevenção de ilícitos, superam os impactos aos direitos dos titulares. A transparência, por sua vez, impõe o dever de informar de forma clara sobre a coleta, uso e retenção desses dados, garantindo o exercício dos direitos previstos na LGPD.

Em síntese, o reconhecimento facial pode desempenhar um papel legítimo e relevante na prevenção à fraude, desde que seu uso seja cuidadosamente balizado por critérios técnicos, jurídicos e éticos que garantam a proteção dos direitos fundamentais e evitem abusos.

Nos casos em que o reconhecimento facial é oferecido como funcionalidade técnica por software, é imprescindível reconhecer que a conformidade com os princípios da LGPD depende não apenas das capacidades da tecnologia, mas também da forma como o controlador a configurar e utilizar. O operador é

responsável por salvaguardas técnicas, porém não detém ingerência sobre a definição da base legal, da finalidade específica ou da proporcionalidade do uso em contextos concretos.

No que tange ao atingimento do princípio da necessidade e da proporcionalidade, tem-se como alternativa a análise da indispensabilidade do reconhecimento facial. Ou seja, avaliação se o reconhecimento facial é a forma mais adequada e, caso seja, medidas minimizem o uso irrestrito do reconhecimento. Nessa ótica, ressalta-se que, para a finalidade de prevenção à fraude, o reconhecimento facial destaca-se como uma tecnologia de suma importância no contexto de proteção do titular. Ao usar dados biométricos únicos, a tecnologia mitiga consideravelmente a ocorrência de acessos indevidos, falsificações e usos fraudulentos de informações pessoais. O reconhecimento facial, portanto, é um recurso que fortalece mecanismos de autenticação, contribuindo significativamente para a proteção dos dados e integridade das operações.

Na ótica do princípio da transparência, é necessário garantir que o titular tenha ciência do tratamento de reconhecimento facial, disponibilizando informações acerca da finalidade deste reconhecimento. No aspecto técnico, medidas de mitigação de vieses e testes de acurácia utilizando uma base ampla e diversificada contribuem para evitar situações de discriminação ilícita ou abusiva. Na visão jurídica, entende-se como mitigador a correta identificação da base legal amparada pelo atingimento dos princípios acima observados. No que tange à visão institucional, as medidas de monitoramento, controle de acesso e rastreamento do tratamento dos dados, conforme já explicitado, visam contribuir com os riscos mapeados neste item.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Os sistemas de reconhecimento facial devem ser concebidos e implementados desde sua origem com base no princípio do *privacy by design*, adotando salvaguardas técnicas e organizacionais que garantam alta acurácia e minimizem riscos aos direitos dos titulares. Para garantir eficácia e confiabilidade, é essencial que esses sistemas sejam treinados com bases de dados amplas, diversificadas e representativas da população, a fim de reduzir

vieses e minimizar erros de identificação, como falsos positivos (identificação incorreta) e falsos negativos (falha na identificação de quem deveria ser reconhecido).

O tratamento de dados biométricos que não permitem a identificação de uma pessoa natural — ou seja, que não configuram dados pessoais nos termos da LGPD — é essencial para o treinamento e aprimoramento de sistemas de reconhecimento facial. Esses dados, quando anonimizados ou utilizados de forma a não tornar possível a reidentificação do titular, são indispensáveis para garantir a eficácia, a equidade e a acurácia desses sistemas, especialmente na redução de vieses e na melhoria da performance técnica dos algoritmos. Diante disso, é fundamental que a ANPD reconheça expressamente essa premissa, conferindo segurança jurídica para o desenvolvimento tecnológico responsável e compatível com os princípios da proteção de dados, sem impor restrições desproporcionais ao uso de informações que não configuram dados pessoais.

Os sistemas de reconhecimento facial devem ser projetados com base nos princípios de privacy by design e privacy by default, incorporando, desde a fase de concepção, medidas técnicas e organizacionais voltadas à precisão, segurança e mitigação de riscos. A utilização de algoritmos robustos e continuamente testados em bases de dados diversificadas é essencial para reduzir a incidência de erros de identificação, como falsos positivos e falsos negativos, especialmente considerando a variabilidade de características demográficas. Adicionalmente, destaca-se a implementação de mecanismos de monitoramento contínuo do desempenho do sistema e rotinas de atualização e revalidação dos modelos utilizados.

No contexto de empresas que atuam como operadoras, é importante destacar que diversos aspectos relacionados à forma de coleta, parametrização e uso dos dados podem ser definidos ou ajustados pelos controladores, de acordo com o ambiente e a finalidade do tratamento. Dessa forma, cabe ao controlador assegurar que tais ajustes estejam alinhados aos princípios da LGPD, considerando os riscos da operação.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

O reconhecimento facial não será mecanismo apropriado quando existirem meios adequados e proporcionais para se alcançar o mesmo resultado sem uso dessa tecnologia, especialmente se houver forma de tratamento menos intrusiva e capaz de atender à finalidade pretendida, inclusive outras formas de autenticação biométrica. Em outras palavras, o reconhecimento facial deve ser evitado sempre que métodos alternativos possam garantir nível de identificação equivalente, ou minimamente suficiente diante dos riscos envolvidos.

Por exemplo, podemos citar algumas soluções alternativas para auxiliar na verificação da identidade do titular:

- Soluções de prevenção a fraudes baseadas em dados para verificar se o número de telefone e outras informações de contato coincidem com as informações apresentadas pelo titular no momento de registro junto à empresa, confirmar se a localização de uma transação corresponde à localização do dispositivo do titular e identificar indícios de práticas fraudulentas, como o SIM Swap.
- Utilização de tecnologias de captação e transmissão de voz para desenvolver formas de verificação da identidade baseadas em validação biométrica da voz – as quais podem ser consideradas menos intrusivas do que a biometria facial, vez que tende a permitir a inferência de menos dados pessoais sensíveis (como dados de saúde ou etnia) do que a biometria facial.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

O tratamento de dados biométricos exige uma abordagem cautelosa e estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras

sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos.

Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes.

Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados.

Com base nisso, questiona-se:

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Diante do alto potencial lesivo decorrente de eventuais violações de dados biométricos, como o roubo de identidade, é indispensável a adoção de medidas técnicas e administrativas robustas para mitigar esses riscos. O setor de tecnologia tem atuado proativamente nesse sentido, incorporando mecanismos avançados de segurança da informação — como criptografia, segmentação de bases, anonimização, controle de acesso e rastreabilidade — desde as fases iniciais do desenvolvimento de produtos e sistemas. Além disso, muitas empresas já implementam práticas sofisticadas de privacy by design e by default, realizando o tratamento de dados biométricos de forma parametrizada, com o objetivo de identificar padrões ou calibrar sistemas, sem que haja identificação ou reidentificação de uma pessoa natural, o que reduz significativamente os riscos à privacidade.

Para garantir a conformidade com a LGPD, é essencial que as organizações adotem parâmetros mínimos de avaliação contínua de riscos, por meio de relatórios de impacto à proteção de dados (RIPDs) e monitoramento de possíveis vieses ou falhas de segurança. A definição de políticas internas claras, a capacitação de equipes e a governança ativa sobre o ciclo de vida dos dados também são medidas fundamentais para assegurar o tratamento responsável e proporcional desses dados sensíveis. Esse conjunto de ações, já amplamente adotado por empresas do setor, demonstra que é possível conjugar inovação tecnológica com proteção integral dos titulares de dados. Alguns parâmetros básicos são:

- a) Definir critério de riscos: estabelecer, com base no apetite de risco organizacional, as regras e os parâmetros para aceitação de riscos;
- b) Identificar os Riscos: contemplando identificar os(as): i) ativos envolvidos; ii) ameaças potenciais a esses ativos; iii) controles existentes; e iv) vulnerabilidades.
- c) Analisar os riscos: identificar os potenciais consequências decorrentes da concretização dos riscos e a probabilidade de sua ocorrência, definindo, por meio de ambos os elementos, o nível do risco.
- d) Tomar decisão: avaliar, de acordo com o critério de riscos, se ele é aceitável e tomar uma decisão – isto é, modificar (mitigar), reter (aceitar), compartilhar ou evitar (elimina) o risco.
- e) Monitoramento: é necessário que os elementos que compuseram a identificação do risco sejam monitorados, para que, em caso de sua

modificação (por exemplo, o surgimento de nova ameaça) os efeitos desta alteração sejam computados na análise do risco.

É de suma importância que os controladores do tratamento dos dados biométricos adotem medidas técnicas e administrativas robustas, entre as quais destacam-se:

- Programa de Segurança da Informação: implementação de medidas de segurança contra qualquer ameaça ao Tratamento dos dados Pessoais;
- Gestão de Acesso: estabelecimento de padrões de controle sobre o Tratamento dos Dados Pessoais com responsabilidades definidas e gestão de acesso tanto de colaboradores quanto de prestadores de serviços, bem como o estabelecimento de mecanismos de autenticação de acesso aos Dados Pessoais;
- Relatório de Tratamento dos Dados Pessoais: manter o registro detalhado de todo o tratamento realizado, como informações quanto ao momento, a duração, a identidade do representante responsável pelo tratamento designado pelas partes e os dados pessoais tratados, inclusive quando tal tratamento é feito para cumprimento de obrigações legais ou determinações por parte de autoridades; e,
- Inviolabilidade dos Dados Pessoais: uso de soluções de gestão dos registros do Tratamento por meio de técnicas que garantam a inviolabilidade dos dados pessoais, como encriptação ou medidas de proteção equivalentes.
- Elaboração de Relatório de impacto DPIA/LIA, quando aplicável.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Para evitar que a exigência de autenticação biométrica em serviços não essenciais configure discriminação ilícita ou prática abusiva, é fundamental que o tratamento desses dados observe os princípios da LGPD bem como esteja devidamente enquadrado em uma das bases legais autorizativas para o tratamento, em especial, da necessidade, não discriminação e transparência, como todo e qualquer tratamento de dados deve observar.

Na situação em que o tratamento do dado biométrico é amparado no consentimento, o titular deve ter garantido o direito ao opt-out, de forma simples, acessível e sem que isso implique em restrições desproporcionais do serviço. A limitação de funcionalidades pode ser considerada legítima, entretanto, quando houver justificativa técnica concreta para sua implementação. Nessa ocasião, tal limitação deve ser previamente comunicada de forma clara e transparente.

Entendemos que a recusa em fornecer a biometria implicaria em exercício de fato do direito de oposição. Consequentemente, o não oferecimento da funcionalidade, serviço ou produto resguardado pelo acesso biométrico será lícito se uma das seguintes condições for satisfeita: (a) não seja faticamente possível ofertar a funcionalidade sem o tratamento de dados biométricos, aplicando-se aqui o mesmo descrito quanto ao consentimento; ou (b) os direitos e interesses protegidos ao se exigir a biometria não sejam sobrepujados pelo direito do titular de não a ofertar – isto é, existe razão pela qual a validação biométrica é necessária, como a existência de bem protegido relevante – é o caso típico dos serviços de telecomunicação, cuja fraude, nos termos já vistos, são comumente meio para condutas criminosas significativamente mais lesivas, para o titular afetado ou para a sociedade globalmente considerada – seja obtendo indevidamente a linha do titular para obter acesso a outros bens e serviços vinculados a ela, inclusive serviços bancários, seja se utilizando da linha fraudulentamente obtida para a práticas de crimes, incluindo fraudes movidas a engenharia social.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

A proteção eficaz no tratamento de dados biométricos exige adoção de boas práticas voltadas à transparência, necessidade e mitigação de riscos discriminatórios. Entre essas práticas, destacam-se:

- Treinamento e Capacitação: oferecer treinamento específico quanto ao tema;
- Políticas e Procedimentos: reforçar as informações de forma detalhada sobre como deve ser realizado o tratamento de dados para essa categoria de dados;
- Relatório de Impacto à Proteção de Dados Pessoais (DPIA), quando aplicável.

Em relação às medidas de transparência, a obrigatoriedade legal se refere ao fornecimento das informações previstas no art. 9º, da LGPD. A forma adequada de disponibilização dessas informações, conforme indicado nos questionamentos nºs 2 e 8, com base no posicionamento do ICO, dependerá de uma série de fatores – como o caso de uso, a natureza do relacionamento com o titular e os elementos envolvidos na atividade de tratamento. Em síntese, quanto mais evidente for a atividade de tratamento analisada – considerando, inclusive, as práticas habituais de mercado e obrigações regulatórias –, menor será a exigência de adoção de práticas ativas de transparência para o fornecimento das informações legalmente requeridas ao titular. A título exemplificativo, dadas as obrigações regulatórias que atingem o setor de telecomunicações, as práticas habituais de mercado e os riscos já abordados relacionados a ocorrência de fraudes no setor e a própria divulgação do uso de biometria facial no setor pela própria ANATEL, entendemos que a disponibilização do Aviso de Privacidade é suficiente para atender às obrigações regulatórias em proteção de dados.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

-

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não

possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Os agentes de tratamento, especialmente no setor de tecnologia, têm avançado significativamente na implementação de práticas que asseguram o respeito aos direitos dos titulares, inclusive em contextos complexos como o tratamento automatizado de dados biométricos. Empresas de tecnologia vêm adotando medidas técnicas e organizacionais que facilitam o exercício dos direitos previstos na LGPD — como o direito à informação clara, ao acesso, à correção de dados e à revogação do consentimento — por meio de interfaces amigáveis, políticas de privacidade mais acessíveis e canais digitais eficientes de atendimento ao titular.

Além disso, o setor tem investido em soluções inovadoras para promover maior transparência, como painéis de controle de dados, logs de acesso e funcionalidades que permitem ao titular visualizar, corrigir ou apagar dados de forma autônoma. No caso específico da biometria, diversas empresas já incorporam salvaguardas como o design voltado à privacidade (privacy by design), o uso de dados pseudonimizados para treinamento de sistemas e a oferta de mecanismos para revisão humana de decisões automatizadas, quando necessário. Esses esforços demonstram um compromisso com o uso ético e seguro de tecnologias avançadas, promovendo a proteção dos dados pessoais sem comprometer a funcionalidade e a inovação.

Cumpra-se destacar que o direito à informação clara, o direito de acesso e à correção dos dados são direitos dos titulares que pressupõem todo e qualquer tratamento, independentemente de o referido tratamento estar ou não inserido no contexto de uma decisão tomada exclusivamente em tratamento automatizado de dados pessoais. Nesse sentido, medidas de transparência, tais quais previsões claras e precisas em políticas de privacidade e divulgação de canais de atendimento são imprescindíveis para que o titular possa exercer seus direitos.

Em relação ao direito de acesso, conforme o ICO, há dificuldade técnica em fornecer os dados biométricos propriamente ditos, uma vez que, em geral, são outputs matemáticos complexos, não compreensíveis ("ilegíveis") por seres humanos. Diante disso, o fornecimento pode ser substituído por uma declaração explicativa, que: (a) justifique a impossibilidade de entrega direta do dado; (b) descreva a natureza do dado em questão; e (c) esclareça como esse dado é mantido pela organização

No que diz respeito à possibilidade de revogação, nos casos em que a base legal para o tratamento dos dados for o consentimento, o titular deve dispor de um canal de fácil acesso, viabilizando a revogação de forma simples, acessível e facilitada. Por sua vez, conforme disposto na LGPD, o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

Dessa forma, enquanto requisito para a garantia e a aplicação do referido direito, é certo que a leitura do dispositivo deve considerar que a revisão ocorra apenas nos casos em que a decisão foi tomada unicamente de forma automatizada, bem como que os interesses dos titulares tenham sido afetados de forma ilícita ou abusiva e contrária à legislação. Nesse sentido, importante destacar que a leitura e interpretação de referente direito do titular deve observar os requisitos dispostos no artigo 20 da LGPD, quais sejam: (i) decisão tomada unicamente com base em tratamento automatizado de dados pessoais; e (ii) decisão que afete os interesses do titular. Com efeito, esses requisitos devem ser observados em qualquer decisão automatizada, seja ela referente ao tratamento de dados biométricos ou qualquer outro tipo de dado. Com efeito, cumpre destacar que, no que tange ao conceito de decisão tomada unicamente com base em tratamento automatizado de dados pessoais, considera-se um processo de tomada de decisão que é totalmente automatizado e exclui qualquer influência humana no resultado. Um processo ainda pode ser considerado totalmente automatizado se um humano insere os dados a serem tratados e, então, a tomada de decisão é realizada por um sistema automatizado.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O princípio do melhor interesse, previsto no art. 14 da LGPD, deve ser interpretado de forma concreta, contextualizada e não apriorística. Essa abordagem está em consonância com o Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU, que destaca o caráter flexível, relacional e multidimensional do conceito, exigindo sua ponderação em conjunto com outros direitos fundamentais. Reconhece-se, ainda, a condição peculiar da criança e do adolescente como pessoas em desenvolvimento, conforme o Estatuto da Criança e do Adolescente (ECA). Nesse sentido, recomenda-se que a ANPD assegure margem de autonomia aos controladores para que possam demonstrar, caso a caso, como o tratamento atende ao melhor interesse, inclusive com a possibilidade de adotar ajustes e salvaguardas adicionais.

A base legal para o tratamento de dados biométricos, ainda que envolva crianças e adolescentes como titulares dos dados, decorre do art. 11 da LGPD. Neste contexto, a própria ANPD, por meio do Enunciado nº 1/2023, acertadamente esclareceu que "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei". Assim, o consentimento, quando adotado como base legal, deve ser inequívoco e refletir claramente as finalidades do tratamento, sendo essencial a transparência com os representantes legais. Por outro lado, o tratamento também pode ser realizado com base em outras hipóteses legais, desde que haja legítima finalidade, proporcionalidade e salvaguardas adequadas.

É importante destacar que o cumprimento do princípio da necessidade não se limita à mera minimização da coleta de dados, mas sim à utilização de dados estritamente necessários para finalidades legítimas, em conformidade com os princípios da LGPD e com o melhor interesse de crianças e adolescentes. Neste contexto, a relação entre proteção dos dados e segurança deve ser avaliada no caso concreto. Casos internacionais ajudam a ilustrar a complexidade dessa ponderação. O uso de dados biométricos por escolas europeias, por exemplo, foi inicialmente considerado incompatível com o GDPR por algumas

autoridades de proteção de dados. A autoridade polonesa (UODO) entendeu que o uso de leitores biométricos para acesso ao refeitório escolar era desproporcional, mesmo com consentimento dos pais, pois existiam meios menos intrusivos para alcançar o mesmo fim. Contudo, o Tribunal Administrativo Provincial de Varsóvia reformou a decisão e considerou que, desde que o tratamento estivesse vinculado a uma finalidade legítima e houvesse consentimento válido, ele seria admissível. O caso evidencia que a compatibilidade entre o tratamento de dados biométricos e os princípios legais depende de uma análise contextual, proporcional e ancorada no melhor interesse do menor.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

A hipótese de Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (Art. 11, II, "g", LGPD"). Quando a hipótese legal é o consentimento, este deve ser inequívoco e contemplar as finalidades para a qual o representante do titular concorda com o tratamento. O tratamento dos dados biométricos de crianças e adolescentes também pode ser amparado em outras bases legais que não o consentimento, especialmente considerando as disposições do Enunciado nº 1/2023 da ANPD. Nesse cenário, é imprescindível que haja a devida transparência do tratamento e suas finalidades para os representantes do menor.

Sobre as medidas técnicas e organizacionais, destacam-se as medidas de segurança relevantes para todo e qualquer tratamento de dados, independentemente de o titular figurar como criança ou adolescentes, quais sejam: implementação de programas de Segurança da Informação, medidas de controle e gestão de acesso e, quando aplicável, elaboração de Relatório de Tratamento dos Dados Pessoais (DPIA).

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Para compatibilizar a prática de verificação de idade com o princípio da necessidade, é essencial que a coleta de dados biométricos seja limitada ao

mínimo necessário para atingir a finalidade pretendida, evitando excessos, tratamentos desproporcionais ou tratamentos a posteriori para outras finalidades. A biometria, por ser um dado sensível, deve ser utilizada apenas quando não houver outra forma menos invasiva de verificar a idade do usuário. Além disso, é fundamental garantir a transparência do processo, com informações claras e acessíveis aos pais ou responsáveis, incluindo a finalidade da coleta, os direitos dos titulares e os mecanismos disponíveis para exercer esses direitos.

O tratamento de dados biométricos para casos de verificação ou estimação de idade de crianças e adolescentes deve priorizar a proteção do menor, evitar riscos à sua dignidade, liberdade e segurança, de forma a se garantir o melhor interesse do menor.



30 de junho de 2025

Waldemar Gonçalves Ortunho Junior
Diretor-Presidente, Conselho Diretor
Autoridade Nacional de Proteção de Dados

Re: Consulta da ANPD sobre Dados Biométricos

A Business Software Alliance (BSA)¹ agradece a oportunidade de fornecer feedback à Autoridade Nacional de Proteção de Dados (ANPD) sobre a consulta pública sobre o tratamento de dados biométricos.

A BSA é a principal defensora da indústria global de software. Nossos membros são empresas de software e tecnologia empresarial que criam produtos e serviços business-to-business para ajudar seus clientes a inovar e crescer. Por exemplo, os membros da BSA fornecem ferramentas, incluindo serviços de armazenamento em nuvem, software de gerenciamento de relacionamento com o cliente, programas de gerenciamento de recursos humanos, serviços de gerenciamento de identidade e software de colaboração. As empresas confiam algumas de suas informações mais confidenciais - incluindo dados pessoais - aos membros da BSA. Nossas empresas trabalham duro para manter essa confiança. Como resultado, as proteções de privacidade e segurança são partes fundamentais das operações dos membros da BSA. cibersegurança,

Apreciamos o foco da ANPD no processamento de dados biométricos consistente com a Lei Geral de Proteção de Dados (LGPD). Nossos comentários enfatizam dois pontos:

- ***Os dados biométricos só devem ser tratados como dados pessoais sensíveis quando forem usados para identificar exclusivamente um indivíduo.*** Isso cria um limite claro e viável para os controladores aplicarem. Também está alinhado com as principais leis globais de proteção de dados, incluindo o Regulamento Geral de Proteção de Dados (GDPR) da UE.
- ***Os dados biométricos suportam atividades importantes, sem identificar exclusivamente um indivíduo.*** Por exemplo, os dados biométricos podem ser usados para distinguir entre uma pessoa e um objeto em um armazém, oferecendo melhores resultados de segurança. Também pode ser usado para contar o volume de pessoas no transporte público. A ANPD não deve tratar os dados biométricos usados dessa forma

¹ Os membros da BSA incluem: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk e Zoom Communications Inc.

como sensíveis, porque os dados são processados sem identificar exclusivamente os indivíduos. Por outro lado, se esses usos fossem confidenciais, os controladores seriam obrigados a identificar esses indivíduos para que pudessem obter consentimento para processar os dados. Isso prejudica as proteções de privacidade, em vez de fortalecê-las.

I. Bloco 1: Definições e Princípios

A BSA aprecia a importância de garantir que as empresas que processam dados biométricos cumpram a LGPD. Respondemos a todas as três perguntas da ANPD sobre a aplicação da LGPD a esse processamento.

1. Quais critérios objetivos devem ser observados para caracterizar os dados como biométricos nos termos da LGPD?

Os dados biométricos só devem ser tratados como confidenciais se forem usados para identificar exclusivamente um indivíduo. Isso cria um padrão claro e se alinha com o GDPR da UE, que a ANPD reconhece que inspirou a LGPD. O artigo 9.º do GDPR proíbe o tratamento de dados biométricos sem consentimento se estes forem utilizados para identificar de forma inequívoca uma pessoa singular.

Resposta BSA: 273 caracteres

2. Que práticas de transparência ativa podem ser exigidas dos controladores que processam dados biométricos, para permitir que os titulares dos dados tenham informações claras sobre o processamento antes de fornecer seus dados?

Os controladores devem adotar medidas alinhadas ao princípio de transparência da LGPD, que visa garantir que os titulares dos dados tenham informações claras sobre como os dados pessoais são tratados. Os controladores também estão sujeitos à obrigação do Artigo 9 de fornecer informações sobre seu processamento, incluindo as finalidades para as quais os dados pessoais são processados.

Resposta da BSA: 300 caracteres

3. Como a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento dos olhos) deve ser tratada em comparação com a biometria tradicional (impressão digital, íris, rosto)? Existem obrigações específicas que possam derivar dessas novas tecnologias, no que diz respeito aos princípios de qualidade e segurança dos dados?

A ANPD deve se concentrar na biometria usada para identificar exclusivamente um indivíduo – e reconhecer que os dados biométricos podem apoiar atividades importantes sem identificar indivíduos. Por exemplo, os dados biométricos podem apoiar a segurança, distinguindo uma pessoa de um objeto em um armazém ou contando os passageiros no transporte público. Esses não devem ser usos sensíveis.

Resposta da BSA: 300 caracteres

II. Bloco 2: Bases legais para processamento.

A LGPD fornece uma série de bases legais para o processamento de dados biométricos. Respondemos a todas as quatro perguntas da ANPD sobre como essas bases legais se aplicam aos dados biométricos.

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em que contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento destes dados?

De acordo com a LGPD, os controladores devem obter consentimento ou confiar em outra base legal nos termos do Artigo 11 para processar dados pessoais confidenciais. A orientação sobre dados biométricos deve ser consistente com o reconhecimento da LGPD de que tais dados podem ser tratados com consentimento ou em outras bases reconhecidas na lei.

Resposta da BSA: 258 caracteres

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de "garantia de prevenção de fraudes" (art. 11, II, "g", LGPD) nos casos de tratamento de dados biométricos? Como conciliar o princípio da necessidade de tratamento de dados biométricos, com a finalidade de proporcionar segurança da informação e acesso a soluções bancárias e financeiras, por exemplo? Que salvaguardas podem ser implementadas para mitigar os riscos às liberdades e direitos fundamentais?

Os dados biométricos podem ser usados para evitar atividades fraudulentas, em benefício de consumidores e empresas. O artigo 11 permite expressamente o processamento para esse fim, a menos que o interesse em tal processamento seja anulado pelos direitos dos indivíduos. As empresas devem avaliar os benefícios e riscos de tal processamento, para apoiar o uso dessa base legal.

Resposta da BSA: 296 caracteres

6. Em determinadas ocasiões, o tratamento de dados biométricos poderá ser realizado para o "cumprimento de obrigação legal ou regulatória" (art. 11, II, "a", LGPD). Quais critérios e salvaguardas devem ser observados nesses casos pelos controladores, especialmente entidades e órgãos públicos, para mitigar riscos e garantir os direitos dos titulares dos dados?

Os controladores devem identificar e avaliar suas obrigações legais e regulatórias de processar dados pessoais sensíveis, incluindo dados biométricos. Para empresas do setor privado, essas obrigações podem vir de estatutos e regulamentos ou ordens específicas de agências governamentais. A orientação deve reconhecer claramente a importância de tal processamento.

Resposta da BSA: 297 caracteres

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, "c", LGPD), mesmo nos casos em que há anonimização dos dados, considerando o cruzamento de bases de dados e a possível possibilidade de posterior reidentificação? Que garantias adicionais poderão ser necessárias para salvaguardar os interesses e direitos das pessoas em causa nesses casos?

As entidades de pesquisa devem realizar estudos alinhados às proteções da LGPD. Isso inclui anonimizar dados pessoais confidenciais sempre que possível. De forma mais ampla, a orientação deve aplicar a LGPD com base na função pretendida e no risco real do uso de uma tecnologia, e não nas características gerais ou capacidades potenciais de uma tecnologia.

Resposta da BSA: 296 caracteres

III. Bloco 3: Tecnologias de Reconhecimento Facial e Aplicação de Tecnologias Emergentes e Inovadoras no Tratamento de Dados Biométricos

É importante garantir que as proteções legais existentes, incluindo a LGPD, continuem a ser aplicadas a tecnologias novas e emergentes. Respondemos a uma das perguntas da ANPD sobre essas tecnologias.

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e para evitar discriminações ilícitas ou abusivas contra determinados grupos sociais? Que salvaguardas técnicas, legais e institucionais devem ser implementadas para mitigar esses riscos?

É importante reconhecer que as tecnologias que tratam dados pessoais estão sujeitas não apenas à LGPD, mas também a outras leis existentes. Pode ser necessário examinar como as leis que proíbem a discriminação ilegal se aplicam ao uso de novas tecnologias. Essas leis devem continuar a proteger contra a discriminação à medida que novas tecnologias são adotadas.

Resposta BSA: 293 caracteres

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados para garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Que mecanismos devem ser adotados para corrigir prontamente essas falhas, especialmente quando o tratamento de dados pessoais por meio do reconhecimento facial é realizado por tecnologias de processamento automatizado?

[Sem resposta]

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Em caso afirmativo, quais e por quê? Quais tecnologias alternativas podem ser utilizadas pelos controladores de forma efetiva para substituir o reconhecimento facial, visando garantir maior segurança em suas operações e com menor impacto na proteção dos titulares dos dados?

[Sem resposta]

IV. Bloco 4: Segurança, Governança e Boas Práticas

A LGPD apoia uma série de boas práticas e governança que podem proteger os direitos dos titulares dos dados e permitir a conformidade. Respondemos a três perguntas sobre como essas práticas e medidas de governança podem ser aplicadas ao processamento de dados biométricos.

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas essenciais para mitigar esses riscos? Além disso, quais padrões mínimos de avaliação e monitoramento de riscos devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção total desses dados sensíveis?

Reconhecemos que a ANPD está considerando emitir orientações sobre avaliações de impacto à proteção de dados (DPIAs) para tratamentos que apresentem certos riscos. Apoiamos a exigência de que os controladores conduzam DPIAs ao processar dados pessoais confidenciais, incluindo dados biométricos, o que é consistente com o GDPR da UE e outras leis globais de proteção de dados.

Resposta BSA: 293 caracteres

12. Considerando que existem serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, que boas práticas devem ser observadas para garantir que esta limitação não constitui uma discriminação ilícita ou abusiva? Em que contextos pode a recusa do titular dos dados em fornecer os seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, justificar, de forma proporcionada e transparente, a limitação da utilização de determinadas funcionalidades?

[Sem resposta]

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir proteção efetiva no tratamento de dados biométricos? Como garantir que os dados biométricos recolhidos são utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva dos utilizadores?

Os controladores devem adotar práticas alinhadas à LGPD, incluindo limites ao tratamento de dados sensíveis. Além disso, a LGPD exige que os controladores que processam quaisquer dados pessoais sejam transparentes sobre suas atividades e adotem medidas de segurança adequadas. Leis além da LGPD também podem proibir a discriminação e outros atos ilegais.

Resposta da BSA: 290 caracteres

14. Como os controladores podem garantir o respeito à autodeterminação informacional dos titulares dos dados em contextos de processamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes, monitoramento de grandes multidões, como em estádios e espaços públicos? Que medidas concretas devem ser adotadas para garantir que os titulares dos dados sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

É importante entender se os dados nesses cenários estão sendo processados com a finalidade de identificar exclusivamente os indivíduos. Nesse caso, deve ser protegido como dados biométricos. No entanto, o processamento de dados que revelam o número de pessoas em uma multidão ou apenas fornecem informações agregadas sobre padrões de tráfego não cria as mesmas sensibilidades.

Resposta da BSA: 295 caracteres

V. Bloco 5: Direitos dos Titulares dos Dados e Grupos Vulneráveis

A LGPD cria uma série de direitos importantes para os indivíduos em seus dados pessoais. Respondemos a uma pergunta sobre como esses direitos se aplicam ao processamento de dados biométricos.

15. Como podem os agentes de tratamento assegurar o respeito pelos direitos dos titulares dos dados, nomeadamente o direito à informação clara, o direito de acesso e retificação dos dados e o direito de retirar o consentimento, como por exemplo em contextos de tratamento automatizado de dados biométricos?

Os direitos criados pela LGPD se aplicam a todos os dados pessoais, incluindo dados biométricos. É altamente recomendável tratar os dados apenas como dados biométricos se forem usados para identificar exclusivamente um indivíduo. Isso também esclarecerá como os novos direitos do titular dos dados se aplicam, porque esses direitos serão atribuídos ao indivíduo que é identificado de forma exclusiva.

Resposta da BSA: 274 caracteres

16. Dada a sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em que hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do artigo 14 da LGPD?

[Sem resposta]

17. Em que hipóteses legais esse tipo de tratamento seria admissível e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

[Sem resposta]

18. Nos casos de verificação ou estimativa de idade por meio do fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento de dados de crianças e adolescentes? Como essas práticas podem ser conciliadas com os princípios da necessidade e do interesse superior da criança?

[Sem resposta]

* * *

Obrigado novamente pela oportunidade de fornecer nossas opiniões. Congratulamo-nos com a oportunidade de nos envolvermos ainda mais com a ANPD nessas questões importantes.

Sinceramente

Kate Goodloe
Managing Director, Policy
Business Software Alliance

Antônio Eduardo Mendes da Silva
Country Manager - Brasil
Business Software Alliance

REFERÊNCIA: TOMADA DE SUBSÍDIOS: DADOS PESSOAIS SENSÍVEIS - DADOS BIOMÉTRICOS

ENTIDADE DESTINATÁRIA: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (“ANPD”)

ENTIDADE CONTRIBUINTE: CÂMARA BRASILEIRA DA ECONOMIA DIGITAL (“CÂMARA-E.NET”)

PRAZO: 02/08/2025

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo “dados biométricos”, mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos - que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

- LGPD e dado biométrico: A Lei Geral de Proteção de Dados (LGPD) não traz definição de “dado biométrico”, limitando-se a enquadrá-lo como espécie de dado pessoal sensível.
- Aplicação prática e teleológica na LGPD: A LGPD adota uma definição taxativa de dados pessoais sensíveis (art. 5º, II). Para fins de enquadramento, é recomendada uma interpretação finalística, ou seja, na ausência de intenção ou finalidade de inferir informações sensíveis, o dado não deve ser considerado sensível. Por exemplo, o uso de fotos ou vídeos disponíveis publicamente, sem extração ou inferência de dados biométricos ou outras informações sensíveis, não configura tratamento de dados pessoais sensíveis. Ainda, deve-se considerar que, de acordo com a LGPD, para aplicação do artigo 11, é preciso que o tratamento de dados pessoais “revele dados pessoais sensíveis e que possa causar dano ao titular”.
- General Data Protection Regulation (GDPR, art. 4.14 e considerando 51): O GDPR estabelece que dado biométrico é o resultado de tratamento técnico específico de características físicas, fisiológicas ou comportamentais que permitam ou confirmem a identificação única de um indivíduo, ao passo que o considerando 51 reforça que fotografias ou vídeos não se enquadram nessa categoria, salvo quando tratados tecnicamente para autenticar ou identificar alguém.
- European Data Protection Board (EDPB): Conforme o EDPB (https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en), enquanto não houver o que se chama de “tratamento técnico específico”, a captação de imagens não se qualifica como tratamento de dados biométricos sensíveis. Somente quando extrai-se e converte-se essas imagens em medições ou templates e essas saídas passam a servir ao propósito de permitir ou confirmar a identificação única do indivíduo é que o conteúdo bruto se enquadra nas “categorias especiais” do art. 9 do GDPR.
- Information Commissioner's Office (ICO): a autoridade do Reino Unido (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/key-data-protection-concepts/>) define dado biométrico como aquele que (i) trata de características físicas, fisiológicas ou comportamentais; (ii) foi objeto de processamento técnico específico; e (iii) permite ou reconhece a identificação de uma pessoa de forma única. Dados biométricos só se tornam “sensíveis” se forem utilizados com a finalidade de identificar uma pessoa de forma inequívoca.
- Autoriteit Persoonsgegevens (AP): A autoridade holandesa (<https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/rules-for-the-use-of-biometrics>) adota entendimento equivalente no sentido de que dado biométrico (i) diz respeito a características pessoais geralmente permanentes; (ii) resulta de tratamento técnico que compara medidas a uma referência; e (iii) tem como propósito estabelecer ou confirmar a identidade de alguém.

- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI): A autoridade mexicana (https://inicio.inai.org.mx/documentosdeinteres/guidatosbiometricos_web_links.pdf) utiliza o GDPR como referência para a definição e apresenta um exemplo que demonstra a imprescindibilidade de um tratamento técnico específico para a caracterização de um dado biométrico: “É o caso da impressão digital, que por si só e isoladamente não identifica seu titular, mas quando entra em um sistema no qual é vinculada a um indivíduo em particular e, posteriormente, novas amostras podem ser comparadas com o modelo previamente registrado, torna-se um dado pessoal, ao tornar identificável seu titular”.
- FPF e usos tecnológicos: O Future of Privacy Forum (<https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric/>) defende que tecnologias que operam sobre dados corporais podem ser organizadas em cinco categorias: detecção, caracterização, rastreamento único e persistente, verificação (1:1) e identificação (1:Many). A detecção simplesmente evidencia a presença de um corpo ou traço físico, por exemplo, “tem alguém ali?”, sem reter informações de identificação pessoal. A caracterização infere atributos como idade, emoções ou condições médicas sem associá-los a um indivíduo reconhecível. O rastreamento único e persistente monitora padrões de movimento ou atividade ao longo do tempo, mas geralmente mantém os dados ligados a identificadores anônimos ou pseudônimos, sem criar vínculo biunívoco com a identidade real. A verificação compara a biometria captada com um template pré-existente numa lógica um-para-um para confirmar se “é mesmo você”, enquanto a identificação realiza buscas um-para-muitos em grandes bases de dados para descobrir quem é o sujeito. **Somente as duas últimas, verificação e identificação, envolvem capacidade de identificação única e, portanto, estão abrangidas pelo conceito de dado biométrico sensível.**
- Conclusão: Apenas os dados pessoais que (i) se referem a características físicas, fisiológicas ou comportamentais de uma pessoa natural, (ii) resultam de tratamento técnico específico, e (iii) são utilizados com a finalidade de identificar univocamente essa pessoa, devem ser enquadrados como dados biométricos sensíveis. A presença simultânea desses três elementos é indispensável para a caracterização do dado como biométrico nos termos do art. 5º, II, da LGPD. Nesse contexto, a ANPD deve evitar interpretações excessivamente amplas que possam desestimular o desenvolvimento de tecnologias inovadoras e de baixo risco, como aplicações de classificação ou organização automatizada de imagens. Em suas futuras orientações, é recomendável que a Autoridade esclareça que: (i) o tratamento realizado com o propósito de identificar univocamente um indivíduo pressupõe a extração e verificação de características biométricas de forma a permitir, com determinado grau de confiança, a associação direta da informação à identidade específica de um titular. É o caso, por exemplo, do uso de tecnologia de reconhecimento facial para autenticar um usuário em um serviço digital, ou da realização de verificação de identidade para fins de prevenção à fraude em serviços financeiros; e (ii) por outro lado, quando o tratamento não tem como finalidade a identificação unívoca do titular, como ocorre no agrupamento automatizado de imagens semelhantes em aplicativos de fotos, ainda que envolva dados derivados de características faciais, ele não deve ser enquadrado como tratamento de dado biométrico sensível. Nesses casos, o dado permanece no âmbito dos dados

peçoais comuns, pois não é utilizado para estabelecer a identidade única do indivíduo. Nessa toada, a ANPD deve ser cautelosa ao avaliar o enquadramento de tecnologias voltadas à detecção, caracterização e rastreamento, que muitas vezes não mantêm vínculo direto com a identidade dos titulares e, portanto, não configuram, por si sós, tratamento de dados biométricos. Como referência prática, destaca-se o sandbox regulatório do ICO sobre a ferramenta de estimativa de idade da Yoti, que reconheceu que determinados usos de características faciais, desde que não sejam utilizados com a finalidade de identificar um indivíduo de forma única, não configuram tratamento de dados biométricos sensíveis (https://ico.org.uk/media2/migrated/4020427/yoti-sandbox-exit_report_20220522.pdf). Outro exemplo, noticiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), é o uso de inteligência artificial para detectar insuficiência respiratória por meio da análise de áudios, sem necessidade de identificar individualmente os titulares (<https://agencia.fapesp.br/inteligencia-artificial-detecta-insuficiencia-respiratoria-por-analise-de-audios/50844>). Assim como no caso do ICO, a aplicação demonstra que determinados tratamentos de características físicas, fisiológicas ou comportamentais, quando incapazes de identificar um indivíduo de forma única, não se enquadram como tratamento de dados biométricos sensíveis.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

- **Transparência e dados biométricos:** As boas práticas de transparência devem orientar todo e qualquer tratamento de dados pessoais, inclusive de dados sensíveis, como os dados biométricos. Medidas que facilitem o acesso dos titulares a informações claras e precisas sobre esse tratamento, especialmente no que se refere à indicação de finalidades legítimas, específicas e explícitas, constituem referência de boas práticas em matéria de transparência.
- **Transparência e proporcionalidade na LGPD:** O princípio da transparência deve ser interpretado de forma proporcional e funcional, considerando o contexto e as circunstâncias da operação de tratamento. Por exemplo, quando o controlador não mantém relação direta com os titulares, entende-se como suficiente a adoção de medidas razoáveis para disponibilizar as informações exigidas pela LGPD em site de acesso público.
- **Transparência em etapas e formatos acessíveis:** A ANPD também deve reconhecer que as informações de transparência podem ser fornecidas ao titular: (i) em diferentes etapas da jornada do usuário, como ao disponibilizar um link claro para o aviso de privacidade no momento de configuração de funcionalidades que envolvam dados biométricos, bem como por meio de avisos just-in-time (no momento oportuno), antes da coleta desses dados; e (ii) por meio de diferentes ferramentas, como imagens ou vídeos, que complementem os avisos formais e tornem a comunicação mais acessível.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

- LGPD e dados biométricos: Relembra-se que a LGPD não define expressamente “dato biométrico”, limitando-se a classificá-lo como dato pessoal sensível. Para fins de enquadramento, é necessária uma interpretação finalística: na ausência de intenção ou finalidade de inferir informações sensíveis, o dato não deve ser considerado sensível. Por exemplo, o uso de fotos ou vídeos disponíveis publicamente, sem extração ou inferência de dados biométricos ou outras informações sensíveis, não configura tratamento de dados pessoais sensível. Além disso, o art. 11 exige que o tratamento revele dato sensível e possa causar dano ao titular.
- Referências conceituais: Segundo o art. 4.14 do GDPR, dato biométrico é o resultado de tratamento técnico específico de características físicas, fisiológicas ou comportamentais que permita ou confirme a identificação única de uma pessoa natural. No mesmo sentido, o ICO (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/#physical>) do Reino Unido estabelece que o dato deve (i) referir-se a características físicas, fisiológicas ou comportamentais, (ii) ser submetido a tratamento técnico específico e (iii) ter como finalidade identificar ou reconhecer uma pessoa de forma única, sendo considerado sensível apenas se utilizado com essa finalidade. Assim, um dato sobre aspecto comportamental é apenas um dos elementos para a caracterização de um dato como biométrico; para enquadramento nesse conceito, são também necessários o tratamento técnico específico e a finalidade de identificar ou reconhecer uma pessoa de forma única.
- Reconhecimento biométrico segundo o ICO (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/#physical>): De acordo com o ICO, “dato biométrico comportamental” refere-se a características biométricas relacionadas a coisas como movimentos, gestos ou habilidades motoras. A simples coleta ou análise desses dados - sem o objetivo de identificar de maneira unívoca um indivíduo ou de maneira que permita tal identificação - não implica a incidência do regime relacionado aos dados biométricos. Somente após a aplicação de algoritmos que extraem e codificam essas características em formatos específicos, utilizados para comparar e identificar indivíduos, o dato assume natureza biométrica. O mero tratamento de dados comportamentais, sem o tratamento técnico específico e a finalidade de identificação, não os torna dados biométricos sensíveis. A necessidade de um tratamento técnico específico também se aplica aos dados comportamentais. Nesse contexto, algoritmos processam essas informações para extrair e codificar padrões únicos de comportamento, gerando modelos matemáticos

que permitem a identificação ou autenticação individual. Portanto, não é a simples coleta ou gravação desses dados comportamentais que configura dado biométrico, mas sim a aplicação dessas técnicas específicas que transformam essas características em informações capazes de identificar unicamente o indivíduo. Digno de nota é o fato de que o ICO deixa explícito que dados biométricos comportamentais referem-se a “movimentos, gestos ou habilidades motoras” e não alcançam aspectos comportamentais relacionados a emoções, sentimentos, etc.

- Imutabilidade e caracterização de dados biométricos: Estudo do European Parliamentary Research Service (EPRS, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf)) destaca que **o termo “biométrico” implica certo grau de imutabilidade, ou seja, refere-se a características ou sinais que a pessoa natural tem pouca ou nenhuma possibilidade de alterar voluntariamente (por exemplo, não se pode mudar o rosto ou o padrão das impressões digitais por escolha própria)**. Por isso, técnicas biométricas podem incluir, por exemplo, a análise da dinâmica de gestos, da assinatura, bem como de voz e do modo de andar. Em contrapartida, o termo não abrange comportamentos que podem ser amplamente controlados pela vontade humana, como hábitos de consumo, histórico de navegação ou o conteúdo de comunicação. Ou seja, a análise de comportamento com o objetivo de inferir interesses não se enquadra no conceito de dado biométrico, pois, além de se tratar de elementos controláveis pela vontade humana, esses dados não passam por um tratamento técnico específico capaz de extrair características únicas que permitam a identificação ou autenticação de um indivíduo.
- Benefícios relatados na implementação: Segundo o Grupo de Trabalho do Artigo 29 (WP29), fabricantes relataram que a adoção de tecnologias biométricas comportamentais no setor financeiro aumentou as taxas de detecção de fraudes e proporcionou maior agilidade na resolução de reivindicações legítimas. O WP29 avaliou que a assinatura dinâmica pode oferecer maior segurança em comparação à assinatura gráfica, por incorporar a análise de características dinâmicas do gesto de escrita, como velocidade, pressão e ritmo, que são únicas e difíceis de falsificar. A Autoridade de Proteção de Dados de Singapura (PDPC) também reconheceu o uso da biometria comportamental como medida voltada à segurança, especialmente em aplicações voltadas à prevenção de fraudes.
- Ausência de obrigações específicas na LGPD: A LGPD não prevê obrigações específicas para o tratamento de dados biométricos comportamentais. A abordagem deve ser orientada, caso a caso, pela finalidade e natureza dos dados biométricos, bem como pelos riscos prováveis, danos e o nível de intrusividade para o indivíduo. Assim, a ANPD deve, por meio de suas orientações e guias, incentivar que as organizações implementem medidas proporcionais, equilibrando os direitos e liberdades individuais com os benefícios das tecnologias biométricas na proteção dos usuários contra fraudes, riscos de segurança e danos online, não apenas no contexto de identificação e cadastro eletrônico. Quaisquer obrigações e medidas devem ser claramente estabelecidas e de fácil implementação para as organizações em diferentes tecnologias.

- Reconhecimento de B-PETs: A ANPD deve reconhecer o papel das Tecnologias de Aprimoramento de Privacidade Biométrica (*Biometric Privacy Enhancing Technologies* - B-PETs) na redução do risco de dano aos indivíduos e na proteção de dados pessoais, e criar incentivos para que as organizações considerem implementar B-PETs apropriadas e proporcionais ao tratamento que realizam. O ICO, por exemplo, aborda as B-PETs em sua orientações sobre dados biométricos (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>).
- Conclusão: O tratamento de dados comportamentais só configura dado biométrico sensível quando preenchidos cumulativamente três requisitos: (i) relação com características físicas, fisiológicas ou comportamentais; (ii) aplicação de tratamento técnico específico (como extração e codificação por algoritmos); e (iii) finalidade de identificação ou autenticação individual. A relativa imutabilidade da característica é um indicativo adicional a ser considerado. A LGPD não prevê obrigações específicas para o tratamento de dados biométricos comportamentais, a aplicação da LGPD a esse tipo de tratamento deve considerar o risco, o dano potencial e o grau de intrusividade do tratamento. É importante que se considere que tecnologias de biometria comportamental, quando bem aplicadas, podem trazer benefícios como segurança e prevenção a fraudes. A adoção de B-PETs deve ser incentivada como salvaguarda proporcional, especialmente em tratamentos mais intrusivos.

BLOCO II – HIPÓTESES LEGAIS

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

- Ausência de hierarquia entre as bases legais do art. 11 da LGPD: Qualquer uma das hipóteses previstas no art. 11 da LGPD pode ser utilizada para legitimar o tratamento de dados pessoais sensíveis, inclusive biométricos. O consentimento não possui caráter preferencial ou hierarquicamente superior às demais bases legais e deve ser analisado conforme a finalidade e o contexto do tratamento. Assim, nos casos em que dados biométricos são tratados nos termos da LGPD, incentivamos a ANPD a fornecer orientações práticas e proporcionais sobre outras bases legais apropriadas para tal tratamento.
- Consentimento é uma alternativa viável mas nem sempre a mais adequada: O uso do consentimento como base legal para o tratamento de dados biométricos é possível, como reconhecido pelo ICO (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/#canweuse>) e pela autoridade de proteção de dados da Holanda (<https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/rules-for-the-use-of-biometrics#use-of-biometrics-with-explicit-consent>). Contudo, em determinadas situações, especialmente quando o tratamento visa a prevenção à fraude em processos de identificação e autenticação de cadastro, como previsto na alínea “g” do art. 11, II, a exigência de consentimento pode ser contraproducente. Isso porque pode inviabilizar mecanismos automatizados de segurança, como autenticação por reconhecimento facial ou impressão digital, que têm por finalidade justamente proteger a identidade e a segurança do próprio titular. Na mesma toada, é possível que o consentimento não seja a hipótese autorizativa mais adequada nos casos em que não há uma relação direta com o indivíduo.
- Consentimento e compensação financeira: Compreendemos a preocupação da ANPD em assegurar que a manifestação de vontade dos titulares seja livre de vícios e interferências externas. No entanto, gostaríamos de compartilhar algumas ponderações sobre o entendimento de que eventual compensação financeira configuraria uma interferência indevida nessa manifestação, comprometendo o requisito de liberdade previsto na LGPD (https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQIHJmJlqCN_XRK_Sh2SMdn1U-tzOf0LPPJDv1Jb7GRBpmimYXBkA639-hvCqJ1dmloainfNr1EcmTkNXyLOteZeNfAIDgST2Zb0J5Xo4ECfdj5lj). Nesse sentido, em artigo recente sobre o tema (<https://www.dropbox.com/scl/fi/e01123dv3itr3hinscjxf/Monetiza-o-de-Dados-Pessoais.-RBV-2025.-WP-v.1.3..pdf?rlkey=xldzsmvci51wzcbq8ni3uwk5p&e=2&st=gzzsw7vo&dl=0>), Rodrigo Valadão defende que: (i) a mera oferta de vantagem pecuniária não invalida o consentimento do titular, não podendo ser presumido o vício de consentimento; (ii) é crucial distinguir entre “influência negativa”

(ameaças, sanções) e "influência positiva" (incentivos), sendo esta última compatível com a validade do consentimento, desde que a voluntariedade da decisão seja preservada; (iii) o direito comparado (Alemanha, França, Itália) e o brasileiro admitem a monetização de dados, com a Diretiva de Conteúdo Digital da União Europeia equiparando o fornecimento de dados pessoais ao pagamento em dinheiro; (iv) programas de fidelização e descontos por dados são exemplos de monetização indireta amplamente aceitos, desde que cumpram os requisitos de transparência e garantam a liberdade de escolha do titular; (v) a autodeterminação informacional possui uma dimensão positiva que permite ao indivíduo decidir sobre a exploração econômica de seus dados, e não apenas impedir o uso predatório; (vi) o regime jurídico para a monetização de dados pessoais pode se basear no modelo de cessão onerosa do direito de imagem, que já concilia aspectos patrimoniais e extrapatrimoniais de direitos da personalidade; (vii) a fiscalização de práticas abusivas deve focar na prova de que o titular não tinha alternativa razoável ou sofreu pressões insuperáveis, e não na proibição genérica da monetização; e (viii) modelos de "Personal Data Exchange" (PDE) e cooperativas de dados buscam empoderar o titular, permitindo-lhe controlar e monetizar seus dados de forma transparente e segura.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de "garantia da prevenção à fraude" (art. 11, II, "g", LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

- Critérios para o tratamento de dados biométricos com base na garantia da prevenção à fraude e à segurança do titular: O enquadramento do tratamento de dados biométricos na hipótese legal de "garantia da prevenção à fraude e à segurança do titular" deve observar os critérios estabelecidos no art. 11, inciso II, alínea "g", da LGPD. Nessa hipótese, o tratamento será permitido quando: (i) tiver como finalidade garantir a prevenção à fraude e a segurança do titular; (ii) for realizado por meio de processos de identificação e autenticação de cadastro em sistemas eletrônicos; (iii) forem respeitados os direitos previstos no art. 9º da LGPD; e (iv) não prevalecerem os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
- Ponderação entre proteção de dados e prevenção a fraude e garantia à segurança: A ANPD deve ponderar a necessidade de adoção de medidas de segurança e de prevenção à fraude com a garantia da proteção dos dados pessoais dos titulares. Essa análise deve considerar princípios expressamente previstos na LGPD, como os da qualidade, da segurança e da prevenção (art. 6º, V, VII e VIII), que impõem aos agentes de tratamento o dever de adotar medidas técnicas e administrativas adequadas para evitar danos e assegurar a integridade dos dados. Além disso, a Constituição Federal estabelece, no art. 5º, XXXII, que o Estado promoverá, na forma da lei, a defesa do consumidor; no art. 170, como um dos princípios da ordem econômica, a defesa do consumidor; e, no art. 6º, a segurança como um direito social. Essa proteção é reforçada ainda pelo art. 6º, I, do Código de Defesa

do Consumidor, que assegura ao consumidor o direito à proteção contra riscos à sua segurança. O uso de dados biométricos com fundamento na base legal da garantia da prevenção à fraude e à segurança do titular, portanto, deve ser analisado à luz do equilíbrio entre segurança e privacidade.

- Dados sobre fraudes e golpes: Nesse sentido, é fundamental que a ANPD considere estudos que evidenciam a dimensão do problema no Brasil. A Pesquisa de Identidade Digital e Fraude 2025, da Serasa Experian, revela que 51% dos entrevistados já foram vítimas de fraude, um aumento significativo em relação aos 42% registrados em 2024 (<https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2025/03/Relatorio-de-Identidade-Digital-e-Fraude-2025-Serasa-Experian.pdf>). Já o Relatório de Tendências de Fraude 2025, 1º semestre, da TransUnion, indica que a perda mediana relatada no Brasil por pessoas que afirmaram ter perdido dinheiro com fraudes on-line, por e-mail, chamada telefônica ou mensagem de texto, foi de US\$ 1.032 (<https://www.transunion.com.br/content/dam/transunion/br/business/collateral/report/fraud-trends/relatorio-de-tendencia-de-fraude-2025-1-semester.pdf>). Além disso, pesquisa do DataSenado aponta que 24% dos brasileiros declararam ter perdido dinheiro, nos últimos 12 meses, em decorrência de algum crime cibernético (https://www.senado.leg.br/institucional/datasenado/relatorio_online/pesquisa_aposta_esportiva/2024/interativo.html#golpes-digitais). Em 2025, até o momento, o Brasil já registrou mais de 2,8 milhões de tentativas de fraude, que, caso se concretizassem, poderiam gerar prejuízos superiores a 40 bilhões de reais (<https://www.serasaexperian.com.br/fraudometro/>). Considerando esse cenário, é essencial que a ANPD reconheça a relevância da base legal prevista na LGPD para a garantia da prevenção à fraude e à segurança do titular, evitando interpretações excessivamente restritivas.
- Lacunas no GDPR e a exceção Holandesa: O GDPR não prevê uma base legal específica (art. 9º) para o tratamento de dados sensíveis com a finalidade de prevenção à fraude e garantia de segurança, limitando-se a autorizar seu uso em situações restritas, como o consentimento livre do titular. A falta de base legal específica para esse fim gera desafios para entidades que precisam usar dados biométricos para prevenção de fraudes e segurança, pois frequentemente dependem do consentimento, o que pode ser inviável, especialmente em relações de trabalho. Reconhecendo essa lacuna, a Holanda adotou uma abordagem distinta ao implementar o GDPR em sua legislação nacional, por meio do Article 29 GDPR Implementation Act (https://www.dataguidance.com/sites/default/files/dutch_general_data_protection_regulation_implementation_act.pdf), que cria uma exceção expressa à proibição geral do tratamento de dados biométricos para identificação única, autorizando-o quando necessário para autenticação ou segurança. A exposição de motivos da lei (https://docs.legal.digital/uavg?utm_source=chatgpt.com#uitzonderingen-inzake-biometrische-gegevens) destaca que o avanço técnico na identificação biométrica torna essencial essa exceção, sob risco de prejudicar práticas consolidadas, como o controle de

acesso em ambientes de trabalho, além de aplicações em setores públicos e privados que dependem da biometria para segurança e prevenção de fraudes. Sem essa exceção, muitas operações legítimas perderiam sua base legal, inviabilizando o uso da biometria para autenticação e proteção quando o consentimento não é viável.

- Interpretação conforme demais princípios como segurança e prevenção: A base legal prevista no art. 11, II, "g" da LGPD, relativa à garantia da prevenção à fraude e segurança do titular, é essencial para garantir a integridade no tratamento de dados pessoais e deve ser interpretada de forma ampla. Sua aplicação não deve se restringir a setores específicos, como o financeiro, mas alcançar diversos contextos em que a prevenção à fraude seja necessária. O uso dessa base deve observar os princípios da proporcionalidade e da razoabilidade, considerando a finalidade do tratamento, o contexto em que ocorre e os direitos dos titulares. Um exemplo é a validação biométrica da identidade de vendedores em plataformas de e-commerce. Essa medida busca assegurar a legitimidade das transações, prevenir fraudes e proteger os consumidores. Como os vendedores recebem pagamentos e emitem notas fiscais, a verificação de identidade, inclusive por biometria facial, mostra-se razoável e proporcional. A biometria pode oferecer maior segurança em comparação com métodos como autenticação multifator, que podem ser burlados por terceiros com acesso a credenciais. Além disso, quando a biometria é utilizada apenas no momento do cadastro, a medida se torna ainda menos invasiva. São comuns os casos de contas fraudulentas criadas com dados de terceiros, resultando em notas fiscais indevidas, cobranças indevidas e disputas judiciais. Há também situações em que produtos não são entregues, gerando prejuízos aos consumidores e riscos jurídicos às plataformas. Nesse contexto, é fundamental que a ANPD reconheça a importância dessa base legal como instrumento legítimo para promover a segurança digital e prevenir fraudes em múltiplos setores.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

- Adequação do tratamento de dados biométricos para cumprimento de obrigação legal ou regulatória: A adequada aplicação da hipótese legal de cumprimento de obrigação legal ou regulatória pressupõe o atendimento a requisitos de segurança e a observância dos princípios balizadores do tratamento de dados pessoais de forma geral. O princípio da necessidade, por exemplo, exige que os dados biométricos sejam utilizados apenas na medida estritamente necessária para o alcance da finalidade, assegurando a disponibilização de informações claras, precisas e acessíveis aos titulares sobre o tratamento realizado. O tratamento desses dados deve estar fundamentado na aplicação desse princípio, em conjunto com outros, bem como em boas práticas de governança e segurança da informação, visando garantir controle, rastreabilidade e proteção eficaz dos dados biométricos. Entre as possíveis salvaguardas a serem implementadas destacam-se o rastreamento, monitoramento, controle de acesso e o registro das operações de tratamento. Ao cumprir uma solicitação legal para divulgar dados biométricos (por exemplo, mediante ordem judicial ou requisição

de autoridade competente), os controladores devem adotar medidas para verificar a legitimidade, a necessidade e a adequação da solicitação, além de garantir que a resposta se limite aos dados estritamente requeridos. Assim, a aplicação adequada da hipótese legal de “cumprimento de obrigação legal ou regulatória”, prevista no artigo 11, II, “a” da LGPD, pressupõe a observância aos princípios da necessidade e da finalidade e a implementação de boas práticas de governança e segurança da informação, com o objetivo de prever medidas de controle e rastreabilidade, bem como de proteção dos dados biométricos.

- Exemplos do uso da base legal de cumprimento de obrigação legal e regulatória para tratamento de dados biométricos: A aplicação dessa base legal pode ser ilustrada por normativos setoriais que preveem o uso de dados biométricos como requisito para maior segurança em determinadas operações, como: Resolução Conjunta nº 6 de 23/5/2023, que dispõe sobre requisitos para o compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras; Circular BCB nº 3.978/2020, que em seu artigo 16 determina que as instituições financeiras adotem procedimentos de identificação que permitam verificar e validar a identidade do cliente; Instrução Normativa nº 138/2022, que em seu artigo 5º estabelece que a averbação da contratação de crédito consignado pelo titular do benefício somente poderá ocorrer mediante contrato firmado e assinado com uso de reconhecimento biométrico, acompanhado da apresentação de documento de identificação oficial válido com foto e do Cadastro de Pessoa Física (CPF), além disso, exige que a autorização para a consignação seja dada de forma expressa, também mediante assinatura com reconhecimento biométrico, vedando expressamente o uso de autorizações por ligação telefônica ou a utilização de gravação de voz como meio de prova da contratação.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

- Conceito de dado anonimizado: O dado anonimizado caracteriza-se por ser o dado que não é capaz de permitir a reidentificação posterior, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (conceito de dado anonimizado previsto no art. 5º, III da LGPD). Uma vez realizado o processo de anonimização, os referidos dados não são considerados dados pessoais, tendo em vista que não é possível identificar o titular. Consequentemente, os dados deixam de ser considerados dados sensíveis.
- Salvaguardas e validação: No caso de utilização de dados anonimizados, as medidas técnicas de anonimização, bem como a aplicação de testes de robustez para validar se os dados estão efetivamente anonimizados, conforme recomendado pela ANPD no Guia de Boas Práticas para Anonimização e Pseudonimização, podem ser consideradas como salvaguardas para viabilizar a eficácia do processo de anonimização dos dados.

- Proteção alternativa com B-PETs: Nos casos em que os dados pessoais não são anonimizados, o uso de B-PETs também pode ser uma proteção importante para os dados biométricos.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

A utilização das tecnologias de reconhecimento facial (Facial Recognition Technologies, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento.

Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

- Reconhecimento vs. detecção facial: Somente se caracteriza como dado biométrico aquele cujo tratamento tem como finalidade a identificação ou autenticação única de um indivíduo. Assim, cumpre destacar a diferença entre reconhecimento e detecção facial. O reconhecimento facial envolve: (i) o mapeamento de pontos e linhas específicas da face; (ii) a comparação com um banco de dados já existente, o qual envolve dados de pessoas identificáveis e identificadas; e (iii) a identificação de pessoas específicas. Por outro lado, a detecção facial é uma técnica que localiza rostos humanos em uma dada imagem ou vídeo, a partir de pontos de referência da face na boca, no nariz, nos olhos e na sobrancelha, e até o posicionamento da face. Logo, a detecção facial: (i) apenas determina se existe ou não algo no formato de um rosto humano naquela imagem ou vídeo; (ii) busca características humanas de forma anonimizada; (iii) não identifica o indivíduo ao qual o rosto pertence; e (iv) não é uma técnica de identificação biométrica e não é considerada como dado biométrico. É o caso, por exemplo, da técnica utilizada para permitir a utilização de filtros, que é chamada de “landmarking” e se vale de modelos de inteligência artificial treinados para localizar a posição do rosto dos usuários dentro do layout de vídeo utilizado pelo aplicativo, que não cria nem coleta padrões biométricos faciais dos usuários.
- Reconhecimento facial, segurança e a aplicação contextual dos princípios da LGPD: A conformidade do uso de tecnologias de reconhecimento facial com os princípios da LGPD deve considerar o contexto brasileiro, marcado por altos índices de fraudes e golpes. Nesse cenário, a interpretação do princípio da necessidade deve levar em conta que mecanismos de reconhecimento facial podem ser pertinentes e proporcionais para fins de identificação e autenticação de titulares, contribuindo diretamente para sua segurança. A LGPD também impõe deveres de segurança, prevenção e qualidade dos dados (art. 6º, V, VII e VIII), em linha com o Código de Defesa do Consumidor, que garante aos consumidores o direito à segurança na prestação de serviços (art. 6º, I). Esses princípios reforçam a legitimidade do uso responsável do reconhecimento facial por empresas de tecnologia, desde que acompanhado de salvaguardas adequadas.
- Relevância do reconhecimento facial: O reconhecimento facial, ao utilizar dados biométricos únicos, é uma tecnologia essencial para a prevenção à fraude e a proteção do titular. Fortalece os mecanismos de autenticação, contribuindo para a segurança dos dados e a integridade das operações, especialmente diante do aumento de fraudes em plataformas digitais. Em contextos como o e-commerce, em que há crescente registro de vendedores fraudulentos e métodos tradicionais de verificação têm se mostrado ineficazes, torna-se necessário adotar soluções mais robustas de verificação de identidade, como o reconhecimento facial. O uso de inteligência artificial generativa, capaz de criar rostos ultrarrealistas, agrava esse cenário, ao passo que o crescimento de cadastros em plataformas globais dificulta ainda mais revisões manuais.
- Salvaguardas técnicas, jurídicas e institucionais para mitigação de riscos: Sob a perspectiva jurídica, a correta identificação da base legal aplicável e o alinhamento com os princípios da LGPD são elementos essenciais para legitimar o tratamento. Do ponto de vista técnico, podem ser implementados mecanismos para mitigar vieses e discriminações ilícitas ou abusivas, o que abrange a realização

de testes de precisão com bases de dados diversificadas, representativas, precisas e atualizadas. Assim, deve-se evitar que a aplicação do princípio da necessidade restrinja excessivamente a coleta de dados a ponto de comprometer a acurácia e a equidade do sistema, o que pode gerar correspondências de baixa qualidade. Por fim, sob a perspectiva institucional, recomenda-se a adoção de controles de monitoramento e acesso e rastreamento das operações de tratamento, assegurando a segurança dos dados e a responsabilização dos agentes envolvidos.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

- Desenvolvimento e mitigação de riscos em sistemas de reconhecimento facial: Recomenda-se que os sistemas de reconhecimento facial sejam concebidos desde a fase inicial com medidas técnicas e organizacionais que assegurem precisão, segurança e mitigação de riscos, alinhadas aos princípios de privacy by design e privacy by default. O engajamento de diferentes partes interessadas (indústria, academia e sociedade civil) pode ser importante para aprimorar o design e a eficácia dessas tecnologias. Porém, é necessário reconhecer que não é possível eliminar totalmente os erros desses sistemas, sendo muitas vezes preciso equilibrar fatores como precisão, recall, equidade, discriminação e necessidade. Medidas proporcionais aos riscos podem ser adotadas, incluindo: informar os usuários sobre a possibilidade de erros, monitorar frequentemente o desempenho do sistema, manter rotinas regulares de atualização e revalidação dos modelos utilizados e realizar testagem frequente dos algoritmos em bases de dados diversificadas e representativas, considerando a variabilidade demográfica.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

- Limitações no uso do reconhecimento facial: Não é recomendável o uso de tecnologias de reconhecimento facial quando o tratamento de dados biométricos acarreta riscos elevados à privacidade dos titulares e quando não há justificativa proporcional para o tratamento, implementação de medidas mitigação de riscos e/ou indicação de base legal adequada.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

O tratamento de dados biométricos exige uma abordagem cautelosa e estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos.

Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes.

Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados.

Com base nisso, questiona-se:

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

- Ausência de medidas específicas e determinadas: Não existe um conjunto definido de medidas de segurança, técnicas e administrativas que devam ser consideradas indispensáveis para mitigar riscos de segurança. Assim, diversas salvaguardas podem

ser implementadas, isoladas ou conjuntamente, para alcançar uma abordagem proporcional e que considere a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento, bem como seu contexto específico.

- Exemplos de medidas técnicas, organizacionais e administrativas: Programa de Segurança da Informação; gerenciamento de acesso; registro das operações de tratamento; inviolabilidade dos dados pessoais; elaboração de relatório de impacto à proteção de dados (RIPD), quando aplicável; finalidades definidas; monitoramento de precisão; política de retenção; implementação de B-PETs; inclusão de cláusulas em contratos com prestadores de serviços; medidas de transparência; tratamento único (one-time), sem armazenamento desnecessário; e dissociação de dados.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

- Abordagem proporcional e observância da LGPD: Não existe um conjunto único de práticas aplicável universalmente. É fundamental adotar uma abordagem proporcional que considere o caso de uso e os riscos ou danos potenciais ao indivíduo, garantindo que o tratamento de dados biométricos esteja enquadrado em uma das bases legais da LGPD e observe os princípios de necessidade, não discriminação e transparência.
- Consentimento e opt-out: Quando o tratamento se basear no consentimento, o titular deve ter a possibilidade de exercer o direito de opt-out de forma simples e acessível, sem restrições desproporcionais ao serviço, sempre que tecnicamente viável. A limitação de funcionalidades pode ser legítima quando houver justificativa técnica concreta, devendo ser previamente comunicada de forma clara e transparente.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

- Boas práticas: Entre boas práticas possíveis, destacam-se a oferta de treinamentos específicos sobre o tema; o reforço, em políticas e procedimentos, de informações detalhadas sobre a forma adequada de tratamento desse tipo de dado; e a elaboração de relatórios de impacto à proteção de dados pessoais, quando aplicável.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes

multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

- Desafios práticos e abordagem proporcional: A ANPD deve reconhecer os desafios práticos na facilitação dos direitos dos titulares de dados quando os dados biométricos foram inseridos em um formato legível por máquina (por exemplo, seguindo o "processamento técnico específico"), de modo que podem não ser legíveis por pessoas e talvez não possam ser fornecidos em outro

formato. A orientação da ANPD, portanto, precisa ser: (i) proporcional; (ii) baseada em princípios; e (iii) suficientemente flexível para fornecer uma estrutura relevante para os métodos utilizados para facilitar os direitos de proteção de dados no contexto de dados biométricos, em linha com a orientação do ICO sobre dados biométricos. Uma abordagem proporcional para aplicar, interpretar e equilibrar os direitos de proteção de dados também deve reconhecer o impacto potencialmente negativo que a redução ou remoção de dados biométricos de um sistema de reconhecimento biométrico ou de um conjunto de dados de treinamento poderia ter no desenvolvimento do sistema (em particular no contexto de IA), incluindo na precisão final do sistema.

- **Transparência e direitos dos titulares:** Os mesmos princípios gerais para facilitar os direitos dos titulares de dados em relação aos dados biométricos aplicam-se a qualquer outro tipo de tratamento. Nesse sentido, medidas de transparência, como: (i) disposições claras e precisas em políticas de privacidade; e (ii) a divulgação de canais de atendimento, são fundamentais para que o titular possa exercer seus direitos. Quando apropriado, diferentes tipos de ferramentas de transparência podem ser usados para oferecer uma gama de informações a grupos vulneráveis, como o uso de vídeos, imagens e diferentes tipos de escrita. No que diz respeito à possibilidade de revogação, nos casos em que a base legal para o tratamento de dados é o consentimento, o titular deve ter um canal de fácil acesso, que possibilite a revogação de maneira simples, acessível e fácil.
- **Decisões automatizadas e artigo 20 da LGPD:** O titular dos dados tem o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. A interpretação dos direitos do titular dos dados deve observar os requisitos do artigo 20 da LGPD: (i) a existência de uma decisão; (ii) tomada unicamente com base em tratamento automatizado, sem qualquer influência humana; e (iii) que afete os interesses dos titulares de maneira ilegal ou abusiva e contrária à legislação.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

- **Hipóteses legais para tratamento de dados biométricos de crianças e adolescentes:** O tratamento de dados biométricos de crianças e adolescentes deve seguir as hipóteses legais previstas no artigo 11 da LGPD, aplicando-se também as regras do artigo 14, que exige respeito ao melhor interesse do menor. Segundo o Enunciado nº 1/2023 da ANPD, esses dados podem ser tratados com base nas hipóteses do artigo 7º ou 11 da LGPD, desde que haja observância e prevalência do melhor interesse da criança ou adolescente. Quando a base legal for o consentimento, ele deve ser claro e específico, abrangendo as finalidades do tratamento e, no tratamento de dados de crianças, fornecido pelo representante legal. É importante também reconhecer a possível tensão entre o consentimento dos pais e o melhor interesse da criança, por exemplo, no que diz respeito ao acesso a determinados serviços. Incentivamos, assim,

a ANPD a considerar essa possibilidade em suas orientações, a fornecer exemplos de casos de uso em que o consentimento dos pais pode ser mais apropriado, e a incentivar os controladores a adotarem uma abordagem orientada pelo contexto. O tratamento pode ocorrer ainda com fundamento em outras bases legais, desde que haja transparência adequada, observando os desafios do consentimento, como desequilíbrios de poder e direitos de revogação. Não há proibição absoluta ao uso de dados biométricos desse grupo, desde que observadas as salvaguardas previstas na lei, como a disponibilização de informações claras e acessíveis.

- Melhor interesse: O princípio do melhor interesse, previsto no art. 14 da LGPD, deve ser interpretado de forma concreta, contextualizada e não apriorística. Esse entendimento está alinhado ao Comentário Geral nº 14 do Comitê dos Direitos da Criança da ONU, que reforça o caráter flexível e multidimensional do conceito, devendo ser ponderado em conjunto com outros direitos fundamentais. Da mesma forma, deve-se reconhecer a condição peculiar da criança e do adolescente como pessoas em desenvolvimento, conforme previsto no ECA. Por isso, recomenda-se que a ANPD assegure margem de autonomia para que os controladores possam demonstrar, caso a caso, como o tratamento atende ao melhor interesse, inclusive permitindo ajustes e salvaguardas adicionais.
- Princípio da necessidade: A ANPD deve reconhecer que o cumprimento do princípio da necessidade não se limita a tratar o menor volume possível de dados, mas sim à utilização dos dados estritamente necessários para alcançar finalidades legítimas, em conformidade com os demais princípios da LGPD e com o melhor interesse de crianças e adolescentes. A tensão entre segurança e proteção de dados deve ser avaliada à luz do caso concreto, permitindo a devida ponderação entre valores eventualmente conflitantes, visto que, em determinados contextos, a coleta de dados pode representar a forma mais eficaz de proteger o melhor interesse de crianças e adolescentes. Assim, é fundamental que os controladores não sejam penalizados por realizarem, de forma justificada, o balanceamento entre o princípio da necessidade e outras obrigações legais, como a de salvaguardar o melhor interesse desse público.
- Divergências sobre o tratamento de dados biométricos de crianças: A ponderação entre os princípios do ecossistema de proteção de dados e o melhor interesse de crianças e adolescentes, assim como o potencial para interpretações divergentes, podem ser observados em um caso em que a UODO (autoridade polonesa de proteção de dados, https://www.edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en) concluiu que o uso de leitores biométricos por uma escola para controle de acesso ao refeitório era ilegal e desproporcional, pois envolvia dados sensíveis e, embora baseado no consentimento dos pais, não era estritamente necessário, já que existiam meios menos intrusivos de identificação. Contudo, posteriormente, o Tribunal Administrativo Provincial de Varsóvia (https://gdprhub.eu/index.php?title=WSA_w_Warszawie_-_II_SA/Wa_809/20), ao analisar o recurso da escola, trouxe um contraponto direto, anulando a decisão e a multa da UODO. O tribunal focou sua argumentação na interpretação do princípio da

minimização de dados. Ele considerou que o tratamento dos dados biométricos não era "excessivo", mas sim "adequado" para o objetivo. Para o Tribunal, a escola teria demonstrado que as alternativas, como o uso de cartões, apresentavam problemas (perda ou esquecimento), o que comprometia a eficiência do processo. Salientou, ainda, que a legislação não exige que o controlador use apenas o "mínimo estritamente necessário" de dados, mas sim que o uso seja proporcional e adequado para o propósito, mesmo que existam outras formas de alcançar o objetivo. Essa interpretação permite a adoção de tecnologias biométricas de aferição de idade, ainda que não sejam estritamente necessárias, enfatizando que o princípio da minimização de dados não deve ser interpretado como um entrave à implementação de soluções que, na prática, se mostrem mais robustas e eficazes para proteger os interesses dos usuários.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

- Hipóteses legais para tratamento de dados biométricos de crianças e adolescentes: O tratamento de dados biométricos de crianças e adolescentes pode ser amparado em qualquer das hipóteses legais previstas no artigo 11, haja visto o disposto no Enunciado ANPD nº 1/2023. Nesse sentido, a hipótese legal de garantia da prevenção à fraude e à segurança do titular ganha especial relevância nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (Art. 11, II, "g", LGPD). Quando a hipótese legal for o consentimento, deve haver transparência quanto às finalidades do tratamento.
- Medidas técnicas e organizacionais: As medidas de segurança aplicáveis a qualquer tratamento de dados devem ser definidas à luz da finalidade pretendida, independentemente de envolver dados biométricos ou dados pessoais de crianças e adolescentes. Tais medidas podem incluir a implementação de programas de segurança da informação, a adoção de controles e gestão de acesso e, quando aplicável, a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

18. Em casos de verificação ou estimativa de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

- Princípio da necessidade: O princípio da necessidade deve ser compreendido não como uma limitação ao tratamento do menor volume possível de dados, mas sim como o uso dos dados essenciais para atingir finalidades legítimas, em consonância com os demais princípios da LGPD e o melhor interesse de crianças e adolescentes. A relação entre a proteção de dados e a segurança deve ser analisada conforme as circunstâncias específicas, permitindo uma ponderação cuidadosa entre valores que possam ser conflitantes. Em certos casos, a coleta de dados adicionais pode ser a medida mais adequada para garantir a proteção do melhor interesse das crianças e adolescentes. Portanto, é crucial que os controladores possam realizar essa ponderação sem risco de

penalização, especialmente quando conciliam o princípio da necessidade com o melhor interesse. Conforme observado acima, algumas tecnologias, como a estimativa de idade - nos quais a imagem é utilizada para estimar a idade do indivíduo sem identificá-lo - e o agrupamento de fotos, não se enquadram na definição de dados biométricos e podem constituir mecanismos de certificação eficazes e proporcionais.

- Proporcionalidade e análise de risco: Como destacado pela Câmara-e.net em outras contribuições, a escolha do mecanismo de aferição de idade deve ser orientada pela proporcionalidade e por uma análise baseada em risco. A aferição de idade pode ser implementada com diferentes níveis de robustez, dependendo do risco. Incentivamos a ANPD a considerar o contexto mais amplo e a permitir escolha e flexibilidade nas soluções de aferição de idade que organizações e plataformas online podem utilizar. Também é importante identificar o motivo específico para o uso de sistemas biométricos na aferição de idade. Por exemplo, os motivos podem variar – para determinar se o usuário é um adulto ou menor de 18 anos, se o usuário tem a idade mínima para os termos de serviço ou a idade do usuário para oferecer uma experiência apropriada à sua faixa etária. Instituições como o EDPB (https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf), o ICO (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/>) e o DPC (https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf) adotam essa abordagem em seus guias e recomendações. Conforme o DPC, a avaliação de riscos deve considerar, entre outros fatores: (i) o tipo de dado pessoal tratado; (ii) a sensibilidade desses dados; (iii) o tipo de serviço oferecido à criança ou ao adolescente; (iv) a acessibilidade dos dados por terceiros; e (v) o tratamento posterior dos dados, incluindo eventuais compartilhamentos com outras organizações e suas finalidades.
- Flexibilidade na definição dos métodos e atenção aos riscos à privacidade: As orientações da autoridade devem priorizar a indicação de exemplos de métodos inadequados, em vez de impor regras rígidas, permitindo que os agentes de tratamento adotem soluções adaptadas ao contexto do serviço, à finalidade do tratamento e ao modelo de negócio.

MINUTA DE CONTRIBUIÇÃO PARA A TOMADA DE SUBSÍDIOS DA ANPD SOBRE DADOS BIOMÉTRICOS

Contribuição elaborada pelo Centro de Estudos de Segurança e Cidadania (CESeC) em parceria com a Defensoria Pública da União (DPU) e com membra(s) do grupo de pesquisa EDHIA da Escola Nacional da Defensoria Pública da União.

Esta contribuição à Tomada de Subsídios da ANPD sobre tratamento de dados biométricos é fundamentada nas evidências empíricas e nos estudos produzidos pelo projeto *Panóptico* do CESeC, pelo relatório [Mapeando a Vigilância Biométrica: Levantamento nacional sobre o uso do reconhecimento facial na segurança pública \(CESeC e DPU, 2025\)](#) e pela experiência em pesquisas colaborativas sobre inteligência artificial, justiça criminal e proteção de dados.

Segundo o monitoramento do [Projeto Panóptico](#), atualmente há 408 projetos ativos¹ de tecnologias de reconhecimento facial na segurança pública brasileira. Essa expansão acelerada ocorreu à revelia de marcos regulatórios específicos, sem padronização técnica, sem avaliações de impacto e à margem de mecanismos de transparência e controle. Como resultado, o tratamento de dados biométricos tem violado princípios fundamentais da Lei Geral de Proteção de Dados, como necessidade, proporcionalidade e não discriminação. Proporciona, também, assim como tem gerado riscos graves à proteção de direitos, especialmente de grupos historicamente vulnerabilizados.

BLOCO I – DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Devem ser considerados dados biométricos todos aqueles derivados de características físicas, fisiológicas ou comportamentais de uma pessoa natural que, por meio de tratamento técnico específico, permitam ou confirmem sua identificação única, como imagens faciais ou dados dactiloscópicos. Essa definição está alinhada ao GDPR (art. 4º, item 14), ao ICO do Reino Unido e às orientações da ANPD na Nota Técnica nº 17/2025. Essa caracterização é essencial para garantir o tratamento diferenciado que os dados biométricos demandam, dada sua natureza sensível e seu potencial lesivo à privacidade e à autodeterminação informativa.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos?

A transparência ativa é uma obrigação legal prevista nos arts. 6º, VI e 9º da LGPD e é essencial para que os titulares compreendam como seus dados são tratados. Os controladores

¹ Projetos ativos são aqueles que estão em teste, em uso, em processo de implantação, os projetos que já possuem algum termo de referência. Isto significa que todas as fases de planejamento e preparação estão em andamento ou foram concluídas, e as tecnologias de reconhecimento facial estão sendo colocadas em prática enquanto uma política pública de segurança.

devem publicar documentos fundamentais em portais de acesso público, incluindo: políticas de privacidade, relatórios de impacto, contratos com fornecedores, fundamentos normativos, critérios técnicos, e localização e abrangência dos dispositivos.

No entanto, dados empíricos mostram que essa transparência está longe de ser garantida no Brasil. Segundo o relatório *Mapeando a Vigilância Biométrica*, apenas 29% dos contratos de aquisição de Tecnologias de Reconhecimento Facial (TRF) analisados estavam disponíveis publicamente, e 64% dos projetos não informam a base legal utilizada para justificar o uso da tecnologia. Além disso, em 84% dos contratos em vigor, não havia qualquer cláusula sobre proteção de dados pessoais, demonstrando descumprimento sistemático dos princípios LGPD.

O relatório [*Vigilância por Lentes Opacas*](#) (CESeC, 2024) demonstrou que, em mais de 70% dos projetos de TRF investigados, não havia qualquer informação sobre fornecedores ou contratos nos portais públicos, e cerca de 80% não apresentavam relatórios de impacto. Esses dados evidenciam o descumprimento sistemático dos deveres de transparência ativa. Uma clara violação ao art. 9º da LGPD, que determina a disponibilização pública de informações sobre o tratamento de dados, especialmente quando realizado pelo poder público.

No campo esportivo, o relatório [*Esporte, Dados e Direitos*](#) revela que nenhum dos estádios analisados publica informações claras sobre os sistemas biométricos utilizados, sobre suas finalidades, sobre o período do armazenamento ou sobre formas de acesso e correção de dados. Mesmo em situações em que o uso da biometria facial era obrigatório para entrada no evento, não havia canais acessíveis para o exercício de direitos pelos titulares.

Diante disso, recomenda-se que a ANPD regule a obrigatoriedade das seguintes práticas de transparência ativa: publicação prévia e periódica de Relatórios de Impacto à Proteção de Dados Pessoais (DPIAs); divulgação da base legal, objetivos do tratamento, tempo de retenção dos dados, fornecedores envolvidos, critérios técnicos adotados e métricas de erro (como falsos positivos e negativos); inclusão de cláusulas contratuais específicas sobre proteção de dados nos instrumentos firmados com empresas fornecedoras; criação de canais acessíveis e funcionais para o exercício dos direitos dos titulares, com linguagem inclusiva e disponibilização em múltiplos formatos; nomeação e visibilidade do encarregado pelo tratamento de dados (DPO), com garantia de resposta adequada e no prazo legal; publicação ativa de dados consolidados sobre o uso das TRFs, incluindo número de identificações, correções, exclusões e solicitações de revisão. Além disso, recomenda-se à ANPD que incentive modelos de certificação pública de boas práticas em transparência biométrica. Tomando como exemplo as experiências promovidas na Europa com base nas diretrizes do *European Data Protection Board* e nos mecanismos de *Data Protection Impact Assessments* previstos no GDPR.

3. De que forma a biometria comportamental deveria ser tratada em comparação à biometria tradicional?

A biometria comportamental, como padrões de digitação, movimento ocular, modo de andar, entonação da voz, entre outros, deve ser tratada com elevado grau de cautela. Conforme artigo 6.2 e Anexo III, do Ato da União Europeia sobre Inteligência Artificial, esse tipo de sistema biométrico é caracterizado como de alto risco, motivo pelo qual sua aplicação é restrita a situações e propósitos específicos, incluindo a obrigatoriedade de estabelecer uma gestão de riscos.

A coleta da biometria comportamental tende a ser contínua e imperceptível para o titular, o que eleva o risco de vigilância permanente e uso indevido. Esse tipo de dado amplia significativamente a assimetria entre agentes de tratamento e titulares e pode ser utilizado para fins que extrapolam a finalidade original, como inferência de emoções, produtividade ou comportamento social. Por isso, devem ser exigidas salvaguardas específicas: proibição de coleta invisível sem consentimento informado, avaliações de impacto obrigatórias, adoção de medidas de minimização, anonimização e limitação de finalidade. A experiência internacional (como nas diretrizes da Commission Nationale de l'Informatique et des Libertés e do European Data Protection Board) aponta para a necessidade de proibir usos invasivos, especialmente em contextos sensíveis como na educação, na saúde, no trabalho e na segurança pública.

Além disso, é necessário vislumbrar que impactos adversos da biometria comportamental podem transcender o nível individual e gerar impactos sociais. Nesse sentido, o trabalho de Martyna Kalvaitytė², ao utilizar métodos mistos de modelagem computacional para a análise de 266 respostas de feedback à consulta da Comissão Europeia sobre a Lei Europeia de IA (EU AI Act) - a fim de abordar a questão de pesquisa de quais são os principais impactos negativos da IA que não são abordados pela regulamentação - aponta que a manipulação dos utilizadores, resultando em efeitos adversos associados às tecnologias de identificação biométrica, e os efeitos sobre os trabalhadores e grupos de crianças estão entre as violações globais dos direitos humanos identificadas como os principais impactos negativos da IA ainda não abordados. O trabalho apresenta argumentos para o reconhecimento da existência de um novo tipo de impacto algorítmico, nomeadamente impactos a nível social, o que a tese de Viviane Dallasta³ denomina de “impactos tecnossociais”, uma vez que advindos das aplicações técnicas da IA, sem a consideração preliminar acerca do impacto social das aplicações, por isso o termo “tecno” precede o

² KALVAITYTĖ, Martina. **Unregulated Negative Impacts of AI: Mixed Methods Analysis of Feedback Responses to the EU AI Act Proposal**. Public Policy Master Thesis. SciencesPo, School of Public Affairs. Abril de 2022. Disponível em:

<<https://www.sciencespo.fr/public/sites/sciencespo.fr/public/files/KALVAITYTE.pdf>>.

³ GROSSI, Viviane Ceolin Dallasta Del. A absoluta prioridade da criança no ambiente digital na era da IA: a Devida Diligência em Direitos Humanos e os impactos tecnossociais da Inteligência Artificial. 2024. Tese (Doutorado em Direitos Humanos) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2024. doi:10.11606/T.2.2024.tde-08112024-165318.

“social”. O reconhecimento e o enfrentamento de tais impactos a nível social é crucial devido à ausência de proteções contra estes impactos sociais negativos.

BLOCO II - HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada?

O consentimento só pode ser considerado válido se for livre, ou seja, não condicionado ao acesso aos serviços essenciais, e se for informado com linguagem clara e acessível. Em contextos como segurança pública, escolas, transporte, saúde e estádios, onde o cidadão não tem real margem de escolha, o consentimento é presumivelmente inválido, dada a assimetria de poder. Essa posição está respaldada pelas diretrizes do European Data Protection Board (EDPB, 2020) e nas decisões da Commission Nationale de l'Informatique et des Libertés (CNIL, França). Na Suécia, a autoridade de proteção de dados multou as escolas que implementaram o reconhecimento facial. Destacou, na ocasião, o vício de consentimento que decorre da posição assimétrica assumida a partir da autoridade moral da direção escolar⁴.

Desse modo, a ANPD deve declarar expressamente a inadequação do consentimento nesses contextos e exigir avaliação de impacto e alternativas menos intrusivas em todos os casos, garantindo que o titular de dados não esteja adstrito ao reconhecimento facial para conseguir acessar os serviços.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude”? Quais salvaguardas devem ser implementadas?

A base legal da “prevenção à fraude” só é legítima quando o risco for iminente, documentado e proporcional ao grau de intrusão do tratamento. A ANPD deve exigir: Relatório de Impacto à Proteção de Dados detalhado; comprovação de que a biometria é a única solução viável; direito de contestação humana; prazo claro de retenção; e exclusão automática após verificação. A aplicação ampla e irrestrita dessa base legal viola o princípio da necessidade (art. 6º, III, LGPD) e pode resultar em discriminação algorítmica.

Vale ressaltar a inexistência de estudos que assegurem que o recurso ao reconhecimento facial evite golpes aos usuários; pelo contrário, por se tratar de um tipo de dado coletado passivamente, pode ampliar as hipóteses de acesso indevido em sistemas eletrônicos, como tem sido reportado frequentemente nas mídias, inclusive em âmbito federal (COUTINHO, Mateus. PF suspeita que 3.000 conta do [Gov.br](https://gov.br) tinham sido fraudadas com biometria⁵).

⁴ SWEDEN. KamR Stockholm. Case N° 5888-20. Swedish DPA vs Upper Secondary School Board. 20.aug.2019. Available at: [KamR Stockholm - Case No. 5888-20 - GDPRhub](https://www.gdprhub.com/cases/5888-20-swedish-dpa-vs-upper-secondary-school-board/). Access at 04.jun.2025.

⁵ UOL Política. 13.05.2025. Disponível em <https://noticias.uol.com.br/politica/ultimas-noticias/2025/05/13/pf-suspeita-de-fraudes-de-reconhecimento-facial-em-3-mil-contas-do-govbr.htm>. Acesso em 24.06.2025).

6. Quais critérios e salvaguardas devem ser observados quando a base legal for “cumprimento de obrigação legal ou regulatória”, especialmente por entidades públicas?

Nos casos em que o tratamento de dados biométricos se baseia na hipótese legal do art. 11, II, “a” da LGPD, é imprescindível que essa obrigação esteja expressamente prevista em norma jurídica específica, acessível ao público e diretamente relacionada à finalidade do tratamento e inserida na competência legal de atuação, caso se trate de entidade pública. A generalidade normativa não pode ser utilizada para legitimar práticas de coleta e uso massivo de dados sensíveis. O relatório elaborado pelo CEsEC em parceria com a Defensoria Pública da União (DPU) revela que, em diversos projetos de TRF no Brasil, essa base tem sido invocada de maneira genérica, sem a apresentação de fundamentos legais claros, tampouco com qualquer forma de controle externo ou avaliação de impacto prévia.

A ausência de uma base legal compromete o princípio da legalidade, da finalidade e o direito à autodeterminação informativa. Além disso, fere as recomendações do Comitê Consultivo da Convenção 108+ do Conselho da Europa. Dentre elas, é estabelecido que o uso de dados biométricos por autoridades públicas precisa ser excepcional, justificado por obrigações legais bem delimitadas e acompanhado de garantias específicas. Dessa forma, a ANPD deve exigir dos controladores públicos que invoquem essa base legal à adoção de critérios rigorosos, entre eles: publicação ativa e acessível da norma jurídica específica que fundamenta o tratamento biométrico; a realização de DPIA, a ser revisada periodicamente; mecanismos de supervisão institucional e auditorias independentes sobre a legalidade e proporcionalidade do uso da tecnologia; disponibilização de canais efetivos de exercício de direitos pelos titulares; e definição de prazos claros para retenção e descarte dos dados coletados, compatíveis com a finalidade legal.

O simples enquadramento do tratamento como decorrente de “obrigação legal” não pode isentar o Estado de demonstrar a estrita necessidade do uso de tecnologias intrusivas como as TRF. Em especial, no campo da segurança pública, o uso de dados biométricos sem legislação específica, sem controle social e sem transparência ativa, conforme documentado pelo projeto Panóptico, implica risco elevado de violações de direitos fundamentais e da própria função protetiva da LGPD.

7. Quais os limites para uso da base legal “estudos por órgãos de pesquisa”, mesmo com anonimização? Quais salvaguardas adicionais seriam necessárias?

Mesmo em pesquisas, dados biométricos exigem salvaguardas específicas, pois sua singularidade aumenta o risco de reidentificação, especialmente em cruzamentos de bases. A anonimização deve seguir padrões técnicos robustos ([ISO/IEC 20889:2018](#)), com cláusulas de irreversibilidade, auditorias de risco e impedimento contratual de reidentificação. A ANPD deve exigir documentação clara sobre métodos utilizados, a submissão da pesquisa aos comitês de ética institucionais independentes, controles técnicos e operacionais de

segurança e critérios para compartilhamento entre instituições. Além disso, recomenda-se proibir o uso de dados biométricos para fins de pesquisa em contextos que envolvam grupos vulneráveis como crianças, população em situação de rua ou privada de liberdade, sem um marco legal claro e salvaguardas excepcionais. A invocação da base de pesquisa não pode se tornar um atalho para legitimar práticas opacas de treinamento algorítmico, como observado nos escândalos envolvendo o uso de bancos biométricos sem consentimento no Brasil e no exterior.

8. Como garantir que o uso de tecnologias de reconhecimento facial observe os princípios da LGPD e evite discriminação?

A garantia de que o uso de tecnologias de reconhecimento facial esteja em conformidade com os princípios da LGPD, especialmente os da necessidade, proporcionalidade, transparência e não discriminação, exige, antes de tudo, a adoção de padrões técnicos rigorosos e auditáveis desde o momento do projeto até a operação contínua dos sistemas. A literatura técnica e os documentos orientadores da European Data Protection Board, da Autoridade de Proteção de Dados do Reino Unido (ICO) e da Convenção 108+ do Conselho da Europa apontam que os sistemas devem obrigatoriamente passar por avaliações de impacto à proteção de dados que incluam não apenas a base legal e a finalidade declarada, mas também a arquitetura do sistema, o tipo de algoritmo usado, o treinamento de modelos e a qualidade da base de referência (base de rostos).

Um dos principais riscos técnicos associados aos sistemas de reconhecimento facial é a alta taxa de erro, sobretudo em grupos sub-representados nos *datasets* de treinamento. Estudos como o *Gender Shades*, de Joy Buolamwini e Timnit Gebru (2018), revelaram que algoritmos de reconhecimento facial comercializados globalmente apresentavam taxas de erro superiores a 30% em mulheres negras, enquanto registravam menos de 1% em relação a homens brancos. Esses vieses discriminatórios ocorrem por fatores como baixa diversidade nos dados de treinamento, variações em iluminação, ângulo e qualidade das imagens, além da própria modelagem algorítmica utilizada.

Para mitigar esses riscos, é necessário exigir que os operadores desses sistemas publiquem, de forma transparente, métricas de desempenho como False Match Rate (FMR), False Non-Match Rate (FNMR) e Equal Error Rate (EER), segmentadas por raça, gênero e idade. Além de garantir a revisão humana qualificada nos casos em que as decisões impactem direitos fundamentais. É igualmente essencial a adoção de mecanismos de criptografia e anonimização robustos (como *templates* canceláveis e *hashing* com *salting*), a limitação de retenção de dados, e a vedação ao uso da tecnologia em ambientes públicos para fins de vigilância generalizada, como recomenda o European Data Protection Board.

Ademais, os sistemas devem registrar logs de uso que permitam rastreabilidade de acessos e comparações, submetendo-se a auditorias independentes, com relatórios publicamente acessíveis. Sem essas salvaguardas técnicas e institucionais, o uso de reconhecimento facial infringe os princípios da LGPD e perpetua práticas discriminatórias disfarçadas de

neutralidade tecnológica, com consequências graves. Tais como falsos positivos, abordagens ilegais e exclusões sociais injustificadas.

Alguns países, como o Reino Unido, reconhecendo os riscos que contornam a utilização de TRFs, definiram autoridades nacionais específicas para o acompanhamento da contratação e da operacionalização de equipamentos que tratem dados biométricos à distância, em tempo real ou diferido⁶. Essas autoridades são responsáveis por realizar o monitoramento, emitir opiniões e produzir relatórios sobre a compatibilidade entre o uso das tecnologias e os direitos fundamentais.

Além disso, a implementação de sistemas de reconhecimento facial deve ser condicionada à lei anterior e limitada aos propósitos específicos para os quais a sua contratação foi definida⁷. Doze princípios são utilizados como bases para aferir a regularidade da TRF: i) propósito específico; ii) revisões periódicas; iii) transparência, iv) responsabilidade, v) prévia regulamentação e comunicação, vi) limitação do armazenamento, vii) restrição de acesso às imagens, viii) respeito aos padrões operacionais aprovados, ix) proteção contra uso indevido, x) auditoria regular, xi) efetividade e xii) atualidade⁸.

No caso europeu, por exemplo, a União Europeia, além de reconhecer que TRFs são sistemas de alto risco de tratamento de dados pessoais e reafirmar a necessidade de prévia autorização legal, estabeleceu um quadro normativo em que a utilização de sistemas de identificação biométrica à distância em tempo real somente pode ocorrer para identificação de pessoa suspeita de prática de delitos com pena máxima superior a quatro anos^[1]. Essa utilização deve observar a limitação geográfica e temporal, bem como ser antecedida de uma avaliação de impacto sobre os direitos fundamentais. A operacionalização de sistemas de reconhecimento facial somente poderá ocorrer também após prévia autorização judicial ou de autoridade administrativa independente.

No relatório “Mapeando a Vigilância Biométrica”, produzido conjuntamente pelo Panóptico e pela DPU, apontamos recomendações na matéria:

- ❖ Proposição e discussão de projeto de lei que preveja, em âmbito nacional, as vedações, os limites e as condicionantes ao uso tecnologias de reconhecimento facial para fins de segurança pública, estabelecendo limites claros para o uso dessa tecnologia, priorizando a proteção de direitos fundamentais, com o estabelecimento da

⁶ UNIÃO EUROPEIA. Regulamento (EU) 2024/1689 do Parlamento Europeu e do Conselho. Cria regras harmonizadas em matéria de inteligência artificial. Jornal Oficial da União Europeia (PT), Série L, 12.jul. 2024. e GENTILE, Giulia. Does Big Brother Exist? Facial Recognition Technology in the United Kingdom. In: The Cambridge Handbook of Facial Recognition in the Modern State. Org.: Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press, 2024, p. 173.

⁷FUSSEY, Pete; MURRAY, Daragh. Independent report on the London Metropolitan Police service's trial of live facial recognition technology. Essex: University of Essex Repository, July, 2019.

⁸REINO UNIDO. Código de Práticas sobre Sistemas de Câmeras de Vigilância. Nov. 2021. Disponível em: <https://www.gov.uk/government/publications/update-to-surveillance-camera-code> . Acesso em 13.02.2025.

suspensão do uso das TRFs para fins de segurança pública até que haja definição em lei;

- ❖ Na regulamentação, devem ser considerados quadros normativos e boas práticas que, reconhecendo a natureza de alto risco de sistemas de reconhecimento facial, que abordem as seguintes medidas:
 - Desenvolvimento de protocolos padronizados de abordagem e uso do reconhecimento facial, que tragam uniformidade, garantam a transparência e o respeito ao devido processo legal;
 - Estabelecimento de mecanismos de auditoria e supervisão independentes para fiscalizar o uso da tecnologia, garantindo a conformidade com as normas de proteção de dados e defesa dos direitos humanos;
 - Auditoria dos contratos em vigência e transparência obrigatória dos novos contratos, para investigar possíveis desvios e mau uso do dinheiro público;
 - Capacitação das forças de segurança e servidores públicos envolvidos para promover informações técnicas sobre a tecnologia e seus efeitos, bem como questões éticas e proteção de dados;
 - Garantia de informação à população sobre o uso da tecnologia, suas implicações e maior conscientização sobre o consentimento livre e informado;
 - Desenvolvimento de mecanismos que garantam o acesso a bases de dados atualizadas e íntegras, como forma de mitigar erros em relação de mandados de prisão inativos;
 - Elaboração e divulgação ampla de relatórios sobre os impactos do uso da tecnologia, fornecendo à população dados sobre eficiência e impactos sociais do reconhecimento facial.
- ❖ Delimitação de critérios e condicionantes, com a devida transparência e sujeito ao controle externo, para a elaboração e utilização da lista de pessoas de interesse dos órgãos policiais, com a indicação das hipóteses que justifiquem, limitação do tempo de inclusão e com a garantia do direito de petição para a retirada dos dados;
- ❖ Definição da necessidade de prévia autorização judicial para a utilização de tecnologias de reconhecimento facial para fins de investigação, persecução ou cumprimento de mandados de prisão vinculados aos crimes que admitam o emprego desse tipo de tecnologia;
- ❖ Identificação das empresas privadas que atuam no planejamento, produção e operação de softwares de coleta, armazenamento e tratamento de dados pessoais para fins de segurança pública, cujo funcionamento deve estar atrelado a prévia autorização pela autoridade administrativa competente;
- ❖ Fixação de período máximo de armazenamento das imagens capturadas e limitação geográfica, com o descarte imediato de imagens faciais de pessoas que não estejam na lista de interesse da Polícia;
- ❖ Definição de limites mínimos de *score* de correspondência para a operacionalização de softwares de reconhecimento facial como forma de mitigar os falsos positivos;
- ❖ Previsão de medidas para não repetição, prevenção e reparação dos danos de pessoas e coletividades atingidas por tratamento discriminatório decorrente do emprego de tecnologias de reconhecimento facial.

9. Como garantir eficácia e correção de falhas como falsos positivos/negativos nos sistemas de reconhecimento facial?

A eficácia e confiabilidade das TRFs só podem ser asseguradas com (i) testes rigorosos em contextos reais e diversos, antes da implementação; (ii) exigência de métricas públicas sobre taxas de erro (como FMR/FNMR – False Match/Non-Match Rates); (iii) auditorias externas e independentes; e (iv) mecanismos de contestação acessíveis aos titulares. Como apontado nos relatórios do CESeC, o Brasil carece de padrões técnicos mínimos e de qualquer tipo de certificação prévia de algoritmos utilizados. Em ambientes como estádios e vias públicas, por exemplo, são registrados altos índices de falsos positivos que resultam em constrangimentos ilegais e detenções injustificadas. O erro técnico não pode ser absorvido como “falha tolerável”. Trata-se antes de um dano real à reputação, à liberdade e à dignidade dos cidadãos.

10. Em que contextos o uso de reconhecimento facial não é recomendado? Quais alternativas menos invasivas podem ser empregadas?

O uso de tecnologias de reconhecimento facial não é recomendado em contextos de vigilância massiva, como eventos públicos, transportes, escolas, centros de compras, e estádios, como alertam a ONU, a Autoridade Europeia de Proteção de Dados (EDPS) e a própria Recomendação 5/2021 da ANPD. Nesses espaços, a coleta se dá de forma, geralmente, indiscriminada, desproporcional e opaca, oferecendo elevado risco de abuso e reforço de estigmas sociais. Alternativas menos intrusivas incluem sistemas de verificação por *QR Code* temporário, cartões magnéticos, *tokens* criptografados e controle por senha. A adoção de tecnologias que minimizem a coleta de dados sensíveis deve ser prioritária. O uso de reconhecimento facial deve ser reservado a contextos excepcionais, com justificativa detalhada e proporcionalidade comprovada, nunca como padrão.

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis?

Dados biométricos, por serem permanentes e não substituíveis, exigem proteção reforçada. Medidas técnicas indispensáveis incluem: criptografia forte dos templates, anonimização ou pseudonimização sempre que possível, retenção limitada, controle rigoroso de acesso e logging com auditoria. Administrativamente, devem ser exigidas avaliações de impacto (DPIA), planos de resposta a incidentes, auditorias periódicas, nomeação de DPOs e políticas claras de governança. Tais requisitos devem ser exigidos como condição mínima de conformidade com a LGPD. Como observado no relatório elaborado pelo CESeC e pela DPU, a maioria dos projetos públicos com reconhecimento facial no Brasil carece dessas salvaguardas. A ANPD deve exigir parâmetros mínimos de avaliação de riscos que incluem análise de viés, reidentificação e impactos em direitos humanos e sobre grupos vulneráveis, assegurando conformidade com a LGPD e normas internacionais.

12. Quais boas práticas devem ser observadas para evitar discriminação ilícita quando funcionalidades não essenciais dependem de biometria?

Nos casos em que funcionalidades específicas de um serviço dependem de autenticação biométrica, os controladores devem garantir alternativas tecnológicas viáveis, como autenticação por token ou senha, para evitar discriminação indireta. Essa prática deve ser acompanhada de avaliações de impacto e consulta pública, principalmente em serviços digitais amplamente utilizados. A recusa do titular em fornecer seus dados biométricos, quando o consentimento for a base legal, não pode acarretar exclusão ou desvantagem desproporcional, a não ser em situações em que o uso da biometria seja tecnicamente indispensável, devidamente justificado e documentado.

13. Quais boas práticas devem ser adotadas para garantir tratamento transparente e responsável?

Entre as boas práticas esperadas estão: publicação de relatórios periódicos de impacto à proteção de dados; disponibilização pública das bases legais e finalidades do tratamento; detalhamento das métricas de erro (FMR, FNMR) por grupo demográfico; canais acessíveis para que titulares possam questionar o uso de seus dados; e mecanismos automatizados de revogação de consentimento. Os projetos de implementação de TRFs devem ser concebidos segundo os princípios de *privacy by design* e accountability, com documentação pública das decisões técnicas e legais.

14. Como garantir autodeterminação informativa em contextos de tratamento massivo e contínuo, como smart cities ou estádios?

Em iniciativas de cidades inteligentes, vigilância urbana ou controle de multidões, como mostrado no relatório [Vigilância por lentes opacas](#), a coleta contínua e opaca de dados biométricos ocorre com baixa ou nenhuma transparência. Para garantir autodeterminação informativa, é essencial que o uso dessas tecnologias esteja submetido a notificações visíveis e acessíveis no local, campanhas de informação pública, mecanismos de exclusão de dados (quando possível), e consulta pública prévia às comunidades afetadas. A coleta massiva sem consentimento informado, sobretudo em espaços com presença de grupos vulneráveis, como crianças, configura violação dos direitos previstos nos artigos 6º e 18 da LGPD. É necessário observar, ainda, os padrões interamericanos de direitos humanos sobre o direito à autodeterminação informativa, conforme explicitado pela corte IDH no caso *Membros da Corporación Colectivo de Advogados "José Alvear Restrepo" Vs. Colômbia*.

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

A garantia desses direitos exige mecanismos acessíveis e contínuos de informação clara sobre o tratamento, incluindo linguagem simples e multicanal (digital e físico), direito à revisão

humana em decisões automatizadas (art. 20 da LGPD), possibilidade real de exclusão de dados e transparência sobre a base legal utilizada. Sistemas implementados em locais públicos, como escolas ou estádios, devem ser informados com antecedência, inclusive com sinalização visual e acessível no local e, sempre que possível, oferecer aos usuários alternativas ao fornecimento de dados biométricos.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O tratamento de dados biométricos de crianças e adolescentes deve observar simultaneamente a LGPD e o Estatuto da Criança e do Adolescente (ECA), que estabelece a prioridade absoluta da proteção integral e do melhor interesse do menor (art. 227 da CF e art. 1º do ECA). Isso implica garantir a participação informada dos pais ou responsáveis por meio de consentimento específico, livre e destacado, além de assegurar canais de comunicação claros e contínuos. A hipótese legal aplicável será, em regra, o consentimento ou, excepcionalmente, o cumprimento de obrigação legal, desde que demonstrada a estrita necessidade. O relatório [Esportes, Dados e Direitos](#) revela o uso de reconhecimento facial em estádios brasileiros sem qualquer aviso prévio ou consentimento dos responsáveis legais, expondo crianças a vigilância estatal indevida, em violação tanto à LGPD quanto ao ECA. Tais práticas devem ser vedadas. A coleta biométrica só pode ocorrer com avaliações de impacto, adoção de medidas técnicas e organizacionais robustas e previsão de alternativas não discriminatórias em caso de recusa ao consentimento.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

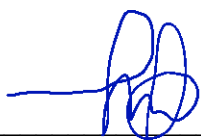
Mesmo nos casos em que haja base legal, como o consentimento ou o cumprimento de obrigação legal, o uso de tecnologias de reconhecimento facial em ambientes educacionais deve ser fortemente desencorajado. A LGPD exige o cumprimento do princípio da necessidade, e o ECA reforça o dever de assegurar proteção integral e priorizar o melhor interesse da criança e do adolescente. O reconhecimento facial, por seu caráter altamente invasivo e os riscos comprovados de discriminação e reidentificação, não se justifica em escolas, onde há alternativas menos intrusivas para fins de controle de frequência e de segurança. Além disso, o consentimento, mesmo quando formalmente obtido, pode não ser livre ou plenamente informado em contextos marcados por assimetrias de poder, como a relação entre escola pública e famílias em situação de vulnerabilidade. Assim, o mais coerente com a LGPD, com o ECA e com boas práticas internacionais é proibir esse tipo de tratamento nessas instituições, garantindo soluções que respeitem a privacidade, o desenvolvimento e a autonomia dos estudantes.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Essa prática deve ser precedida de avaliação de impacto, demonstrando que não há alternativa menos intrusiva. Sempre que possível, deve-se optar por meios não biométricos ou sistemas que não retenham os dados. O tratamento deve ser limitado à finalidade específica, com clara exclusão após o uso, e não pode ser usado para fins secundários, como de publicidade. A coleta de biometria apenas para fins de acesso a entretenimento digital, sem garantias, viola os princípios da necessidade e do melhor interesse da criança e do adolescente previstos na LGPD.

Com esta contribuição, buscamos colaborar de forma construtiva com o processo regulatório conduzido pela ANPD, oferecendo subsídios baseados em evidências empíricas, experiências de campo e boas práticas nacionais e internacionais. Reforçamos a importância de uma regulação robusta, transparente e centrada na proteção de direitos fundamentais, especialmente diante do avanço do uso de tecnologias biométricas em contextos de alta sensibilidade. Colocamo-nos à disposição para aprofundar o diálogo e contribuir com informações adicionais que fortaleçam a atuação da Autoridade em defesa da privacidade, da autodeterminação informativa e da justiça social.

Reiteramos nossa disposição para contribuir com o tema e para esclarecimentos adicionais. Certos da relevância da temática e da importância da atuação da ANPD, subscrevemo-nos:



Pablo Nunes
Coordenador do Centro de Estudos
de Segurança e Cidadania (CESeC)



Thallita Lima
Coordenadora de Pesquisa do Centro
de Estudos de Segurança e Cidadania



Gabriel Saad Travassos
Defensor Público Federal
Membro do Grupo de Trabalho Rua

Lutiana Valadares Fernandes Barbosa
Defensora Pública Federal
Membra do Grupo de estudos EDHIA da ENADPU

Frederico Aluísio Carvalho Soares
Defensor Público Federal
Defensor Nacional de Direitos Humanos



Rio de Janeiro, 01 de agosto de 2025
OFÍCIO PRESI-167/2025

Ao Senhor
WALDEMAR GONÇALVES ORTUNHO JÚNIOR
Diretor-Presidente da
Autoridade Nacional de Proteção de Dados - ANPD

Ref.: Tomada de Subsídios sobre Tratamento de Dados Pessoais Sensíveis - Dados Biométricos

Prezado Senhor,

A **Confederação Nacional das Seguradoras – CNseg**, entidade associativa que congrega as Federações que representam as empresas integrantes dos segmentos de seguros, resseguros, previdência privada e vida, saúde suplementar e capitalização, vem apresentar, na forma abaixo, as suas contribuições à **Tomada de Subsídios sobre Tratamento de Dados Pessoais Sensíveis - Dados Biométricos**, através das respostas às 18 (dezoito) questões formuladas pela ANPD, organizadas conforme os blocos identificados abaixo:

Bloco I - Definições e princípios:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Considerando os pronunciamentos da ANPD, em especial a publicação do 2º volume da série "Radar Tecnológico", que tratou de biometria e reconhecimento facial, bem como aqueles emitidos pela *Commission Nationale de l'Informatique et des Libertés* (CNIL), pelo *Information Commissioner's Office* (ICO), *Office of the Privacy Commissioner* (Canadá) e o Regulamento Geral de Proteção de Dados (GDPR), entendemos que devem ser considerados, cumulativamente, os seguintes critérios para caracterizar um dado como biométrico:

- (i) a informação deve ser relativa a características físicas, fisiológicas ou comportamentais únicas de uma pessoa natural identificada ou identificável; e
- (ii) o tratamento do dado deve ter a finalidade de autenticar ou identificar (individualizar) a pessoa natural, mediante o uso de tecnologias específicas, dotadas da capacidade de reconhecimento automático, sob pena de não ser considerado um dado biométrico.



Cumpramos ressaltar que, embora a finalidade acima referida não seja uma característica do dado pessoal em si, no contexto do tratamento de dados biométricos, a finalidade estará associada ao uso da tecnologia para individualizar o titular de forma única ou inequívoca, de acordo com o que dispõe o GDPR.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

De acordo com o que dispõe o art. 9º, da LGPD, cabe ao controlador disponibilizar, de forma clara, adequada e ostensiva, as seguintes informações sobre o tratamento: (i) finalidade; (ii) forma e duração, ressalvados os segredos comercial e industrial do controlador; (iii) identificação do controlador (e do encarregado, se houver), incluindo os dados de contato; (iv) informações sobre o uso compartilhado de dados pelo controlador e a finalidade; (v) responsabilidade dos agentes que realizarão o tratamento; e (vi) direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

Assim, entendemos que o controlador tem a possibilidade de utilizar diversos meios para prestar ao titular as informações indicadas acima e outras que julgar relevantes sobre o tratamento, podendo publicar, a seu critério, políticas e avisos de privacidade em sua página na internet.

O controlador poderá, ainda, utilizar-se de práticas de transparência ativa, a depender da viabilidade e contexto do tratamento, como o uso de sinais visuais (placas, cartazes, adesivos) e de folhetos físicos e/ou digitais (com *QR code*). O objetivo dessas práticas é dar visibilidade aos titulares, por meio dos canais de coleta, sobre os detalhes do tratamento de dados realizado, destacando a coleta do consentimento, quando aplicável.

O controlador deverá avaliar os contornos específicos do tratamento realizado, identificando as práticas consideradas mais eficazes para que, no caso concreto, o titular possa tomar conhecimento do tratamento realizado e de seus direitos.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Não vislumbramos razão para que eventual regulação venha a conferir tratamento diferenciado à biometria comportamental em relação à biometria fisiológica, chamada no enunciado de "tradicional", visto que ambas buscam atingir o mesmo propósito, qual seja, o de reconhecer ou identificar a pessoa natural.

É necessário destacar que a biometria comportamental não desconsidera fatores fisiológicos, o que pode, inclusive, dificultar a identificação e classificação do tipo de biometria que está sendo empregado. O modo de caminhar, por exemplo, embora à primeira vista seja um aspecto comportamental, também está relacionado à fisiologia da pessoa, como o tamanho da perna ou a alguma doença. Logo, não parece necessário, nem adequado adentrar nos pormenores para distinguir, apenas para fins meramente regulatórios, a biometria comportamental da biometria tida como tradicional.

Por fim, em relação às obrigações decorrentes do uso da biometria, cumpre reconhecer que os dados biométricos permitem a identificação única do titular, mas que eventualmente podem sofrer modificações ao longo do tempo, sendo considerados, além de dados sensíveis, um tipo de dado dinâmico e não estático, o que exige maior atenção em todas as fases do tratamento.

Assim, para atender os princípios da segurança e da qualidade dos dados, o controlador poderá elaborar RIPD nos casos recomendados e adotar as medidas que se apresentarem apropriadas para assegurar que os dados estarão protegidos e atualizados.

As medidas a serem adotadas deverão ser definidas pelo controlador à luz do caso concreto, levando em consideração, especialmente, os riscos reais à segurança da informação, as vulnerabilidades do sistema utilizado para o tratamento de dados e os danos que poderão ser causados ao titular.

Bloco II - Hipóteses legais

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Em linha com pronunciamento da ANPD proferido através do guia orientativo sobre a aplicação da LGPD no contexto eleitoral, o consentimento para autorizar o tratamento de qualquer dado pessoal sensível, inclusive dado biométrico, deve observar os seguintes requisitos: (i) para ser considerado livre, o titular deve poder escolher entre aceitar ou recusar a realização do tratamento sem consequências negativas ou intervenções do controlador que possam viciar ou prejudicar a manifestação de sua vontade; (ii) para ser considerado específico e destacado, é recomendável que o consentimento conste separadamente do texto principal ou que use recursos para evidenciá-lo, com especificação dos dados que serão tratados e a respectiva finalidade; (iii) para ser considerado informado, o titular deve receber informações suficientes sobre o tratamento, que lhe permitam uma avaliação consciente; e, por fim, (iv) para ser considerado inequívoco, a manifestação de vontade deve ser clara, obtida sem interferência.

Necessário destacar que nem sempre o consentimento será a base legal apropriada, por exemplo na hipótese do art. 11, II, "g" da LGPD, quando o tratamento de dados biométricos for necessário para a "garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos", o que ocorre, por exemplo, para fins de controle de acesso a sistemas com a verificação e autenticação do titular e engloba todos os tratamentos necessários para essas finalidades.

O consentimento não deve ser a única base legal a fundamentar o tratamento da biometria. Se o consentimento for a base legal mais aplicável a determinado fluxo, deverá ser obtido por meio de manifestação clara e destacada, desvinculada de outros termos de consentimento. Não será adequado quando há assimetria de poder, como em relações trabalhistas ou quando o tratamento é necessário para prevenção à fraude. No mercado segurador, o uso de biometria fundamentado na base legal prevenção à fraude é essencial tanto para a segurança das seguradoras quanto para proteger seus clientes.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de "garantia da prevenção à fraude" (art. 11, II, "g", LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Para a adequada aplicação da hipótese de garantia da prevenção à fraude é preciso observar os critérios estabelecidos no próprio texto do art. 11, II, "g", da LGPD, sendo eles: (i) o tratamento deve ter por finalidade garantir a prevenção à fraude e a segurança do titular; (ii) o tratamento deverá ser realizado em processos de identificação e autenticação de cadastro do titular em sistemas eletrônicos englobando todas as atividades de tratamento necessárias para tanto, desde a coleta, armazenamento, tratamento técnicos específicos, eventual compartilhamento, além de outros tratamentos necessários; (iii) deverão ser resguardados os direitos mencionados no art. 9º da LGPD; e (iv) o tratamento não deverá ser realizado se restar constatado que no caso concreto prevalecem direitos e liberdades fundamentais do titular que exijam a proteção de seus dados pessoais.

Necessário também avaliar a proporcionalidade do tratamento e identificar, concretamente, as salvaguardas apropriadas para resguardar direitos e liberdades fundamentais do titular, como a utilização de criptografia e armazenamento seguro, realização de auditorias periódicas de acessos e uso dos dados e treinamento contínuo, com políticas internas sobre o uso de dados biométricos.

Nesse sentido, a biometria deve ser utilizada para autenticar operações, identificar riscos de transações (atípicas ou suspeitas) e validar a identidade do titular, entre outros, conforme avaliado pelo controlador no contexto do tratamento. O tratamento deve observar os

princípios da necessidade e finalidade, sendo proporcional ao risco e tecnicamente justificado.

O tratamento de dados biométricos com base na prevenção à fraude é essencial para as seguradoras, para garantir a manutenção da sustentabilidade do setor e a proteção dos titulares, sendo utilizada, por exemplo, para:

- (i) Autenticação no aplicativo da seguradora, impedindo acessos indevidos a informações de seguros e resgates indevidos de alto valor;
- (ii) Validação de identidade na contratação de seguros, reduzindo fraudes através de documentos falsos;
- (iii) Prevenção de fraudes em sinistros, sendo utilizada, inclusive, como prova de vida do titular.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

O principal critério a ser observado pelo controlador no tratamento de dados biométricos para o cumprimento de obrigação legal ou regulatória é a avaliação da real necessidade da atividade que será realizada. Em razão da natureza do dado e da sua acentuada sensibilidade, é recomendável que o controlador avalie a necessidade do tratamento sob perspectivas distintas, para limitar o tratamento aos dados estritamente necessários para alcançar a finalidade almejada. Além disso, para avaliar se o tratamento é necessário e se pode estar amparado na base do art. 11, II, “a” da LGPD, o controlador deve ser capaz de demonstrar a relação entre o tratamento do dado biométrico e o cumprimento da obrigação legal ou regulatória. Por exemplo, no setor securitário, as normas aplicáveis ao setor, inclusive de gerenciamento de riscos e segurança, também podem basear o tratamento de dados biométricos.

O tratamento de dados biométricos para cumprimento de obrigação legal ou regulatória deve atender, de igual forma, os princípios da LGPD, como finalidade, necessidade, adequação e transparência. Ademais, a finalidade do tratamento dos dados biométricos deve ser aquela estipulada pela lei ou regulamento, devendo o controlador avaliar a necessidade da atividade de tratamento de dados biométricos que será realizada.

Com relação às salvaguardas para mitigar riscos e garantir os direitos dos titulares, há de se destacar que o pressuposto do exercício de qualquer direito é conhecê-lo. Logo, entende-se que as principais salvaguardas devem ser voltadas a conferir transparência ao tratamento, de modo a assegurar que o titular possa, caso assim deseje, exercer os direitos previstos na LGPD.

Como possíveis medidas a serem adotadas à critério do controlador para a mitigação de riscos e garantia de direitos dos titulares no uso da base legal do cumprimento de obrigação legal ou regulatória, destacamos a realização do RIPD, uso de criptografia, controle de acesso, monitoramento e testes de vieses.

Quanto ao uso dessa base legal por entidades e órgãos públicos, é recomendável que sejam seguidas as orientações já divulgadas pela ANPD no guia que abordou o tratamento de dados pessoais pelo Poder Público, especialmente para que nesses casos o tratamento observe estritamente o interesse público.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, "c", LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Para o uso adequado da base legal do art. 11, II, "c", da LGPD, inclusive quanto às salvaguardas dos interesses e direitos dos titulares, o controlador pode observar as orientações da ANPD constantes no guia que abordou o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas, e, particularmente quanto aos dados biométricos, deve restringi-los ao estritamente necessário.

Deve, além disso, avaliar com muita cautela a própria necessidade e proporcionalidade do tratamento em relação à finalidade da pesquisa que será realizada. Por outro lado, quanto ao risco de eventual reidentificação de dados biométricos que tenham sido anonimizados, recomenda-se que o controlador adote processo de gestão de risco, observando, para tanto, as diretrizes sugeridas no estudo preliminar elaborado pela ANPD sobre o tema.

Considerando a alta singularidade dos dados biométricos, o controlador poderá adotar, a seu critério, a utilização de técnicas robustas de anonimização testada, pseudonimização, controle rigoroso de acesso, proibição de reuso indevido.

Bloco III - Tecnologias de reconhecimento facial (FRTS) e aplicação de tecnologias emergentes e inovadoras no tratamento de dados biométricos

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

As tecnologias de reconhecimento facial são utilizadas como medidas de segurança no setor de seguros para fins de prevenção e combate à fraude, principalmente para confirmação da identidade e acesso a cadastros e resgate de valores, não devendo haver qualquer óbice desnecessário ao uso da biometria, dada a sua importância para o setor segurador e para a proteção do consumidor.

Para garantir que o uso de tecnologias de reconhecimento facial esteja em conformidade com os princípios mencionados no enunciado e mitigar os riscos de discriminação ilícita ou abusiva sobre determinados grupos sociais, o controlador pode adotar, dentre outras, as seguintes medidas: (i) tratar somente os dados estritamente necessários; (ii) utilizar, sempre que possível, técnicas de anonimização e/ou pseudonimização; (iii) avaliar a necessidade do tratamento orientado pela lógica de buscar alternativa menos intrusiva, a critério do controlador; (iv) utilizar meios eficazes para dar conhecimento ao titular sobre o tratamento; (v) disponibilizar canais efetivos para atendimento do titular que queira exercer os seus direitos, inclusive o de se opor ao tratamento e o de revogar o consentimento, quando for o caso; (vi) estabelecer políticas de controle de acesso aos dados biométricos tratados; (vii) elaborar RIPD; e (viii) adotar medidas de proteção dos dados pessoais e da privacidade compatíveis com os riscos reais, as vulnerabilidades do sistema utilizado para o tratamento de dados e, principalmente, os danos que poderão ser causados ao titular.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Para garantir que os sistemas de reconhecimento facial sejam projetados e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, o controlador deve considerar a acurácia dos sistemas como elemento central da conformidade do tratamento.

Para tanto, o controlador precisa garantir que: (i) o sistema tenha precisão estatística compatível com a finalidade de uso; (ii) sejam realizados testes periódicos para identificar e corrigir vieses e evitar que ocorram tratamentos discriminatórios; (iii) sejam adotadas medidas efetivas para corrigir tempestivamente erros de identificação; e (iv) sejam adotadas medidas de transparência para garantir que os titulares possam tomar conhecimento do tratamento que será realizado e possam exercer os seus direitos.

O sistema deve estar amparado em base robusta e diversa, ser validado tecnicamente, auditado periodicamente e prever mecanismos de contestação e correção de erros, com governança clara sobre decisões automatizadas e mitigação de falsos resultados. O treinamento com dados diversos reduz erros, podendo evitar falsos negativos/positivos e

corrigir falhas de reconhecimento. Ademais, a análise de logs de erros são recursos para correção de falhas e realização de testes periódicos visando identificação e correção de vieses, evitando que ocorram tratamentos discriminatórios ilícitos e abusivos.

No que diz respeito às medidas de correção tempestiva de erros de identificação, entende-se necessário que sejam avaliadas à luz do caso concreto. Com efeito, recomenda-se a elaboração de RIPD visando à identificação dos riscos do tratamento e das medidas mitigatórias pertinentes. Não parece apropriado determinar antecipadamente as medidas que deverão ser adotadas pelo controlador, que precisam levar em consideração o contexto específico do tratamento e os reais riscos envolvidos.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

O uso de tecnologias de reconhecimento facial não é recomendado, por exemplo, em alguns tipos de serviços onde a autenticação de acesso não é necessária, pois os serviços ofertados não estão diretamente atrelados à autenticação da identidade do indivíduo. Adicionalmente, não se recomenda o uso de tais tecnologias em espaços públicos sem finalidade clara.

Entretanto, para serviços que necessitam da garantia e validação automatizada da identidade do indivíduo, principalmente visando a prevenção à fraude e segurança, como por exemplo, de bancos e serviços de seguros e saúde, a utilização dessa tecnologia, observadas as adequadas salvaguardas técnicas e de segurança, tem se mostrado efetiva. Não se deve, portanto, que eventual, alteração regulatória desestimule o seu uso de quando o objetivo for mitigar fraudes e garantir a segurança do titular.

As alternativas ao uso de tecnologias de reconhecimento facial incluem autenticação multifatorial, *tokens* digitais e físicos ou validação documental assistida, conforme análise do caso.

Bloco IV - Segurança, governança e boas práticas

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

O controlador, de acordo com a sua realidade, poderá avaliar a adoção das seguintes medidas, que devem ser consideradas exemplificativas, para mitigar riscos de violação de dados biométricos:

- (i) controle, segregação e limitação de acesso, incluindo processos de autenticação, autorização e auditoria;
- (ii) realização de registro cronológico das alterações da base de dados de referência;
- (iii) utilização de criptografia para proteger os dados biométricos;
- (iv) manutenção das informações armazenadas pelo tempo mínimo necessário;
- (v) elaboração de plano de resposta a incidentes de segurança;
- (vi) estabelecimento de obrigações contratuais com prestadores de serviços que participam do tratamento de dados;
- (vii) uso de hash único e randomizado por dado;
- (viii) mascaramento e embaralhamento de dados em ambientes não produtivos;
- (ix) auditorias periódicas;
- (x) monitoramento, multifator de autenticação para manuseio dos dados e logs de acesso.

O controlador também deve levar em consideração seu porte e o contexto fático para determinar os parâmetros de avaliação de riscos e monitoramento a serem adotados, como plano de resposta a incidentes, backup seguro, testes de intrusão e descarte adequado dos dados.

Para que as medidas sejam eficazes é preciso que sejam adequadas às reais ameaças para a segurança da informação, aos reais riscos a que o titular estará sujeito e às vulnerabilidades do sistema utilizado. Nesse sentido, é recomendável que o controlador reavalie periodicamente as medidas adotadas, para assegurar que continuem eficazes, através do RIPD.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Para assegurar que o tratamento seja legítimo nessas hipóteses é recomendável que o controlador, como boa prática, faça uma avaliação de proporcionalidade. Para tanto, ele deverá considerar a necessidade do tratamento em relação aos riscos que o titular do dado estará exposto.

Sendo assim, se ficar evidenciada a presença de riscos desproporcionais que possam levar à discriminação do titular, é recomendável que o tratamento não seja realizado e sejam avaliadas alternativas menos intrusivas. A existência de risco ao titular não deve, entretanto, ser entendida como uma proibição ao tratamento, desde que o risco possa ser mitigado por meio de salvaguardas adequadas.

Com efeito, se for possível ao controlador demonstrar a proporcionalidade do tratamento e a mitigação de riscos, será legítima a restrição do uso de determinadas funcionalidades ao titular que se negar a fornecer seus dados biométricos. Podemos ter como exemplo contextos em que a segurança do titular ou da organização pode ser colocada em risco caso não se confirme a identidade do titular ou quando não estiver disponível meio alternativo igualmente seguro.

No mercado segurador, em seguros de vida, a biometria pode ser essencial para prevenir fraudes e, neste caso, por exemplo, a recusa em fornecer selfie como prova de vida pode inviabilizar a aceitação/contratação digital do produto.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

O controlador poderá adotar políticas e avisos de privacidade que registrem a realização de tratamento de dados biométricos e aplicar medidas organizacionais e técnicas para proteger o dado pessoal sensível, bem como realizar as comunicações necessárias aos titulares para dar transparência quanto ao tratamento e sua finalidade, a depender do contexto do tratamento.

Para garantir maior proteção ao tratamento, o controlador poderá realizar atualização periódica relativa à qualidade dos dados e avaliações periódicas de risco, com atualização contínua das medidas de segurança, bem como elaborar RIPD para avaliar discriminação ilícita e abusiva, garantindo proporcionalidade e aderência à LGPD.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

O questionamento não se aplica às empresas seguradoras.

Bloco V - Direitos dos titulares e grupos vulneráveis

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Os agentes de tratamento podem garantir o respeito aos direitos dos titulares mediante o uso de avisos de privacidade que descrevam o tratamento realizado, com destaque para a coleta do consentimento (quando for a base aplicável), bem como através de sinalizações de coleta e de monitoramento de ambiente, a depender do contexto do tratamento.

Devem ser assegurados canais acessíveis para solicitação de informações, correção de dados e revogação do consentimento, com linguagem clara e registros que garantam rastreabilidade, o fornecimento da informação e a transparência das operações de tratamento, como, por exemplo, viabilizando o exercício de direitos via app, site ou SAC.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O questionamento não se aplica às empresas seguradoras.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

O tratamento de dados pessoais de crianças e adolescentes pode se basear em qualquer base legal, conforme posicionamento da ANPD externado no enunciado nº 1/2023, *verbis*: “[o] tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei”.

A efetiva adequação do uso da base legal e a avaliação das medidas técnicas e organizacionais apropriadas para evitar abusos, vazamentos ou acessos indevidos dependerão do caso concreto. Nesse sentido, é recomendável que quando houver o tratamento de dados biométricos de crianças e adolescentes, o controlador elabore RIPD, observando a minimização dos dados e a finalidade legítima e específica do tratamento.



A participação informada dos pais ou responsáveis deve ocorrer através do uso de linguagem adequada e o sistema deve garantir proteção contra acesso e uso indevidos.

Como medidas técnicas e organizacionais a serem adotadas para evitar abusos, vazamentos ou acessos indevidos, é possível citar a disponibilização de canal de contato, o uso de criptografia, controle de acesso restrito, auditoria e revisão periódica contra acessos não autorizados.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

O questionamento não se aplica às empresas seguradoras.

Colocando-se à disposição para eventuais esclarecimentos adicionais, a CNseg apresenta os protestos de consideração e respeito.

Atenciosamente,

Dyogo Oliveira
Diretor-Presidente

BLOCO 1 – Definições e Princípios

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

- Dados referentes a características exclusivas do indivíduo: impressões digitais, íris, palma da mão, DNA;
- Finalidade do tratamento/uso do dado: autenticação ou identificação;
- Mecanismos técnicos empregados na identificação do indivíduo: processamento automatizado.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

- Aviso de privacidade sobre biometria em camadas (linguagem simples na camada inicial e informações detalhadas nas camadas posteriores);
- Legal Design para auxiliar na compreensão das informações sobre o tratamento;
- Política de privacidade com seção específica sobre biometria;
- Sinalização explícita sobre o uso da biometria em ambientes públicos ou privados;
- Informe e disponibilização facilitada sobre outras possibilidades que não seja o uso de biometria (ex. crachá de acesso).

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A biometria comportamental, por estar associada a padrões de comportamento, é variável, dependente de contexto e do ambiente e está sujeita a alterações, o que não acontece com a biometria tradicional. Por esse motivo, é preciso garantir:

- Validação contínua da tecnologia e dos seus resultados;
- Gestão de erro e calibração dos algoritmos;
- Monitoramento ativo de falsos positivos/negativos;
- Obrigações reforçadas de transparência e avaliação de impacto.

BLOCO 2 – Hipóteses Legais

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Para que o consentimento de dados biométricos seja válido, recomenda-se que:

- Utilize recursos do Privacy by Design para facilitar a compreensão;
- Seja oportunizado ao titular não fornecer seus dados biométricos sem que isso implique impossibilidade de acesso a serviço/produto;
- O procedimento de revogação seja simples e no mesmo formato/canal da sua concessão.

O consentimento não deve ser adotado em contextos que envolvam:

- Relações contratuais desequilibradas/assimetria de poder;
- Prestação de serviços essenciais, ex.: saúde, educação, transporte público;
- Ausência de alternativa razoável ao tratamento, quando o titular não pode negar ou revogar o consentimento sem sofrer ônus desproporcional.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

O principal critério é o da necessidade, ou seja, somente utilizar dados biométricos se for a opção de autenticação/verificação de identidade mais eficaz e não houver outras formas menos invasivas ou custosas para tanto.

Para a prevenção de fraudes no setor bancário, o uso de biometria com base no princípio da necessidade deve ser justificado com a comprovação de que outras alternativas, como autenticação via senhas por exemplo, não são eficazes o suficiente para garantir a segurança do titular. Deve-se utilizar a biometria apenas para serviços financeiros que requerem maior segurança por apresentarem mais risco ao titular erros na autenticação/verificação.

Em relação às salvaguardas, sugere-se:

- uso de pseudonimização e criptografia;

- auditoria contínua para verificar a conformidade com as melhores práticas do mercado e atualizações da legislação;
- limitação de acesso a funcionários específicos;
- período de retenção e processo de descarte bem definidos.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

- uso de pseudonimização e criptografia;
- auditoria contínua para verificar a conformidade com as melhores práticas do mercado e atualizações da legislação;
- limitação de acesso a funcionários específicos;
- período de retenção e processo de descarte bem definidos;
- treinamento e capacitação da equipe.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

A finalidade do uso de dados biométricos da pesquisa deve ser transparente e justificada. Sugere-se especificar no protocolo de pesquisa como os dados biométricos serão utilizados, como serão armazenados e por quanto tempo, além da utilização de técnicas de anonimização e pseudonimização.

BLOCO 3 – Tecnologias de reconhecimento facial (frts) e aplicação de tecnologias emergentes e inovadoras no tratamento de dados biométricos

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Sugere-se:

- Definir previamente o escopo e duração do tratamento;

- Realizar auditorias regularmente com publicação do referido relatório;
- Realizar estudos com enfoque nos vieses da tecnologia, garantindo uma amostra de dados equilibrada em relação a etnias, idades, gêneros, condições físicas, etc;
- Ter uma política institucional de proteção de dados orientada para o uso ético dos dados;
- Realizar treinamento em proteção de dados para os desenvolvedores e operadores da tecnologia.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

- Base de dados diversificada com imagem de pessoas de diferentes etnias, idades, gêneros para evitar viés e erros sistemáticos;
- Qualidade das câmeras e sensores para garantir a fidelidade das imagens, inclusive para operar em condições variadas de iluminação e distância;
- Possibilidade e previsão de revisão humana periódica;
- Possibilidade do titular de contestar a decisão automatizada e solicitar uma revisão humana.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

- A utilização de reconhecimento facial em ambientes de trabalho ou em instituições de ensino – alternativa: cartões de acesso ou tokens.
- Utilização de reconhecimento facial como parte de um processo automatizado de tomada de decisão para autorização de crédito, segurança bancária ou seleção de candidatos para emprego, uma vez que podem resultar em decisões discriminatórias ou injustas, - alternativa: revisão humana das decisões.

BLOCO 4 – Segurança, governança e boas práticas

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Técnicas: criptografia; anonimização e pseudonimização; controle de acesso; retenção e descarte seguros.

Administrativa: políticas e diretrizes internas voltada ao uso ético e segurança dos dados e a gestão de incidentes, treinamentos para equipe com essas temáticas e realização de relatório de impacto para o fluxo.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

A organização deve justificar de maneira clara e transparente porque a autenticação biométrica é necessária para o serviço, descrevendo a finalidade do tratamento, o benefício para o titular e as alternativas possíveis.

A recusa do consentimento pode justificar restrição ao acesso apenas de funcionalidades específicas que requerem alto nível de segurança, devendo o restante dos serviços utilizar outras formas/menos invasivas de validação.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

- Realizar auditorias regularmente com publicação do referido relatório;
- Realizar estudos com enfoque nos vieses da tecnologia, garantindo uma amostra de dados equilibrada em relação a etnias, idades, gêneros, condições físicas, etc.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos?

Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

- Cartazes e sinalizações visíveis nos locais em que o tratamento é realizado;
- Informe no momento da compra de ingressos;
- Informe nos canais de comunicação oficial dos controladores;
- Plataforma ou interface simples para o titular consultar, corrigir ou solicitar a eliminação de seus dados biométricos, de modo transparente e eficiente.

BLOCO 5 – Direitos dos titulares e grupos vulneráveis

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

- Fornecer os avisos de privacidade em linguagem simples, com destaque para o tratamento automatizado e os critérios de tomada de decisão;
- Canal eletrônico e físico acessíveis, a exemplo de formulário online ou atendimento presencial, para que o titular exerça seus direitos;
- Processos automáticos de exclusão dos dados biométricos conforme prazo legal e/ou solicitação.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

- Tornar essas informações públicas, por meio site da instituição e/ou mídia institucional e reforçar essas informações no ato de matrícula/inscrição;
- Esse tipo de tratamento só seria possível se realizado no melhor interesse da criança, ou seja, quando comprovado necessário para segurança ou bem-estar da mesma.

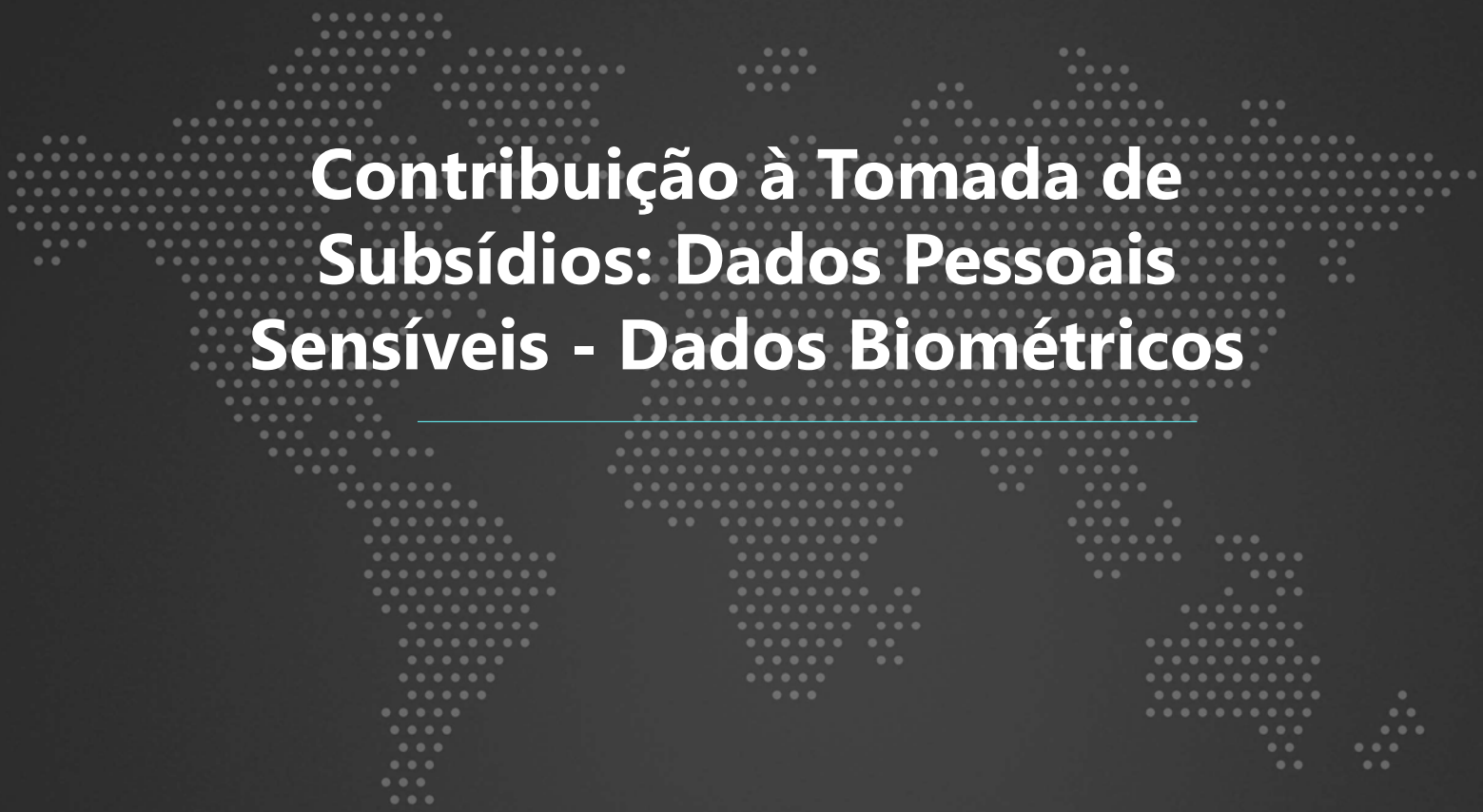
17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Hipóteses que autorizam o tratamento de dado sensível, desde que salvaguardado o melhor interesse da criança, mas, de preferência, o consentimento específico e em destaque por um dos pais ou responsáveis do menor.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

- Optar pela autodeclaração + identificadores físicos (documentos)
- Adaptar as ferramentas de verificação de idade aos graus de desenvolvimento da criança e do adolescente





Contribuição à Tomada de Subsídios: Dados Pessoais Sensíveis - Dados Biométricos

São Paulo, 1º de agosto de 2025

À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Via e-mail:

DANIEL ADVOGADOS vem, respeitosamente, apresentar suas contribuições no âmbito da Tomada de Subsídios sobre Dados Pessoais Sensíveis - Biométricos.

Cumpre ressaltar que este Escritório também manifestou suas considerações via "Participa + Brasil", mas, em razão da extensão dos apontamentos e limitação de caracteres da plataforma, entendeu por bem encaminhar a íntegra por meio da presente comunicação.

Por fim, este escritório aproveita para congratular a abertura da Autoridade às Consultas Públicas e renovar seus votos de estima e consideração.

Atenciosamente,

TECNOLOGIA, PRIVACIDADE E PROTEÇÃO DE DADOS
DANIEL ADVOGADOS

Bloco I – DEFINIÇÕES E PRINCÍPIOS**1) Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?**

A Lei Geral de Proteção de Dados Pessoais (LGPD) classifica os dados biométricos como uma das categorias de dados pessoais sensíveis (art. 5º, II), mas não especifica critérios técnicos objetivos para sua caracterização. Diante dessa lacuna, é legítimo recorrer à interpretação comparada, especialmente ao Regulamento Geral de Proteção de Dados da União Europeia (GDPR), assim como às orientações de autoridades e estudos europeus, cujas definições e orientações técnicas têm sido referência para autoridades e especialistas brasileiros, inclusive para a própria ANPD.

Nesse sentido, conforme estabelecido por autoridades e estudos europeus, a caracterização de um dado como biométrico exige a presença de três critérios cumulativos¹:

- (i) o dado deve estar relacionado a características físicas, fisiológicas ou comportamentais de uma pessoa natural: O dado deve derivar de um atributo corporal ou padrão comportamental único, como impressões digitais, feições faciais, retina, voz ou forma de digitar;
- (ii) deve ter sido submetido a um tratamento técnico específico: O dado deve ter sido submetido a tratamento técnico, por meio de algoritmos ou extração de padrões, com o objetivo de converter esse traço em um modelo de identificação. Dados brutos, como uma simples foto ou gravação, não são considerados dados biométricos, a menos que sejam processados tecnicamente com essa finalidade específica; e
- (iii) deve possibilitar ou confirmar a identificação única da pessoa a quem se refere: O dado deve ser utilizado, ou ter o potencial de ser utilizado, para identificar ou autenticar o titular. A efetiva identificação não precisa ocorrer: basta a possibilidade real e objetiva de vinculação à identidade da pessoa.

¹ EDPB. **Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo**. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf

Segundo o guia da Information Commissioner's Office (ICO), apenas informações processadas tecnicamente para capturar atributos corporais (como tom de voz, padrões de digitação, feições faciais) com a finalidade de identificação individual podem ser consideradas dados biométricos. Gravações brutas, por si só, não se enquadram nessa categoria se não forem tecnicamente processadas com essa finalidade específica²

Esse entendimento é corroborado também pelo Parlamento Europeu, que ao tratar de reconhecimento facial e outras tecnologias, classifica como biométricos os dados que resultam de análise técnica de traços corporais (como forma do rosto ou padrão de marcha), desde que aptos a estabelecer correspondência com uma identidade específica³. Assim, uma imagem facial digital, por si só, não é automaticamente um dado biométrico, mas poderá ser assim classificada caso seja tratada por sistemas de reconhecimento facial ou equivalentes.

Tese: Na ausência de critérios técnicos definidos pela LGPD, a caracterização de um dado como biométrico deve seguir interpretação sistemática e comparada, sendo considerado assim quando resultar do tratamento técnico específico de características físicas, fisiológicas ou comportamentais, com o objetivo de permitir ou confirmar a identificação inequívoca da pessoa natural.

2) Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

O tratamento de dados biométricos, por envolver categorias especiais e riscos mais elevados à privacidade, exige a adoção de práticas de transparência ativa que sejam acessíveis, compreensíveis e adaptadas ao contexto da coleta. Nos termos do art. 6º, VI da Lei Geral de Proteção de Dados Pessoais (LGPD), a transparência é um dos princípios fundamentais da proteção de dados, implicando o dever de garantir aos titulares o acesso claro e fácil às informações sobre o tratamento de seus dados antes da coleta.

² INFORMATION COMMISSIONER'S OFFICE. *Guide to biometric data and biometric technologies*. London. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/>.

³ EUROPEAN PARLIAMENT. *Regulating Facial Recognition in the EU*. Brussels, 2021. p. 5. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA\(2021\)698021_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf)

Nesse sentido, é possível exigir dos controladores práticas como o fornecimento de informações prévias, claras e destacadas, seja por meio de avisos físicos, digitais ou audiovisuais, conforme o meio e o ambiente da coleta (ex: dispositivos móveis, terminais físicos, câmeras de autenticação). Conforme orientações da Autoridade de Proteção de Dados do Reino Unido (ICO), os controladores devem fornecer informações claras no momento ou antes da coleta, por meio de avisos visuais, digitais ou físicos, em linguagem adequada ao público-alvo⁴.

Além disso, deve-se considerar uma boa prática o princípio do “*design em camadas*”: apresentar inicialmente os pontos mais relevantes de forma concisa, como a finalidade do tratamento, base legal, tempo de retenção, compartilhamentos e direitos dos titulares, com acesso complementar a conteúdos mais detalhados por meio de QR codes, links, menus interativos ou documentos físicos de apoio. Isso favorece o equilíbrio entre clareza e completude da informação, especialmente em ambientes digitais com restrições de espaço.

Nos casos em que os dados biométricos forem utilizados para decisões automatizadas ou categorização comportamental, a transparência deve incluir a explicação dos critérios usados para o tratamento e os possíveis efeitos sobre os titulares, bem como canal direto de contato com o encarregado pelo tratamento, para dúvidas relacionadas à biometria.

Tese: Controladores que realizam tratamento de dados biométricos devem adotar práticas de transparência ativa que garantam ao titular, no momento ou antes da coleta, o acesso claro às finalidades, bases legais, critérios de retenção, eventuais compartilhamentos e direitos previstos na LGPD. Essas informações devem ser apresentadas em linguagem acessível, adaptada ao público-alvo, por meio de interfaces físicas ou digitais, e estruturadas preferencialmente em camadas. Sempre que houver uso de biometria em decisões automatizadas ou categorização comportamental, devem ser fornecidas explicações adicionais sobre os critérios envolvidos, seus possíveis efeitos e meios eficazes de contato com o encarregado pelo tratamento.

⁴ INFORMATION COMMISSIONER'S OFFICE. *Guide to biometric data and biometric technologies*. United Kingdom, Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/>

3) De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A biometria comportamental, que inclui tecnologias como reconhecimento de voz, padrão de digitação, movimento ocular e dinâmica de locomoção, apresenta diferenças substanciais em relação à biometria tradicional (como digitais, íris ou forma do rosto), tanto em sua natureza técnica quanto nos riscos à privacidade. Por isso, seu tratamento jurídico e regulatório deve ser mais cauteloso, observando não apenas os princípios gerais da LGPD, mas também obrigações específicas derivadas da sua complexidade e opacidade técnica.

A literatura especializada classifica os traços biométricos em dois grandes grupos: os chamados *strong biometrics*, que são características físicas estáveis e estruturais (como impressões digitais, íris ou forma do rosto). Têm estabilidade temporal e são normalmente usados para fins de autenticação ou identificação individual; e os *weak* ou *soft biometrics*, que compreendem comportamentos dinâmicos, muitas vezes inconscientes, como padrão de digitação, entonação vocal, ritmo de caminhada, gestos, posturas, reações faciais e até estilo de escrita. Essas características podem variar ao longo do tempo e em diferentes contextos, o que introduz maior grau de incerteza e ambiguidade no tratamento dos dados⁵.

Essa distinção tem implicações diretas na proteção de dados. Por exemplo, a biometria comportamental permite inferências que vão além da identificação: poderia levar a inferências de estados emocionais, condições de saúde, tendências cognitivas ou comportamentos futuros⁶.

No plano internacional, o Parlamento Europeu distingue dois conceitos centrais: *biometric categorisation*, que se refere à classificação de pessoas com base em características como gênero, idade ou origem étnica; e *biometric detection*, que envolve a captação de sinais para identificar estados ou intenções temporárias, como medo, fadiga ou agressividade⁷.

⁵ EUROPEAN PARLIAMENT. *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects*. Brussels: Policy Department for Citizens' Rights, 2021. p. 12–15.

⁶ ENISA. *Behavioural Biometrics – Emerging trends and privacy issues*. European Union Agency for Cybersecurity, 2022.

⁷ EUROPEAN PARLIAMENT. *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects*. Brussels: Policy Department for Citizens' Rights, 2021..

Diante desses riscos, é recomendável para a biometria comportamental:

- Realização de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), com ênfase em riscos de discriminação algorítmica, viés de treinamento e erros de classificação;
- Governança algorítmica, com auditoria periódica dos sistemas de machine learning e explicabilidade das decisões;
- Adoção de medidas de segurança adequadas à criticidade do tratamento, como pseudonimização, criptografia, segregação de bases de dados e, sempre que possível, técnicas de anonimização compatíveis com o ciclo de vida do dado;
- Revisão periódica da finalidade e da proporcionalidade do tratamento, para evitar ampliação indevida de escopo (função creep), especialmente quando o dado passa a ser usado para inferências emocionais ou preditivas.

Tese: A biometria comportamental pode inferir informações sobre o estado emocional, mental ou de saúde do indivíduo. Sempre que for o caso, é recomendada a elaboração de avaliação de impacto com ênfase em discriminação e viés algorítmico e adoção de medidas de segurança compatíveis com a criticidade dos dados tratados, como anonimização, criptografia e governança técnica por *design*.

Bloco II – HIPÓTESES LEGAIS

4) Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece os critérios de validade para o consentimento como base legal, especialmente quando se trata do tratamento de dados pessoais sensíveis, como os dados biométricos. Para ser juridicamente válido, o consentimento deve ser livre, informado, inequívoco, específico e fornecido de forma destacada, ou seja, não pode decorrer de silêncio, omissão ou cláusulas genéricas em políticas extensas. Nesse sentido, para garantir a validade do consentimento no tratamento de dados biométricos, os controladores devem considerar que a sua obtenção seja realizada por meio de medidas reforçadas de clareza, autonomia e acessibilidade.

Esse entendimento é reforçado por autoridades estrangeiras, como o Information Commissioner's Office (ICO) e a Agência Espanhola de Proteção de Dados (AEPD).

Conforme a ICO, o consentimento deve ser granular, separado por finalidades específicas, obtido antes da coleta, de forma destacada e livre de coação. Não basta incluir o aceite em cláusulas genéricas ou em políticas extensas; é necessário que a manifestação do titular seja inequívoca e destacada⁸. A AEPD complementa que o consentimento não é válido quando o titular não dispõe de alternativas reais. Em serviços não essenciais, deve-se sempre oferecer meios alternativos ao uso de biometria, como cartões ou senhas. Também é necessário permitir a revogação do consentimento a qualquer momento, de forma tão simples quanto a aceitação inicial, inclusive com sistemas que comuniquem a revogação a terceiros que tenham recebido os dados⁹.

Além disso, deve-se fornecer material informativo que aborde: quais dados estão sendo coletados; finalidades específicas (como autenticação, categorização ou detecção); classe de terceiros com acesso aos dados; e os direitos do titular. Esses requisitos são fundamentais para assegurar a autodeterminação informativa e a validade do consentimento em contextos de risco elevado.

No entanto, o consentimento não é uma base legal adequada em todos os contextos. O próprio art. 11, II da LGPD elenca hipóteses legais autônomas e mais apropriadas para o tratamento de dados sensíveis, inclusive sem consentimento, como quando necessário para: prevenção à fraude e à segurança do titular. Os métodos de autenticação biométrica são de extrema relevância para garantir maior segurança, prevenção à fraude e acessibilidade a serviços digitais, de forma que não deve ser possível a eventual fraudador optar por meios menos seguros de autenticação para o cometimento de ilícitos. Ademais, se é de responsabilidade do controlador a adoção de medidas técnicas e administrativas apta a proteção de dados pessoais, não é possível o cerceamento da utilização de determinadas técnicas para essa finalidade.

Tese: O consentimento para o tratamento de dados biométricos só será válido quando for obtido de forma livre, informada, específica, destacada e inequívoca, o que exige a adoção de medidas como: apresentação clara das finalidades, facilitação da revogação e linguagem acessível ao público-alvo. Contudo, o consentimento não é base legal adequada quando o tratamento se destina à prevenção à fraude e segurança do titular, casos em que se aplicam as hipóteses do art. 11, II da LGPD, e o uso da biometria deve

⁸ INFORMATION COMMISSIONER'S OFFICE. *Guide to biometric data and biometric technologies*. United Kingdom, Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/>

⁹ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*. Madrid, 2023.

ocorrer com base em deveres do controlador voltados à proteção de dados e mitigação de riscos.

5) Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A aplicação da hipótese legal de prevenção à fraude para o tratamento de dados biométricos exige a comprovação de três condições cumulativas: necessidade, proporcionalidade e adequação em relação à finalidade. Nesse sentido, considerando que é responsabilidade do controlador a adoção de medidas de segurança técnicas e administrativas aptas a proteção dos dados pessoais, e que em muitos âmbitos, como o consumerista ou o trabalhista, ele arcará com eventuais danos patrimoniais decorrentes de violações de segurança, é essencial compreender que reside em seu âmbito de avaliação a determinação de quais mecanismos de segurança estão aptos a proteção dos dados sob sua responsabilidade. De outro modo, o controlador poderia ser responsabilizado por violação de segurança aos dados pessoais ao mesmo tempo em que se cerceou a utilização de método que garante maior robustez de segurança.

Vale ainda lembrar que algumas autoridades europeias exigem que a biometria seja utilizada apenas quando não houver meios menos invasivos disponíveis, como a ICO¹⁰. No caso da LGPD, a prevenção à fraude encontra fundamento próprio e embora esteja sob o princípio da necessidade, não está sob a subsidiariedade para prevalência de outras medidas de segurança. A opção do legislador levou em conta o cenário numeroso de fraudes no Brasil, que lidera em rankings regionais (América Latina) e globais sobre o tema, ao mesmo tempo em que universaliza serviços digitais relevantes para novos segmentos da população, que em razão do menor acesso à produtos e serviços, encontram maior dificuldade para autenticar sua identidade no digital. Ou seja, é importante ressaltar que no Brasil, a biometria tem um papel importante na garantia da segurança e da prevenção à fraude na universalização de serviços digitais.

¹⁰ INFORMATION COMMISSIONER'S OFFICE. *Guide to biometric data and biometric technologies*. United Kingdom, Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/>

Tese: Deve-se considerar que está no âmbito de responsabilidade e, portanto, de atuação do controlador a ponderação sobre a necessidade, proporcionalidade e adequação de uso de biometria para a finalidade de prevenção à fraude. De outra forma, haveria cerceamento do uso de medida de segurança mais robusta em detrimento da responsabilidade do próprio controlador. Além disso, é importante interpretar com a devida cautela o posicionamento de autoridades europeias que exigem a subsidiariedade para o uso de biometria em casos de prevenção à fraude. O mesmo não ocorre no Brasil, que estabeleceu base legal própria para a prevenção à fraude, de forma compatível com o nosso numeroso cenário de fraudes e universalização de serviços digitais.

6) Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

O tratamento de dados biométricos com base no art. 11, II, “a” da LGPD, isto é, para o cumprimento de obrigação legal ou regulatória pelo controlador, somente será legítimo se houver previsão normativa clara, específica e compatível com os princípios da proteção de dados, especialmente os da necessidade, finalidade, proporcionalidade e segurança (art. 6º, LGPD). Isso vale de forma ainda mais rigorosa quando se trata de órgãos e entidades públicas, em razão do princípio constitucional da legalidade estrita (art. 37, caput, da Constituição Federal).

Nesses casos, o controlador deve demonstrar de forma documentada:

- a imprescindibilidade do uso da biometria para o cumprimento da obrigação legal, demonstrando que não há outra medida menos intrusiva igualmente eficaz;
- a compatibilidade da finalidade com o uso da biometria, ou seja, o dado deve ser estritamente necessário ao fim pretendido, sem ampliar indevidamente seu escopo de utilização;
- a limitação do tratamento ao mínimo necessário, incluindo tempo de retenção; e
- a vedação expressa ao uso secundário dos dados, exceto se houver nova base legal válida e transparente.

Como boas práticas de salvaguarda técnica e organizacional, recomenda-se a anonimização, Criptografia de templates biométricos, limitação de acesso por perfis autorizados e auditorias periódicas dos sistemas utilizados. A Agência da União Europeia para a Cibersegurança (ENISA) alerta que os templates biométricos são altamente persistentes e, caso sejam expostos, não podem ser renovados como uma senha tradicional, exigindo proteção redobrada com técnicas de descentralização e minimização de dados.

Além disso, conforme o entendimento da própria ANPD em seus guias de boas práticas, é recomendável que o controlador, sempre que houver risco elevado, realize um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), sobretudo quando houver risco de discriminação, monitoramento em larga escala ou uso de tecnologias sensíveis, como reconhecimento facial em espaços públicos.

Tese: O tratamento de dados pessoais com base em obrigação legal ou regulatória deve ser amparado por norma clara e específica que assegure segurança jurídica e previsibilidade aos titulares. Além disso, é imprescindível que o tratamento observe os princípios da necessidade, idoneidade e proporcionalidade, de modo que o uso dos dados biométricos seja estritamente necessário para atingir a finalidade legítima. Para tanto, o controlador deve comprovar que o sistema adotado é adequado para alcançar o objetivo pretendido, considerando as limitações e riscos inerentes à tecnologia biométrica, como possíveis erros e vieses. A medida deve ainda ser equilibrada, de modo que os benefícios superem os impactos sobre os direitos dos titulares, acompanhada de salvaguardas técnicas e administrativas que garantam transparência, segurança e respeito aos direitos fundamentais.

7) Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

O tratamento de dados biométricos para fins de pesquisa deve observar limites rigorosos de necessidade, proporcionalidade, segurança e interesse público, dado o alto potencial de inferência de dados sensíveis e potencial uso posterior indevido desses dados, ainda que pseudonimizados ou anonimizados. Conforme destaca a ICO, só se admite o uso de dados de categoria especial em pesquisa se for possível demonstrar que esse uso é necessário para

atingir o objetivo científico ou seja, que constitui o meio mais razoável e proporcional disponível¹¹.

Além disso, a mesma orientação exige que a atividade de pesquisa (i) não seja suscetível de causar danos substanciais ou sofrimento significativo aos titulares e (ii) esteja ancorada em interesse público. Esses critérios devem ser demonstrados de forma documentada, com avaliação prévia e contínua dos riscos, especialmente em pesquisas que envolvam inferências emocionais, cognitivas ou comportamentais a partir de dados biométricos.

Do ponto de vista técnico, a literatura evidencia que a anonimização de dados biométricos enfrenta desafios adicionais em relação a outros tipos de dados, pois tais informações são intrinsecamente vinculadas à identidade e ao corpo do indivíduo. Muitos algoritmos de desidentificação apresentam fragilidades frente à combinação com outras bases, sendo insuficientes para garantir privacidade robusta¹².

Nesse cenário, é essencial implementar salvaguardas adicionais, como anonimização combinada com *differential privacy*, criptografia homomórfica, segregação de dados, limitação estrita de acesso e controle de reuso, medidas que podem ser de difícil aplicação em órgãos de pesquisa nos termos da lei. Também se recomenda submeter o projeto de pesquisa à revisão de comitês éticos e incluir cláusulas claras de exclusão, revogação e proteção aos grupos vulneráveis. Por fim, os dados coletados devem ser usados exclusivamente para a finalidade científica justificada, vedado seu uso para identificação, categorização ou aplicação prática sem nova base legal.

Tese: O tratamento de dados biométricos para fins de pesquisa deve demonstrar a necessidade do uso desses dados biométricos para alcançar seus objetivos de forma proporcional e razoável, não havendo alternativa menos invasiva. Além disso, é imprescindível que o tratamento não cause danos substanciais significativo aos indivíduos, respeitando princípios éticos e legais. Além disso, o tratamento deve estar claramente vinculado ao interesse público, justificando o benefício social da pesquisa. É fundamental implementar salvaguardas adicionais, como garantir a anonimização eficaz para minimizar riscos de reidentificação, adotar medidas técnicas e

¹¹ INFORMATION COMMISSIONER'S OFFICE. *Guide to biometric data and biometric technologies*. London. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/>.

¹² HANISCH, Simon et al. *Privacy-Protecting Techniques for Behavioral Biometric Data: A Survey*. IEEE Access, 2022.

organizacionais robustas e assegurar transparência e responsabilidade durante todo o processo.

Bloco III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8) Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

A utilização de tecnologias de reconhecimento facial, mesmo quando fundada em uma hipótese legal prevista na LGPD, deve observar rigorosamente os princípios previstos no art. 6º da lei, com destaque para os princípios da necessidade, proporcionalidade, transparência e não discriminação. Isso implica que o uso dessa tecnologia deve ser estritamente necessário à finalidade pretendida, de modo que não existam meios menos invasivos para atingir o mesmo resultado, e que o impacto sobre os direitos fundamentais dos titulares, especialmente de grupos vulneráveis, seja minimizado. Além disso, é imprescindível garantir que o tratamento não resulte em violações de direitos decorrentes de vieses algorítmicos, historicamente associados à raça, gênero, idade e classe social.

Do ponto de vista técnico e jurídico, os controladores devem implementar salvaguardas robustas que incluam: (i) avaliações de impacto à proteção de dados pessoais (RIPD) com foco específico em vieses algorítmicos e riscos de discriminação; (ii) medidas de segurança e governança algorítmica, como auditorias periódicas, testes de acurácia por grupo demográfico, uso de bases de dados balanceadas e técnicas de explicabilidade; (iii) limitação da coleta e do armazenamento de dados ao mínimo necessário, com controle de acesso rigoroso e retenção limitada no tempo.

Institucionalmente, é fundamental garantir transparência ativa e participação social no desenvolvimento e na implementação dessas tecnologias. Isso pode incluir a publicação de políticas de uso, realização de consultas públicas, funcionamento de comitês de ética e diversidade.

Tese: O uso de tecnologias de reconhecimento facial, mesmo quando amparado por base legal, deve observar os princípios da necessidade, proporcionalidade, transparência e não discriminação, exigindo salvaguardas técnicas (como auditorias e explicabilidade), jurídicas (avaliação de impacto e limitação de uso) e institucionais (participação social), a fim de mitigar riscos de discriminação e garantir a proteção efetiva dos direitos fundamentais.

9) Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, "LGPD") estabeleceu diversas salvaguardas, incluindo direitos, princípios e normas que ressaltam a importância de adotar mecanismos para proteger os titulares de dados. Nesse contexto, o artigo 46, §2º, da LGPD impõe a obrigatoriedade de implementar medidas de segurança, tanto técnicas quanto administrativas, desde a fase de planejamento até a execução de produtos ou serviços. A adoção do conceito de *Privacy by Design* ("PbD"), embora não citado expressamente na LGPD, é amplamente compatível com o seu conteúdo normativo, exigindo que a proteção de dados seja integrada ao ciclo de vida completo do produto ou serviço. Isso implica em incorporar mecanismos de mitigação de riscos desde a concepção dos sistemas de reconhecimento facial, como controle de acesso, pseudonimização e minimização de dados.

Sistemas de reconhecimento facial podem ser projetados para garantir alta eficácia e confiabilidade adotando práticas como: (i) o uso de bases de dados diversas, representativas e balanceadas quanto a características demográficas (gênero, raça, idade), a fim de evitar vieses algorítmicos; (ii) testes rigorosos e contínuos de acurácia e desempenho, tanto em ambientes simulados quanto reais; (iii) calibração frequente dos modelos com métricas transparentes, como taxas de falsos positivos e falsos negativos, segregadas por grupo populacional; e (iv) uso de frameworks confiáveis de inteligência artificial com auditoria externa. Esses elementos devem ser acompanhados de uma governança de dados clara, com políticas internas que definam papéis, responsabilidades e protocolos de resposta em caso de falhas técnicas ou éticas.

Para corrigir tempestivamente eventuais falhas, especialmente em casos de tratamento automatizado, é essencial adotar mecanismos como: (i) revisão humana obrigatória para decisões que gerem efeitos jurídicos ou relevantes aos titulares, conforme o art. 20 da LGPD; (ii) utilização de comitês de revisão ética e técnica com autonomia para suspender ou corrigir decisões automatizadas; (iii) implantação de sistemas de monitoramento contínuo e alarmes em tempo real que detectem padrões anômalos; (iv) disponibilização de canais ágeis de contestação e retificação aos titulares afetados; e (v) realização de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) atualizados periodicamente. Essas práticas contribuem para um ciclo de confiança, inovação e respeito aos direitos fundamentais.

Tese: Sistemas de reconhecimento facial podem ser projetados de forma eficaz e confiável por meio da aplicação consistente do *Privacy by Design*, incluindo o uso de bases de dados representativas, testes regulares de acurácia, calibração contínua de modelos e mecanismos de auditoria algorítmica. Para minimizar falsos positivos e negativos, é essencial garantir diversidade demográfica nos dados, monitoramento técnico permanente e validação independente. A correção tempestiva de falhas em tecnologias de tratamento automatizado exige a implementação de revisão humana obrigatória, comitês de supervisão ética, canais de contestação acessíveis aos titulares e atualização constante dos Relatórios de Impacto. Com esses mecanismos, é possível equilibrar inovação e segurança jurídica, promovendo o uso responsável da tecnologia sem comprometer os direitos dos titulares.

10) É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

A literatura especializada, as autoridades europeias de proteção de dados e o *Artificial Intelligence Act* da União Europeia apontam de forma consistente que o uso de TRF remoto, em tempo real e em espaços públicos, especialmente sem o conhecimento ou interação do titular dos dados, impõe riscos desproporcionais aos direitos fundamentais, incluindo a privacidade, a não discriminação, a liberdade de expressão, a liberdade de reunião e a autodeterminação informacional.

A vigilância biométrica em larga escala compromete a autonomia individual e pode induzir efeitos inibitórios sobre o comportamento social e político dos cidadãos, pois a possibilidade

constante de monitoramento invisível restringe o exercício livre de direitos. Essa preocupação é agravada pelo potencial de uso da TRF em contextos de controle populacional ou policiamento discriminatório, como demonstra o histórico de aplicações em investigações criminais baseadas em bancos de dados enviesados.

Além disso, há riscos técnicos relevantes. O reconhecimento facial apresenta taxas significativamente maiores de erro para grupos raciais e étnicos minorizados, mulheres e pessoas idosas, levando a falsos positivos ou falsos negativos que podem resultar em discriminação, constrangimento e danos reputacionais. Isso ocorre porque os algoritmos muitas vezes são treinados com dados pouco representativos, reproduzindo desigualdades estruturais no processo decisório automatizado. Mesmo sistemas auditados e com supervisão humana não eliminam completamente os riscos de viés e rotulagem indevida.

O próprio Parlamento Europeu já defendeu moratórias ou proibições totais da TRF em locais como escolas, hospitais e espaços culturais, recomendando inclusive que a Comissão Europeia avalie sua completa exclusão de ambientes públicos¹³. No mesmo sentido, o *Artificial Intelligence Act* classifica como prática proibidas a categorização biométrica com base em dados sensíveis (como origem étnica, orientação sexual ou opiniões políticas), e restringe o uso de TRF em tempo real no espaço público para fins de aplicação da lei a situações excepcionais, exigindo fundamentação legal, avaliação de impacto sobre direitos fundamentais, autorização judicial e salvaguardas estritas de tempo, local e escopo pessoal.

Diante desses fatores, o uso da TRF não deve ser adotado em ambientes educacionais, de saúde, culturais, comerciais abertos ao público, nem em locais de circulação massiva, como transporte público e vias urbanas, salvo quando expressamente previsto em lei com base em interesse público substancial, e desde que sujeito a controle da autoridade prévio e medidas de mitigação de riscos.

Tese: O uso remoto e em tempo real do reconhecimento facial em espaços públicos impõe riscos desproporcionais à privacidade, liberdade e não discriminação. A vigilância biométrica em larga escala ameaça a autonomia individual, podendo restringir direitos e promover discriminação, especialmente devido a vieses técnicos que afetam minorias e grupos vulneráveis. Assim, o uso da TRF deve ser proibido em espaços públicos e privados sensíveis, salvo exceções legais fundamentadas e controladas previamente pela autoridade de proteção de dados.

¹³ See European Parliament [resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector, 2020/2017\(INI\)](#).

Bloco IV - SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS**11) Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?**

Dado o impacto significativo de uma violação de dados biométricos que, por sua natureza, são únicos, permanentes e não substituíveis, as organizações que realizam tratamento automatizado dessas informações devem adotar um conjunto de medidas técnicas e administrativas robustas, em linha com os princípios da LGPD. Entre as medidas de segurança técnicas destacam-se: (i) criptografia forte dos dados biométricos tanto em repouso quanto em trânsito; (ii) controles rígidos de acesso com autenticação multifator para operadores e sistemas; (iii) testes periódicos de vulnerabilidades e análise de código-fonte para prevenir brechas. No campo das medidas administrativas, impõem-se como essenciais: (i) treinamentos regulares com equipes técnicas e jurídicas sobre privacidade e proteção de dados; (ii) políticas internas de resposta a incidentes; (iii) plano de continuidade de negócios e recuperação de desastres; e (iv) formalização de contratos com operadores e fornecedores com cláusulas específicas de segurança e responsabilização.

Além dessas medidas, a avaliação e o monitoramento dos riscos devem ser contínuos e baseados em parâmetros mínimos que garantam a conformidade com os arts. 46 e 49 da LGPD. Nesse sentido, recomenda-se exigir das organizações: (i) elaboração obrigatória de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) sempre que houver tratamento biométrico em larga escala ou uso automatizado com potencial de impacto relevante ao titular; (ii) revisão periódica dos RIPDs, ao menos anual ou sempre que houver mudança significativa na tecnologia ou na finalidade do tratamento; (iii) implementação de indicadores-chave de desempenho (KPIs) de segurança, como taxa de incidentes, tempo médio de resposta e índice de conformidade; (iv) auditoria externa independente ao menos uma vez por ano para validar os controles de proteção de dados; e (v) canal interno de denúncias e gestão de riscos com reporte direto à alta administração. Esses parâmetros mínimos asseguram que a gestão de riscos seja efetiva, transparente e proporcional à sensibilidade dos dados biométricos tratados.

Assim, o setor empresarial pode cumprir com sua função de desenvolver soluções inovadoras e eficientes, sem abrir mão da segurança jurídica e da confiança do titular.

Tese: Para mitigar os riscos relacionados ao tratamento de dados biométricos, é indispensável que as organizações adotem medidas técnicas como criptografia robusta, autenticação multifator, e testes contínuos de segurança, bem como medidas administrativas como treinamentos, planos de resposta a incidentes, políticas de continuidade de negócios e cláusulas contratuais específicas com operadores. Quanto aos parâmetros mínimos de avaliação de riscos e monitoramento, devem ser exigidos: elaboração e atualização periódica de Relatórios de Impacto (RIPD), uso de indicadores de segurança, auditorias externas regulares e canais internos de reporte de riscos. Esses mecanismos garantem a conformidade com a LGPD e fortalecem a proteção integral de dados biométricos, permitindo que o setor privado atue com responsabilidade e segurança jurídica no desenvolvimento de tecnologias sensíveis.

12) Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Quando uma funcionalidade específica de um serviço não essencial depende tecnicamente da autenticação biométrica, como, por exemplo, acesso rápido via reconhecimento facial em um app, ou login automático com impressão digital em um clube de fidelidade, é fundamental que sejam adotadas boas práticas que garantam que essa limitação técnica não resulte em discriminação ilícita ou abusiva. Como exemplos de boas práticas, é possível citar como uma primeira medida, a garantia da transparência, de modo que a organização deve comunicar de forma clara, acessível e prévia aos titulares o motivo pelo qual a biometria é tecnicamente necessária para aquela funcionalidade. Também é recomendável a realização de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) nos termos da LGPD, especialmente quando a biometria for requisito exclusivo para a funcionalidade.

Outra boa prática é o respeito ao princípio da necessidade e minimização (art. 6º, III da LGPD). Isto é, a biometria só deve ser exigida se não houver meios alternativos que ofereçam segurança ou funcionalidade equivalentes. Se a funcionalidade exige biometria para garantir integridade, personalização ou autenticação reforçada, é necessário demonstrar isso de forma objetiva, com base em critérios técnicos ou de risco. Além disso, é recomendável que

a exigência da biometria não bloqueie o acesso ao serviço como um todo, mas apenas àquela funcionalidade específica, evitando uma exclusão indireta ou desproporcional.

Além disso, mesmo que tecnicamente necessária, a funcionalidade não deve ser apresentada como “recompensa” para quem autoriza o uso de dados sensíveis, pois isso pode configurar discriminação indireta. Em suma, a biometria pode ser tecnicamente exigida em funcionalidades específicas, desde que essa exigência seja proporcional, transparente, justificada e não coercitiva.

No que tange à recusa do titular ao fornecimento de dados biométricos, quando o tratamento se baseia no consentimento, tal negativa pode justificar a restrição ao uso de determinadas funcionalidades apenas quando estiver claramente demonstrado que não há alternativas técnicas equivalentes para garantir a segurança, integridade ou funcionamento da funcionalidade. Nesses casos, é legítimo que a recusa implique na limitação de acesso.

Por exemplo, em um serviço de pagamento digital, pode ser justificável condicionar o uso de uma função de pagamento por aproximação à autenticação facial, se isso for necessário para evitar fraudes ou acessos indevidos. Já em um sistema de telemedicina, o acesso ao histórico clínico sensível pode exigir biometria por segurança. Nessas hipóteses, a restrição é proporcional à recusa do consentimento. De toda forma, a recusa não pode comprometer o serviço principal, mas apenas funcionalidades que sejam dependentes da biometria e cuja indisponibilidade não represente violação a direitos fundamentais.

Ainda assim, recomenda-se que a organização ofereça alternativas razoáveis, mesmo que menos eficientes, quando possível. Por exemplo, autenticação via token, senha, ou autenticação em dois fatores. Isso garante que o usuário não seja compelido a consentir apenas para não perder acesso ao serviço, o que invalidaria o próprio consentimento. A recusa, portanto, pode justificar limitações, mas somente se tais limitações forem transparentes, tecnicamente justificadas e não resultarem em exclusão abusiva do titular.

Tese: A exigência de biometria em funcionalidades não essenciais é legítima quando tecnicamente indispensável, desde que acompanhada de justificativa transparente, medidas de minimização e sem excluir o titular do serviço principal. A recusa do consentimento pode justificar a limitação de acesso a funcionalidades específicas, desde que proporcional, comunicada previamente e sem configurar tratamento discriminatório. A oferta de vantagens exclusivas com base no fornecimento de dados biométricos, sem alternativa técnica equivalente, pode representar discriminação indireta, vedada pela LGPD.

13) Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Para conferir uma proteção eficaz no tratamento de dados biométricos, os controladores devem adotar boas práticas específicas, alinhadas aos princípios e deveres previstos na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018). Dentre as boas práticas recomendadas destacam-se: (1) a realização prévia de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando houver alto risco; (2) a adoção de Privacy by Design, com segurança e proteção de dados incorporadas desde a concepção dos sistemas; (3) a minimização de dados, tratando apenas as informações estritamente necessárias; (4) a segregação de bases de dados sensíveis; e (5) a adoção de protocolos de segurança robustos, como criptografia, controle de acesso e anonimização quando possível.

Além disso, é essencial garantir que o tratamento de dados biométricos ocorra de forma transparente e responsável, prevenindo a discriminação ilícita ou abusiva. Isso implica fornecer ao titular informações claras, acessíveis e compreensíveis sobre a finalidade da coleta, a base legal, e os direitos assegurados. O uso dos dados não deve gerar tratamento desigual ou vantagem indevida para quem aceita fornecer biometria, especialmente quando o consentimento for a base legal. Condicionar funcionalidades ou benefícios ao fornecimento de biometria, sem justificativa técnica real, pode configurar discriminação indireta, o que é expressamente vedado pela LGPD. Também é fundamental garantir que o titular possa revogar seu consentimento a qualquer momento, bem como oferecer meios alternativos de acesso ao serviço, sempre que tecnicamente viável.

A adoção de mecanismos de governança em privacidade também é recomendada, como a definição de políticas internas claras sobre o ciclo de vida dos dados biométricos, treinamentos periódicos para equipes e a designação de um Encarregado pelo Tratamento de Dados Pessoais (DPO). Ferramentas como auditorias internas regulares, testes de proporcionalidade e avaliações de risco contínuas ajudam a garantir que a biometria seja usada apenas quando estritamente necessária, e que seu uso não exponha os titulares a vulnerabilidades desproporcionais. Essas práticas contribuem para a conformidade legal e fortalecem a confiança dos usuários, especialmente em setores como saúde, segurança, tecnologia e serviços financeiros, onde o uso da biometria é mais frequente e sensível.

Tese: A proteção eficaz no tratamento de dados biométricos exige a adoção de medidas técnicas e organizacionais que assegurem sua utilização proporcional, transparente e justificada. Cabe ao controlador garantir a segurança da informação, respeitar os princípios da LGPD e prevenir práticas discriminatórias diretas ou indiretas. O uso responsável da biometria deve se fundamentar em necessidade técnica real, ser informado de forma clara ao titular e estar sujeito a mecanismos de controle, revisão e mitigação de riscos contínuos.

14) Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

Em contextos de tratamento contínuo e massivo de dados biométricos, como em iniciativas de cidades inteligentes, monitoramento de multidões ou vigilância em espaços públicos, o respeito à autodeterminação informativa dos titulares deve ser assegurado por meio de mecanismos proporcionais e tecnicamente viáveis. É fundamental reconhecer que esses ambientes apresentam características operacionais específicas que muitas vezes inviabilizam abordagens tradicionais baseadas em consentimento prévio individual. Assim, é necessário adotar uma combinação de medidas de transparência, minimização de dados e governança responsável. Isto é, faz-se necessária uma abordagem estruturada, clara e acessível que permita aos titulares serem informados de maneira efetiva e exercerem seus direitos mesmo diante da complexidade do ambiente.

A informação aos titulares pode ser viabilizada por meio de sinalização clara e acessível nos ambientes de coleta, com linguagem simples e objetiva sobre a finalidade do tratamento, o agente controlador, e os canais para o exercício de direitos. No plano internacional, que pode nos servir como referência, as Diretrizes 3/2019 do Comitê Europeu para a Proteção de Dados (EDPB)¹⁴ recomendam a adoção de uma estratégia de transparência em dois níveis:

¹⁴ Comitê Europeu para a Proteção de Dados (EDPB). *Diretrizes 3/2019 sobre o tratamento de dados pessoais por meio de dispositivos de vídeo*, versão 2.0, adotada em 29 de janeiro de 2020. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf

1. **Primeiro nível – sinalização visível e contextual:** Implantação de sinais de aviso facilmente perceptíveis e inteligíveis, colocados em pontos estratégicos (ao nível dos olhos antes do ingresso na área monitorada), contendo informações básicas e essenciais sobre o tratamento biométrico, como a existência da vigilância, finalidades, identidade do controlador, direitos dos titulares e eventuais tratamentos extraordinários (por exemplo, transmissão a terceiros ou conservação dos dados). Estes sinais devem ser adequados ao contexto local e permitir que o titular compreenda a área sob monitoramento e decida sobre sua permanência.
2. **Segundo nível – informações detalhadas e acessíveis:** Disponibilização de informações completas e pormenorizadas em meios acessíveis ao público, preferencialmente fora da área de vigilância, como websites, QR codes, balcões de atendimento ou números telefônicos. Tal acesso deve ser facilitado, inclusive para indivíduos que não estejam no local da vigilância, garantindo transparência plena.

Para assegurar que os titulares possam exercer controle efetivo sobre seus dados biométricos, recomenda-se ainda a implementação das seguintes medidas concretas:

- Disponibilização de canal para o exercício dos direitos do titular, tais como acesso, retificação, eliminação e limitação do tratamento.
- Aplicação dos princípios da minimização e limitação do tratamento, restringindo a coleta àquilo estritamente necessário.

Em síntese, mesmo em situações desafiadoras de difícil transparência, como o tratamento biométrico em massa e contínuo em espaços públicos, os controladores devem empregar uma combinação integrada de sinais visuais claros, informações detalhadas acessíveis, ferramentas de controle e governança robusta, para garantir o pleno respeito à autodeterminação informativa dos titulares.

Tese: Em tratamentos biométricos contínuos e massivos, a autodeterminação informativa deve ser garantida por um conjunto de medidas proporcionais que combinem transparência acessível, canais eficazes para o exercício de direitos e práticas robustas de governança. A regulação deve considerar a viabilidade técnica e os contextos de aplicação, evitando rigidez normativa que possa prejudicar soluções legítimas e de interesse coletivo.

Bloco V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS**15) De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?**

Para garantir o respeito aos direitos dos titulares no tratamento automatizado de dados biométricos, incluindo o direito à informação clara, ao acesso, à correção e à revogação do consentimento, é necessário adotar práticas que tornem esses direitos exequíveis mesmo em cenários de alta complexidade tecnológica. A clareza da informação deve ser priorizada, com comunicações adaptadas ao nível de compreensão do público envolvido, incluindo linguagem acessível, visual simplificada e formatos multiplataforma (como cartazes, notificações digitais, e interfaces amigáveis em aplicativos ou sites). É importante que o tratamento automatizado não seja percebido como um processo opaco, o que demanda transparência ativa por parte dos agentes de tratamento.

Os direitos de acesso e de correção podem ser operacionalizados por meio de canais específicos e bem divulgados, que permitam ao titular identificar os dados coletados e solicitar sua atualização, quando aplicável. Em situações em que os dados biométricos são vinculados a uma identidade persistente (como em sistemas de reconhecimento facial), deve-se garantir que a base de dados permita esse tipo de correção, com controles de segurança que evitem fraudes ou acessos indevidos.

A revogação do consentimento, quando este for a base legal aplicável, deve ser tão simples quanto a sua concessão. Isso implica em disponibilizar mecanismos acessíveis para que o titular possa retirar seu consentimento a qualquer momento, com efeitos claros e previsíveis. Em sistemas automatizados, recomenda-se que esse processo seja viabilizado por meios digitais, preferencialmente nos mesmos canais por onde se deu a coleta ou autorização inicial. Ainda assim, é importante reconhecer que nem todo tratamento biométrico se fundamenta em consentimento, e nesses casos os direitos devem ser assegurados com base na finalidade legítima, proporcionalidade e medidas de mitigação de riscos.

Tese: O respeito aos direitos dos titulares em tratamentos automatizados de dados biométricos exige um compromisso ativo com a transparência, simplicidade nos mecanismos de controle e atenção à proporcionalidade no uso da tecnologia. A regulação deve valorizar medidas práticas, seguras e tecnicamente viáveis para

assegurar o exercício real desses direitos, considerando as particularidades de cada contexto de uso.

16) Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O tratamento de dados biométricos de crianças e adolescentes em contextos como escolas e espaços recreativos exige máxima cautela jurídica e ética. Esses dados são classificados como sensíveis (LGPD, art. 5º, II) e referem-se a uma população em condição peculiar de desenvolvimento, exigindo o privilégio do princípio do melhor interesse, nos termos do art. 14 da LGPD.

1. Participação informada dos pais ou responsáveis

A garantia da participação informada passa por um compromisso com a transparência ativa e contínua sobre as finalidades de uso deste dado. Essa comunicação deve ser feita tanto por meio de avisos de privacidade quanto por ações pedagógicas inclusivas, adaptadas à idade e nível de compreensão dos alunos e genitores, conforme o §6º, do artigo 14 da LGPD. Os responsáveis podem ser incentivados pela escola a discutir essa possibilidade com seus filhos. Por fim, é importante que as escolas ofereçam métodos alternativos de acesso aos serviços, quando possível.

2. Hipóteses legais admissíveis

Embora todas as bases legais do artigo 11 da LGPD sejam, em tese, aplicáveis ao tratamento de dados biométricos, a escolha da hipótese adequada deve considerar a finalidade específica do tratamento e observar o princípio da necessidade (art. 6º, II). Ou seja, é essencial avaliar se a atividade realizada por escolas ou espaços recreativos realmente demanda o uso de dados biométricos e se não há alternativa menos invasiva.

A base legal da proteção da vida ou da incolumidade física (art. 11, II, “e”) pode ser cabível em situações excepcionais, como localização de crianças desaparecidas ou ações emergenciais de salvamento. Já a base da prevenção à fraude e à segurança do titular (art. 11, II, “g”) é especialmente pertinente quando a biometria é usada para controle de acesso, autenticação ou proteção da integridade física das crianças.

Embora o consentimento dos responsáveis seja juridicamente possível, sua exigência pode ser inviável operacionalmente em contextos de segurança, reforçando a importância de uma avaliação proporcional da base legal mais adequada ao caso concreto.

3. Condições para alinhamento ao princípio do melhor interesse (art. 14 da LGPD)

Para garantir que o tratamento esteja alinhado ao princípio do melhor interesse, conforme exige o artigo 14 da LGPD, é imprescindível demonstrar que a biometria é necessária para alcançar o objetivo pretendido, e que foram consideradas alternativas menos intrusivas. Além disso, devem ser implementadas salvaguardas como minimização da coleta, restrição de acesso aos dados, armazenamento seguro, auditorias periódicas e eliminação das informações tão logo cessada a finalidade. Também é importante garantir canais acessíveis para que os pais ou responsáveis possam exercer os direitos dos menores, inclusive com a possibilidade de obter informações claras sobre seu funcionamento.

Tese: O tratamento de dados biométricos de crianças e adolescentes exige transparência e participação informada dos pais ou responsáveis, com informações claras sobre a finalidade e os direitos envolvidos. A escolha da base legal deve considerar o contexto e a necessidade do tratamento: a proteção da vida (art. 11, II, “e”) pode ser usada em situações excepcionais, enquanto a prevenção à fraude e à segurança (art. 11, II, “g”) é adequada para controle de acesso e proteção em ambientes institucionais. Para estar em conformidade com o art. 14 da LGPD, o tratamento deve ser proporcional, necessário e demonstrar claramente que atende ao melhor interesse da criança ou adolescente.

17) Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Este tipo de tratamento de dados biométricos é admissível nas hipóteses em que ele se mostra necessário para monitorar o comportamento de crianças e adolescentes em ambientes que possam representar algum risco à sua segurança ou bem-estar, tanto em contextos presenciais (como escolas, espaços recreativos ou instituições de acolhimento) quanto digitais. Nesses casos, o tratamento pode ser legitimado, por exemplo, com base no artigo 11, II, alínea “g” da LGPD (prevenção à fraude e à segurança do titular) ou, em situações excepcionais, pela alínea “e” (proteção da vida ou da incolumidade física). A escolha da tecnologia biométrica deve ser precedida por uma análise de risco do ambiente específico,

demonstrando que o uso da biometria é proporcional, necessário e mais eficaz do que alternativas menos intrusivas.

Para garantir a participação informada dos pais ou responsáveis, recomenda-se a adoção de estratégias de comunicação acessíveis e contínuas, com explicações claras sobre a finalidade do tratamento, os dados envolvidos, os direitos dos titulares e os canais de contato disponíveis. Essa informação pode ser disponibilizada em formatos físicos e digitais (como formulários explicativos, notificações nos portais institucionais, QR Codes e painéis informativos em locais de entrada), sempre com linguagem adequada ao público. É fundamental garantir que os responsáveis possam exercer os direitos dos menores, inclusive questionar o tratamento, solicitar informações ou requerer a exclusão dos dados, quando aplicável.

Quanto às medidas técnicas e organizacionais, é essencial implementar protocolos de segurança que minimizem riscos de acesso indevido, uso abusivo ou vazamento dos dados. Isso inclui criptografia, controles de acesso, segregação de dados, monitoramento de logs, anonimização ou pseudonimização, limitação do prazo de retenção e revisões periódicas de segurança. Também é recomendável a elaboração de relatórios de impacto à proteção de dados (RIPD) para documentar a justificativa do tratamento e mitigar riscos, especialmente quando envolver tecnologias de identificação automatizada ou vigilância contínua.

Tese: O tratamento de dados biométricos de crianças e adolescentes pode ser admissível quando demonstrada sua real necessidade diante de riscos concretos no ambiente de uso, e desde que fundado em base legal compatível, como a prevenção à fraude e à segurança do titular. A participação informada dos pais ou responsáveis deve ser viabilizada por meio de comunicação clara e acessível, e o tratamento deve estar condicionado à adoção de medidas técnicas e organizacionais robustas que garantam a proteção da privacidade e dos direitos desses grupos vulneráveis.

18) Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

A verificação ou estimação de idade por meio de dados biométricos, especialmente em plataformas digitais e jogos acessíveis a crianças e adolescentes, exige cautela quanto à legalidade, proporcionalidade e finalidade do tratamento. Por envolver dados sensíveis de

grupos vulneráveis, esse tipo de prática deve ser adotado quando estritamente necessário para garantir o cumprimento de obrigações legais, como restrições etárias, ou a proteção contra riscos relevantes ao desenvolvimento físico, mental e moral do público infantojuvenil.

Entre os critérios a serem observados, destacam-se: (i) a justificativa técnica e legal para o uso da biometria em vez de outros métodos menos intrusivos; (ii) a minimização de dados, coletando-se apenas o necessário para estimar ou verificar a idade, sem retenção indevida de características biométricas; (iii) a limitação da finalidade, com vedação de reutilização dos dados para outras finalidades, como perfis comportamentais ou marketing direcionado; e (iv) a adoção de medidas que garantam a transparência e o controle pelos pais ou responsáveis, inclusive com canais para revisão, correção ou eliminação dos dados tratados.

Para compatibilizar essa prática com os princípios da necessidade (art. 6º, II) e do melhor interesse da criança e do adolescente (art. 14), é fundamental demonstrar que a verificação etária via biometria é o único meio eficaz de proteger o titular em determinada situação, como o acesso a conteúdos restritos ou interações em plataformas com alto risco de exposição. Além disso, deve-se priorizar a retenção mínima, anonimização e auditoria constante. A exigência de relatório de impacto à proteção de dados (RIPD), nesse contexto, é especialmente relevante para documentar a proporcionalidade e as salvaguardas adotadas.

Tese: A verificação ou estimação de idade por biometria só se justifica quando for comprovadamente necessária para proteger crianças e adolescentes em ambientes digitais de risco, sendo imperativo limitar a coleta ao estritamente necessário, adotar salvaguardas técnicas rigorosas e garantir a supervisão dos responsáveis legais. O tratamento deve ser orientado pelos princípios da minimização, transparência e pelo melhor interesse do menor, evitando qualquer uso abusivo ou desproporcional da tecnologia.

OFÍCIO Nº ED-0018/2025

São Paulo, 1º de agosto de 2025.

À
Autoridade Nacional de Proteção de Dados
ANPD - Coordenação-Geral de Normatização

Assunto: Tomada de Subsídios: Dados pessoais e sensíveis – dados biométricos

Prezados Senhores,

1 A Federação Brasileira de Bancos ("FEBRABAN"), associação civil sem fins lucrativos representativa do setor financeiro, Associação Brasileira das Empresas de Cartões de Crédito e Serviços (ABECS), submetem, para vossa apreciação, suas considerações acerca da Tomada de Subsídios acima referenciada, que tem como objetivo coletar informações, evidências e perspectivas de diversos setores da sociedade sobre o tratamento de dados biométricos, visando a elaboração de materiais orientativos ou regulamentos que promovam a proteção de dados pessoais e a inovação responsável.

2 As considerações estão em anexo.

Respeitosamente,

FEBRABAN

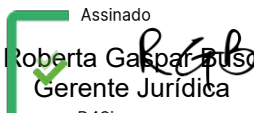
vicente.dechiara@febraban.org.br

Assinado


Luis Vicente Magni De Chiara
Diretor executivo de Assuntos Jurídicos
D4Sign

roberta.buso@febraban.org.br

Assinado


Roberta Gaspar Buso
Gerente Jurídica
D4Sign

ABECS

marcelot@abecs.org.br

Assinado


Marcelo Takeyama
Diretor Jurídico, Autorregulação e Compliance
D4Sign

Av. Brigadeiro Faria Lima / 4.300, 4º andar
04538-132 / São Paulo-SP / Brasil


febraban.org.br

Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos**BLOCO I - DEFINIÇÕES E PRINCÍPIOS**

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo “dados biométricos”, mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos - que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

A Lei Geral de Proteção de Dados Pessoais (“LGPD”) classifica os dados biométricos como dados pessoais sensíveis, em seu artigo 5º, II: “Art. 5º Para os fins desta Lei, considera-se: (...) II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou **biométrico, quando vinculado a uma pessoa natural.**”

Embora a LGPD não apresente uma definição específica de “dado biométrico”, é possível extrair alguns critérios para caracterizar um dado pessoal como dado biométrico. Destarte, não há dados intrinsecamente biométricos, mas dados pessoais que podem se tornar biométricos quando enquadrados, **cumulativamente**, nos critérios abaixo indicados.

1. **Características físicas/fisiológicas únicas:** Origem em características físicas e fisiológicas inerentes, únicas, relativamente estáveis e distintivas do titular, tais como, impressão digital, padrões únicos da geometria facial e pontos nodais do rosto, padrões únicos de íris, voz, geometria da mão/veias da palma. No âmbito do GDPR, são também considerados dados biométricos os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural que permitam ou confirmem a identificação única dessa pessoa natural, nomeadamente imagens faciais ou dados datiloscópicos (artigo 4º, n.º 14, GDPR). Nem todas as características comportamentais são dados biométricos, mas cita-se como exemplo padrão de digitação (o ritmo e a pressão com que uma pessoa digita) e assinatura dinâmica (a forma e a pressão ao escrever uma assinatura).
2. **Resultante de tratamento técnico específico:** Para que a característica única seja considerada um dado biométrico, deve ter sido submetida a um tratamento técnico específico (como, por exemplo, em ambiente automatizado ou passível de automatização) ou que extraia padrões de forma a permitir a identificação ou autenticação de uma pessoa. Por exemplo,

uma fotografia de uma pessoa, não é um dado biométrico por si só. Caso essa foto seja tratada em um sistema de reconhecimento facial que a converta em um *template* biométrico para identificar ou autenticar uma pessoa, ela se torna parte de um tratamento de dado biométrico. Essa, inclusive, é a interpretação pacificada na Europa, incluída no Recital 51¹ do *General Data Protection Regulation* da União Europeia (“GDPR”).

3. **Capacidade de identificar ou autenticar um indivíduo de forma única e vinculação à pessoa natural.** Para ser considerado dado biométrico, como dado sensível, necessariamente deve estar vinculado a uma pessoa natural, como mencionado no art. 5º, II, da LGPD e deve ser capaz de identificar uma pessoa. Se o tratamento dos dados não conseguir identificar e/ou autenticar, de forma única, um indivíduo perante outro ou diante de um grupo próximo ou presente, o requisito não será cumprido.

A ausência de qualquer um desses critérios pode fazer com que o dado não se enquadre como dado biométrico sob a LGPD.

¹**Recital 51 do GDPR:** “The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person”

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

As boas práticas de transparência devem balizar todo e qualquer tratamento de dados, independentemente do dado ser caracterizado como dado pessoal sensível. Importante destacar que as práticas de transparência podem variar, inclusive a depender do contexto da coleta e do tratamento dos dados biométricos e da base legal aplicável.

Assim, cada controlador deve definir a melhor forma de cumprir o princípio da transparência, não sendo recomendada a imposição de formato ou meio para cumprimento de tal princípio sob pena de não ser o formato ou meio mais adequado a todos os controladores e prejudicando, por fim, a obtenção de informações relevantes ao próprio titular de dados.

De qualquer forma, em atenção ao princípio da transparência, o controlador deve fornecer ao titular informações claras e precisas acerca da realização do tratamento, informando se há tratamento de tratamentos biométricos e sua finalidade. Como exemplo de transparência ativa, entendemos que o mais importante é a inclusão dessas informações na política de privacidade, que ainda se mostra o principal instrumento de transparência aplicável na relação entre controlador e titular e que também já contém outras informações importantes, como canais e meios para exercício dos direitos do titular e outras informações sobre o tratamento de dados pessoais.

Ademais, a depender do contexto da coleta e de outros tratamentos dos dados biométricos, pode ser dada transparência a esse respeito na jornada do titular, caso aplicável e viável. Ainda, caso o consentimento seja utilizado como a base legal para o tratamento desses dados, o próprio instrumento do consentimento pode trazer tais informações ao titular.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A priori, retomando os critérios indicados na resposta ao item 1, cabe destacar que, dados comportamentais e biometria comportamental são conceitos que não se confundem. Enquanto os dados comportamentais são informações gerais sobre ações da pessoa, a biometria comportamental consiste no resultado do tratamento, por meio técnico específico, de determinados dados

comportamentais para a finalidade específica de identificação e autenticação única de uma pessoa.

Essa distinção é bastante relevante dentro dos contextos de coleta de dados comportamentais para fins de prevenção às fraudes em ambientes digitais, dentro dos quais pode haver o tratamento de informações para verificar se o comportamento da pessoa que está naquela jornada apresenta indícios de fraude ou não.

Como exemplo, trazemos a coleta de tempo que a pessoa percorrendo a jornada leva para preencher seus dados pessoais, que, comparado ao tempo médio de outras pessoas da mesma faixa etária, região demográfica e aparelhos móveis com características semelhantes, mostrou-se excessivamente longo o que pode ser um indicativo de que a pessoa está consultando dados que deveria saber de pronto.

Esses dados comportamentais não podem ser entendidos como dados biométricos pois, não apresentam todos os critérios objetivos para tanto, tendo em vista que não há a utilização de modelos biométricos cuja finalidade seja autenticar ou identificar um indivíduo. Ou seja, nem todo o dado comportamental é um dado biométrico, seja pela natureza daquele dado específico, seja pela finalidade e contexto de sua utilização.

Ultrapassada essa relevante distinção conceitual, cabe ainda sinalizar que, enquanto a biometria tradicional trata de dados físicos mais estáticos, a biometria comportamental analisa padrões dinâmicos. Especificamente sobre a utilização de dados biométricos potencialmente classificados como “comportamentais”, conforme indicado no enunciado, tais como “reconhecimento de voz, padrões de digitação, movimento ocular”, quando avaliados comparativamente à biometria tradicional (digital, íris e face), como já mencionado, a utilização desses dados comportamentais deve ser avaliada de acordo com o contexto do tratamento e a finalidade específica.

A biometria comportamental é mais comumente usada como forma de autenticação contínua do usuário como forma de detectar que, ainda que a pessoa tenha se autenticado como sua biometria física (biometria tradicional) ou de outra forma, ainda é aquela mesma pessoa que está acessando as funcionalidades do dispositivo/aplicação.

Esses sinais são coletados em tempo real e variam conforme o contexto, permitindo, inclusive, detecção de usos robóticos, sequestro de sessão ou engenharia social que a biometria digital, a íris ou face, analisadas isoladamente, bem como outras formas de autenticação, nem sempre capturam.

Sobre a importância do uso dos dados biométricos comportamentais, especialmente em um país no qual o furto de aparelhos telefônicos com exigência, pelo criminoso, de desbloqueio do aparelho e, muitas vezes, dos aplicativos de instituições financeiras, vale trazer trecho do relatório do “ESTUDO EXPERIMENTAL DA BIOMETRIA COMPORTAMENTAL PARA AUTENTICAÇÃO CONTÍNUA DE USUÁRIOS EM APLICAÇÕES BANCÁRIAS”, da Universidade de Brasília:

“Isso permite tornar a experiência do usuário melhor, bem como reduzir o número de fraudes baseadas no roubo de credenciais, pois, neste cenário, além de roubar as credenciais, seria necessário que o criminoso tivesse um comportamento semelhante ao usuário vítima de fraude na interação com o dispositivo no momento de digitação da senha e na interação com a aplicação.”¹¹

Também citamos outras aplicações técnicas que se mostram aplicáveis quanto ao uso dessa categoria de dados para fins de prevenção à fraudes e maior segurança na jornada de clientes no setor financeiro: autenticação contínua em sessões bancárias online para detecção de fraudes em aplicações e transações financeiras, tais como com base em padrões anômalos de digitação e navegação, de proteção contra tomada de controle remoto de dispositivos ou contas por meio de análise de interação comportamental e reforço de autenticação multifator com dados de comportamento para mitigar riscos de *phishing* e ataques de engenharia social, identificação de *bots* e acessos automatizados maliciosos em plataformas digitais. Tais usos permitem fortalecer significativamente a integridade dos sistemas e reduzir exposição a riscos do titular sem comprometer a experiência do usuário.

Ressaltamos que a utilização desses dados para a finalidade de prevenção e mitigação de fraudes e que visem trazer maior segurança aos titulares é medida fundamental para as medidas técnicas, operacionais e sistemáticas que as instituições financeiras adotam para proteger os próprios titulares,

reduzindo perdas patrimoniais e garantindo a integridade do sistema financeiro nacional.

Dessa forma, esse tipo de tratamento dos dados biométricos comportamentais para autenticação contínua do titular, prevenção à fraudes e segurança é crucial, devendo ser resguardado o uso da tecnologia em prol da segurança dos titulares, inclusive como uma camada dinâmica de defesa necessária contra fraudadores, a qual também pode basear-se na aplicação do art. 11, II, g, da LGPD, que autoriza o tratamento de dados pessoais para as finalidades de garantia de prevenção à fraude e segurança do titular, dispensando o consentimento como a base legal aplicável.

Quanto à existência de “obrigações específicas”, é certo que a LGPD não estabeleceu requisitos ou obrigações específicas aplicáveis ao tratamento de dados biométricos comportamentais. Entendemos que não há necessidade de observância de obrigações adicionais específicas com relação aos dados de biometria comportamental, que deve ser tratada à luz dos mesmos princípios e requisitos legais previstos na LGPD, tais como a observância dos princípios da finalidade, necessidade, qualidade de dados e segurança, por exemplo.

Com isso, deve-se considerar os contornos específicos – e não necessariamente obrigações adicionais – quanto à aplicação de determinados princípios, como o da qualidade dos dados (art. 6º, V, da LGPD) e da segurança (art. 6º, VII, da LGPD) no contexto da biometria comportamental, na medida em que esse tipo de dado envolve padrões dinâmicos e variáveis que podem se alterar com o decorrer do tempo (como voz, digitação e movimento ocular).

Assim, é importante levar em consideração a natureza dinâmica e variabilidade dos dados comportamentais, que são mais voláteis e contextuais, adotando-se mecanismos de validação e atualização dos modelos de identificação que leve em conta as variações decorrentes da variabilidade natural do comportamento humano, buscando melhor acurácia das informações.

De qualquer forma, é também possível haver um tratamento mais flexível no que tange à biometria comportamental, considerando o seu caráter em geral menos identificável de forma isolada, em comparação à biometria tradicional, tendo em vista que os dados são tratados com foco em padrão de comportamento e não em característica física fixa. Por exemplo, em caso de eventual acesso indevido a esse dado, é menos provável que tal dado possa ser utilizado de forma indevida ou cause prejuízos ao titular, tendo um menor potencial de risco.

Como no caso de biometria tradicional, pode-se considerar a adoção de avaliações de impacto à proteção de dados.

Em resumo, a biometria comportamental não substitui a biometria tradicional, mas é totalmente complementar, adicionando uma dimensão essencial de proteção à autenticação, inclusive ao detectar atividades suspeitas em tempo real, sendo crucial para prevenção de fraudes e cibersegurança. O seu tratamento não demanda, necessariamente, obrigações adicionais, mas deve-se levar em conta a natureza e contexto dos dados biométricos comportamentais na adoção de tais medidas.

¹ESTRELA, Priscila Moraes Argôlo Bonfim; AMARAL, Dino Macedo; ALBUQUERQUE, Robson de Oliveira; GIOZZA, William Ferreira; AMVAME-NZE, Georges Daniel; NERY, Alexandre Solon. <https://ppee.unb.br/wp-content/uploads/2023/01/CIACA.pdf>

BLOCO II – HIPÓTESES LEGAIS

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a

operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

De início, é importante ressaltar que o consentimento não é a única base legal aplicável ao tratamento de dados biométricos, sendo possível o seu tratamento com fundamento em outras bases legais do art. 11 da LGPD, para o atingimento de finalidades legítimas, como nos casos de garantia da prevenção às fraudes, à segurança do titular e para o cumprimento de obrigações legais e regulatórias.

No contexto do setor financeiro, é importante ponderar que o tratamento de dados biométricos se mostra indispensável para preservar a segurança dos titulares e do próprio sistema financeiro. Nas hipóteses em que o tratamento destes dados for necessário para o atendimento das finalidades de prevenção a fraudes, de garantia da segurança do titular e/ou de cumprimento de normas regulatórias, inclusive atreladas a segurança dos titulares, das instituições e do sistema financeiro, o consentimento não deve ser considerado hipótese legal adequada para o tratamento de dados biométricos, podendo ser aplicadas outras bases legais.

Importante destacar que, eventual limitação quanto à aplicação das demais bases legais, além do consentimento, poderia, inclusive, comprometer a própria segurança do titular. Por exemplo, em uma jornada dentro do aplicativo de um banco que utiliza a verificação facial por selfie como mecanismo de autenticação e proteção contra fraudes, restringir o tratamento dos dados biométricos apenas à hipótese legal do consentimento permitiria que agentes mal-intencionados simplesmente recusassem a coleta de seus dados biométricos, frustrando as medidas de segurança necessárias para a prevenção à fraude e segurança do titular. Com isso, o sistema não conseguiria distinguir entre o verdadeiro titular e um terceiro de posse de credenciais roubadas tentando acessar indevidamente a conta bancária do titular, ou mesmo abrir indevidamente uma conta e/ou contratar produtos e serviços se passando pelo titular.

Deste modo, o consentimento não deve ser considerado adequado ao tratamento de dados biométricos quando a negativa do titular em consentir criar óbice ou dificuldade ao controlador na adoção de medidas de segurança e/ou no cumprimento de obrigações legais ou regulatórias e nem quando seja possível basear nas outras hipóteses legais. Dessa forma, o consentimento deve ser entendido como base legal apropriada nos casos em que o titular possa optar pelo tratamento dos seus dados biométricos, sua solicitação não represente risco significativo aos direitos do titular, nem inviabilize o cumprimento de obrigações legais ou regulatórias, o atendimento ao interesse público ou a adequada execução de contratos.

Nesse sentido, nas situações em que o consentimento se mostrar adequado, a coleta deverá ser livre, específica, destacada, informada e inequívoca. Para garantir isto, recomenda-se seguir os seguintes parâmetros:

(i) Design de interfaces claras e acessíveis:

- a. Utilizar linguagem simples, evitando jargões técnicos.
- b. Quando o consentimento for obtido por escrito ou via tela de aplicativo/website, ele deve aparecer de forma que permita sua identificação de modo facilitado pelo titular, podendo ocorrer por diferentes formas, por exemplo, com destaque visual, em campo/tela.

A definição de rol taxativo ou opção por um único formato de obtenção do consentimento não é recomendável, considerando que os formatos podem variar conforme o meio em que o consentimento seja obtido e as necessidades do

controlador, tais como o atendimento de cláusulas padrão ou exigências regulatórias aplicáveis à sua atividade.

- (ii) **Finalidade específica e destacada;**
- (iii) **Mecanismo de revogação:** Disponibilização de canal para revogação do consentimento;
- (iv) **Registro e comprovação do consentimento:** Manter logs ou registros eletrônicos que comprovem a manifestação do titular.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Antes de se avaliar a aplicação adequada da hipótese legal de 'garantia da prevenção à fraude' no tratamento de dados biométricos, é fundamental contextualizar o cenário atual enfrentado pelo setor financeiro brasileiro e pela sociedade brasileira, marcado por um ambiente especialmente agressivo em termos de fraudes financeiras. Golpes e fraudes por canais eletrônicos se intensificaram entre 2023 e 2024. Em termos financeiros, houve um crescimento de 17% nas fraudes realizadas por canais eletrônicos e com cartões, passando de R\$ 8,6 bilhões em 2023 para R\$ 10,1 bilhões em 2024. Em contrapartida, observou-se uma redução de 14% nas fraudes documentais, que caíram de R\$ 4,2 bilhões para R\$ 3,6 bilhões no mesmo período¹. Esses dados evidenciam uma migração dos golpistas para o ambiente digital. Neste sentido, parte expressiva das ações criminosas envolve tentativas de invasão e abertura indevida de contas bancárias por meios cada vez mais sofisticados, fazendo com que as instituições financeiras precisem atualizar constantemente suas medidas e ações de segurança para proteger os titulares.

Nesse cenário, a coleta e o tratamento de dados biométricos se mostram necessários para a segurança financeira e promover o acesso seguro a soluções, produtos e serviços para dezenas de milhões de brasileiros, inclusive pela criticidade de todo o setor financeiro para o país e para sociedade.

Além disso, cumpre destacar as obrigações prudenciais e regulatórias impostas ao setor financeiro quanto à necessidade de adoção de controles relacionados à segurança. Resoluções do Banco Central e de outros reguladores do sistema financeiro, além de normativos de prevenção à lavagem de dinheiro e ao financiamento ao terrorismo exigem que as instituições adotem mecanismos técnicos e administrativos para o gerenciamento do risco desses riscos, visando à redução de fraudes, segurança e preservação da integridade e solidez do sistema financeiro. Inclusive, há situações em que o Judiciário estabelece responsabilidade objetiva de instituições financeiras quando o cliente sofre prejuízo decorrente de falha de segurança: se o controlador deixar de empregar salvaguardas compatíveis com os riscos conhecidos, responde pelos danos independentemente de culpa. A adoção de biometria, seja ela tradicional ou comportamental, como camada de defesa demonstra diligência ao mostrar que a instituição implementou a tecnologia mais eficaz disponível contra agentes cada vez mais sofisticados.

Ademais, é evidente também a aplicação dos princípios estabelecidos na LGPD, tais como necessidade, transparência, finalidade, não discriminação, segurança e adequação, além da implementação de medidas técnicas e administrativas. Nesse contexto, importante ressaltar que as instituições financeiras, de modo geral, possuem controles e processos para proteção dos dados coletados, tais como salvaguardas técnicas robustas como criptografia, segregação lógica da base biométrica, controle de acesso mais robusto às bases de dados contendo dados biométricos, detecção de vivacidade e bloqueio de *deep-fakes*, métricas de erro ou vieses etc.

Por fim, essencial destacar que os tratamentos dos dados biométricos, tradicionais ou comportamentais, englobados pela base legal prevista no art. 11, II, g, da LGPD são todos aqueles necessários para atingir a finalidade de prevenção a fraudes e segurança do titular e em relação à sua identificação e autenticação. Para que seja possível atingir essas finalidades, são necessários

diversos tratamentos dos dados biométricos, tais como a sua coleta, tratamento técnico específico biométrico, inclusão e/ou validação desses dados em bases de dados, inclusive com eventual compartilhamento com terceiros, implementação de medidas de segurança técnicas e administrativas, entre outros tratamentos. Assim toda essa cadeia de tratamentos está incluída nessa base legal, pois são necessários para a sua operacionalização. Esse ponto é de crucial importância.

¹FEBRABAN, 2025.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Inicialmente, importante ressaltar que o tratamento de dados biométricos com fundamento no cumprimento de obrigação legal ou regulatória pode se dar tanto no contexto de entidades e órgão públicos, como no setor privado, em especial aqueles regulados, tal como o setor financeiro, em que há diversas obrigações voltadas à preservação da segurança e à garantia de correta identificação e autenticação de clientes, desde o acesso ao ambiente bancário e financeiro (físico ou digital) até a efetivação de transações financeiras e contratação de produtos e serviços.

Neste sentido, não obstante a existência de outras bases legais, como a prevista no art. 11, II, g, da LGPD, a base legal de cumprimento de obrigações legais e regulatórias, especialmente no contexto do setor financeiro, é também aplicável às atividades das instituições financeiras, que podem também utilizar essa base legal quando o tratamento de dados biométricos for realizado para cumprir referidas normas e regulamentos, inclusive as que dispõem sobre segurança, não só dos usuários ou das instituições, mas de todo o sistema financeiro. Como já mencionado, existem várias normas que exigem que as instituições financeiras gerenciem riscos, inclusive de fraudes, bem como implementem medidas de segurança.

Assim como indicado na resposta ao item 5 desta tomada de subsídios, todos os tratamentos necessários para o atingimento dessas finalidades de cumprimento de obrigações legais e regulatórias devem ser considerados nela incluídos.

Em relação aos critérios e salvaguardas a serem observados pelos controladores que efetuem o tratamento de dados biométricos com base no cumprimento de obrigação legal ou regulatória, podem ser adotadas medidas técnicas de segurança para prevenir a exposição ou acesso indevido de dados, tais como controles de acesso às bases de dados e criptografia; armazenamento em módulos seguros; quando possível, segregação de outras bases de dados; prazo de retenção adequado, elaboração de Relatório de Impacto à Proteção de Dados Pessoais (“RIPD”) nas situações em que for aplicável etc., além da observância da norma e/ou regulamento aplicável e das demais obrigações e princípios da LGPD, como o da transparência e da minimização dos dados (necessidade).

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

O tratamento de dados para realização de estudos por órgãos de pesquisa deve observar os princípios da LGPD, tais como: ter uma finalidade específica; tratar os dados mínimos necessários; segregar os dados de pesquisa de outros bancos de dados, conforme aplicável; restringir o acesso; implementar controles de governança, assim como adotar a anonimização sempre que possível. Ressalta-se que pelo disposto no art. 12 da LGPD, dados anonimizados não são considerados dados pessoais para os fins da LGPD, sendo, portanto, referida legislação inaplicável em relação ao

tratamento de tais dados.

Em relação aos dados anonimizados, os limites aplicáveis passam pela adoção de medidas para evitar e/ou mitigar a reidentificação dos titulares.

Como salvaguardas adicionais recomenda-se política de eliminação de dados, monitoramento efetivo e periódico e formalização de Termo de Responsabilidade dos pesquisadores, além de aplicação de requisitos de segurança e elaboração de RIPD.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

A utilização das tecnologias de reconhecimento facial (*Facial Recognition Technologies*, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento. Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Para que o uso de tecnologias de reconhecimento facial (FRTs – *Facial Recognition Technologies*) respeite os princípios da necessidade, proporcionalidade, transparência e não discriminação, recomenda-se adotar uma abordagem integrada que combine salvaguardas técnicas, jurídicas e institucionais, sempre adaptadas ao contexto específico da operação.

Em primeiro lugar, convém demonstrar a necessidade de utilização de FRTs, o que envolve mapear e documentar o processo de avaliação e opção pela adoção de tal tecnologia (p. ex., prevenção de fraudes). Aqui, é importante ressaltar que, considerando o atual cenário brasileiro, em que técnicas de fraude e golpes se sofisticam rapidamente, o uso de FRTs é crucial para elevar significativamente o nível de segurança, protegendo os titulares de acessos indevidos e ações mal-intencionadas. Nesse sentido, o uso de FRT no setor financeiro é essencial e necessário para salvaguardar a segurança dos titulares e de todos o sistema.

Quanto à proporcionalidade, sugere-se equilibrar o benefício esperado com o impacto nos direitos

fundamentais, considerando, também, o contexto do tratamento em que as FRTs são utilizadas. Além disso, os dados tratados devem ser limitados ao necessário para atingir as finalidades pretendidas e devem considerar o contexto do tratamento.

A transparência pressupõe informar o titular de forma clara e acessível sobre o tratamento de dados biométricos e sua finalidade, além dos direitos assegurados e canais de contato, preferencialmente na política de privacidade da instituição. Em meios físicos, placas ou sinalizações visíveis podem ser adequadas, quando viável; em ambientes digitais, avisos eletrônicos e políticas de privacidade mais detalhadas são, em regra, boas práticas, sendo que o grau de detalhe pode variar conforme a complexidade do tratamento, ressaltando a necessidade de também proteger o segredo empresarial. Em cenários de alto risco, recomenda-se a elaboração ou atualização de RIPD, de acordo com as orientações definidas pela ANPD.

Para mitigar discriminação ilícita ou abusiva, recomenda-se a realização de testes e ações que visam a identificação, medição e mitigação de vieses e discriminações ilícitas ou abusivas. Métricas de acurácia devem ser monitoradas, com atualização dos modelos sempre que se identifiquem disparidades, além de medidas de acompanhamento e reporte que possibilitem identificação e remediação de eventuais discriminações indevidas.

Dessa forma, tais diretrizes se desdobram em três dimensões:

- Técnicas – alguns exemplos:
 - (i) Criptografia;
 - (ii) Pseudonimização ou anonimização, sempre que aplicável e considerando o contexto e finalidade do tratamento;
 - (iii) Mecanismos *anti-spoofing* (prova de vida, detecção de máscaras etc.).
 - (iv) Trilhas de auditoria e registros de acesso;
 - (v) Testes periódicos de segurança e de acurácia/viés.
- Jurídicas – alguns exemplos:
 - (i) Identificação da base legal apropriada para dados sensíveis (art. 11, LGPD);
 - (ii) Cláusulas contratuais adequadas com fornecedores;
 - (iii) Políticas de privacidade e canais para exercício dos direitos do titular aplicáveis.
- Institucionais – alguns exemplos:
 - (i) Adoção de princípios de *Privacy & Security by design* ao longo de todo o ciclo de vida do sistema;
 - (ii) Comitê multidisciplinar (ética, privacidade, tecnologia) e Encarregado de Dados (DPO);
 - (iii) Adoção e organização códigos/guias de ética internos e/ou códigos de conduta setorializados;
 - (iv) Programas de treinamento e conscientização;
 - (v) Auditorias internas;
 - (vi) Plano de resposta a incidentes.

Por fim, cumpre enfatizar que as salvaguardas aqui descritas devem ser compreendidas como boas práticas recomendadas, cabendo a cada controlador avaliar, à luz do seu contexto operacional, dos riscos inerentes às suas atividades e de suas capacidades orçamentárias e técnicas, quais medidas são efetivamente adequadas e proporcionais ao caso concreto. Essas diretrizes não pretendem estabelecer obrigações uniformes ou exaustivas, mas servir de referência para a construção de programas de conformidade que possam evoluir de modo gradativo e realista, evitando que se atribua às empresas o ônus de implementar salvaguardas que ultrapassem suas possibilidades atuais ou que não se justifiquem diante da finalidade e do risco envolvidos.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Os sistemas de reconhecimento facial (FRTs) devem ser projetados com base nos princípios de

privacy by design e privacy by default, incorporando, desde a fase de concepção, medidas técnicas e organizacionais voltadas à precisão, segurança e mitigação de riscos. De modo geral, os sistemas de reconhecimento facial/biométricos utilizam mecanismos automatizados, os quais viabilizam a sua implementação e trazem segurança.

Nesse sentido, algumas medidas podem ser adotadas, tais como:

- (i) **Avaliação de impacto e testes:** Ainda na fase anterior à implementação do sistema, recomenda-se a realização de avaliações de impacto, para identificar riscos relacionados ao tratamento dos dados pessoais dos titulares, riscos de falsos positivos/negativos e impactos sobre grupos vulneráveis. Como boa prática, podem ser estabelecidas métricas alvo, testes e pilotos no contexto da adoção do sistema. Simulações em ambientes controlados para medir taxas de erro e ajustar parâmetros.
- (ii) **Treinamento com bases de dados diversas e representativas:** Desde a concepção desses sistemas, se mostra recomendável, com a direção de mitigar efeitos negativos e trazer maior confiabilidade e eficácia, o emprego de conjuntos de treinamentos amplos e representativos em termos de gênero, cor/raça, idade e condições ambientais, ajustando limiares de confiança de acordo com o risco de cada aplicação. Assim, a utilização de algoritmos robustos e continuamente testados em bases de dados diversificadas é essencial para reduzir a incidência de erros de identificação, como falsos positivos e falsos negativos, buscando maior acurácia em diferentes perfis (gênero, raça, idade, por exemplo) especialmente considerando a variabilidade de características demográficas.
- (iii) **Governança, monitoramento e atualização:** É importante monitorar o desempenho do sistema de forma contínua, inclusive métricas como taxa de erro, tempo de resposta, podendo haver a supervisão humana nos processos necessários, além da avaliação e atualização dos modelos com base em novos dados e *feedbacks* operacionais. Além disso, é importante que haja canais de contato para que o titular afetado por erro de identificação possa contestar e solicitar revisão.

A governança desses sistemas, que, considerando a natureza da sua operação, também podem ser considerados como sistemas de Inteligência Artificial, enquanto inexistente regulamentação específica, podem variar de acordo com cada organização. De toda forma, uma avaliação que pode ser recomendável é a de adoção de **frameworks internacionais consolidados**, como o *NIST AI Risk Management Framework*, a série ISO/IEC e/ou IEEE. Esses padrões fornecem um vocabulário comum, uma estrutura de avaliação de risco e um roteiro de governança que controladores podem adaptar ao seu porte e ao seu setor sem ficarem presos a soluções tecnológicas específicas.

Em paralelo, sempre que tecnicamente viável e considerando o contexto e a operação de FRTs, pode ser aplicável a conversão de imagens em *templates* criptografados ou *hashes* matemáticos, bem como recursos de detecção de vivacidade (*liveness*) para prevenir ataques com fotos, vídeos ou máscaras.

Também podem ser boas práticas: o monitoramento e acompanhamento de métricas e a configuração de alertas que avaliam o desempenho e, consequentemente, a aplicação de ações de melhoria contínua na operação de FRTs; a criação de ciclos de retreinamento, e a condução de *red-teaming*, auditorias para reavaliar vulnerabilidades, outros sinais de degradação do sistema e vieses residuais.

Não menos importante, os controladores também devem adotar, em linguagem clara e acessível, medidas de transparência aos titulares quanto ao tratamento dos seus dados.

Importa reconhecer, contudo, que mesmo com todas essas salvaguardas subsistem fatores que podem impactar o desempenho dos FRTs, tais como variáveis técnicas relacionadas a qualidade dos sensores, iluminação, representação demográfica no *dataset*, entre outros aspectos. Por isso, a profundidade e o formato de aplicação das medidas devem levar em conta tais fatores, considerando que não há solução “tamanho único”.

Em síntese, as medidas devem ser avaliadas caso a caso, levando em conta capacidades técnicas e orçamentárias, riscos específicos e a evolução constante dos marcos legais, a fim de equilibrar inovação, segurança, proteção dos titulares e não frear o avanço tecnológico.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Destaca-se que o reconhecimento facial é, em geral, a medida de segurança mais forte e eficaz para o ecossistema financeiro. Nesse sentido, não identificamos situações afetas ao setor financeiro em que não seria recomendado o uso de reconhecimento facial e entendemos que não devem ser definidas situações específicas que limitem a adoção dessa tecnologia.

De modo geral, o controlador deve definir, no caso concreto e considerando o contexto do tratamento e diversos outros fatores, inclusive técnicos, para adotar a solução mais adequada ao caso concreto, seja tal solução biométrica ou por outros meios, bem como de forma combinada.

Embora seja legítimo que a ANPD reconheça os riscos inerentes ao uso de dados biométricos faciais, amplificados pela percepção europeia, é igualmente relevante perceber que, no ecossistema financeiro e de meios de pagamento e no contexto crítico que o Brasil enfrenta relacionado à golpes e ataques cada vez mais sofisticados, o reconhecimento facial tornou-se a barreira antifraude mais robusta justamente porque cruza variáveis dinâmicas (selfie viva, prova de vida, checagem em tempo real) que as alternativas não conseguem replicar com o mesmo grau de certeza. Assim, é importante preservar essa camada dada a sua importância para segurança.

Portanto, a discussão regulatória não deveria desencorajar o uso de FRTs quando o objetivo é mitigar fraudes e segurança. Em vez disso, pode focar na consolidação de salvaguardas proporcionais, e na sugestão de boas práticas de minimização. Dessa forma, protege-se o titular sem comprometer a integridade das transações financeiras nem criar incentivos involuntários para agentes mal-intencionados explorarem lacunas de segurança mais brandas.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

O tratamento de dados biométricos exige uma abordagem cautelosa e estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos.

Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes.

Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para

garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados.

Com base nisso, questiona-se:

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Em atenção ao enunciado desta pergunta, especialmente ao uso da expressão “indispensáveis”, é importante ressaltar que, com a finalidade de preservar a neutralidade tecnológica, a ANPD deve evitar o estabelecimento de um rol taxativo ou um “padrão mínimo único”, pois a eficácia de cada contramedida depende do contexto (volume e tipo de dados, criticidade do serviço, porte e maturidade da organização).

A LGPD já impõe que os agentes adotem medidas aptas (art. 46) e que comprovem sua eficácia pelo Princípio da Responsabilização e Prestação de Contas (art. 6, X). Com isso, cabe aos controladores demonstrar, via governança própria, RIPD ou processos equivalentes, que os riscos foram identificados e tratados com proporcionalidade.

Com isso, abaixo indicamos recomendações de medidas técnicas, administrativas e parâmetros de avaliação e monitoramento que podem, em um rol não taxativo, ser avaliado pelos controladores no exercício de atividades de tratamento de dados biométricos.

(i) **Recomendação de medidas técnicas:**

- a. Criptografia;
- b. Quando aplicável, o armazenamento de *templates* não reversíveis (*hash* ou vetor numérico);
- c. Detecção de vivacidade (*liveness*) e mecanismos anti-*spoofing* para fotos, vídeos, *deepfakes* ou máscaras;
- d. Segurança de infraestrutura: segmentação de rede, *firewalls* e IDS/IPS, aplicação tempestiva de *patches* e varreduras de vulnerabilidade regulares;
- e. Controle de acesso estrito e segregação de funções;
- f. *Trusted Execution Environment* (TEE) ou *secure container* para processamento local de dados sensíveis, sempre que a plataforma do usuário suportar;
- g. Plano de backup e recuperação de desastres.

(ii) **Recomendação de medidas administrativas:**

- a. Programa de segurança da informação e implementação de políticas aplicáveis, cobrindo coleta, uso, descarte de dados e resposta a incidentes;
- b. Avaliação de risco e realização de um RIPD, quando necessário, contendo o mapeamento dos dados, bases legais, medidas adotadas dentre outras informações aplicáveis;
- c. Treinamento de colaboradores e terceiros, reforçando cultura de privacidade e segurança;
- d. Auditorias, testes de penetração e exercícios de *red-teaming* para revisar controles técnicos e identificar vieses ou vulnerabilidades;
- e. Plano de resposta a incidentes com funções, SLAs e fluxo de comunicação à ANPD e aos titulares conforme o art. 48 da LGPD;
- f. Gestão de fornecedores: cláusulas contratuais que imponham padrões equivalentes de segurança.

(iii) **Parâmetros de avaliação e monitoramento sugeridos**

- a. Mapeamento de dados biométricos;
- b. Modelagem de ameaças para identificar vetores como *adversarial inputs*, *ransomware*;
- c. Estabelecimento de indicadores operacionais e de monitoramento, tais como tempo

- de detecção e resposta, tentativas de acesso bloqueadas, desvios de desempenho;
- d. Avaliação/monitoramento de logs e alertas de anomalia;
- e. Revisão periódica de políticas aplicáveis;
- f. Monitoramento de vulnerabilidades e aplicação tempestiva de correções.

Em suma, tais práticas formam um arcabouço de defesa, mas **não devem ser impostas como checklist obrigatório**. O ponto determinante é que as salvaguardas selecionadas sejam aptas, eficazes, proporcionais e revisadas de forma contínua para acompanhar a evolução das ameaças e das tecnologias.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

A biometria é uma proteção importante contra fraudes. Em ambientes onde golpes digitais são frequentes, esse fator de autenticação reforçado pode ser necessário até em serviços considerados “não essenciais”.

Exigir o dado biométrico, especialmente no contexto do sistema financeiro é legítimo e não deve ser considerado como discriminação ilícita ou abusiva. Uma vez que o uso de biometria se mostra como medida necessária para fins de prevenção a fraude e segurança, ou, ainda, para entregar a experiência desejada pelo próprio titular (por exemplo, login instantâneo, assinaturas eletrônicas rápidas ou recursos personalizados que dependem da confirmação inequívoca de identidade), de modo que a utilização de biometria pode ocorrer em substituição ou em adição a outros métodos, tais como login, senha, códigos por SMS etc. Como mencionado anteriormente, o controlador deve avaliar o caso concreto para decidir sobre as medidas adotadas, biométricas ou não.

Ademais, a transparência aos titulares, quanto ao tratamento dos seus dados biométricos e a finalidade, também se mostra essencial. Recomenda-se aos controladores que informem, na própria jornada e/ou em políticas de privacidade, os tratamentos de dados biométricos, os benefícios ao usuário (tais como a proteção) e os riscos inerentes ao seu não uso, quando possível.

Nos cenários em que a atividade de tratamento de dados for baseada no consentimento, quando entendida pelo controlador como base adequada, o Controlador deve informar ao titular se, em caso de recusa, houver impedimento para determinada ação ou acesso a algum serviço ou funcionalidade, garantindo-se o fornecimento da informação quanto à consequência da recusa ao titular.

Por fim, para que a exigência do dado biométrico seja amplamente compreendida – e, portanto, melhor aceita – também recomendamos um esforço coordenado de educação pública que vá além da atuação transparente e propositiva dos controladores. Campanhas multissetoriais, conduzidas em linguagem simples e acessível, podem explicar por que a biometria se tornou uma resposta técnica eficaz à escalada de golpes digitais, conscientizando os titulares que ela reduz fraudes de identidade, oferece autenticação mais rápida e dificulta o uso indevido de credenciais vazadas. Essas ações informativas devem partir não só do setor privado, mas também de autoridades e órgãos reguladores, a fim de criar mensagens consistentes, guias práticos e canais de esclarecimento que alcancem diferentes perfis da população. Ao demonstrar, de forma transparente, as vantagens concretas do tratamento biométrico – bem como as salvaguardas exigidas pela LGPD e normas setoriais – esse ecossistema colaborativo fortalece a confiança pública, promove inclusão digital segura e estabelece uma base comum de entendimento sobre o uso de tecnologias e medidas de segurança.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Entendemos que os controladores devem adotar salvaguardas que cubram todo o ciclo de vida do dado biométrico, tais como RIPD e medidas técnicas e de governança proporcionais e alinhadas aos princípios e diretrizes da LGPD.

Abaixo indicamos boas práticas e recomendações específicas que podem ser adotadas por controladores no tratamento dessa categoria de dados, sem prejuízo de outras medidas já indicadas em outras respostas desta Tomada de Subsídios:

- (i) **Privacy e Security by design**
 - a. Integrar requisitos de privacidade e cibersegurança desde a fase de projeto, limitando a coleta ao estritamente necessário e descrevendo a finalidade do tratamento;
- (ii) **Segurança técnica**
 - a. Criptografia;
 - b. Controle de acesso aos dados biométricos;
 - c. Adoção de medidas de detecção de vivacidade (*liveness*) e mecanismos *anti-spoofing* para barrar autenticação para barrar fotos, vídeos ou *deepfakes*;
 - d. Manter varredura de vulnerabilidades, patches de segurança atualizados e logs atualizados em tempo real;
- (iii) **Governança, políticas e pessoas**
 - a. Adoção e estabelecimento de políticas e procedimentos internos, com papéis claros;
 - b. Auditorias e monitoramento de tratamento de atividades de tratamento de dados biométricos dentro da organização por equipes de Privacidade e, também, pelas próprias áreas responsáveis pela operação da funcionalidade de autenticação;
 - c. Treinamento de colaboradores e ações de conscientização sobre proteção de dados;
 - d. Participação e implementação de comitês multidisciplinares, quando aplicável;
- (iv) **Transparência ativa**
 - a. Apresentar ao titular, em linguagem clara e simples, se há tratamento e a finalidade da coleta dos dados biométricos e outras informações relevantes, como o compartilhamento desses dados com terceiros e os direitos aplicáveis;
 - b. Exclusivamente quando se aplicar unicamente a base legal do consentimento, os controladores devem obter a autorização destacada, específica e revogável dos titulares;
- (v) **Prevenção de vieses e discriminação**
 - a. Uso de bases de treinamento diversificadas em gênero, raça/cor, idade e outros parâmetros aplicáveis;
 - b. Documentação de resultados, RIPD e mecanismos de identificação e correção de eventuais disparidades e incidentes identificados;
 - c. Condução de ações de *red-teaming*;
- (vi) **Resposta a incidentes e accountability**
 - a. Planos de resposta a incidentes e erros no processo de autenticação, seguindo as determinações legais e boas práticas;
 - b. Registro das atividades de tratamento de dados que realizam uso de dados biométricos e documentação de medidas, políticas e procedimentos realizados que visam a proteção e uso regular e legítimo de dados biométricos.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

Abaixo estão as principais medidas de equilíbrio que podem ser apontadas:

- (i) **Avaliação de risco:** Elaborar um RIPD específico para cada projeto de monitoramento massivo, demonstrando necessidade, proporcionalidade e medidas que visam combater a discriminação ilícita e o viés;

- (ii) **Transparência:** Sinalização física nos locais monitorados, com linguagem simples. Dessa forma, os titulares teriam transparência e informações sobre o tratamento dos seus dados biométricos. Paralelamente, também seria positivo a realização de campanhas educativas para explicar por que a biometria é usada, como os dados são protegidos e quais são os direitos do cidadão;
- (iii) **Controles técnicos:** Adoção de medidas técnicas que promovem maior segurança no tratamento de dados biométricos, como por exemplo armazenamento seguro das imagens e *hashs* biométricos, criptografia, sistemas *anti-spoofing*, segmentação de rede e controle de acesso;
- (iv) **Mecanismos de direitos e supervisão:** Disponibilização de meios públicos e gratuitos para que a população possa solicitar informações e exercer os direitos previstos na LGPD. Também seria recomendável a supervisão humana nos processos necessários, dentro do contexto de tratamento e da tomada de decisões de ações coercitivas;
- (v) **Vedação de abusos e discriminação ilícita:** Antes de colocar o sistema em produção completa, recomenda-se a submissão do projeto a pilotos e testes para acurácia e equidade. Ademais, também se mostra recomendável que os controladores mantenham métricas operacionais (falsos positivos, falsos negativos e taxa de match). Estabelecer procedimentos para recalibrar o modelo quando necessário.

No mais, é importante ressaltar que o uso de dados biométricos e FRTs em espaços acessíveis ao público já vem mostrando resultados concretos quando o objetivo é segurança pública ou proteção de pessoas. Alguns exemplos internacionais podem ser indicados:

- A cidade de Londres prendeu mais de 540 foragidos entre 2020 e 2024 com operações pontuais de *Live Facial Recognition*¹;
- Johannesburg registra de 10 a 15 prisões diárias graças à rede *Vumacam*²;
- Singapura mantém baixos índices de crime ao integrar FRTs ao programa Safe City³.

No Brasil, a ferramenta também vem sendo utilizada.

Ao mesmo tempo, o quadro crítico da segurança, especialmente em grandes centros brasileiros exige soluções eficazes – inclusive parcerias entre a iniciativa privada e o Poder Público – mas com salvaguardas que preservem a privacidade e mitiguem riscos de usos abusivos e ilegítimos.

O reconhecimento facial em ambientes públicos pode ser importante para a proteção da segurança pública. O desafio não está em proibir a tecnologia, mas em governá-la com rigidez e proporcionalidade: base legal adequada, transparência, arquitetura com minimização de dados, auditorias de viés e canais efetivos para o exercício de direitos dos titulares, buscando a segurança, mas sem abrir mão do direito fundamental à privacidade e à não discriminação.

¹ *Metropolitan Police Makes Over 500 Arrests Using Live Facial Recognition Technology, UKNIP* – 07/12/2024. Disponível em: https://uknip.co.uk/news/uk/breaking/metropolitan-police-makes-over-500-arrests-using-live-facial-recognition-technology/?utm_source=chatgpt.com#google_vignette

² *'Gatvol' Lesufi teams with Vumacam's CCTV network to fight crime in Gauteng, News24* – 13/02/2024. Disponível em: https://www.news24.com/business/companies/gatvol-lesufi-teams-with-vumacams-cctv-network-to-fight-crime-in-gauteng-20240213?utm_source=chatgpt.com

³ *Taking stock of physical crime cases in 2024 and how the Police continue to safeguard every day!, Police GOV Singapore Police Force*. Disponível em: <https://www.police.gov.sg/Media-Room/Police-Life/2025/02/Four-Things-You-Should-Know-About-the-Annual-Crime-Brief-2024>

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos

desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Primeiramente, é importante ressaltar que o direito à informação clara, o direito de acesso e à correção dos dados são direitos dos titulares que pressupõem todo e qualquer tratamento, independentemente de o referido tratamento estar ou não relacionado à dados biométricos e/ou inserido no contexto de uma decisão tomada exclusivamente em tratamento automatizado de dados pessoais.

Nesse sentido, medidas de transparência, tais quais previsões claras em políticas de privacidade, pontos de coleta (quando aplicável), e divulgação de canais de atendimento são relevantes para que titular possa exercer seus direitos.

No que diz respeito à possibilidade de revogação, entendemos ser aplicável nos casos em que a base legal para o tratamento dos dados for unicamente o consentimento, o titular deve ter ciência das consequências dessa revogação e das eventuais limitações aplicáveis. Para isso, é necessário dispor de um canal de fácil acesso, viabilizando a revogação de forma simples, acessível e facilitada.

Por sua vez, conforme disposto na LGPD, o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. Dessa forma, enquanto requisito para a garantia e a aplicação do referido direito, é certo que a leitura do dispositivo deve considerar que a revisão ocorra apenas nos casos em que a decisão foi tomada unicamente de forma automatizada, bem como que os interesses dos titulares tenham sido afetados de forma ilícita ou abusiva e contrária à legislação.

Nesse sentido, importante destacar que a leitura e interpretação de referente direito do titular deve observar os requisitos dispostos no artigo 20 da LGPD, quais sejam: (i) decisão tomada unicamente com base em tratamento automatizado de dados pessoais; e (ii) decisão que afete os interesses do titular. Com efeito, esses requisitos devem ser observados em qualquer decisão automatizada, seja ela referente ao tratamento de dados biométricos ou qualquer outro tipo de dado.

Cumprido destacar que, no que tange ao conceito de decisão tomada unicamente com base em tratamento automatizado de dados pessoais, considera-se um processo de tomada de decisão que é totalmente automatizado e exclui qualquer influência humana no resultado.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

Para o tratamento de dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, se mostra essencial a aplicação do princípio do melhor interesse, avaliando não apenas a legitimidade do tratamento dos dados, mas também os benefícios

ao menor.

Neste sentido, o tratamento de dados biométricos de menores pode ser indispensável em situações que visem a segurança, prevenção a fraudes e autenticação do menor, podendo ser considerado, por si só, realizado no melhor interesse do menor.

A participação informada dos pais e/ou responsáveis, através da transparência por meio políticas de privacidade e de aviso claro e destacado, utilizando-se de linguagem simples e sinalização local, pode ser recomendável.

Ademais, os controladores podem avaliar, por exemplo, a necessidade da coleta de determinados dados, a adoção de medidas técnicas e administrativas que possam mitigar riscos de segurança, monitoramento de acurácia e outras métricas quanto ao funcionamento do sistema de reconhecimento facial para mitigação de erros, imprecisões e discriminação ilícita, por exemplo.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

O tratamento de dados biométricos de crianças e adolescentes é admissível quando, caso a caso, atende ao princípio do melhor interesse (art. 14 da LGPD) e quando se enquadra em algumas das hipóteses legais previstas no art. 11, da LGPD. Inclusive, como já de conhecimento geral, a própria ANPD, mediante o Enunciado CD/ANPD nº 1, de 22 de maio de 2023, estabeleceu esse entendimento, não limitando a coleta e o tratamento de dados de menores de idade ao consentimento específico.

Neste sentido, para o tratamento de dados biométricos, além do consentimento, vislumbra-se como principais bases legais que possibilitam o tratamento: a garantia da prevenção à fraude e à segurança do titular (art. 11, II, “g”, LGPD); cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, II, “a”, LGPD); e exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (art. 11, II, “d”, LGPD) e demais hipóteses previstas no art. 11, II, da LGPD.

De toda forma, principalmente para crianças, a participação informada dos responsáveis pode ser exercida mediante aviso em linguagem simples em política de privacidade explicando o dado coletado e a finalidade do tratamento, bem como a indicação de canais para dúvidas e suporte junto ao Encarregado de Proteção de Dados.

Para evitar abusos, vazamentos ou acessos indevidos, o controlador deve adotar medidas técnicas e organizacionais eficazes e aplicáveis ao contexto da atividade de tratamento de dados, independentemente do titular figurar como criança ou adolescente, como por exemplo a coleta mínima (criação e manutenção do *hash* da imagem, quando aplicável), criptografia, segregação da base, controle de acesso restrito, detecção de *spoofing* e vivacidade, dentre outras medidas que se demonstrem aplicáveis. A aplicação de tais medidas deve avaliar o contexto da atividade de tratamento de dados e a capacidade do agente na sua implementação.

Ademais, quando aplicável, também se mostra recomendável a confecção de um RIPD, para avaliação e documentação dos riscos atrelados à atividade de tratamento, a proporcionalidade e necessidade do uso dos dados para a finalidade almejada e as ações/medidas adotadas na mitigação desses riscos.

18. Em casos de verificação ou estimativa de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Para compatibilizar a prática de verificação ou estimativa de idade em plataformas digitais e jogos, o controlador deve, antes de tudo, limitar a coleta ao mínimo necessário para atingir a finalidade pretendida, evitando excessos ou tratamentos desproporcionais. Este tipo de tratamento deve priorizar a proteção do menor, evitar riscos à sua dignidade, liberdade e segurança, de forma a se garantir o melhor interesse do menor.

Tecnicamente, podem ser medidas recomendáveis a detecção de vivacidade para evitar *deepfakes*,

criptografia e logs, anonimização, testes periódicos de acurácia e viés demográfico, além de canal para exercício dos direitos do titular.

Além disso, é fundamental garantir a transparência do processo, com informações claras e acessíveis aos pais ou responsáveis, incluindo a finalidade da coleta, os direitos dos titulares e os mecanismos disponíveis para exercer esses direitos, garantindo-se assim, a participação informada dos responsáveis.

ED-0018 - Manifestação Febraban e Abecs - Dados Biométricos pdf
Código do documento 508b665a-f663-4488-968c-d88934242394



Assinaturas



ROBERTA GASPAR BUSO

Assinou

RGB



Luis Vicente Magni De Chiara

Assinou

Lucas C.



Marelo Takeyama

Assinou

Marelo Takeyama

Eventos do documento

01 Aug 2025, 15:42:44

Documento 508b665a-f663-4488-968c-d88934242394 **criado** por PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b). - DATE_ATOM: 2025-08-01T15:42:44-03:00

01 Aug 2025, 15:47:12

Assinaturas **iniciadas** por PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b). - DATE_ATOM: 2025-08-01T15:47:12-03:00

01 Aug 2025, 15:48:35

ROBERTA GASPAR BUSO **Assinou** (5ddc9e9a-9c5d-493b-92ca-05a9e2f52f9c) - IP: 18.231.121.116 (ec2-18-231-121-116.sa-east-1.compute.amazonaws.com porta: 8104) - Documento de identificação informado: 306.633.378-79 - DATE_ATOM: 2025-08-01T15:48:35-03:00

01 Aug 2025, 15:52:35

LUIS VICENTE MAGNI DE CHIARA **Assinou** - IP: 18.231.174.19 (ec2-18-231-174-19.sa-east-1.compute.amazonaws.com porta: 29964) - Documento de identificação informado: 293.346.478-09 - DATE_ATOM: 2025-08-01T15:52:35-03:00

01 Aug 2025, 16:46:32

MARELO TAKEYAMA **Assinou** - IP: 186.204.63.68 (bacc3f44.virtua.com.br porta: 41432) - Documento de identificação informado: 255.964.638-25 - DATE_ATOM: 2025-08-01T16:46:32-03:00

Hash do documento original

(SHA256):a3c80bc70dcd07cd9a72a46358b839244ddcd30e4dfa5e45361502927e9c72e8

(SHA512):0c86fa6f76d910b1eaf736bbf03565753ddab032f4e404ad27a91db542f80f02effff46647aa996d5422b0269f1005e1d89ac3a7d932911385e475e9869505c6

Esse log pertence **única e exclusivamente** aos documentos de HASH acima



Esse documento está assinado e certificado pela D4Sign

Integridade certificada no padrão ICP-BRASIL

Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.

Nas linhas abaixo se encontram Relatório complementar atinente as respostas aos quesitos elaborados em sede da Tomada de Subsídios sobre Dados Biométricos¹, encaminhando em nome da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP).

- Resposta aos Quesitos

BLOCO I - DEFINIÇÕES E PRINCÍPIO

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Com base no entendimento da Autoridade de Proteção de Dados do México (INAI) [1], do Comitê Europeu para a Proteção de Dados (*European Data Protection Board* – EDPB) [2] e do art. 16 ter da Lei de Proteção de Dados Chilena [3], consideram-se dados biométricos aqueles que, cumulativamente, atenda aos seguintes requisitos:

- (a) estejam relacionados a características físicas, fisiológicas, comportamentais ou traços de personalidade de um titular de dados; e
- (b) resultem de um tratamento específico (em regra, uma forma de medição), cuja finalidade seja identificar, de maneira única, o titular.

Dessa forma, imagens captadas em vídeo, fotografias, gravações de voz ou dados semelhantes não devem ser, em si mesmos, considerados dados biométricos. Apenas é dado biométrico o resultado do tratamento desses dados com o objetivo de identificar unicamente o indivíduo retratado e sejam armazenados dessa forma (em igual sentido segue a Consideranda 51 do Regulamento Geral de Proteção de Dados da Europa – GDPR). Nesse sentido, destaca o EDPB:

“The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual” [2].

Nesse sentido, como a própria ANPD menciona o Regulamento Europeu (GDPR) – que sabidamente inspirou a redação da LGPD, é enfático ao pontuar, em seu art. 9º, que os dados associados a biometria do indivíduo (cf. definidos no art. 4º da GDPR) apenas são considerados categoria especial de dado (isto é, dados pessoais sensíveis) **somente quando se destinam à identificação de um indivíduo específico**. Em outras palavras, dados sobre a fisionomia ou outras características biológicas de alguém somente possuem caráter especial quando usados para identificação desta pessoa no mundo real. Entendemos recomendável que o Brasil adote semelhante abordagem, de modo que apenas sejam abrangidos pelo conceito dados concretamente utilizados para identificar alguém de forma exclusiva – não abarcando, portanto, apenas aqueles que tenham o mero potencial de fazê-lo.

Para evitar dúvidas imaginemos o seguinte cenário: instituição Financeira, utiliza sistema de reconhecimento facial para validar a identidade de seus clientes, no qual pontos de biometria (características únicas do indivíduo, como distância entre os olhos e formato do maxilar [4]) são

¹ <https://www.gov.br/participamaibrasil/ts-dados-biometricos>. Acesso em 09.06.2025

extraídos do documento de identidade do cliente e comparados com pontos extraídos de uma fotografia (*selfie*) tirada na hora pelo titular. Nesse exemplo, os dados biométricos não são as fotografias (do documento de identidade ou da *selfie*), mas os pontos biométricos dela extraídos e utilizados para identificação única do titular. Assim, caso, por exemplo, em um incidente de segurança, seja exposta apenas a foto do titular, não terá sido exposto dado biométrico do titular, mas apenas a sua fotografia, que é dado pessoal.

[1] Disponível em: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf.

Acesso em 09.06.2025

[2] Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf. Acesso em 09.06.2025

[3] Disponível em: <https://www.diariooficial.interior.gob.cl/publicaciones/2024/12/13/44023/01/2583630.pdf>. Acesso em 09.06.2025

[4] Disponível em: <https://blog.zapsign.com.br/en/reconhecimento-facial/>. Acesso em 09.06.2025

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Não são todas as categorias de dados sobre o corpo de determinado indivíduo que permitem a sua identificação. Além disso, não é porque determinada categoria de dados sobre o corpo permite ou pode ser usado potencialmente para identificar um indivíduo que o uso efetivo do dado é feito com essa finalidade. Seguindo o mencionado no item anterior, deve-se reiterar que o que realmente importa para determinar se dados relacionados a características biológicas de um indivíduo são dados biométricos é se eles são efetivamente utilizados com o propósito de identificar de forma inequívoca o titular de dados.

Conforme a Autoridade de Dados do Reino Unido (ICO), não existe metodologia única aplicável a todos os casos sobre como a transparência pode ser garantida, incluindo medidas ativas a serem adotadas pelos controladores. A forma mais eficiente de ser transparente ao titular quanto ao uso de seus dados biométricos deverá ponderar fatores, como: i) o caso de uso; ii) a natureza de relacionamento com o titular; e iii) os dados envolvidos na atividade de tratamento [1].

Nesse sentido, quanto mais óbvia a atividade de tratamento em análise, considerando as práticas habituais de mercado e a natureza do relacionamento com o titular, menor a exigência de práticas ativas de transparência. Exemplificamos:

(a) Imaginemos que uma empresa utilize câmeras instaladas em via pública para realizar a identificação biométrica de indivíduos. Nessa hipótese, em que não há expectativa razoável do titular quanto à coleta de seus dados biométricos e nem relacionamento prévio entre os

titulares e a empresa, é legítimo que a controladora tenha esforço adicional no cumprimento do dever de transparência, o qual pode ser concretizado, por exemplo, mediante a instalação de placas em local de fácil visualização, antes da entrada na área monitorada, contendo informações gerais sobre a atividade de tratamento, bem como os meios para acesso a informações mais detalhadas e para o exercício dos direitos dos titulares – em cenário assemelhado, esta ANPD entendeu que referidas medidas foram suficientes, vide Nota Técnica nº 29/2024/FIS/CGF/ANPD, §6.1.4 [2].

(b) Situação distinta é aquela em que o tratamento de dados pessoais ocorre no contexto da validação da identidade do titular, durante a contratação ou utilização de produto ou serviço – por exemplo, a verificação biométrica no processo de abertura de conta bancária ou contratação de empréstimo. Trata-se de prática consolidada no mercado, em que a coleta de dados biométricos é clara e previsível para o titular. Nesses casos, entende-se que o fornecimento do Aviso de Privacidade ao longo da jornada do usuário – ou, no caso de atendimento presencial, por meio de QR Codes disponibilizados em telas, cartazes ou materiais similares dentro do local físico, ou informações prestadas oralmente a respeito da atividade de tratamento e sua finalidade – é suficiente para assegurar o dever de transparência.

[1] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>. Acesso em 09.06.2025

[2] Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-29_2024.pdf. Acesso em 09.06.2025

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

É essencial avaliar cuidadosamente se e quando os dados comportamentais devem ser qualificados como dados biométricos, porque características comportamentais nem sempre apresentam a estabilidade ou a exclusividade necessária para identificação confiável. O escopo da definição deve ser **limitado** àqueles casos em que o tratamento possui o propósito de identificar alguém de forma exclusiva, de modo a evitar a captura de ampla gama de dados não identificadores.

Dito isso, destacamos que mesmo nessas hipóteses – isto é, quando dados comportamentais configuram dados biométricos, não existem obrigações legais específicas que distinguem as diferentes modalidades de biometria facial, não podendo eventual regulamentação sobre a legislação criar uma obrigação distinta, onde a legislação não a traz, o que implicaria em violação do princípio da legalidade.

Nesse sentido, apesar de tanto a INAI [1][2] quanto o ICO [3] diferenciarem dados biométricos físicos e fisiológicos daqueles comportamentais, nenhuma das autoridades traz obrigações específicas aplicáveis de forma diversa.

[1] Disponível em: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf.

Acesso em 09.06.2025

[2] Disponível em: <https://home.inai.org.mx/wp-content/uploads/GuiaBiometricos-Dic2024.pdf>. Acesso em 09.06.2025

[3] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/>. Acesso em 09.06.2025

BLOCO II - HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Em relação aos requisitos de validade, entendemos que os seguintes cuidados devem ser adotados:

a) Livre: o titular deve ter efetiva opção em não consentir. Isso significa, com base no Guia do ICO[1], que: i) os titulares devem ser aptos a negar ou revogar o consentimento sem nenhum prejuízo, ressalvadas, com base no guia do EDPB [2], aquelas hipóteses em que o tratamento de dados biométricos for essencial para que o titular não sofra esse prejuízo e o consentimento seja a única base legal aplicável; e ii) existam soluções alternativas ofertadas aos titulares que lhes permitam acessar produtos/serviços/benefícios sem o tratamento da biometria facial, ressalvada, nos mesmos termos, as hipóteses em que os produtos/serviços/benefícios em si mesmos dependam da biometria facial para atingir sua finalidade. Além disso, o consentimento deve ser específico e para finalidade única, não havendo vício de vontade (coação, erro ou fraude). Para fins de esclarecimento, em acordo com o guia do EDPB, a presença de incentivos aos titulares de dados não compromete o consentimento livre.

b) Informado: conforme o Guia da ANPD sobre *cookies* [3], para ser válido, o consentimento requer o fornecimento de informações completas e adequadas ao titular, permitindo a ele tomar decisão consciente, sendo certo que o conjunto mínimo de informações necessárias consta do art. 9º, da LGPD. Com base no Guia do EDPB [2] e na NBR ISO/IEC 29184 [4], a forma de apresentação dessas informações pode se operar em dois modelos principais, que são perfeitamente aplicáveis ao consentimento para dados biométricos:

- Termo de consentimento, que deverá ser avaliado pelo Titular, mais adequado para a coleta de consentimento por meios físicos, embora seja possível o seu uso em meio digital – por exemplo, apresentando um termo de consentimento em tela para leitura do titular.
- O fornecimento de informações em camadas, método adequado para ambientes digitais. Nesse modelo a prestação de informações é dividida, em regra, em duas camadas: na primeira, em que o titular de dados efetivamente manifesta seu consentimento (por exemplo, ao marcar um *checkbox*), são apresentadas as informações mais relevantes e impactantes, como a finalidade do tratamento e a existência de dados biométricos. Nessa

mesma camada deve ser disponibilizado meio de acesso à segunda camada informacional – como botão “saiba mais”. Na segunda camada é fornecida ao titular a íntegra das informações requeridas no art. 9º, da LGPD, em regra por meio da disponibilização do Aviso de Privacidade ou de um Termo de Consentimento.

(c) Inequívoco: não pode haver dúvida quanto à manifestação de vontade do titular. O consentimento, portanto, não pode ser presumido por omissão, conforme citado guia da ANPD[3].

(d) Específico: conforme o EDPB [2], existindo a possibilidade de uso do dado biométrico para mais de uma finalidade, caso cada uma dessas finalidades dependa do consentimento, ele deve ser obtido de forma individual para cada uma delas. Apesar da necessidade de o consentimento ser para finalidades delimitadas, sua coleta é desnecessária para finalidades diversas, quando o tratamento de dados pessoais para as finalidades adicionais se fundamenta em outra base legal. Por exemplo: se uma organização coleta dados biométricos de voz com base no consentimento para fins de detecção de emoções e personalização da experiência, poderá utilizar esses mesmos dados, sem novo consentimento, em atividades de prevenção a fraudes, desde que essas estejam amparadas na hipótese legal do art. 11, II, “g”, da LGPD.

(e) Destacado: pensando em experiência mais fluida para o usuário e em otimização de fluxos, o consentimento pode ser coletado de forma conjunta para dados pessoais e sensíveis, especialmente quando a finalidade não puder ser atingida sem o tratamento de ambos os tipos de dados, havendo destaque específico no texto quanto ao tratamento dos dados sensíveis.

O consentimento não será a base legal adequada nas situações em que os requisitos de validade não podem ser satisfeitos, tipicamente isso transcorrerá em duas situações:

- Quando não for viável oferecer alternativa à biometria facial ao titular de dados, sempre que permitido por exigências de segurança. Por exemplo, em processos de prevenção a fraudes, nos quais eventual opção poderia facilitar a atuação de fraudadores.
- Quando inexistir relação direta entre o Controlador e o Titular – hipótese, por exemplo, do monitoramento de espaço público, em que a coleta de consentimento é impossível.

[1] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>. Acesso em 09.06.2025

[2] Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em 09.06.2025

[3] Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>. Acesso em 09.06.2025

[4] Disponível em: <https://www.normas.com.br>. Acesso em 09.06.2025

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do

tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A hipótese legal de “garantia da prevenção à fraude” deve ser interpretada de forma abrangente, de modo a incluir o uso de dados biométricos de qualquer forma que proteja, previna ou permita a investigação de possíveis ameaças de fraude, à integridade, segurança, assédio e outras ações ilegais que envolvam práticas de potencial roubo de identidade ou assemelhadas que demandem a autenticação da identidade do indivíduo. Por exemplo, essa base legal deve abranger o uso de dados biométricos para ajudar a restaurar o acesso dos usuários a contas invadidas, para detectar o uso indevido da imagem de figuras públicas ou a geração de *deep fakes* de figuras públicas, para investigar possíveis falsificações de identidade e muito mais.

Conforme Guia sobre o Legítimo Interesse da ANPD [1], os requisitos para o enquadramento do tratamento de dados biométricos na base legal de “prevenção à fraude” são semelhantes aos aplicáveis ao legítimo interesse. Nesse sentido, são aplicáveis os mesmos critérios do Teste de Balanceamento para enquadramento no “legítimo interesse”, ressalvada a proibição de tratamento de dados pessoais sensíveis.

Isso não implica dizer que a realização prévia de Teste de Balanceamento seja medida obrigatória para garantir a licitude da atividade, pois inexistente obrigação legal nesse sentido. Nesse sentido destacamos a posição do ICO [2]:

“There is no obligation in the UK GDPR to do an LIA, but it is best practice to conduct one and it is difficult to meet your obligations under the accountability principle without it.

The LIA encourages you to ask yourself the right questions about your processing and objectively consider what the reasonable expectations of the individuals are and any impact of the processing on them.

Conducting an LIA helps you ensure that your processing is lawful. It helps you to think clearly and sensibly about your processing and the impact it could have on the individual.

Recording your LIA also helps you demonstrate compliance with the principles and appropriate organisational measures in line with your accountability obligations under Articles 5(2) and 24”.

Assim, o Teste de Balanceamento auxilia a organização a demonstrar o enquadramento na base legal, mas sua ausência, por si só, não implica em ilicitude da atividade de tratamento – o que requererá demonstração concreta de que os requisitos mínimos não foram satisfeitos.

Ao tratar do princípio da necessidade, o ICO esclarece que ele não se traduz em absoluta essencialidade, mas no fato de que a atividade de tratamento seja “uma forma direcionada e proporcional de alcançar o objetivo” (*“targeted and proportionate way of achieving your*

purpose)” – isto é, a finalidade do tratamento. Essa foi, também, a condição apontada pelo ICO para o tratamento de dados biométricos para a “prevenção ou detecção de atos ilícitos” [4].

Assim, por exemplo, no caso de soluções bancárias, considerando as rotinas habituais do mercado, o uso de biometria é, em regra, possível com base no art. 11, II, g, tendo em vista o bem jurídico protegido contra fraudes (a vida financeira do titular) e o impacto significativo que pode decorrer para o titular, caso agentes maliciosos acessem serviços financeiros em seu nome. De todo modo, esses riscos podem ser endereçados por salvaguardas, como a pseudonimização.

Em relação às salvaguardas a serem implementadas, recomendamos atenção especial às medidas de segurança apontadas pelo ICO [5], pelo INAI [6] e pela Autoridade de Dados da Coreia do Sul [7], as quais sintetizamos em duas categorias:

(a) Medidas mais relevantes:

- Controles de acesso aos dados biométricos;
- Realização de testes de penetração;
- Implementação de política de segurança da informação;
- Criptografia dos dados pessoais, tanto em trânsito quanto em repouso;
- Realização de varredura (*scan*) de vulnerabilidades nos sistemas que tratam dados biométricos, com adoção de medidas corretivas;
- Registro, em logs, de todos os acessos aos dados biométricos;
- Armazenamento de dados biométricos de forma segregada de outras informações; e
- Quando houver contratação de fornecedor, realização de processo adequado de *due dilligence*.

(b) Medidas adicionais:

- Restringir o armazenamento de dados biométricos ao *template* com minúcias das impressões digitais, evitando a guarda da representação completa da impressão; e
- Avaliar a adoção de controles previstos em normas reconhecidas internacionalmente, como a ISO/IEC 24745:2022.

Além do mais, como forma de garantir o respeito aos princípios da necessidade e minimização de dados, podem ser apropriadas, na medida em que se façam possíveis para a finalidade a que se destinam, outras medidas de pseudonimização (isto é, além da criptografia) e, quando possível, anonimização.

[1] Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em 09.06.2025

[2] Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/#why_LIA. Acesso em 09.06.2025

[3] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/>. Acesso em 09.06.2025

[4] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>. Acesso em 09.06.2025

[5] Disponível em <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>. Acesso em 09.06.2025

[6]

Disponível em: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf. Acesso em 09.06.2025

[7] Disponível em: <https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do#none>. Acesso em 09.06.2025

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Em relação às salvaguardas a serem adotadas para mitigação de riscos, entendemos que devem ser as mesmas aplicáveis aos agentes de tratamento que utilizam a base legal de “prevenção à fraude”, conforme descrito no quesito nº 5, sempre que possível no caso concreto. Isso porque as medidas de proteção de dados devem ser proporcionais aos riscos envolvidos, independentemente da base legal utilizada para justificar o tratamento. Assim, os controles e as salvaguardas adequados para mitigar os riscos decorrentes do uso de dados biométricos permanecem os mesmos, seja a base legal “prevenção à fraude”, “cumprimento de obrigação legal” ou outra prevista na LGPD.

Nessa linha segue o ICO [1], que não traz distinção às medidas de segurança recomendadas entre as diferentes bases legais para o tratamento de dados biométricos.

Quanto aos critérios para o enquadramento do tratamento de dados biométricos na base legal do art. 11, II, “a”, da LGPD, entendemos que este não deve ser limitado às raras hipóteses em que a regulação expressamente comanda o tratamento de dados biométricos, devendo abranger também aquelas situações em que o tratamento de dados biométricos é meio razoável de se conformar com as normas legais. Por exemplo, por força da Circular BCB nº 3.978/2020, as instituições financeiras devem possuir processos que permitam verificar e validar a identidade dos clientes:

Art. 16. As instituições referidas no art. 1º devem adotar procedimentos de identificação que permitam verificar e validar a identidade do cliente.

§ 1º Os procedimentos referidos no caput devem incluir a obtenção, a verificação e a validação da autenticidade de informações de identificação do cliente, inclusive, se necessário, mediante confrontação dessas informações com as disponíveis em bancos de dados de caráter público e privado.

Não seria razoável arguir que a utilização de dados biométricos para atender, com base nos riscos concretos da Instituição Financeira, esse dever de validação da identidade não seja enquadrável com o cumprimento da referida obrigação legal. Entendimento nesse sentido violaria a *ratio* da existência da base legal em análise, que é garantir a harmonização do sistema jurídico, permitindo aos agentes de tratamento segurança ao executar atividades de tratamento razoavelmente necessárias ao atendimento de obrigações legais.

Por fim, em relação às atividades de tratamento executadas pelo Poder Público, para garantir a observância dos direitos dos titulares de dados, especialmente nas situações em que não existe relacionamento direto entre o titular e o poder público, é necessária a implementação de medidas de transparência, de modo que o titular possa conhecer a existência da atividade de tratamento e exercer seus direitos.

[1] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>. Acesso em 09.06.2025

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

A anonimização não é requisito para a realização de estudos por órgãos de pesquisa, conforme posição desta ANPD, em seu guia para tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas:

“Em conjunto, esses dispositivos legais indicam que a anonimização ou a pseudonimização de dados pessoais não foram instituídas pela LGPD como medidas de segurança impositivas, isto é, que devem ser adotadas em todo e qualquer caso de estudos e pesquisas.

Da mesma forma, a LGPD não estabeleceu a anonimização ou a pseudonimização como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais para fins de realização de estudos e pesquisas, devendo-se reconhecer, inclusive, que, em alguns casos, a identificação dos titulares pode ser imprescindível para os objetivos da pesquisa.

A leitura mais adequada – e que decorre, em especial, do uso da expressão “sempre que possível” tanto nos arts. 7º e 11 quanto nos arts. 13 e 16 – é a de que a LGPD optou por um modelo mais flexível, que busca equilibrar a proteção de dados pessoais com as peculiaridades e os propósitos de realização dos mais diversos estudos e pesquisas”[1].

Deste modo, o termo “necessária” empregado no questionamento não é aplicável, pois não sendo a anonimização mandatória, não é obrigatória a adoção de medidas adicionais em razão do risco de reidentificação.

Nesse sentido, o que deve ser avaliado não é a existência do risco de reidentificação afinal, a própria ANPD já reconheceu, em seu Estudo Preliminar sobre Anonimização [2], que tal risco está sempre presente – , mas o grau desse risco e as medidas técnicas e organizacionais adotadas para reduzi-lo a nível aceitável.

As medidas a serem adotadas devem, portanto, ser proporcionais ao risco concreto de reidentificação. Ainda assim, é recomendável que incluam salvaguardas que minimizem os potenciais danos ao titular em caso de violação ou tentativa de reidentificação. Nesse sentido, conforme bem destaca o ICO [3], é fundamental a adoção de mecanismos que assegurem a irreversibilidade e a não vinculabilidade (*unlinkability*) dos *templates* biométricos – ou seja, que dificultem a engenharia reversa para *obtenção* de informações sobre a aparência do indivíduo e impeçam que tais dados sejam facilmente associados à pessoa a quem se referem ou reutilizados em diferentes sistemas ou bases de dados.

[1] Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>. Acesso em 10.06.2025

[2] Disponível em: <https://www.gov.br/participamaisbrasil/blob/baixar/37060>. Acesso em 10.06.2025

[3] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>. Acesso em 10.06.2025

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

O questionamento apresentado busca resposta para três quesitos: (a) como garantir a transparência no uso de reconhecimento facial; (b) como garantir a sua necessidade e proporcionalidade; e (c) como evitar a discriminação.

Em relação aos quesitos de transparência, aplicam-se as considerações já apresentadas no quesito nº 2: as medidas de privacidade devem ser definidas conforme análise contextual,

levando em conta diversos fatores, especialmente o caso de uso, a natureza do relacionamento com o titular e as características da atividade de tratamento [1]. De modo geral, quanto mais evidente for a atividade de tratamento para o titular, menor será a exigência de práticas adicionais de transparência ativa.

Assim, se, por exemplo, uma empresa de vigilância utiliza câmeras instaladas em via pública para realizar a identificação biométrica de indivíduos, é necessário que sejam adotadas medidas ativas de transparência – como a instalação de placas ou sinalizações visuais em local de fácil visualização, antes da entrada na área monitorada, contendo informações gerais sobre a atividade de tratamento, bem como os meios para acesso a informações mais detalhadas e para o exercício dos direitos dos titulares. Por outro lado, quando o tratamento de dados biométricos é prática consolidada e conhecida no mercado, como no contexto da validação da identidade do titular durante a contratação ou utilização de um produto ou serviço, o fornecimento do Aviso de Privacidade ao longo da jornada do usuário é suficiente para assegurar o dever de transparência.

Em relação ao princípio da necessidade, como visto no quesito nº 5, ele não se refere a absoluta essencialidade, mas na necessidade de que a atividade de tratamento seja “uma forma direcionada e proporcional” de alcançar a finalidade do tratamento (“*targeted and proportionate way of achieving your purpose*”) [2]. Para tanto, com base no guia da INAI [3], é relevante que o controlador considere a adoção, dentre outros, dos seguintes cuidados:

- Sendo possível, descartar as amostras biométricas, armazenando apenas os *templates* gerados a partir dessas amostras, que serão utilizadas para comparações futuras – essa medida, contudo, pode não ser viável nos casos em que a manutenção da amostra seja necessária para comprovar que determinada ação foi executada pelo titular. É a hipótese, por exemplo, da manutenção da fotografia do titular nas hipóteses em que ele se utilize da biometria facial para assinar um contrato, como forma de demonstrar em juízo caso questionado que o serviço foi, de fato, contratado pelo titular. Coletar e tratar o número mínimo de amostras biométricas possível, preferindo, sempre que não for prejudicial ao objetivo perseguido, sistemas de verificação em detrimento dos de identificação.
- Buscar garantir a maior exatidão das amostras biométricas, de modo a limitar o volume de amostras biométricas necessárias.

Por sua vez, quanto a mitigação de vieses discriminatório, é recomendável, com base nos posicionamentos do ICO, em seus guias sobre biometria e IA [4][5], que:

- Se busque garantir adequada representatividade de diferentes etnias e gêneros na base de dados de treino do modelo.
- Realizar testes e avaliações para verificar a existência de vieses discriminatórios.
- Realizar testes, utilizando ferramentas disponíveis no mercado para verificar a estrutura e as *features*/métricas da solução de IA
- Testar a acuracidade estatística da solução utilizada.
- Adotar processos para o tratamento de erros, especialmente que minimizem seu impacto ao titular, inclusive a possibilidade de o titular questionar o resultado do sistema de reconhecimento facial.

[1] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>. Acesso em 09.06.2025

[2] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>. Acesso em 09.06.2025

[3] Disponível em: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf. Acesso em 09.06.2025

[4] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-fairly/>. Acesso em 10.06.2025

[5] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/>. Acesso em 10.06.2025

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Todas as medidas voltadas a garantir a alta eficácia e confiabilidade (ou seja, a melhoria do desempenho) de sistemas de reconhecimento facial devem ser proporcionais aos riscos concretos associados à sua utilização. Por exemplo, sistema empregado para o monitoramento de espaços públicos com o objetivo de identificar indivíduos foragidos da justiça exige, via de regra, nível de desempenho mais elevado do que solução destinada à autenticação de indivíduos para acesso a prédio empresarial, tendo em vista os potenciais danos morais e sociais decorrentes de identificação incorreta. Assim, as medidas elencadas a seguir devem ser compreendidas como recomendações a serem consideradas, conforme a avaliação de risco do sistema em questão, e não como exigências obrigatórias ou universais.

Considerando que sistemas de Reconhecimento Facial são soluções de inteligência artificial, para garantir o seu desempenho são recomendáveis as mesmas ações aplicáveis aos modelos de IA. Nesse sentido, como base no Guia de IA e Proteção de Dados do ICO [1], e seu respectivo *toolkit* de riscos [2], recomendamos que os seguintes controles sejam considerados:

- Durante a **etapa de planejamento**, é recomendável determinar, para os fins a que a solução se destina, o nível de acuracidade estatístico mínimo para a solução. Nesse sentido, é essencial que a escolha pelo controlador dos dados a serem tratados se dê após avaliação técnica que verifique que tipos de dados podem garantir maior segurança e efetividade à finalidade, sempre levando-se em conta a necessidade, a adequação e a proporcionalidade. Desta forma, torna-se possível estabelecer se a situação concreta exige dado preciso e único (por exemplo, imagem de íris) ou, em casos de menor risco de comprometimento de segurança, se pode atingir a finalidade visada com dados menos únicos e com menor acurácia, como imagens faciais ou forma da mão.

- Durante a **etapa de seleção e aquisição de dados**, é recomendável, considerando o público para o qual a solução de IA se destina, garantir que os dados de treinamento: (i) são adequadamente representativos, completos e exatos; (ii) foram corretamente rotulados; e (iii) foram considerados e abordados os riscos de *Overfitting* e *Underfitting*.
- Durante a **etapa de teste e validação**, é recomendável realizar testes documentados para: (i) verificar a acuracidade estatística da solução, tanto global, quanto em relação a grupos relevantes, verificando o atendimento do nível mínimo de desempenho definido; (ii) foram realizados testes para detectar possíveis problemas de *Overfitting* e *Underfitting*; e (iii) adotar medidas corretivas – como retreinar o sistema ou redefinir parâmetros – em caso de falhas nos testes.
- Na etapa **de colocação em produção e monitoramento**, é recomendável: (i) considerar a disponibilização, às pessoas sob riscos de danos substanciais a seus direitos fundamentais, de mecanismo para que questionem resultados da solução – isto é, exercício do direito de revisão; (ii) adotar práticas de monitoramento ou testes periódicos, de modo a garantir que a acuracidade estatística da solução é mantida; e (iii) manter cópias das iterações anteriores de IAs que continuem a aprender após a sua colocação em produção, de modo a possibilitar o seu retorno, caso novas iterações apresentem degradação em seu desempenho.

[1] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>. Acesso em 11.06.2025

[2] Disponível em: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffkr3mveig%2Fai_and_data_protection_risk_toolkit_v11.xlsx&wdOrigin=BROWSELINK. Acesso em 11.06.2025

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

O reconhecimento facial não será mecanismo apropriado quando os benefícios, e o bem jurídico, que a aplicação de reconhecimento facial almeja resguardar não for proporcional aos riscos aos direitos e liberdades aos titulares afetados.

Em contextos educacionais, por exemplo, o uso para controle de presença pode representar monitoramento excessivo, impactando negativamente o direito à educação. No âmbito de processos seletivos e contratações, o uso do reconhecimento facial para análise de expressões faciais durante entrevistas representa um risco concreto de discriminação e reforço de vieses algorítmicos, comprometendo a equidade do processo. A tecnologia também é complexa em eventos políticos ou manifestações, onde pode ser usada para identificar e eventualmente perseguir manifestantes.

Em relação às tecnologias alternativas, existem outras informações que podem ser utilizadas como apoio ou em substituição ao reconhecimento facial, sempre de acordo com o caso concreto. Por exemplo, a Autoridade de Dados da Coreia [1], em seu guia sobre dados biométricos traz estes exemplos:

- Para acesso a instalações físicas ou dispositivos em geral, a utilização de dados obtidos a partir da digital do indivíduo, adoção de cartões de acesso ou senhas complexas.
- Para acesso a aplicativos, adoção de: i) autenticação por Serviços de Resposta Automática (o usuário recebe chamada telefônica automática e precisa seguir determinadas instruções para confirmar sua identidade); ou ii) tokens ou senhas temporárias encaminhadas via SMS, e-mail ou aplicativo autenticador previamente validados.

Outro mecanismo útil na prevenção de fraudes é a utilização de dados provenientes do setor de telecomunicações. Soluções baseadas nesses dados permitem, por exemplo, verificar se o número de telefone e outras informações de contato coincidem com os registros das operadoras, confirmar se a localização de uma transação corresponde à localização do dispositivo do titular e identificar indícios de práticas fraudulentas, como o SIM Swap. Por exemplo, a ANATEL destaca a utilização de dado de telecomunicação por instituições financeiras “para prevenir fraudes no sistema financeiro, as prestadoras disponibilizam informações para os bancos, possibilitando que adotem providências preventivas relativas às movimentações financeiras atreladas ao número do celular envolvido em troca de chip” [2].

Para que as organizações possam, quando apropriado e considerando os riscos envolvidos, adotar mecanismos alternativos ao reconhecimento facial, é fundamental que a ANPD promova a construção de um ecossistema regulatório que estimule a pesquisa e o desenvolvimento de soluções seguras e eficazes, o que só é possível pela flexibilidade do controlador de adaptar suas práticas a diferentes casos concretos, inclusive com a evolução das diferentes tecnologias, sempre de modo a não obstar de antemão a implementação de tecnologias inovadoras e avançadas de privacidade. [1] Disponível em: <https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do#none>. Acesso em 11.06.2025.

[2] Disponível em: <https://www.gov.br/anatel/pt-br/assuntos/dicas-contras-fraudes/golpes-atuais-mais-comuns>. Acesso em 13.06.2025

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Como já apontado no quesito de nº 5, com base nos posicionamentos do ICO, INAI e da Autoridade de Dados da Coreia, estas são as medidas de segurança que entendemos essenciais para a proteção de dados biométricos:

- Controles de acesso aos dados;
- Realização de testes de penetração
- Implementação de política de segurança da informação;
- Criptografia dos dados pessoais, tanto em trânsito quanto em repouso;
- Realização de varredura (*scan*) de vulnerabilidades nos sistemas que tratam dados biométricos, com adoção de medidas corretivas;
- Registro em logs de todos os acessos aos dados biométricos;
- Armazenamento de dados biométricos de forma segregada de outras informações; e
- Quando houver contratação de fornecedor, realização de processo adequado de *due diligence*.

Em relação aos parâmetros mínimos a serem adotados para a mensuração e o monitoramento de riscos de segurança, não entendemos existir diferença entre a metodologia empregada no contexto da biometria facial e as práticas adotadas para outros riscos de cibersegurança. Nesse sentido, com base na ISO/IEC 27005:2023 [1], estes são os parâmetros básicos:

a) **Definir critério de riscos:** estabelecer, com base no apetite de risco organizacional, as regras e os parâmetros para aceitação de riscos; e

b) **Identificar os Riscos:** identificar os(as): i) ativos envolvidos; ii) ameaças potenciais a esses ativos; iii) controles existentes; e iv) vulnerabilidades. Em relação a ameaças no contexto da biometria facial, entendemos ser relevante considerar os ataques típicos, descritos no guia do Centro de Cibersegurança Nacional do Reino Unido (NCSC) [2]:

- **Ataques de apresentação:** são exibidos como os mais comuns para biometria facial. Neles é utilizado artefato (como uma fotografia) para falsificar a validação da identidade.
- **Interceptação do resultado de sensores:** ataque voltado a modificar ou interceptar os dados gerados pelo sensor – isto é, os *inputs* captados do mundo físico (a foto, gravação, leitura da biometria ou quaisquer outros) com o objetivo de burlar o sistema ou prejudicar o seu funcionamento.
- **Subversão da Integridade da Inscrição:** ataque voltado a inscrever, no registro de alguém, dados biométricos de outra pessoa, fraudando, desta forma, a biometria facial.
- **Ataque a bancos de dados:** alteração de dados durante a sua transmissão ou armazenamento.
- **Ameaça interna:** ações executadas por profissionais que se utilizam de suas credenciais e seus acessos legítimos para a execução de condutas criminosas
- **Ataques aos Sistemas de TI:** ataques típicos de segurança aos sistemas de TI que sustentam a operação.
- **Ataques de negação de serviço:** ataques voltados a tornar o sistema indisponível. Esses ataques podem ser utilizados para forçar a organização a operar em uma rede menos segura, assim, é necessário que a

infraestrutura técnica de contingência tenha segurança equivalente à do sistema biométrico.

c) **Analisar os riscos:** identificar as potenciais consequências decorrentes da concretização dos riscos e a probabilidade de sua ocorrência, definindo, por meio de ambos os elementos, o nível do risco.

d) **Tomar decisão:** avaliar, de acordo com o critério de riscos, se ele é aceitável e tomar uma decisão – isto é, modificar (mitigar), reter (aceitar), compartilhar ou evitar (eliminar) o risco. A depender da decisão plano de ação pode precisar ser elaborado e executado.

e) **Monitoramento:** é necessário que os elementos que compuseram a identificação do risco sejam monitorados, para que, em caso de sua modificação (por exemplo, o surgimento de nova ameaça) os efeitos desta alteração sejam computados na análise do risco.

Em relação ao primeiro questionamento (isto é, quais boas práticas devem ser observadas para garantir que a limitação não configure discriminação ilícita ou abusiva), reiteramos os pontos já descritos no quesito nº 8.

[1] Disponível em: <https://www.normas.com.br>. Acesso em 11.06.2025

[2] Disponível em: <https://www.ncsc.gov.uk/collection/biometrics>. Acesso em 12.06.2025

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Em relação ao primeiro questionamento, entendemos que, além das medidas já indicadas no quesito nº 8, é fundamental considerar a acessibilidade da ferramenta utilizada (por exemplo, indivíduos com deficiência visual podem ter significativa dificuldade na utilização de soluções dessa natureza) [1]. Assim, é importante que as organizações ponderem esse desafio de acessibilidade e busquem a adoção de mecanismos para mitigá-los. Em situações nas quais seja possível confirmar a deficiência visual do indivíduo, buscar, excepcionalmente, processos alternativos de autenticação, ainda que não ofereçam o mesmo grau de proteção, sempre que esses processos não comprometam a finalidade e a segurança do tratamento.

Em relação ao tratamento baseado no consentimento, entendemos que a negativa de tratamento de dados biométricos pode implicar em rejeição de determinada funcionalidade quando a funcionalidade efetivamente depender do tratamento de dados biométrico. Por exemplo:

- Caso instituição financeira ofereça a possibilidade de confirmar transações por biometria ou senha, é lícito não fornecer a funcionalidade de confirmação por biometria, caso o titular não ofereça o consentimento.
- Rede de academias pode dar aos seus clientes a opção de acessar as suas instalações por meio de validação biométrica ou da digitação de senha vinculada ao seu número

de matrícula [2] – a não oferta do consentimento impossibilitará o acesso facilitado via biometria facial.

No contexto da base legal do consentimento, não deve ser admitido que sua negativa impeça o titular de acessar serviço ou funcionalidade cuja operação não dependa, de fato, da coleta de dados biométricos.

Nos demais casos, entendemos que a recusa em fornecer a biometria implicaria em exercício de fato do direito de oposição. Consequentemente, o não oferecimento da funcionalidade, serviço ou produto resguardado pelo acesso biométrico será lícito se uma das seguintes condições for satisfeita: (a) não seja concretamente possível ofertar a funcionalidade sem o tratamento de dados biométricos, aplicando-se aqui o mesmo descrito quanto ao consentimento; **ou** (b) os direitos e interesses protegidos ao se exigir a biometria não sejam sobrepujados pelo direito do titular de não a ofertar – isto é, existe razão pela qual a validação biométrica é necessária, como a existência de bem protegido relevante [3].

[1] Disponível em: <https://www.vice.com/en/article/facial-recognition-apps-are-leaving-blind-people-behind/>. Acesso em 12.06.2025

[2] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>. Acesso em 12.06.2025

[3] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>. Acesso em 12.06.2025

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Retomamos as respostas já oferecidas aos quesitos n°s 2, 5, 8 e 11.

Em relação aos mecanismos adequados de proteção, além da necessidade de avaliação de riscos de cibersegurança, seguindo os passos já elencados no quesito de n° 11, reforçamos os controles apontados no quesito de n° 8, com base nos guias de diversas autoridades de dados (ICO, INAI, Autoridade de Dados da Coreia).

Em relação às medidas de transparência, a obrigatoriedade legal se refere ao fornecimento das informações previstas no art. 9º da LGPD. A forma adequada de disponibilização dessas informações, conforme indicado nos quesitos n°s 2 e 8, com base no posicionamento do ICO, dependerá de uma série de fatores – como o caso de uso, a natureza do relacionamento com o titular e os elementos envolvidos na atividade de tratamento.

Em síntese, quanto mais evidente for a atividade de tratamento analisada – considerando, inclusive, as práticas habituais de mercado –, menor será a exigência de adoção de práticas ativas de transparência para o fornecimento das informações legalmente requeridas ao titular.

Ainda, a implementação de *privacy-enhancing technologies* deve ser incentivada como boa-prática – ainda que não mandatória ao tratamento de dados biométricos, sempre que possível, de forma a incrementar a privacidade dos titulares através da limitação de possibilidades de identificação, inclusive por processos de anonimização. Nesse sentido, são relevantes as tecnologias indicadas pelo ICO, como privacidade diferencial, *secure multi-party computation* (SMPC) e criptografia homomórfica.[1]

Por fim, em relação ao risco de discriminação, reitera-se as medidas já apontadas no quesito de nº 8, baseadas no posicionamento do ICO.

[1] Disponível em: <https://www.gov.uk/government/publications/privacy-enhancing-technologies-cost-benefit-awareness-tool>

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

Em relação ao direito de informação, conforme já destacado na resposta ao quesito nº 2, em contextos nos quais não há expectativa razoável por parte dos titulares quanto à coleta de seus dados biométricos, e nem relação prévia entre os titulares e a empresa controladora, é exigido esforço adicional no cumprimento do dever de transparência.

Esse dever pode ser atendido, por exemplo, por meio da instalação de placas em locais de fácil visualização contendo informações gerais sobre a atividade de tratamento, além da indicação dos meios para obtenção de informações mais detalhadas e para o exercício dos direitos dos titulares. Igualmente, podem ser disponibilizados em locais fixos (paredes, totens, televisões, entre outros) QR Codes, que direcionam para a Política de Privacidade da organização, a qual deve conter as informações elencadas na legislação.

Situação semelhante já foi analisada por esta Autoridade, que entendeu como adequadas essas providências de transparência, conforme consta da Nota Técnica nº 29/2024/FIS/CGF/ANPD, §6.1.4 [1].

[1] Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-29_2024.pdf. Acesso em 09.06.2025

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Para além das práticas de transparência já expostas nos quesitos anteriores, entendemos que o atendimento aos direitos dos titulares deve ser assegurado, considerando as especificidades da tecnologia biométrica.

Em relação ao direito de acesso, conforme o ICO [1], há dificuldade técnica em fornecer os dados biométricos propriamente ditos, uma vez que, em geral, são *outputs* matemáticos complexos, não compreensíveis (“ilegíveis”) por seres humanos. Diante disso, o fornecimento pode ser substituído por uma declaração explicativa, que:

- (a) justifique a impossibilidade de entrega direta do dado;
- (b) descreva a natureza do dado em questão; e
- (c) esclareça como esse dado é mantido pela organização.

É importante destacar que isso não impede o fornecimento de outras informações relacionadas ao processo de validação biométrica do titular, como, por exemplo, seu identificador pessoal (como o CPF), ou, quando houver, as amostras biométricas a partir das quais os *templates* foram extraídos, nas hipóteses em que esses dados sejam armazenados pelo controlador.

Quanto ao direito de correção, o ICO também ressalta que ele não se aplica à correspondência probabilística entre o dado fornecido pelo titular e os registros da base de dados, uma vez que tal correspondência é de natureza estatística [1]. No entanto, esse direito pode ser exercido nos casos em que haja erro na associação entre o *template* biométrico e o identificador do titular, ou quando uma alteração física relevante tornar necessário atualizar o *template*.

Para viabilizar esse direito, é essencial que os *templates* biométricos adotem a característica de serem “revogáveis e renováveis” – ou seja, que possam ser substituídos por novos *templates*, sem manter vínculo técnico com os anteriores [2].

No que se refere à revogação do consentimento, seu atendimento também pressupõe que o *template* biométrico seja efetivamente revogável, ou seja, passível de cancelamento.

Contudo, é importante ressaltar que a revogação não implica, necessariamente, a exclusão do histórico de autenticações já realizadas, uma vez que podem existir finalidades autônomas que justifiquem a manutenção desses registros, independentemente do consentimento – como, por exemplo, o cumprimento de obrigações legais ou regulatórias, ou a necessidade de preservação de registros para fins de auditoria ou segurança.

[1] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>. Acesso em 12.06.2025

[2] Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>. Acesso em 12.06.2025

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível?

Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

Como já reconhecido pela ANPD em seu Enunciado CD/ANPD nº 1/2023 [1], o tratamento de dados pessoais de crianças e adolescentes pode se fundamentar em qualquer das hipóteses legais previstas no art. 11º, da LGPD, desde que observe e assegure o melhor interesse do menor.

Assim, respeitados os requisitos para enquadramento e demonstrado que a atividade de tratamento visa efetivamente atender ao melhor interesse da criança ou do adolescente, o tratamento de dados biométricos desses titulares poderá se apoiar em qualquer uma das bases legais previstas no referido dispositivo legal.

No que tange à transparência e participação dos pais ou responsáveis, embora o ordenamento jurídico britânico (*Protection of Freedoms Act 2012*) adote modelo distinto, permitindo o tratamento de dados biométricos de menores apenas mediante consentimento parental, as orientações constantes no guia do governo do Reino Unido [2] podem servir como referência, desde que adaptadas ao contexto normativo brasileiro.

Nesse sentido, além da inclusão do tratamento de dados biométricos no aviso de privacidade, recomenda-se, sempre que viável:

- A comunicação formal aos pais ou responsáveis legais, contendo informações claras sobre a atividade de tratamento, sua finalidade e fundamentos;
- A indicação de canais de contato para o exercício de direitos e para a obtenção de informações adicionais; e
- Caso aplicável, a disponibilização de meios para oposição à atividade de tratamento, com instruções destacadas e acessíveis sobre como fazê-lo.

Por fim, em relação ao melhor interesse da criança, sua avaliação sempre deverá ser casuística, requerendo a consideração de alguns fatores, especialmente:

- O bem jurídico, notadamente o interesse do menor, que se busca resguardar – o que permite avaliar se a intrusão na privacidade do titular é proporcional ao interesse resguardado.
- A existência de soluções alternativas menos intrusivas, principalmente se referidas soluções forem aptas a atender o mesmo fim com similar desempenho.
- Consideração da volatilidade de certas informações biométricas de crianças e adolescentes e seu impacto na finalidade almejada (por exemplo, traços faciais podem sofrer alterações substantivas durante o período de puberdade), o que pode afetar fins que requeiram o tratamento de dados por período prolongado [3].

[1] Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf>.

Acesso em 12.06.2025

[2] Disponível em:
https://assets.publishing.service.gov.uk/media/62d7d76c8fa8f50c012d14df/Biometrics_Guidance_July_2022.pdf Acesso em 12.06.2025

[3] Disponível em:
https://quno.org/sites/default/files/resources/QUNO_Briefing%20Paper_Biometric%20data%20of%20CPACTO_SEP2020.pdf. Acesso em 12.06.2025

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Em relação às hipóteses legais e a participação informada dos pais e responsáveis, aplica-se o já descrito no tópico anterior. Isto é:

- **Em relação às hipóteses legais:** conforme reconhecido pela ANPD no Enunciado CD/ANPD nº 1/2023, o tratamento de dados pessoais de crianças e adolescentes pode se basear em qualquer das hipóteses legais do art. 11 da LGPD, desde que respeite, de forma prioritária, o melhor interesse do menor. Assim, é admissível o uso de dados biométricos de crianças e adolescentes, desde que a base legal seja devidamente justificada e a atividade de tratamento esteja claramente orientada à proteção de seus interesses.
- **Em relação às informações a serem prestadas:** além de fornecer informações no aviso de privacidade da organização, é importante que se realize a comunicação formal dos pais e responsáveis, quando possível, oferecendo as informações essenciais da atividade de tratamento e os mecanismos para o exercício de direitos.

Por fim, no tocante às medidas de segurança, aplicam-se as diretrizes já estabelecidas nos quesitos nºs 5 e 11.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

A adoção de mecanismos de verificação de idade deve considerar: a) o contexto específico em que essa verificação é realizada; b) o grau de acuracidade da solução tecnológica adotada; e c) a existência de meios menos intrusivos que sejam capazes de atingir resultado equivalente.

1. Contexto da verificação de idade: essa análise é essencial para avaliar a compatibilidade da coleta de dados biométricos com o princípio da necessidade e com a salvaguarda do melhor interesse da criança e do adolescente. Conforme orienta a Autoridade de Proteção de Dados do Reino Unido (ICO) [1], a técnica empregada para verificar a idade deve ser proporcional aos riscos que o serviço e o tratamento de dados representam para menores de idade.

Por exemplo, o uso de biometria facial para validar o acesso a jogos ou plataformas que contenham conteúdo adulto – ou que exponham o menor a riscos típicos do ambiente digital, como a interação com desconhecidos potencialmente mal-intencionados – pode ser considerado proporcional e alinhado ao melhor interesse do menor. Por outro lado, para

finalidades menos sensíveis, como o recebimento de *newsletter* informativa, a simples autodeclaração pode ser suficiente.

2. Acuracidade da tecnologia adotada: outro aspecto relevante é o nível de precisão da tecnologia utilizada. Tecnologias de estimação de idade com base em biometria são mais propensas a erros [2] [3]. Por essa razão, entende-se que a combinação de análise documental (documentoscopia) com a verificação da correspondência entre o titular e o documento apresentado tende a oferecer maior confiabilidade.

3. Existência de meios alternativos menos intrusivos: também deve ser avaliada a viabilidade de soluções alternativas que, no caso concreto, se revelem menos invasivas e apresentem um grau de acuracidade similar – ou ao menos suficiente diante dos riscos efetivos de acesso indevido de menores. Além disso, o exercício da ponderação deve considerar a eficiência da solução: por vezes, tecnologias biométricas podem funcionar de maneira muito mais eficiente e precisas do que as alternativas disponíveis – que, por exemplo, embora possam funcionar individualmente consideradas, não são escaláveis, não podendo, portanto, atender as demandas concretas da organização. Nesse sentido, não se deve simplesmente excluir, de antemão, a possibilidade de uso de tecnologias biométricas pela mera existência de alternativas.

A título exemplificativo, destacam-se os seguintes mecanismos[2][3]:

- **Autodeclaração**, como o fornecimento da data de nascimento pelo próprio usuário.
- **Validação de cartão de crédito**, mediante uma transação de valor irrisório (ex. R\$0,01) para confirmar a titularidade e idade do usuário.
- **Análise de padrões de uso online**, com inferência da idade a partir de comportamento digital, conteúdo acessado, entre outros dados.
- **Verificação offline**, por meio da conferência presencial de documentos antes de autorizar o acesso.
- **Consentimento parental**, quando for possível comprovar, de maneira confiável, a identidade e autoridade do responsável legal.
- **Aferição de idade no nível dos sistemas operacionais e lojas de aplicativos**, repassada pelo OS/App store para as aplicações aí disponíveis para que possam oferecer experiências apropriadas à idade do usuário.

Em suma, a adoção de biometria facial como ferramenta de verificação de idade deve ser cuidadosamente ponderada em cada caso concreto, à luz do princípio do melhor interesse da criança e do adolescente, considerando os riscos envolvidos e os impactos potenciais decorrentes do tratamento de dados biométricos.

[1] Disponível em: <https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/age-assurance-for-the-children-s-code/3-age-assurance-methods/>. Acesso em 12.06.2025

[2] Disponível em: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA\(2023\)739350_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf). Acesso em 12.06.2025

[3] Disponível em: <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>. Acesso em 12.06.2025

São Paulo (SP), 01 de agosto de 2025.

Rony Vainzof² | Caio Lima³ | Jean Santana⁴

² Consultor de Proteção de Dados da FecomercioSP e Sócio do VLK Advogados

³ Sócio do VLK Advogados

⁴ Advogado do VLK Advogados

Tomada de Subsídios sobre Tratamento de Dados Biométricos

Contribuição da Equipe do Encarregado de Proteção de Dados da Fundação Getulio Vargas em relação ao uso de dados biométricos para garantia de prevenção à fraude.

Junho de 2025

Participação:

Aline Faria da Silva
Jordan Vinícius de Oliveira
Laila Sá Ferreira
Lays Gomes Martins
Taís Povill Rocha



UTILIZAÇÃO DE SISTEMAS DE BIOMETRIA

Em relação especificamente ao disposto ao artigo 11, II, alínea *g* da LGPD (Lei 13.709/2018), considera-se que o uso de tecnologias biométricas, independentemente da modalidade (impressão digital, reconhecimento facial, voz, etc.), só é admissível quando atendidos os seguintes requisitos legais e técnicos previstos na LGPD:

1. Requisitos legais

É preciso observar uma das hipóteses mencionadas na alínea supramencionada, quais sejam:

Se a entidade responsável for a controladora (requisito necessário):

- (a) Prevenção à fraude, mediante receio devidamente justificado em risco robusto e concreto, após realizado teste de balanceamento com os direitos e garantias dos titulares. Ex.: o acesso a uma sala de servidores de alto grau de sigilo de uma instituição só é feito mediante o reconhecimento da datiloscopia digital dos funcionários autorizados a ingressarem no ambiente para fins de manutenção (nesta hipótese, o mero uso de um cartão de acesso/crachá poderia ser insuficiente para assegurar o devido controle de ingresso no ambiente, uma vez que esse cartão poderia ser emprestado ou furtado por um terceiro, o que justificaria o “risco robusto e concreto”); ou
- (b) Garantia da segurança do titular, também mediante receio devidamente justificado em risco robusto e concreto, após realizado teste de balanceamento com os direitos e garantias dos titulares. Ex.: caso o titular solicite a realização de uma transação bancária relevante a partir de padrões incomuns para o seu perfil (como o acesso mediante um novo aparelho telefônico ou uma transação realizada para um destinatário incomum) é justificável, em nome de sua segurança, que a instituição financeira que presta serviços a ele empregue uma tecnologia dotada dos melhores padrões de reconhecimento facial (ex.: a partir de uma câmera 3D e validações ativas do titular nas interações com o software) para autenticar a validade da operação;

Se a referida entidade for operadora (boa prática):

- Autorização e/ou requisição por escrito da instituição Controladora, preferencialmente mediante parecer do qual participou ou anuiu o seu Encarregado de Proteção de Dados. Ex.: uma administradora de condomínio recebeu uma ordem de implementar equipamento de autenticação biométrica para o ingresso em determinado recinto específico. Esta administradora, mera contratada do condomínio, deve requisitar um parecer do encarregado da contratante, de modo a viabilizar a operação.

Neste ponto, a recomendação se trata de uma boa prática e não de uma exigência obrigatória, uma vez que a operadora não possui necessário poder de decisão sobre o tratamento de dados, mas meramente executa as ordens da controladora.

2. Requisitos técnicos

Além de base legal adequada, a adoção de sistemas biométricos deve ter:

(a) Um protocolo específico para tratamento de erros, como falsos positivos, falsos negativos e outros incidentes operacionais. Ex.: um sistema de reconhecimento facial para ingresso em determinado ambiente deve possuir um protocolo alternativo para o caso da verificação de

identidade de determinada pessoa não puder ser concluída, como o acionamento da equipe de portaria para checagem de documentos e autorização de ingressos em um ambiente de acesso restrito; e

(b) Existir um Relatório de Impacto pronto e que atenda aos requisitos previstos na LGPD e regulamentos pertinentes. Especificamente, neste ponto, salienta-se a importância de políticas claras para backup dos dados, sua criptografia, o controle de acesso à base de informações e, ainda, a atualização do sistema operacional e aplicações envolvidas.

APÊNDICE ÚNICO - FUNDAMENTOS JURÍDICOS

O tratamento de dados biométricos implica em riscos elevados, sendo notável que as soluções tecnológicas que realizam o tratamento de dados biométricos podem coletar mais informações do que realmente são necessárias para a finalidade do tratamento de dados pessoais. Por exemplo, em determinados sistemas biométricos baseados em reconhecimento facial, podem ser tratados dados que revelem a origem racial ou étnica, bem como podem ser extraídas informações sobre problemas de saúde, físicos ou psicológicos, de um determinado indivíduo. Esses dados pessoais são classificados como sensíveis (art.5º, II da LGPD) e apenas podem ser tratados nas hipóteses previstas no art. 11¹ da LGPD.

No caso de controles de frequência, por exemplo, a Autoridade Espanhola de Proteção de Dados (AEPD) recomenda² que seria necessário avaliar a existência de uma justificativa robusta para o tratamento adicional de dados sensíveis (biométricos) no lugar de dados não sensíveis (ex.: cartões de acesso ou similares) que já alcancem a mesma finalidade.

Trazendo o link para a LGPD, o artigo 6º, III, prevê o princípio da necessidade, estipulando-o como a *"limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados"*. Logo, além da não excessividade (existência de dados que não serão utilizados), o princípio também se pauta pela proporcionalidade e pertinência, situação na qual a utilização de dados sensíveis para uma finalidade já realizada de forma satisfatória com dados não sensíveis perderia a razoabilidade. Caso exista alternativa menos invasiva, a implementação de um sistema que trate dados biométricos não é justificável.

¹ Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da [Lei nº 9.307, de 23 de setembro de 1996 \(Lei de Arbitragem\)](#);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

² AEPD. *Guía sobre Tratamientos de Control de Presencia Mediante Sistemas Biométricos*, p. 07-8; 17. Nov. 2023. Agencia Española Protección Datos. Disponível em: <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf>. Acesso em 29 out. 2024.

Dito isso, compreende-se que o uso de sistemas biométricos deve-se limitar ao mínimo necessário, sempre observados os requisitos legais.

Tomada de Subsídios Dados Biométricos

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Uma abordagem para a classificação de dados como biométricos deve buscar a construção de critérios jurídicos objetivos, visando oferecer maior previsibilidade aos agentes de tratamento. Nesse sentido, com uma análise inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) e nas explicações trazidas pela [Autoriteit Persoonsgegevens](#), sugere-se os seguintes critérios: 1. Natureza do dado, 2. O uso e método de tratamento, 3. A finalidade ou resultado do tratamento.

Nessa linha, o critério de natureza dos dados sugere que dados biométricos são aqueles que dizem respeito a características físicas, fisiológicas ou comportamentais de uma pessoa, geralmente permanentemente.

O critério do método de tratamento dos dados, por sua vez, envolve a submissão dos dados por processamento técnico específico, pelo qual os dados são analisados usando meios técnicos e, posteriormente, comparados com uma determinada referência para identificação de alguém. Conforme a [Information Commissioners Office \(ICO\)](#), do Reino Unido, o processamento técnico específico é "uma operação de processamento - ou um conjunto de operações - que pode ser aplicada às características físicas, fisiológicas ou comportamentais de uma pessoa, tornando possível sua identificação exclusiva".

Por fim, o critério do objetivo ou resultado do tratamento deve considerar que dados biométricos são aqueles que passam - ou podem passar - por tratamento com o objetivo específico de estabelecer ou confirmar a identidade de uma pessoa física.

Dessa forma, a caracterização de um dado como biométrico se consolida não apenas pela sua origem em características pessoais, mas pela combinação de seu tratamento por meios técnicos específicos com o objetivo de identificar um indivíduo. A adoção de uma abordagem com critérios cumulativos como essa é útil para evitar que uma interpretação excessivamente ampla, focada apenas na natureza do dado, resulte em restrições que possam afetar negativamente a atividade econômica, a inovação, entre outras operações de tratamento de dados.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

É dever dos controladores que tratam dados biométricos garantir que os titulares recebam informações precisas, completas e de fácil acesso, seja antes ou no exato momento da coleta de seus dados.

Nesse sentido, as [diretrizes da ICO](#) servem como um bom parâmetro sobre o conteúdo essencial dessa comunicação. Assim, o titular deve ser informado sobre as finalidades específicas do tratamento, a hipótese legal que o autoriza, os tipos de dados que serão coletados e os eventuais destinatários. Adicionalmente, é preciso esclarecer o período de retenção dos dados biométricos ou os critérios para sua definição, detalhar os direitos do titular previstos na LGPD, como a possibilidade de revogar o consentimento, e informar sobre a existência de qualquer obrigação legal ou contratual para o fornecimento dos dados, bem como os dados de contato do controlador. Esse dever de transparência, contudo, deve ser equilibrado com a necessidade legítima de proteção a segredos comerciais e informações confidenciais dos controladores, nos termos do artigo 6º, inciso VII, da LGPD, o que exige cuidado na forma e no grau de detalhamento das informações fornecidas ao titular.

Todas essas informações devem ser apresentadas de maneira concisa e com linguagem simples, a fim de reduzir a assimetria informacional. A escolha do meio deve ser adaptada ao contexto. Em ambientes digitais, por exemplo, boas práticas incluem o uso de painéis de controle (*dashboards*) e notificações em camadas ou "*just-in-time*", que surgem no momento da interação. Já em espaços físicos, recomenda-se o uso de sinalização visual clara, códigos QR que levem a informações detalhadas e o suporte de equipes treinadas para orientar os titulares.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A distinção entre biometria tradicional (i.e., que utiliza características físicas para identificar indivíduos) e biometria comportamental (i.e., que identifica padrões individuais sobre como os indivíduos atuam ou interagem com dispositivos para identificá-los) não necessariamente deve gerar obrigações específicas e diferentes para cada tipo de tratamento de dados biométricos nestes contextos. Isso porque a utilização dessas informações sensíveis dependerá essencialmente do contexto em que se inserem - portanto, uma não deve ser considerada melhor ou, por outro lado, mais "arriscada" do que outra *a priori*, demandando sempre uma análise contextual, para verificação de sua eficácia e potenciais riscos caso a caso.

Considerando que muitos usos de tecnologias de biometria estão associados a finalidades de identificação/autenticação de indivíduos ou combate à fraude, é de extrema importância garantir a qualidade dos dados, em especial para confirmar que

são efetivamente relacionados aos indivíduos considerados. A falta de qualidade de dados biométricos pode levar a erros nessas finalidades e a uma redução da performance de sistemas que utilizam esses dados, podendo até mesmo gerar resultados falsos. Neste sentido, a adoção de medidas de controle de qualidade e monitoramento podem ser úteis para se manter a qualidade desses dados ao longo do tempo.

Ademais, com relação ao princípio da segurança, é importante que os agentes utilizem medidas técnicas e administrativas capazes de proteger os dados biométricos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Contudo, cumpre frisar que a aplicação dos referidos princípios de qualidade e segurança não é exclusiva ao tratamento de dados biométricos - i.e., estes deverão ser aplicados independentemente da natureza dos dados.

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

A possibilidade de utilização do consentimento como base legal para o tratamento de dados biométricos pode incentivar um ciclo de hipercoleta difícil de conter. A generalização dessa prática transfere aos titulares a responsabilidade por decisões que afetam não apenas sua privacidade individual, mas também a segurança de ecossistemas inteiros de autenticação que utilizam dados biométricos como credencial.

A exposição desse tipo de dado, uma vez vazado, não pode ser revertida, e seus efeitos podem ser permanentes tanto para os indivíduos quanto para sistemas mais amplos. Esse cenário demanda uma reflexão preliminar sobre os impactos estruturais da adoção do consentimento como hipótese principal para o tratamento desses dados, especialmente quando a escolha do titular é moldada por fatores como conveniência tecnológica, ausência de alternativas e desconhecimento dos riscos.

A LGPD admite o consentimento como uma das bases legais para o tratamento de dados pessoais sensíveis, desde que seja livre, informado, específico, destacado e inequívoco. No caso de dados biométricos, no entanto, essas condições são de difícil concretização, sobretudo em contextos marcados por desequilíbrios informacionais, pressões indiretas e impossibilidade prática de recusa. Nesses casos, o consentimento tende a ser mais formal do que efetivo, o que compromete sua validade jurídica e reduz sua aptidão para assegurar os direitos dos titulares.

Sempre que possível, o tratamento deve ser amparado por outras bases legais mais adequadas, como a prevista no art. 11, II, “g”, nos casos em que o dado seja indispensável para a prevenção de fraudes e para a segurança do titular, respeitados os direitos e liberdades fundamentais. Quando, excepcionalmente, o consentimento for utilizado, recomenda-se a implementação de salvaguardas adicionais, como a oferta de alternativas não biométricas, a apresentação clara dos riscos envolvidos, a exclusão imediata dos dados em caso de revogação e a realização de avaliações de impacto para justificar sua adoção. Tais medidas são essenciais para mitigar os riscos decorrentes da fragilidade estrutural do consentimento como base legal para dados biométricos.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A aplicação da hipótese de prevenção à fraude exige demonstração concreta de que o uso de dados biométricos é indispensável para mitigar riscos específicos e que não há alternativa menos invasiva. No contexto financeiro, sua adoção pode ser proporcional, desde que restrita a finalidades claramente delimitadas, como autenticação de transações de alto risco.

Para compatibilizar o uso da biometria com o princípio da necessidade, é essencial restringir a coleta ao mínimo necessário, evitar reutilização para outras finalidades e justificar tecnicamente a escolha. A coleta ampla, preventiva ou desvinculada de risco real compromete a legalidade do tratamento, mesmo sob essa base.

Ainda, devem ser adotadas salvaguardas como: realização de Relatório de Impacto à Proteção de Dados (RIPD), limitação de prazo de retenção, medidas de segurança avançadas (criptografia, controle de acesso, segregação de dados), transparência quanto às finalidades e garantia de revisão humana em decisões automatizadas. A biometria não deve ser usada como atalho para conveniência, mas apenas quando estritamente necessária e tecnicamente justificada.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos

controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Quando o tratamento de dados biométricos se fundamenta no cumprimento de obrigação legal ou regulatória, é essencial que a norma em questão seja explícita quanto à exigência a tipo de dado sensível. Isto porque a mera existência de uma obrigação genérica não autoriza a coleta de biometria.

Assim, a interpretação deve ser restritiva e orientada pelo princípio da necessidade, admitindo-se o tratamento apenas quando o dado biométrico for indispensável para cumprir o dever legal.

O controlador, portanto, deve comprovar que não há meio menos invasivo de atingir a finalidade prevista na norma. Mesmo diante de obrigação legal, deve-se adotar salvaguardas já anteriormente mencionadas, como: RIPD, controle de acesso e rastreabilidade, políticas de retenção mínima, descarte seguro, segregação de bases, e transparência com os titulares.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, “c”, LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

O tratamento de dados biométricos por órgãos de pesquisa, nos termos do art. 11, II, “c”, da LGPD, deve estar vinculado a finalidades exclusivamente acadêmicas, científicas ou estatísticas, de interesse público, sendo vedado o uso para fins comerciais. A base legal deve ser definida a partir da finalidade do tratamento, e não da natureza biométrica dos dados.

Embora a LGPD não exija anonimização para essa hipótese, sua adoção é recomendável como medida de mitigação de riscos, especialmente considerando o alto potencial de identificação dos dados biométricos. Nesses casos, é essencial avaliar se a anonimização é tecnicamente suficiente para descaracterizar os dados como pessoais, conforme os critérios do art. 12.

Caso os dados não possam ser considerados anonimizados, o tratamento deve observar integralmente as exigências aplicáveis a dados pessoais sensíveis. Mesmo quando a anonimização for considerada eficaz, recomenda-se a adoção de salvaguardas

adicionais, como controle de acesso, registro das operações, limitação do uso ao escopo da pesquisa, avaliação por comitês de ética e revisão periódica das técnicas de anonimização. Deve-se vedar expressamente tentativas de reidentificação, sujeitando-as à responsabilização.

Essas precauções visam mitigar o risco de reidentificação futura, que pode comprometer os direitos dos titulares e gerar insegurança jurídica quanto ao regime de proteção aplicável.

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Caso a base legal não seja o consentimento, o controlador precisa comprovar que inexistem alternativas menos invasivas para alcançar o objetivo. Se o tratamento se basear no consentimento, conforme detalhado anteriormente, este deve ser plenamente válido, o que implica, entre outros fatores, na oferta de uma opção funcionalmente equivalente para quem não deseja fornecer seus dados. A justificativa para sua adoção não pode se basear em mera conveniência operacional ou em um apelo genérico à inovação.

As implicações do uso dessa tecnologia ultrapassam a esfera da privacidade individual e alcançam o campo da discriminação sistêmica. Estudos demonstram que algoritmos de reconhecimento facial possuem uma performance menos acurada com determinados grupos sociais, como pessoas negras, mulheres e pessoas trans, resultando em vieses que podem levar a violações de direitos fundamentais, especialmente em contextos críticos como segurança pública e vigilância em massa.

No entanto, é válido destacar que esses desafios não são exclusivos de tecnologias de reconhecimento facial. Outras tecnologias biométricas e sistemas automatizados de tomada de decisão com base em dados pessoais sensíveis podem apresentar problemas similares. Assim, soluções normativas e técnicas não devem se restringir a uma tecnologia específica, sob pena de se tornarem insuficientes diante da evolução e diversificação de métodos de identificação e análise automatizada.

Diante disso, incluem-se entre as possíveis salvaguardas jurídicas e institucionais a realização prévia de RIPD e a condução de auditorias algorítmicas independentes para avaliar vieses, a proibição do uso da tecnologia para finalidades de altíssimo risco, como

vigilância indiscriminada, e a garantia do direito à revisão humana das decisões automatizadas. Do ponto de vista técnico, as mitigações incluem o treinamento dos modelos com dados demograficamente diversos e a preferência por sistemas descentralizados.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Na criação de sistemas de reconhecimento facial, a minimização de erros de identificação e garantia de maior qualidade dos resultados pode ser obtida através da utilização de meios técnicos preventivos, incluindo técnicas avançadas de aprimoramento da qualidade de algoritmos, tais como *multi-scale feature fusion* (processo que envolve a extração de imagens em diferentes escalas e resoluções, combinando-as para fornecer informações contextuais aos algoritmos) e *spatial attention* (processo que envolve direcionar a atenção para uma área específica e filtrar distrações, para ajudar a melhorar o foco em partes específicas de imagens).

Outras técnicas para garantir maior eficácia e confiabilidade de sistemas de reconhecimento facial podem envolver o aprimoramento de dados, alterando imagens com rotações e ajustes de brilho, para criar conjuntos de dados mais refinados; verificação de vida, de maneira a confirmar se há uma pessoa natural sendo reconhecida (evitando enganos por fotografias ou máscaras, por exemplo), inclusive através do uso de outros dados como reconhecimento de voz ou marcha; e aprimoramentos contínuos do desenvolvimento da qualidade de algoritmos, através de testes periódicos com seus resultados e eliminação de resultados duplicados, por exemplo.

Além da adoção de medidas de mitigação quando do desenvolvimento de sistemas de reconhecimento facial, é importante também considerar mecanismos corretivos a serem implementados na utilização prática desses sistemas. Neste sentido, auditorias periódicas e a supervisão dos resultados gerados pelos sistemas de reconhecimento facial (humana ou automatizada) são importantes para identificar eventuais vieses que necessitem de correção, de maneira a possibilitar intervenções tempestivas e evitar riscos de discriminação ilícita ou abusiva ou resultados errôneos.

De todo modo, a utilização de mecanismos preventivos e corretivos deverá observar a liberdade de iniciativa, o estado da arte da tecnologia disponível, possíveis limitações

técnicas e financeiras, bem como a viabilidade de adoção dessas medidas por diferentes tipos de agentes, de modo a evitar uma desproporcionalidade regulatória, capaz de gerar obrigações demasiadamente onerosas aos agentes.

Além disso, cumpre frisar que algumas das medidas para garantir maior acurácia dos dados coletados por sistemas de reconhecimento facial podem exigir novos dados; ou o tratamento de dados para novas finalidades, incluindo a prevenção e correção de vieses.

Neste sentido, é importante que a interpretação do princípio da necessidade/minimização previsto na LGPD não parta de uma interpretação meramente quantitativa, mas também qualitativa, de modo a compreender a necessidade de novos dados para o atingimento da finalidade de garantir maior acurácia e qualidade dos resultados obtidos. Com relação ao tratamento para novas finalidades, é importante que os agentes forneçam transparência adequada, observando-se o segredo comercial e industrial.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Em geral, a proibição *a priori* de tecnologias - como aquelas de reconhecimento facial - pode gerar riscos à inovação, à concorrência e mesmo à segurança e eficiência. Contudo, a utilização da tecnologia de forma indiscriminada também pode apresentar riscos, através de vieses discriminatórios abusivos ou ilícitos, usos abusivos (como perseguição de minorias ou limitação de liberdades individuais) e vigilância em massa violando a privacidade de indivíduos, por exemplo. Portanto, deve-se buscar um equilíbrio que possibilite eventuais restrições do uso de reconhecimento facial apenas em casos em que se verifiquem riscos concretos aos direitos e interesses de indivíduos, com base em critérios já estabelecidos em lei; e, em casos em que esses riscos não sejam claros, possibilitar a adoção de mitigações, a fim de garantir o fomento e o desenvolvimento de inovações tecnológicas e os benefícios que tais tecnologias podem representar.

A título de exemplo, o uso de tecnologias de reconhecimento facial em locais públicos, no âmbito da segurança pública, já foi considerado não-recomendado [pelas Diretrizes 05/2022 do Conselho Europeu de Proteção de Dados \(EDPB\)](#), que entende que o tratamento de dados biométricos neste contexto não equilibra adequadamente os interesses privados e públicos, representando uma interferência desproporcional nos

direitos dos titulares dos dados. Tal hipótese poderia ser uma situação não-recomendada também pela ANPD, dentro de suas competências (i.e., levando em consideração que a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais).

Por outro lado, a utilização de tecnologias de reconhecimento facial em locais privados - como em condomínios, para permitir o acesso de indivíduos -, ou para identificação/autenticação para acesso a determinados serviços e/ou combate à fraude (como em aplicativos de bancos, visando a segurança dos titulares), não necessariamente precisaria ser não-recomendada, podendo contar com medidas de mitigação de eventuais riscos que a aplicação da tecnologia pode representar. Neste caso, algumas medidas que podem ser tomadas pelos agentes de tratamento são:

- observar os princípios da necessidade e finalidade, tratando apenas os dados biométricos necessários para a finalidade exclusiva a que se referem, sem utilização desses dados para outras finalidades que não sejam previamente informadas aos titulares;
- nos casos em que isso seja factível, oferecer a possibilidade de que os indivíduos possam optar por outros meios menos invasivos para garantir o mesmo acesso, tais como a utilização de cartões ou tags, caso assim solicitem, de modo a não criar restrições excessivas condicionadas à coleta de dados pessoais sensíveis (o que poderia, inclusive, fragilizar a validade de eventual consentimento, caso esta fosse a base legal aplicável no caso concreto, em razão do descumprimento do requisito "livre");

[Obs.: no caso da utilização de tecnologias de reconhecimento facial para prevenção/combate à fraude, essa possibilidade não poderá ser fornecida aos titulares, já que seus direitos e liberdades fundamentais não prevalecerão em relação à finalidade de garantir segurança ao titular. Os agentes de tratamento poderão justificar o referido tratamento na base legal do art. 11, II, g da LGPD.]

- oferecer transparência aos titulares sobre o fato de que seus dados biométricos serão tratados, por meio da utilização de tecnologias de reconhecimento facial, para finalidades específicas, garantindo sua legítima expectativa com relação ao tratamento; e

[Obs.: no caso da utilização de tecnologias de reconhecimento facial para prevenção/combate à fraude, é importante que essa transparência equilibre o direito à informação com a garantia

da segurança dos titulares, de modo a evitar que agentes mal-intencionados possam utilizar essa transparência para burlar os sistemas de segurança e combate à fraude, por exemplo.]

- utilizar medidas de segurança técnicas e administrativas apropriadas, a fim de proteger os dados pessoais sensíveis tratados de eventuais acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Considerando que os dados biométricos são imutáveis e de alta sensibilidade, sua violação por meio de vazamentos ou uso indevido acarreta danos graves e, em muitos casos, irreparáveis, como o roubo de identidade e a exposição contínua do titular a riscos futuros. Por essa razão, sua proteção demanda a implementação de salvaguardas técnicas e administrativas de alto padrão, fundamentadas em uma análise de risco contínua, contextualizada e proporcional à criticidade do tratamento.

Ademais, tendo em vista que cada situação de tratamento envolverá características técnicas, operacionais e regulatórias distintas, é fundamental que as orientações da ANPD sejam suficientemente flexíveis, responsivas e adaptáveis à diversidade de contextos, permitindo soluções eficazes e proporcionais aos riscos identificados.

Dito isso, uma abordagem moderna e alinhada aos princípios da LGPD — especialmente os princípios da prevenção, da segurança e da necessidade — envolve o uso de Tecnologias de Aprimoramento da Privacidade aplicadas à biometria (*Biometric PETs*). Nesse sentido, por exemplo, a [norma ISO/IEC 24745/2022](#) estabelece um padrão internacional de segurança baseado em três pilares fundamentais:

- irreversibilidade para assegurar que o *template* biométrico não possa ser revertido para reconstruir a característica física original da pessoa;
- desvinculação para impedir que o *template* seja utilizado para rastrear o indivíduo em diferentes sistemas ou bases de dados, protegendo sua identidade contextual; e
- revogabilidade como forma de permitir que um *template* comprometido seja substituído, de forma funcionalmente análoga à troca de uma senha, o que é essencial diante da impossibilidade de "reemitir" uma biometria natural.

Adicionalmente, uma prática altamente recomendável, especialmente em dispositivos móveis ou aplicações sensíveis, é a verificação no dispositivo (*on-device*), que mantém o *template* armazenado localmente, sob controle direto do titular, minimizando riscos relacionados à transmissão e ao armazenamento em servidores centrais.

Essas medidas técnicas devem ser acompanhadas por uma governança organizacional robusta, que inclua:

- a elaboração de um RIPD, conforme o art. 38 da LGPD, para avaliar e mitigar os riscos específicos desse tratamento;
- a implementação de protocolos de resposta a incidentes que contemplem vazamentos de dados biométricos;
- realização de testes de segurança recorrentes, como testes de penetração, varreduras de vulnerabilidade e auditorias independentes; e
- o estabelecimento de processos formais de avaliação e revisão periódica das medidas adotadas, com registro documental, como forma de demonstrar a *accountability* da organização.

Por fim, é essencial que haja capacitação continuada das equipes técnicas e de governança sobre os riscos associados ao tratamento de biometria, bem como a adoção de uma cultura organizacional voltada à minimização do uso de dados sensíveis.

Nesse contexto, recomenda-se que a atuação da ANPD se concentre na emissão de orientações gerais que sirvam de referência para a implementação de boas práticas, sem engessar o desenvolvimento tecnológico. Isso permitirá que diferentes setores e agentes econômicos adaptem suas soluções de forma proporcional, segura e juridicamente responsável, incentivando, ao mesmo tempo, a inovação e a proteção de direitos fundamentais.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

O uso de dados biométricos em serviços não essenciais, especialmente quando fundamentado no consentimento, deve observar rigorosamente os princípios da autodeterminação informativa, da necessidade, da transparência e da não

discriminação. Trata-se de dados sensíveis e imutáveis, cujo tratamento exige justificativa proporcional e demonstração clara de indispensabilidade para a funcionalidade pretendida.

Por se tratar da principal base legal em contextos facultativos, o consentimento deve ser livre, informado, específico, destacado e inequívoco — e isso inclui garantir a real liberdade de escolha do titular. Assim, não basta apenas obter um “aceite” formal: é preciso assegurar que o titular compreenda de forma clara as implicações do uso de sua biometria e, sobretudo, que possa recusar esse tratamento sem sofrer prejuízos ou constrangimentos indevidos.

Nesses casos, é indispensável garantir que a recusa do titular em fornecer seus dados biométricos não resulte, por si só, em restrições indevidas ou em tratamento desproporcionalmente desfavorável. Funcionalidades centrais de um serviço — como navegação, compra ou pagamento em uma plataforma de e-commerce — não podem ter a autenticação biométrica como condição exclusiva de acesso. Ela pode ser oferecida como uma opção de conveniência, mas nunca como única via para fruição do serviço. Como orienta o [ICO do Reino Unido](#), condicionar o acesso a um serviço ao uso de biometria compromete a liberdade de escolha do titular e pode tornar o consentimento inválido.

A necessidade e adequação do tratamento, aqui, parecem ser elementos-chave. A autenticação biométrica apenas deveria ser exigida se for objetivamente indispensável à execução do contrato, o que demanda comprovação quanto a tal necessidade pelo controlador. Fora dessas hipóteses, o titular deveria sempre contar com alternativas equivalentes. Por exemplo, a autenticação por impressão digital poderia ser substituída por métodos como senha e token, o que, além de mitigar riscos, também promove a inclusão de pessoas que, por motivos físicos ou técnicos, não possam utilizar soluções biométricas.

Nesse contexto, a principal salvaguarda contra a discriminação no acesso a serviços é justamente a disponibilização de alternativas funcionais equivalentes, permitindo que a recusa ao tratamento de dados biométricos não se traduza em exclusão ou limitação de acesso. A ausência dessas alternativas pode configurar prática abusiva, ainda que disfarçada de exigência técnica.

Por fim, é importante destacar que, embora o princípio da não discriminação esteja previsto na LGPD, sua função principal não é definir a necessidade do dado para uma atividade de tratamento (requisito de cabimento do tratamento), mas sim impedir que os dados pessoais sejam tratados com finalidades discriminatórias (controle sobre a

finalidade do tratamento). Por isso, a proteção do titular, nesse cenário, deve se ancorar tanto no princípio da necessidade quanto no rigor do consentimento como base legal, exigindo a demonstração clara de que a coleta e o uso da biometria são estritamente necessários à finalidade pretendida, e que a concordância do titular foi obtida de forma genuinamente livre e informada.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

É sabida e irrefutável a sensibilidade envolvida no tratamento de dados biométricos, especialmente diante de seu potencial de identificação única e de impactos sobre direitos fundamentais. Todavia, também se reconhece que a LGPD adota uma abordagem baseada no risco, bem como o fato de que o tratamento de dados pessoais – ainda que restrito à categoria sensível “dados biométricos” – pode ocorrer em múltiplos contextos de uso. Por essa razão, é fundamental que recomendações de boas práticas preservem flexibilidade regulatória, de forma a contemplar a diversidade de cenários legítimos e fomentar inovação responsável, sem incorrer em engessamento normativo.

Nesse sentido, é essencial que eventuais diretrizes da ANPD sejam orientativas, e não prescritivas, permitindo adaptações conforme:

- a finalidade do tratamento;
- o grau de sensibilidade do contexto (por exemplo, autenticação versus vigilância);
- as tecnologias empregadas (biometria facial, impressões digitais, retina etc.); e
- a complexidade dos fluxos de dados e da cadeia de agentes envolvidos.

Adicionalmente, ainda que o tratamento de dados biométricos possa, em certas condições, resultar em discriminação ilícita e abusiva, é importante destacar que tais riscos não decorrem exclusivamente do uso de tais dados, tratando-se de um fenômeno com raízes sociais, jurídicas e institucionais mais amplas. No âmbito da proteção de dados, a LGPD pode – e deve – colaborar para a mitigação desses riscos, mas não constitui instrumento isolado suficiente para enfrentá-los de maneira estrutural. Assim, é desejável que a ANPD atue em articulação com outros órgãos públicos, reguladores setoriais e entidades da sociedade civil, promovendo uma abordagem transversal.

No contexto internacional, autoridades internacionais têm promovido um conjunto de boas práticas e salvaguardas técnicas e organizacionais que, embora não devam ser

copiadas de forma acrítica, oferecem referenciais úteis e que, ainda que não devam ser estabelecidos como obrigatórios em toda e qualquer situação, podem ser reconhecidos como fatores positivamente considerados pela autoridade:

1. RPID prévio e contínuo

O EDPB exige a realização de uma *Data Protection Impact Assessment* antes de qualquer tratamento biométrico com risco elevado ([Directive 05/2022](#) e Art. 35 do GDPR). O [ICO do Reino Unido](#) segue a mesma lógica para uso de biometria em vigilância e autenticação. Já o [Office of the Privacy Commissioner \(OPC\)](#) do Canadá recomenda integrar avaliações éticas e de risco antes da adoção de tecnologias sensíveis, estando, atualmente, em processo de discussão de um guia referente ao tratamento de dados biométricos.

No contexto brasileiro, seria desejável que a elaboração e o uso do RIPD fossem apontados não apenas como obrigação legal (arts. 32 e 38 da LGPD), mas reforce que sua elaboração, enquanto instrumentos estruturantes da boa governança, será positivamente considerado pela autoridade. Essa valorização não deve ser compreendida apenas como exigência formal, mas sim como mecanismo que reconheça e estimule controladores que adotem condutas diligentes e contextualizadas, inclusive com benefícios regulatórios indiretos, como:

- a demonstração documentada da proporcionalidade do tratamento;
- a fundamentação prévia de decisões automatizadas envolvendo biometria; e
- a mitigação de riscos reputacionais e legais mediante abordagem preventiva.

Ademais, a elaboração de RIPDs consistentes pode funcionar como critério de boa-fé e diligência nos processos fiscalizatórios, auxiliando a própria ANPD na diferenciação de práticas abusivas e de práticas fundamentadas em avaliações técnicas. Tal reconhecimento regulatório reforça a lógica da autorregulação incentivada, compatível com os artigos 50 e 55-J, inciso VII, da LGPD.

Assim, a sugestão concreta se resumiria à inclusão em eventuais diretrizes de uma ênfase explícita na importância estratégica do RIPD como elemento central das boas práticas no uso de biometria, e que esse documento seja valorizado como evidência de conformidade proporcional ao risco, fator atenuante em eventuais apurações e critério positivo de *accountability* organizacional.

2. Políticas de minimização

O princípio da minimização de dados é um dos pilares centrais das boas práticas internacionais em proteção de dados, estando expressamente previsto no artigo 5(1)(c) do GDPR e incorporado nas diretrizes interpretativas do EDPB. Ele também é

reconhecido em marcos técnicos, como a [*Special Publication 800-63-3 do National Institute of Standards and Technology \(NIST\)*](#), que orienta a configuração de sistemas biométricos com base na restrição do volume e da finalidade dos dados processados.

No Brasil, a LGPD já incorpora esse princípio de forma transversal, sobretudo no artigo 6º, inciso III, ao exigir que o tratamento de dados pessoais esteja claramente vinculado ao mínimo necessário para a realização de suas finalidades.

Nesse sentido, sugere-se que a ANPD estimule a adoção e valorização de políticas organizacionais que implementem concretamente a lógica da minimização e da estrita necessidade, inclusive como evidência de maturidade em governança e conformidade. Controladores que adotem tais práticas, de maneira documentada e auditável, demonstrariam não apenas adequação à LGPD, mas também:

- maior controle interno sobre os fluxos de dados e seus riscos associados;
- compromisso institucional com a autodeterminação informativa dos titulares; e
- capacidade de responder, com clareza, a questionamentos sobre a licitude e a proporcionalidade do tratamento.

Tais políticas poderiam incluir, por exemplo, limitações técnicas na captação e armazenamento de dados biométricos, definição de perfis de acesso restrito, eliminação automática de dados não utilizados, e vedação contratual ao uso secundário não previsto, configurando um modelo preventivo e autônomo de responsabilidade corporativa.

Dessa forma, propõe-se que eventuais diretrizes reconheçam expressamente que a implementação de políticas internas estruturadas de minimização e uso necessário constituirá critério positivo de avaliação regulatória, inclusive para fins de reconhecimento público, priorização em programas de cooperação, ou como atenuante em eventuais processos sancionatórios, quando demonstrada de forma transparente e consistente.

3. Incentivo a modelos treinados com dados representativos

Com o avanço exponencial da inteligência artificial, o tratamento de dados biométricos tem deixado de ser um processo puramente estático e passou a integrar modelos de aprendizado de máquina, sistemas de inferência probabilística e aplicações preditivas, especialmente no reconhecimento facial, de voz e de padrões comportamentais. Nesse novo cenário, a qualidade e a diversidade dos dados utilizados para o treinamento de modelos algorítmicos se tornaram elementos determinantes tanto para a precisão técnica, quanto para a prevenção de discriminações ilícitas e abusivas.

É extensamente sabido que bases de dados enviesadas ou não representativas do contexto local podem induzir sistemas (especialmente biométricos) a erros sistemáticos, frequentemente com recortes étnico-raciais, geracionais ou de gênero.

No Brasil, dada sua pluralidade étnica e regional, e sua posição ainda majoritariamente como consumidor de soluções tecnológicas globais, torna-se fundamental que a ANPD reconheça e valorize, de maneira explícita, iniciativas voltadas à personalização, adaptação e desenvolvimento de modelos biométricos treinados com dados representativos da realidade brasileira.

Esses esforços, todavia, não são triviais: exigem acesso a dados de qualidade, infraestrutura técnica (computação, curadoria, segurança), tempo, equipe especializada e, sobretudo, um ambiente jurídico-regulatório estável e colaborativo. A criação de incentivos para parcerias entre entes públicos e privados, centros de pesquisa e startups pode ser um caminho para viabilizar essa transformação.

Assim, sugere-se que a ANPD assuma um papel proativo não apenas como reguladora, mas como fomentadora de articulações interinstitucionais, promovendo parcerias público-privadas, diálogo com centros de pesquisa e startups nacionais, e estratégias cooperativas com outras agências do Estado (como BNDES, MCTI, CNPq e agências setoriais), de modo a estruturar um ambiente favorável ao desenvolvimento de bases de dados representativas e modelos treinados com responsabilidade, diversidade e transparência.

4. Transparência eficaz, não excessiva

A transparência é um dos fundamentos centrais da LGPD (art. 6º, inciso VI) e elemento estruturante do direito à autodeterminação informativa.

Contudo, no tratamento de dados biométricos – sobretudo quando apoiado em sistemas complexos como modelos de reconhecimento facial e inferência automatizada – a forma como se comunica com o titular é tão importante quanto o conteúdo comunicado.

Experiências internacionais demonstram que transparência ineficaz ou excessivamente técnica pode ser contraproducente. Entidades como EDPB, o ICO e o OPC orientam que a transparência deve ser funcional, contextualizada e segmentada, inclusive por meio de modelos de avisos em camadas ("*layered notices*") e comunicação multicanal, adaptados à complexidade do público e à natureza do tratamento.

No Brasil, essa lógica deve ser reforçada pela ANPD, reconhecendo que exigir transparência absoluta e tecnicamente densa pode inviabilizar a compreensão pelo público em geral, além de expor:

- segredos industriais e know-how proprietário, comprometendo a vantagem competitiva dos desenvolvedores e operadores de tecnologia; e
- elementos técnicos sensíveis, que poderiam ser explorados por agentes maliciosos para burlar ou manipular o sistema biométrico (por exemplo, engenharia reversa de padrões ou simulações de falsos positivos).

Portanto, recomenda-se que a ANPD valorize estratégias de transparência que privilegiem a clareza, a proporcionalidade e a efetividade comunicacional, respeitando o princípio da finalidade e a segurança operacional dos sistemas.

Além disso, devem ser reconhecidas como boas práticas:

- o uso de ícones visuais e avisos físicos em ambientes públicos (por exemplo, câmeras com reconhecimento facial em metrô ou estádios);
- a disponibilização de portais informativos acessíveis, com FAQs, vídeos explicativos ou simulações interativas; e
- a oferta de mecanismos padronizados de consulta e esclarecimento de dúvidas.

Assim, controladores que adotem modelos eficazes de comunicação com o titular seriam positivamente valorizados, por exemplo, por meio de inclusão em catálogos de boas práticas, programas de certificação, ou como indicadores de *accountability* robusta em processos de monitoramento regulatório.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

O tratamento contínuo e massivo de dados biométricos, especialmente em espaços públicos ou semipúblicos - como em iniciativas de cidades inteligentes, sistemas de transporte, monitoramento de multidões em estádios, centros comerciais e espaços urbanos - coloca desafios reais à efetivação dos direitos dos titulares e à concretização da autodeterminação informativa.

Antes de tudo, é importante recordar que, conforme o artigo 4º, inciso III da LGPD, o tratamento de dados pessoais realizado exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou repressão de infrações penais não está sujeito à LGPD, devendo ser regido por legislação específica. Nesses casos, eventuais

manifestações da ANPD devem respeitar essa limitação normativa, limitando-se a orientações principiológicas de proteção de direitos e boas práticas gerais, sem pretensão normativa direta sobre tais operações.

Nos casos em que o tratamento massivo de dados biométricos ocorra no âmbito da iniciativa privada ou de parcerias público-privadas, aplicando-se a LGPD, os desafios de transparência e controle individual devem ser enfrentados com soluções técnicas, jurídicas e institucionais coordenadas. Não é razoável esperar que a informação seja dada ou o consentimento seja obtido por meios convencionais em cada ponto de contato.

Diante disso, em casos de tratamento contínuo e massivo de dados, a autodeterminação informativa depende não apenas (e, possivelmente menos) dos controladores, mas também de iniciativas públicas de conscientização e educação em privacidade. Nesse sentido e das competências institucionais da ANPD (art. 55-J, especialmente o quanto estabelecido nos incisos III, VI, VII, VIII, X, XI e XXIII), parece-nos essencial que a autoridade atue como promotora ativa da construção de soluções institucionais, setoriais e tecnológicas que permitam o exercício eficaz dos direitos dos titulares em contextos de difícil transparência como, por exemplo:

- publicação de guias orientativos adaptados ao contexto urbano e coletivo;
- incentivo à criação de mecanismos automatizados e intuitivos de comunicação com o titular;
- articulação de parcerias público-privadas e interagências para implantação de plataformas conjuntas de governança informacional; e
- valorização de soluções escaláveis de informação e controle como fatores positivos na avaliação de conformidade regulatória.

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Os direitos e obrigações relativos à informação, ao acesso, à correção e à revogação do consentimento são aplicáveis a todos os dados pessoais. Contudo, a metodologia para garantir exigir adaptações e a implementação de formas e sistemas distintos conforme há fatores de risco, como o envolvimento de grupos vulneráveis como crianças e adolescentes. Assim, para garantir tais direitos durante o tratamento de dados de crianças e adolescentes é preciso assegurar que os menores de idade e seus responsáveis estejam igualmente bem-informados sobre o tratamento dos dados, assim como as formas de acessá-los, corrigi-los e de revogar o consentimento para tratá-los.

Nessa linha, é preciso assegurar que os menores de idade recebam informações sobre o tratamento de seus dados em uma linguagem clara e adequada à sua idade, como destaca a ICO, do Reino Unido, no documento "[Age appropriate design: a code of practice for online services](#)". Além disso, estimula-se a prática de fornecer informações em "pequenas porções" e de forma contextualizada quando o dado é coletado ou utilizado para facilitar a compreensão da informação.

Nessa linha, conforme as [Guidelines on transparency under Regulation 2016/679](#), do EDPB, o responsável pelo tratamento de dados de crianças deve assegurar que o vocabulário, o tom e o estilo da linguagem utilizada são adequados e têm significado para as crianças, para que a criança destinatária das informações reconheça que a mensagem/informação lhe é dirigida. Nessa linha, a criança não perde seu direito à informação e transparência sobre o tratamento de seus dados quando o consentimento é dado pelos seus responsáveis. Pelo contrário, a criança tem direito à essa transparência enquanto durar o tratamento de seus dados, reconhecendo-se que, nos casos de crianças muito novas e sem idades para serem alfabetizadas, as medidas de transparência também podem se dirigir aos responsáveis pela criança.

Similarmente, as [Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment](#) da *Personal Data Protection Commission* de Singapura recomendam que é necessário garantir que as crianças possam retirar o consentimento para o tratamento de seus dados pessoais com a mesma facilidade com que fornecem o consentimento para o tratamento de tais dados.

Por fim, é necessário que a informação seja clara e acessível ao responsável do menor de idade cujos dados serão tratados, de forma que é necessário garantir que a informação não chegou apenas à criança, mas aos seus responsáveis, para que o consentimento informado dos pais ou responsáveis seja possível. Mecanismos que permitam garantir que o responsável da criança efetivamente foi aquele que ofertou o consentimento são bem-vindos.

Em resumo, é necessário garantir a informação efetiva e clara aos menores de idade, a cada momento em que dados são coletados e tratados, em linguagem adequada e simples, independentemente de os responsáveis legais já terem ofertado o consentimento para o tratamento de tais dados. Em particular, a sensibilidade dos dados biométricos deve ficar clara, de forma que a definição e consequências do tratamento de dados biométricos seja adequadamente explicada ao titular e seus responsáveis em linguagem apropriada.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O tratamento de dados biométricos de crianças e adolescentes pode se dar em diversos contextos, seja no mundo físico ou digital. A participação informada de pais ou responsáveis legais, conforme prevista na LGPD e no Estatuto da Criança e do Adolescente (ECA), dependerá de como a relação entre o agente de tratamento se dá com os titulares crianças e adolescentes nestes contextos, de modo a garantir informações adequadas sobre o tratamento dos menores de idade aos pais e responsáveis legais, para que possam tomar decisões a respeito do tratamento ou assistir os menores em suas decisões, quando/se necessário, respeitada a autonomia progressiva desses titulares.

Com relação às hipóteses em que o tratamento de dados biométricos de crianças e adolescentes seria admissível, cumpre frisar que, tendo em vista a diversidade de contextos em que este tratamento pode ocorrer, a regulação de situações específicas em que esse processamento deveria ser permitido seria inviável, ou geraria o risco de não abarcar todas as possibilidades de tratamento, representando risco excessivo à inovação. Portanto, recomendamos uma abordagem diferente, que envolva a adoção de parâmetros que considerem o contexto do tratamento de dados biométricos desses titulares menores de idade, visando e/ou considerando a proteção de seu melhor interesse.

No que diz respeito às possíveis bases legais aplicáveis ao tratamento de dados biométricos de crianças e adolescentes, tal análise também dependerá do contexto em que os dados estão inseridos para a aplicação das hipóteses previstas no art. 11 da LGPD - observando-se o [Enunciado 01/2023](#) da ANPD, que permite a aplicação de quaisquer bases legais para o tratamento desses titulares, desde que observado seu melhor interesse.

Especificamente no caso de escolas e locais recreativos, mencionado expressamente na presente Tomada de Subsídios, cumpre notar que, embora a utilização de dados biométricos neste contexto possa representar benefícios - como controle de acesso, aumento de segurança ou mesmo identificação/autenticação, por exemplo -, tal tratamento deverá ser proporcional e ocorrer de forma protetiva, considerando a privacidade e os melhores interesses dos titulares envolvidos.

Neste sentido, o tratamento de dados biométricos de crianças e adolescentes em escolas e locais recreativos deverá:

- ser necessário e observar o princípio da necessidade/minimização;
- ocorrer apenas para finalidades específicas, legítimas e proporcionais, de modo a evitar abusos quando do tratamento (como, por exemplo, monitoramento por meio de tecnologias de reconhecimento facial para aplicação de multas a pais/responsáveis legais que não chegam no horário para buscar seus filhos, ou mesmo detecção de emoções que possam gerar discriminações, incluindo vieses raciais);
- ser precedido de transparência adequada, tanto aos menores quanto aos seus pais/responsáveis legais, sobre como seus dados estão sendo processados (como, por exemplo, informações sobre a coleta de imagens por meio de câmeras de reconhecimento facial, em quais espaços e para quais finalidades);
- contar com mecanismos de segurança técnicos e administrativos robustos, aptos a garantir a proteção dos dados biométricos de menores de idade; e
- ser suscetível a revisão, de modo a evitar consequências negativas a crianças e adolescentes, bem como permitir o exercício de outros direitos pelos titulares (incluindo oposição com relação ao processamento de seus dados neste contexto).

Em consonância com as [diretrizes da ICO](#), bem como com os critérios adotados pela ANPD para aferição de tratamentos de alto risco, é importante frisar que o tratamento de dados biométricos de crianças e adolescentes provavelmente levará à necessidade de elaboração de um relatório de impacto à proteção de dados pessoais (RIPD), caso seja realizado em larga escala e/ou afete significativamente interesses e direitos fundamentais.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Novamente, cumpre frisar que a LGPD permite o tratamento de dados pessoais de crianças e adolescentes com base em qualquer uma das hipóteses legais previstas na lei, não se limitando exclusivamente ao consentimento dos pais ou responsáveis. Essa interpretação foi reforçada pela ANPD no [Enunciado nº 01/2023](#), que dispõe que o tratamento de dados pessoais de crianças e adolescentes pode se fundamentar em qualquer uma das bases legais previstas nos artigos 7º e 11 da LGPD, desde que observado o princípio do melhor interesse da criança e do adolescente.

Ademais, não existe uma hierarquização entre as bases legais previstas na LGPD. Assim, não há uma base legal "preferencial" ou obrigatória, sendo necessária a adequação contextual, em que o agente de tratamento analisa elementos como a finalidade específica do tratamento, a natureza dos dados, os riscos envolvidos e o grau de maturidade dos titulares para escolher a base legal mais adequada no caso concreto.

Como referência internacional, a abordagem da [ICO](#) é semelhante, uma vez que permite o uso de variadas bases legais para o tratamento de dados de crianças, desde que haja clareza sobre a base escolhida e essa esteja alinhada com os princípios de necessidade, proporcionalidade e segurança.

Mais uma vez, a participação informada de pais ou responsáveis legais, conforme prevista na LGPD e no ECA, dependerá de como a relação entre o agente de tratamento se dá com os titulares crianças e adolescentes nestes contextos, de modo a garantir informações adequadas sobre o tratamento dos menores de idade aos pais e responsáveis legais, para que possam tomar decisões a respeito do tratamento ou assistir os menores em suas decisões, quando/se necessário.

É importante destacar que, com relação a adolescentes, levando-se em consideração que esses indivíduos possuem maior capacidade de discernimento e maturidade, é importante que tanto a aplicação de bases legais quanto a participação informada de pais e responsáveis com relação a titulares adolescentes observem sua autonomia e desenvolvimento progressivos, de modo a respeitar sua autodeterminação informativa, mesmo em situações envolvendo a coleta e utilização de dados sensíveis (como dados biométricos).

Em termos de medidas técnicas e organizacionais, os agentes de tratamento devem implementar mecanismos robustos para proteger os dados biométricos de crianças e adolescentes em razão da natureza dessas informações, incluindo por meio de controles/restrições de acesso, anonimização ou pseudonimização (quando possível), criptografia, treinamento periódico das equipes a respeito de boas práticas para o processamento dessas informações, revisão contínua da finalidade dos tratamentos e mecanismos de auditoria interna, por exemplo.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Inicialmente, cumpre frisar que a utilização de mecanismos de verificação, estimativa e/ou garantia de idade que funcionam por meio do fornecimento de dados biométricos podem ser utilizados em diversos contextos - incluindo plataformas digitais e jogos, mas não se limitando a este escopo -, que poderão representar mais ou menos riscos e exigir critérios mais ou menos robustos, a depender de uma análise contextual.

Note-se também que, no âmbito das bets, o [Tribunal de Justiça do Distrito Federal e Territórios \(TJDFT\) recentemente publicou decisão](#) esclarecendo que a NSX Brasil comprovou a implementação de sistemas de biometria necessários para impedir o acesso de menores de idade a casas de apostas online. Portanto, o próprio Judiciário entende que a utilização de mecanismos de garantia de idade por meio do fornecimento de dados biométricos seria possível e não seria proibida no contexto brasileiro.

Com relação ao princípio da necessidade, é imperioso reconhecer que não há uma incompatibilidade a priori desse princípio com a utilização de mecanismos de garantia de idade que utilizem dados biométricos para permitir ou bloquear acesso a e/ou continuidade de utilização de serviços. Essas ferramentas, sejam utilizadas de forma avulsa ou conjunta com outros mecanismos, podem ser compatibilizadas com o princípio da necessidade por meio do tratamento de dados biométricos estritamente necessários e visando finalidades específicas, evitando-se a utilização desses dados sensíveis para outras finalidades que não estejam associadas à garantia de idade.

Já com relação à compatibilização de mecanismos de garantia de idade que utilizem dados biométricos para permitir ou bloquear acesso a e/ou continuidade de utilização de serviços com o princípio do melhor interesse, é importante que as ferramentas utilizadas visem o melhor interesse dos menores de idade - como, por exemplo, evitar que tenham acesso a conteúdo impróprio para a sua faixa etária ou que estejam expostas a riscos incompatíveis com sua idade. Tal é o caso de mecanismos de estimativa de idade que permitem a identificação de contas de indivíduos que possuam indícios de serem administradas por crianças, de modo a tomar providências com relação a essas contas.

Por fim, os mecanismos de garantia de idade que utilizem dados biométricos para permitir ou bloquear acesso a e/ou continuidade de utilização de serviços deverão observar alguns critérios, incluindo:

- indicação de base legal apropriada para o processamento das informações sensíveis de crianças e adolescentes;
- observação do princípio da minimização, de modo a tratar apenas os dados estritamente necessários para as referidas finalidades (os quais podem envolver

- dados biométricos, como no caso de mecanismos de estimativa de idade, desde que proporcionais e voltados à proteção dos menores de idade);
- oferecimento de transparência a respeito do tratamento de dados biométricos de crianças e adolescentes para permitir acesso a e/ou continuidade de utilização de serviços;
 - utilização de mecanismos de segurança técnicos e administrativos robustos para a proteção desses dados pessoais, incluindo por meio de alinhamento de responsabilidades por meio de cláusulas contratuais com eventuais terceiros que forneçam serviços de garantia de idade por meio da utilização de dados biométricos; e
 - elaboração e manutenção de relatório de impacto à proteção de dados pessoais (RIPD), caso o tratamento neste contexto seja realizado em larga escala e/ou afete significativamente interesses e direitos fundamentais, incluindo por meio da documentação de justificativas para o uso desses mecanismos, os riscos envolvidos e as medidas adotadas para mitigá-los.

Resposta à Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos da Autoridade Nacional de Proteção de Dados

Agosto de 2025

São Paulo, 1º de agosto de 2025

Introdução à Tomada de Subsídios sobre Dados pessoais sensíveis - dados biométricos

O Idec - Instituto de Defesa de Consumidores é uma associação de consumidores sem fins lucrativos, criada em julho de 1987 e mantida por seus associados. A missão do Idec é a defesa dos consumidores, na sua concepção mais ampla, representando-os nas relações jurídicas de qualquer espécie, promovendo a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com total independência política e econômica.

O Idec atua nacionalmente representando consumidores e tem legitimidade reconhecida por autoridades do poder público. Em sua atuação nos temas de proteção de dados pessoais, o Idec mantém constante monitoramento de práticas de mercado que possam ferir direitos dos consumidores, especialmente no que tange ao aumento de sua vulnerabilidade.

Em que pese a justa preocupação de todas as partes em relação ao combate às fraudes e nas ações de segurança pública, cabe dizer que, em qualquer caso, a prática de coleta de dados sem informação clara quanto ao tratamento das informações pode violar direitos básicos do consumidor, ao qual é garantido o direito à segurança, à liberdade de escolha e à informação adequada e clara sobre os serviços prestados pela empresa, previstos no art. 6º, incisos I, II e III, do Código de Defesa do Consumidor. Ainda, a Lei Geral de Proteção de Dados (Lei nº. 13.709/2018) determina requisitos para o devido tratamento dos dados pessoais, impondo como seus princípios a adequação, necessidade e não discriminação. Para tanto, a Lei impõe que qualquer processo de tratamento de dados pessoais tenha uma base legal e seja proporcional, de acordo com as finalidades pretendidas, e norteados pela transparência e segurança a seus titulares.

A LGPD também diferencia dados pessoais de dados pessoais sensíveis. Dados pessoais sensíveis, de acordo com o art. 5º, I e II, são aqueles que dispõem *"sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"*, tendo seu tratamento mais restrito pela lei, inclusive em termos de bases legais que podem embasar o tratamento. Tal conceito de dados pessoais sensíveis também abrange a biometria facial, dado biométrico vinculado a uma pessoa natural, que identifica um indivíduo por meio de suas características faciais.

É particularmente preocupante, para este instituto, a disseminação indiscriminada da coleta de dados biométricos, que exigem especial cautela em sua utilização. Trata-se de dados pessoais sensíveis dos consumidores, sobre os quais qualquer operação sujeita-se à necessidade de consentimento livre, informado, específico e destacado do titular (art. 11, inciso I) ou justificado por outra base legal, nos termos da LGPD, de forma transparente ao consumidor.

Frise-se, ainda, que o uso desse tipo de informações requer um exame detido de proporcionalidade, no qual devem ser considerados os riscos aos cidadãos - como o risco de incidentes de segurança - em relação aos seus potenciais benefícios. Ou seja, havendo medidas de menor risco para os direitos de titulares de dados, essas devem ser tomadas.

Essa preocupação é central caso seja utilizada a base legal de prevenção a fraudes, já que o artigo 11, inciso II, alínea "g", dispõe que devem ser "resguardados os direitos mencionados no art. 9º desta Lei" e excetua a utilização dessa base legal "no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". Em se tratando de dados biométricos, essa preocupação é intensificada, visto que são dados únicos e que estão sendo tratados em sistemas (de reconhecimento facial) que vem sendo objeto de diversos questionamentos, inclusive em termos de sua moratória ou banimento.

A partir disso, cabe dizer que a prática da coleta de dados por meio de reconhecimento facial sem informação transparente e clara ao consumidor quanto ao tratamento das informações, assim como sem base legal válida e informada, viola direitos fundamentais do cidadão, garantidos pelo artigo 5º, incisos X e LXXIX, da Constituição Federal, estes sendo a intimidade, a vida privada, a imagem e a proteção de dados pessoais. Também viola direitos expressos no Código de Defesa do Consumidor, como segurança (artigo 6º, inciso I), o direito à liberdade de escolha (artigo 6º, inciso II), o direito à informação adequada e clara sobre os serviços prestados pela empresa (art. 6º, inciso III) e o direito a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais (Lei nº. 12.965/2014 - Marco Civil da Internet - art. 7º, inciso VIII).

Neste sentido, este Instituto e o centro independente de pesquisa InternetLab lançaram o Guia para uso responsável do Reconhecimento Facial pelo Setor Privado, que contém orientações sobre a necessidade de transparência sobre a coleta e armazenamento dos dados biométricos, informando a pessoa submetida ao reconhecimento facial, no mínimo, (i) todos os seus direitos, (ii) em quais hipóteses os dados serão compartilhados com terceiros, (iii) o prazo do tratamento e (iv) as condições de armazenamento das informações, entre outras. Por fim, consideramos que o mais importante é garantir que a pessoa que está sendo alvo do tratamento de dados tenha sempre uma alternativa menos gravosa, sem que isso inviabilize o acesso ao serviço ou à obtenção do produto.

Destaca-se que este Instituto, por meio de Ação Civil Pública (processo nº 1090663-42.2018.8.26.0100) ajuizada em face da ViaQuatro, responsável pela construção e manutenção da Linha 4 - Amarela do metrô de São Paulo, obteve decisão judicial favorável em segunda instância, com fixação de multa, contra a utilização de reconhecimento facial sem a expressa informação aos consumidores. Adotando posicionamento similar, em 2020, a Senacon (Secretaria Nacional do Consumidor) condenou a Hering por ter utilizado reconhecimento facial em sua loja no Shopping Morumbi, em São Paulo. O processo administrativo foi aberto após a Senacon ter conhecimento da notificação do Idec, que solicitou à empresa esclarecimentos sobre a adoção da tecnologia.

Aqui, também reiteramos nossa preocupação com o impacto desproporcional de sistemas de vigilância, como os de reconhecimento facial, sobre populações vulneráveis, especialmente pessoas negras e LGBTQIA+, permite afirmar que o sistema a ser implementado ofende o direito à igualdade e à não discriminação, entendidos aqui à luz das normas constitucionais (art. 5º, caput e XLI da CRFB) e dos tratados internacionais ratificados pelo Brasil (com destaque ao Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos).

Em relação às pessoas negras e trans, são muitos os casos, públicos e notórios, aqui e no exterior, nos quais os sistemas de reconhecimento facial resultaram em gravíssimos erros baseados na discriminação algorítmica¹.

As violações massivas à privacidade promovidas por tecnologias de vigilância afetam de maneira desproporcional crianças e adolescentes, para os quais as políticas devem ser adotadas tendo em vista o seu melhor interesse (art. 6º do ECA); e as pessoas negras, promovendo discriminação racial (art. 5º, caput e XLI da CRFB). De igual forma, pessoas trans também sofrem discriminação algorítmica.

Nesse sentido, a Lei Geral de Proteção de Dados estabelece que tratamento de dados pessoais, inclusive nos meios digitais, deve ter como fundamento o respeito aos direitos humanos, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º), sendo que a atividade de tratamento de dados pessoais deve observar o princípio da não discriminação (art. 6), do que decorre a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

O direito internacional dos direitos humanos também oferece insumos e ferramentas de análise quando se discute as relações entre privacidade e utilização de tecnologias como as de reconhecimento facial em espaços públicos ou outros espaços acessados pelo público.

¹ Linha do Tempo do Racismo Algorítmico: casos, dados e reações. Disponível em: <https://tarciziosilva.com.br/blog/destaques/posts/racismo-algoritmico-linha-do-tempo/>

A ofensa à privacidade repercute, ainda, em ofensas aos direitos à liberdade de expressão e à liberdade de associação e reunião, como interpretados à luz do Pacto Internacional de Direitos Civis e Políticos pelo Comitê de Direitos Humanos da ONU e pelas Relatorias Especiais da ONU sobre Liberdade de Reunião e sobre Liberdade de Expressão.

Nesse contexto, vale destacar ainda que a Relatoria Especial para Liberdade de Expressão da ONU já se manifestou no sentido de reconhecer o direito ao anonimato como um aspecto importante do direito à liberdade de expressão e à privacidade².

Ainda no tocante à liberdade de expressão, é importante destacar que o então relator especial para Liberdade de Expressão da ONU fez uma chamada em junho de 2019 em favor de uma moratória global imediata da venda, transferência e o uso de ferramentas de vigilância, o que inclui tecnologias de reconhecimento facial. Nesse sentido, o relator afirmou que

"ferramentas de vigilância podem interferir nos direitos humanos, desde o direito à privacidade e liberdade de expressão até os direitos de associação e reunião, crença religiosa, não discriminação e participação pública". E ainda não estão sujeitos a nenhum controle global ou nacional eficaz".³

Defendeu ainda que os Estados adotem salvaguardas nacionais que estejam de acordo com o direito internacional dos direitos humanos para proteger os indivíduos da vigilância ilegal, incluindo o desenvolvimento de mecanismos públicos que aprovem e supervisionem tecnologias de vigilância.

Conectadas aos riscos à liberdade de expressão, há também as ameaças à liberdade de associação trazidas pelo uso de reconhecimento facial em espaços públicos. A liberdade de associação e reunião pacífica, garantida pelo Artigo 20, parágrafo 1 da Declaração Universal dos Direitos Humanos (DUDH) e reforçada no Artigo 21 do PIDCP, no artigo 15 da Convenção Americana sobre Direitos Humanos e no Artigo 5(d), ix da Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial⁴.

O Relator Especial da ONU sobre Liberdade de Reunião e Associação Pacífica declarou que "deve ser proibido o uso de técnicas de vigilância para fins de vigilância indiscriminada e não direcionada daqueles que exercem seu direito de reunião e associação pacífica, tanto em espaços físicos quanto digitais"⁵.

² Relatório sobre criptografia, anonimato e a estrutura dos direitos humanos da Relatoria Especial para a liberdade de expressão, A/HRC/29/32, 22 de maio de 2015.

³ Disponível em: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736>

⁴ Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, 21 de dezembro de 1965, UN Treaty Series, vol. 660, p. 195.

⁵ A/HRC/41/41 17 de maio de 2019, para 57.

Em geral, as ameaças ao exercício desses direitos estão relacionadas ao efeito inibidor (ou efeito inibitório - em inglês, *chilling effect*) que pode ser causado pelo uso dessas tecnologias em espaços públicos ou acessíveis ao público e diz respeito à alteração do comportamento por indivíduos submetidos a monitoramento⁶. Por exemplo: o uso de tecnologias de reconhecimento facial durante protestos pode desencorajar as pessoas a participar desse tipo de movimentação e até mesmo facilitar o rastreamento e perseguição de ativistas, impactando negativamente o exercício da democracia participativa⁷.

Em termos de precaução, o Data Protection Impact Assessment (DPIA), que serviu de fonte inspiradora para a criação da ferramenta do relatório de impacto na LGPD, tem como objetivo a identificação, mitigação e prevenção de riscos e altos riscos aos titulares de dados.

Nesse sentido, assim como na regulação europeia, o relatório de impacto está intimamente associado a uma perspectiva de risco, ou seja, identificar, mitigar e, principalmente, prevenir riscos aos indivíduos e coletividades que possam ser afetados.

Percebe-se que, assim como na regulação ambiental, há uma grande preocupação com a prevenção, isto é, com a não ocorrência do dano, haja visto que muitas vezes os danos são irreparáveis. Portanto, a ideia fundamental por trás do relatório é um diagnóstico de prevenção e não de reparação.

Se o objetivo é prevenir danos irreparáveis, precisa ser feito anteriormente à tomada de decisões. Isso porque a identificação e avaliação dos riscos envolvidos deve ser feita de forma a instrumentar a tomada de medidas e ações que previnam sua ocorrência, podendo incluir ações que sejam, inclusive, a não adoção da tecnologia - no caso da identificação de riscos excessivamente altos e não mitigáveis, como é o caso do reconhecimento facial em locais públicos.

⁶ O relatório do Alto Comissariado das Nações Unidas para Direitos Humanos sobre o impacto de novas tecnologias na promoção e proteção dos direitos humanos no contexto de assembleias, incluindo protestos pacíficos, traz em seu parágrafo 34 que: O surgimento da **tecnologia de reconhecimento facial levou a uma mudança de paradigma** [...] pois aumenta drasticamente a capacidade de identificar todos ou muitos participantes em uma reunião de forma automatizada. Isso é particularmente problemático se a tecnologia de reconhecimento facial em tempo real for implementada, permitindo a identificação em tempo real, bem como a vigilância direcionada e o rastreamento dos participantes. **A identificação incorreta em tempo real também pode levar a intervenções indevidas em assembleias pacíficas pelas forças de segurança.** Os efeitos negativos do uso de tecnologia de reconhecimento facial sobre o direito de reunião pacífica podem ser de amplo alcance [...]. Muitas pessoas se sentem desencorajadas a se manifestar em locais públicos e expressar livremente suas opiniões, quando temem ser identificadas e sofrer consequências negativas. (Tradução livre, grifos nossos)

⁷ Para dar um exemplo, o Ministério do Interior na Índia, em fevereiro de 2020, prendeu 1100 pessoas que participaram de protestos pacíficos, identificando-as com o uso do reconhecimento facial. Ver India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP (em inglês).

Nesse sentido, para evitar que o RIPD se torne um arquivo protocolar para o *compliance*, estático e esquecido, deve servir como “uma ferramenta efetiva de governança de dados, que reflita uma análise dos tratamentos de dados realizados e ajude na tomada de decisões futuras”.⁸ Assim, qualquer ação tomada para prevenir e mitigar riscos deve ser tomada anteriormente à contratação da tecnologia e ao gasto e comprometimento público. Isso porque qualquer análise de risco *a posteriori* já está amarrada aos gastos e decisões tomadas anteriormente, sendo tendenciosa qualquer análise de risco realizada.

Ainda assim, independente das salvaguardas e mitigações que poderiam ter sido realizadas para a tecnologia em questão, os riscos aqui descritos oferecidos por essa vigilância constante, massiva e indiscriminada são insuperáveis, não sendo admissíveis que ameaças como essas aos direitos de igualdade, não discriminação, privacidade e liberdade de expressão e associação sejam apenas mitigadas. Nesse sentido, plataformas de videomonitoramento são – em si mesmo – uma violação dos direitos e das liberdades das pessoas⁹, logo, é incompatível com os direitos humanos, razão pela qual não deve ser utilizada.

Neste sentido é o posicionamento conjunto do Comitê Europeu de Proteção de Dados (EDPB) e da Autoridade Europeia para a Proteção de Dados (EDPS),¹⁰ que solicitam o banimento do uso de reconhecimento facial, identificação biométrica e outros mecanismos de vigilância em espaços públicos. A medida considera que tais sistema de inteligência artificial ferem direitos fundamentais em sua essência, razão pela qual não devem ser utilizados para fins de segurança pública.¹¹

É nesse sentido também que o Considerando 84 do GDPR estabelece que se os resultados da avaliação apresentarem um elevado grau de risco, sem que seja possível o atenuamento através de medidas adequadas, será necessário consultar a autoridade de controle antes de se proceder ao tratamento de dados pessoais. Em outras palavras, o RIPD não serve para assumir todo e qualquer risco de tratamento de dados pessoais, desde que adotadas certas salvaguardas, mas, também pode servir para concluir pela não adoção da tecnologia quando os riscos são excessivamente altos e incompatíveis com os direitos dos titulares.

⁸ GOMES, Maria Cecília O. Relatório de impacto à proteção de dados: Uma breve análise da sua definição e papel na LGPD. Revista do Advogado, São Paulo, n. 144, p. 174-183, nov. 2019. P. 14

⁹ TIRE MEU ROSTO DA SUA MIRA. Carta Aberta. Disponível em: <https://tiremeurostodasuamira.org.br/carta-aberta/> Acesso em: 01 de junho de 2022.

¹⁰ EUROPEAN DATA PROTECTION SUPERVISOR. EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. 2021. Disponível em: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en Acesso em 06 de jun. de 2022.

¹¹ GOMES, Sheley. Europa avança para o banimento do reconhecimento facial. **Carta Capital**, 2021. Disponível em: <https://www.cartacapital.com.br/blogs/intervozes/europa-avanca-para-o-banimento-do-reconhecimento-facial/> Acesso em 06 de jun. de 2022.

A LGPD tem como um de seus princípios a prevenção - a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII) -, que é, em grande medida, concretizado via a realização do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), visto que este tem como finalidade a prevenção e mitigação de riscos às liberdades civis e aos direitos fundamentais.

Por fim, vemos que é perceptível a incompatibilidade da captura e tratamento massivos de dados pessoais por sistemas de vigilância, como os de reconhecimento facial, com a legislação: por ser massivo e indiscriminado, não cumpre o requisito da finalidade específica, além de se mostrar desproporcional.

A LGPD incorporou em seu texto legal o conceito de proporcionalidade, enquanto juízo prévio necessário às atividades de tratamento de dados. Pela disciplina legal, sendo as atividades de tratamento de dados pessoais devem observar a finalidade, a adequação e a necessidade da medida, com vistas a restringir, o mínimo possível, o direito do titular.

É evidente que o tratamento massivo e indiscriminado de dados pessoais por meio de sistemas de monitoramento biométricos são desproporcionais.

Como se vê, a discussão sobre vigilância em espaços públicos representa uma limitação de diversos direitos humanos e fundamentais, desde a perspectiva constitucional e internacional.

É um fato, público e notório, reconhecido nacional e internacionalmente: os sistemas de vigilância biométrica têm reforçado a discriminação racial e não foram criados ou pensados para reconhecer padrões que não sejam de homens brancos. Em um país marcado e definido pelo racismo estrutural, a implementação destas tecnologias serve ao propósito discriminatório.

Contribuições do Idec:

Abaixo, o Idec apresenta respostas à Resposta à Tomada de Subsídios: Dados pessoais sensíveis - dados biométricos da Autoridade Nacional de Proteção de Dados

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo "dados biométricos", mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos - que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Todo dado pessoal vinculado a uma característica física do titular é considerado dado biométrico, incluindo atributos imateriais (como a voz), ou comportamentais, como o padrão de digitação e estilo de andar (também chamado de "*gait*")^[1]. Isso independe de o dado permitir uma identificação individual, como a íris ou a digital, ou apenas uma categorização genérica ou coletiva, como etnia ou gênero.

Diversos países tratam dados biométricos como sensíveis, exigindo proteção reforçada. A União Europeia, por meio do GDPR, define dados biométricos como

“dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos” [2]. A Austrália adota padrão semelhante e considera como dados biométricos o rosto, impressões digitais, íris, palma da mão, assinatura e voz [3]. Nos Estados Unidos, embora não haja norma federal, leis estaduais como a BIPA, em Illinois, impõe normas rígidas, como a proibição de comercializar essas informações [4]. Em todos os casos, há um ponto comum: a coleta e o uso desses dados devem estar fundamentados em finalidade clara, segurança reforçada e respeito aos direitos do titular.

Referências

[1] Hanisch, S., Arias-Cabarcos, P., Parra-Arnau, J., & Strufe, T. (2021). *Privacy-protecting techniques for behavioral biometric data: a survey*. Disponível em <<https://arxiv.org/abs/2109.04120>> Acesso em 08 jul. 2025.

[2] Cf. Art. 4, (14) <https://www.privacy-regulation.eu/pt/4.htm>

[3] Cf. [Biometric scanning | OAIC](#)

[4] Cf. [Biometric Information Privacy Act \(BIPA\) | ACLU of Illinois](#)

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Ainda que se utilize base legal fundamentada no inciso II do art. 11 da LGPD, controladores que tratam dados biométricos devem adotar práticas de transparência ativa que permitam ao titular compreender, antes da coleta, como e por que seus dados serão utilizados.

É necessário fornecer **aviso de privacidade claro**, com destaque para a natureza sensível dos dados e (i) descrição objetiva das finalidades do tratamento, como autenticação, segurança ou *marketing*, e inclusive as finalidades secundárias. (ii) Devem ser identificados o controlador e seus canais de contato, bem como (ii) a base legal que fundamenta o tratamento. Também é essencial indicar (iii) os direitos do titular (como acesso, correção, exclusão e revogação do consentimento) e os meios para exercê-los.

As informações também devem detalhar: (iv) a utilização de dispositivos de coleta de dados, incluindo especificações sobre o hardware e o software empregados; (v) quais dados são coletados, a forma de tratamento e as finalidades específicas para as quais são utilizados; (vi) o prazo e as condições de retenção, armazenamento e descarte, juntamente com as medidas de segurança adotadas; (vii) as hipóteses de

compartilhamento com terceiros; e (viii) eventuais riscos envolvidos no tratamento dos dados.

Tais informações devem ser apresentadas de maneira clara, acessível e destacada, evitando serem intrincadas em contratos de adesão, e podem ser veiculadas por meio de dispositivos visíveis como tablets, televisores ou placas nos locais de coleta, além de alertas indicando o uso da tecnologia e câmeras visíveis e facilmente identificáveis.

Essas exigências refletem preocupações já identificadas em estudos acadêmicos recentes. Bisztray et al. (2022), por exemplo, no artigo *"Emerging Biometric Modalities and their Use: Loopholes in the Terminology of the GDPR and Resulting Privacy Risks"* [1], evidenciam que a regulação vigente tende a oferecer menor proteção a certos atributos biométricos extraídos automaticamente (como expressões faciais, postura, idade aparente ou estado emocional) em comparação às modalidades clássicas de identificação, como impressão digital ou íris. Dantcheva et al. (2016) [2] denominam esses atributos de "traços suaves" (*soft biometric traits*), os quais, embora não permitam identificação direta, são amplamente utilizados para classificar, ranquear ou inferir características dos indivíduos, com potenciais impactos sobre sua autonomia e privacidade.

Adicionalmente, é imprescindível que haja a possibilidade de o titular ter acesso ao espaço, produto, serviço ou funcionalidade mesmo que não consinta com a coleta de seus dados biométricos, tendo em vista que uma considerável parte dos serviços não possui a biometria como finalidade do próprio serviço e plenamente aplicável a essa exceção da lei. Essa alternativa garante que o consentimento, quando aplicável, seja de fato livre e não condicionado à prestação do serviço, respeitando o direito à liberdade de escolha do consumidor [3].

O uso da biometria não deve ser obrigatório, salvo quando for parte integrante do próprio serviço ou para cumprimento das hipóteses permissivas do art. 11, inciso II da LGPD, e que o direito de escolha do titular deve prevalecer, com o controlador avaliando métodos menos invasivos de garantir a segurança e oferecendo alternativas que não envolvam o fornecimento de dados pessoais sensíveis. Profissionais de atendimento ao público devem estar cientes dessas políticas para prestar informações e sanar dúvidas.

Referências

[1] Bisztray, T., Gruschka, N., Bourlai, T., & Fritsch, L. (2021). *Emerging biometric modalities and their use: Loopholes in the terminology of the GDPR and resulting privacy risks*. In 2021 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1-5). IEEE. Disponível em <<https://arxiv.org/abs/2211.12899>> Acesso em 08 jul. 2025.

[2] Dantcheva et al. (2016) *apud* Bisztray, T., Gruschka, N., Bourlai, T., & Fritsch, L. (2021). *Emerging*

biometric modalities and their use: Loopholes in the terminology of the GDPR and resulting privacy risks. In 2021 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 2-3). IEEE. Disponível em <<https://arxiv.org/abs/2211.12899>> Acesso em 28 jul. 2025.

[3] DE MARI, João. *Moradora se recusa a cadastrar reconhecimento facial em condomínio; veja dilemas na implantação da tecnologia.* G1, 19 jul. 2025. Disponível em <<https://g1.globo.com/sp/sao-paulo/noticia/2025/07/19/moradora-se-recusa-a-cadastrar-reconhecimento-facial-em-condominio-veja-dilemas-na-implantacao-da-tecnologia.ghtml>>

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

A biometria comportamental exige tratamento tão, ou ainda mais, rigoroso quanto a biometria tradicional, pois ambas envolvem dados pessoais sensíveis, com direitos e deveres correspondentes. A jurisprudência e a atuação regulatória no Brasil já demonstraram a importância dessa diferenciação.

No caso Hering [1], foi constatada a coleta indevida de expressões faciais em provadores inteligentes, sem informação clara ou consentimento dos consumidores. De forma similar, o projeto ViaQuatro instalou câmeras em portas de trens para análise de reações emocionais sem o devido aviso de privacidade [2] e, em 2024, o TikTok foi multado em R\$23 milhões de reais no Maranhão por coletar e compartilhar dados biométricos faciais de usuários, incluindo menores, sem consentimento [3].

Como essas tecnologias dependem de variáveis contextuais e probabilísticas, há maior risco de falsos positivos ou negativos, o que impõe atenção redobrada ao princípio da qualidade dos dados [4]. O controlador deve assegurar que os dados coletados sejam exatos, pertinentes e atualizados, com mecanismos de correção e validação constantes.

No aspecto da segurança, a natureza contínua e muitas vezes invisível da coleta comportamental exige medidas específicas, como controle de acesso rigoroso, criptografia, gestão de riscos algorítmicos e auditoria constante dos sistemas. Além disso, deve haver transparência quanto aos critérios utilizados para identificação, permitindo que o titular compreenda as implicações de decisões automatizadas baseadas nesse tipo de biometria.

Referências

[1] IDEC. *Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial.* São Paulo,

26 ago. 2020. Disponível em
<<https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial>>

[2] IDEC. *Idec vence ação contra uso de reconhecimento facial e ViaQuatro é condenada a pagar indenização de R\$500 mil.* São Paulo, 12 mai. 2023. Disponível em
<<https://idec.org.br/release/idec-vence-acao-contra-uso-de-reconhecimento-facial-e-viaquatro-e-condenada-pagar>>

[3] CUTRIM, L. *TikTok é condenado pela Justiça do MA a pagar R\$ 500 a usuários no Brasil por coleta indevida de dados.* G1, 07 mar. 2024. Disponível em
<<https://g1.globo.com/ma/maranhao/noticia/2024/03/07/tiktok-e-condenado-pela-justica-do-ma-a-pagar-r-500-a-usuarios-por-coleta-indevida-de-dados.ghtml>>

[4] Alonso-Fernandez, Fernando, Julian Fierrez, and Javier Ortega-Garcia. "Quality measures in biometric systems." *IEEE Security & Privacy* 10.6 (2011): 52-62. Disponível em
<<https://arxiv.org/abs/2111.08704>> Acesso em 03 jul. 2025

BLOCO II – HIPÓTESES LEGAIS

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Deve-se estabelecer um conjunto normativo restritivo para exceção ao consentimento ao tratamento de dados biométricos. Sobretudo pela natureza sensível e invasiva da coleta desses dados, é necessário que o consentimento seja privilegiado em detrimento de outras bases legais, tal como protegido pela redação do art. 11 da LGPD. No entanto, sabe-se que o consentimento é, muitas vezes, sujeito à coleta "pró-forma", sem efetivo conhecimento e aceitação do usuário. A adoção de boas práticas é fundamental para que o consentimento não seja fornecido de forma desinformada e viciada pelos titulares.

Recomenda-se que os titulares permaneçam podendo ter acesso ao espaço, produto, serviço ou funcionalidade ainda que não consentam com a captura dos dados biométricos, quando possível. Ou seja, que se garanta uma alternativa aos usuários, independentemente da base legal mobilizada. É imprescindível que essa opção alternativa seja apresentada de maneira ostensiva ao titular de dados.

Além disso, a obtenção do consentimento deve ocorrer antes do início da coleta de dados biométricos e dependerá de uma ação positiva do titular.

É necessário que se mantenha a impossibilidade de tratamento de dados pessoais biométricos com base no legítimo interesse, em conformidade com o Guia de Legítimo Interesse da ANPD, tendo em vista que é necessária a vinculação do tratamento a um uso específico e que tal base legal não está presente no rol do art. 11, inciso II da LGPD, visto que dados biométricos são dados sensíveis (art. 5º, inciso II).

O Idec tem atuado ativamente contra o uso de reconhecimento facial em serviços de transporte público, como nas ações contra a ViaQuatro [1], Metrô de São Paulo, e o PL nº 865/2019 no Estado de São Paulo [2], que autorizava o uso de reconhecimento facial no Metrô e na CPTM, e foi vetado após articulação com parceiros. Além disso, tem feito um esforço para informar consumidores sobre seus direitos, como no caso de utilização de biometria em condomínios.

Referências

[1] IDEC. *Idec vence ação contra uso de reconhecimento facial e ViaQuatro é condenada a pagar indenização de R\$500 mil.* São Paulo, 12 mai. 2023. Disponível em <<https://idec.org.br/release/idec-vence-acao-contra-uso-de-reconhecimento-facial-e-viaquatro-e-condenada-pagar>>

[2] IDEC. *Organizações cobram veto total a PL de reconhecimento facial no Metrô de SP.* São Paulo,

09 mar. 2021. Disponível em
<<https://idec.org.br/idec-na-imprensa/organizacoes-cobram-veto-total-pl-de-reconhecimento-facial-no-metro-de-sp>>

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A base da “prevenção à fraude” (art. 11, II, g) só se aplica se houver necessidade, proporcionalidade e vínculo direto com a finalidade e a segurança da operação (art. 6º, incisos I, II, III e IV).

O trecho final da alínea “g” (*“exceto no caso de prevalecerem direitos e liberdades fundamentais do titular”*) deve ser interpretado de maneira ampliativa. Na prática do tratamento de dados biométricos para prevenção a fraudes, embora comum como forma de autenticação, expõe o titular a riscos irreversíveis, como fraudes por imitadores de voz ou *deepfakes*, e perda definitiva do controle sobre seus dados, caso vazem. Nesse sentido, esta base legal deve ser interpretada de maneira a não impor somente uma modalidade de autenticação, mas com o fornecimento de alternativas menos invasivas ao titular de dados.

Apesar disso, normas como a Resolução 738/2020 da ANATEL têm ido na contramão dessa cautela, permitindo que operadoras exijam a coleta de biometria facial para autenticação na contratação remota de serviços de telecomunicação, sem prever alternativas equivalentes [1]. Nesse sentido, o Idec questionou empresas como Claro, Vivo, Mercado Livre, BTG Pactual e Itaú por imporem o reconhecimento facial como condição para contratação ou cancelamento de serviços, acesso a contas ou reembolsos [2]. Defende-se que o consumidor não deve ser forçado a entregar seu dado biométrico, uma vez que há alternativas menos invasivas e com equivalente ou superior segurança na autenticação. Por isso, recomendamos que se privilegie a transparência e alternativas viáveis ao uso compulsório de dados sensíveis.

Ainda, é necessário que se fale em problemas de acessibilidade que podem inviabilizar o acesso a serviços que se utilizam de mecanismos. O uso obrigatório de tecnologias biométricas, como o reconhecimento facial, pode excluir pessoas com baixo letramento digital, que enfrentam dificuldades até mesmo com tarefas básicas. Segundo a pesquisa TIC Domicílios 2023, do Cetic.br [3], o Brasil demonstra baixa

habilidade digital geral da população, o que pode ser exemplificado por dados como: (i) somente 37% dos usuários de internet no Brasil instalou programas no computador ou aplicativos no celular ou (ii) 39% adotou medidas de segurança para privacidade.

Essa exclusão é ainda mais acentuada entre idosos, PCDs, pessoas racializadas, pessoas com baixa escolaridade e moradores de áreas rurais. Relatos de problemas no uso do reconhecimento facial em situações como acesso à plataforma Gov.br ou nos cadastros em apps como Ifood [4] mostram que muitos usuários não conseguem operar adequadamente essas ferramentas, enfrentando falhas técnicas ou constrangimentos. Assim, em paralelo ao conceito de conectividade significativa, a autodeterminação informativa vai além do acesso e concessão de dados pessoais. Ela requer a capacidade de uso efetivo da tecnologia; por isso, exigir biometria sem oferecer alternativas acessíveis pode reforçar desigualdades e violar direitos básicos de acesso a serviços, incluindo a serviços públicos.

Os brasileiros se preocupam com o fornecimento de seus dados biométricos em maiores proporções do que com outros tipos de dados pessoais sensíveis, tais como orientação sexual e cor ou raça. É o que revela a 2ª edição da pesquisa "Privacidade e proteção de dados pessoais: perspectivas de indivíduos, empresas e organizações públicas no Brasil" [5], lançada pelo Comitê Gestor da Internet no Brasil (CGI.br). Segundo o estudo, 32% dos usuários de Internet com 16 anos ou mais no país relataram ficar "muito preocupados" e outros 28% "preocupados" diante desse tipo de situação – juntas, as proporções alcançam 60%. Entre os usuários que mencionaram essa preocupação em fornecer dados biométricos, a percepção de risco está associada com maior frequência à impressão digital e ao reconhecimento facial, cuja soma da porcentagem de indivíduos "preocupados" e "muito preocupados" alcançou 86% e 82%, respectivamente.

O estudo também mostra que as organizações para as quais os usuários mais ficam apreensivos em fornecer dados biométricos são: instituições financeiras (37% "muito preocupados" e 36% "preocupados"), órgãos de governo (35% e 38%) e transporte público (34% e 37%).

Salientamos que a mudança da coleta de biometria facial para íris, ou voz, ou digital, tampouco é uma medida de segurança a longo prazo, visto que apenas torna uma corrida entre mecanismos de segurança e golpistas que se utilizam de tecnologias cada vez mais complexas e capazes de coletar, processar e imitar dados biométricos, exigindo dos titulares informações biométricas cada vez mais sensíveis e invasivas, como a íris.

É indispensável, nesse sentido, prever alternativas não biométricas ao acesso, garantir que o titular não seja obrigado a fornecer dados sensíveis e implementar salvaguardas como criptografia, controle de acesso, RIPD e auditorias, sobretudo

quando envolver tratamento em larga escala. Isso não exclui a possibilidade da utilização de dados sensíveis, mas garante escolha ao titular para que, na sua autodeterminação informativa, opte pela modalidade que mais lhe é adaptada. Tal alternativa é essencial para proteger liberdades e direitos e, inclusive, prevenir discriminação e inclusive exclusão indevida no acesso a serviços, sejam serviços no mercado (o que poderia inclusive gerar uma violação do Código de Defesa do Consumidor, constituindo uma recusa indevida de prestação do serviço) ou serviços públicos e de interesse público.

Recomenda-se, então, a adoção de **critérios** como (i) necessidade de comunicação prévia à ANPD para utilização desse mecanismo, sobretudo em tratamentos de larga escala ou com outras características que agravem a vulnerabilidade dos titulares; (ii) apresentação de eficiente e adequado sistema de segurança de armazenamento dos dados; (iii) a oferta de meio alternativo de acesso a produto, serviços e funcionalidade, se possível sem a coleta de dados sensíveis.

Referências

[1] BRASIL. Agência Nacional de Telecomunicações. *Resolução nº 738, de 21 de dezembro de 2020. Altera o Regulamento dos Serviços de Telecomunicações para incluir disposições sobre sigilo, prevenção à fraude e ações de apoio à segurança pública, e dá outras providências*. Diário Oficial da União: seção 1, Brasília, DF, p. 179, 24 dez. 2020. Disponível em: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1495-resolucao-738>. Acesso em: 03 jul. 2025.

[2] IDEC. *Denúncias de consumidores faz Idec notificar cinco empresas por uso obrigatório de biometria facial*. São Paulo, 28 nov. 2023. Disponível em: <https://idec.org.br/release/denuncias-de-consumidores-faz-idec-notificar-cinco-empresas-por-uso-obrigatorio-de-biometria>. Acesso em: 03 jul. 2025.

[3] CETIC.br. *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2023*. São Paulo : Comitê Gestor da Internet no Brasil, 2024. Disponível em https://cetic.br/media/docs/publicacoes/2/20241104102822/tic_domicilios_2023_livro_eletronico.pdf. Acesso em 25 jul. 2025.

[4] MAGALHÃES, J. Justiça condena iFood a indenizar entregador do DF por danos morais após 'falha racista' em reconhecimento facial; entenda. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2025/06/30/justica-condena-ifood-a-indenizar-entregador-do-df-por-danos-morais-apos-falha-racista-em-reconhecimento-facial-entenda.ghtml>. Acesso em 31 jul. 2025.

[5] [CETIC.br](https://cetic.br). *Privacidade e proteção de dados pessoais: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em <https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2023/> Acesso em 31 jul. 2025.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

A primeira diretriz diz respeito à **transparência ativa**: é essencial que os titulares sejam informados, de forma clara, acessível e destacada, sobre os dados que serão coletados, as finalidades específicas do tratamento, os prazos de retenção, as condições de armazenamento, as medidas de segurança adotadas, as hipóteses de compartilhamento com terceiros e os riscos envolvidos.

Essa comunicação deve ser feita antes do início da coleta, de maneira visível e com profissionais capacitados para prestar esclarecimentos. Um estudo de Agrawal et al. (2020) [1] demonstra como arquiteturas públicas de dados devem ser construídas com base em princípios de finalidade limitada, controle de acesso e supervisão contínua, assegurando que o tratamento de dados sensíveis como biometria ocorra de forma ética e proporcional.

Outro aspecto fundamental refere-se à segurança. Devido à natureza imutável dos dados biométricos, que não podem ser alterados ou revogados após um acidente de segurança, os sistemas utilizados pelos controladores devem adotar medidas técnicas reforçadas, como criptografia em repouso e em trânsito, controle de acesso baseado em níveis de sensibilidade, gestão de riscos e de incidentes, bem como protocolos de notificação imediata em caso de violação. Nesse sentido, o trabalho de Grierson et al. (2024) [2], *A Framework for the Security and Privacy of Biometric System Constructions under Defined Computational Assumptions*, propõe um modelo técnico que integra segurança criptográfica modular com garantias formais de privacidade, adequado a ambientes públicos e altamente sensíveis.

Além disso, é indispensável garantir que o exercício dos direitos previstos na LGPD esteja plenamente acessível aos titulares, o que exige a criação de canais diretos de atendimento e exercício de direitos, prazos razoáveis e procedimentos transparentes para acesso, correção, oposição, exclusão e portabilidade de dados.

Por fim, a adoção da biometria no setor público deve ser precedida de análise prévia de proporcionalidade, na qual a entidade responsável deverá demonstrar a estrita necessidade da coleta de dados biométricos para o cumprimento da obrigação legal, a inviabilidade de métodos alternativos menos intrusivos e as salvaguardas adicionais que serão adotadas para proteger os direitos dos titulares.

Referências

[1] Agrawal, P., Singh, A., Raghavan, M., Sharma, S., & Banerjee, S. (2020). *An operational*

architecture for privacy-by-design in public service applications. Disponível em: <https://arxiv.org/abs/2006.04654>. Acesso em 08 jul. 2025.

[2] Grierson, S., Buchanan, W. J., Thomson, C., Galeb, B., & Eckl, C. (2024). *A Framework for the Security and Privacy of Biometric System Constructions under Defined Computational Assumptions*. Disponível em: <https://arxiv.org/abs/2411.17321>. Acesso em 08 jul. 2025.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, "c", LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

Mesmo para esse tipo de tratamento haja previsão de anonimização "sempre que possível", a anonimização por si só não elimina completamente os riscos ou as obrigações do controlador.

A coleta e o processamento inicial da biometria já configuram tratamento de dados pessoais sensíveis, e dados anonimizados ainda podem ser utilizados para formar perfis comportamentais de pessoas identificáveis. Informações como vetores faciais, padrões de íris ou digitais, mesmo sem identificação nominal, podem ser reconectadas a indivíduos com o uso de outras bases, técnicas estatísticas ou inteligência artificial. Nesses casos, o uso para fins acadêmicos ou científicos não elimina o dever de adotar medidas rigorosas de proteção e o respeito aos direitos dos titulares.

Assim, salvaguardas adicionais são essenciais, das quais se pode destacar a minimização dos dados coletados ao estritamente necessário, transparência completa e acessível sobre todo o ciclo de vida dos dados aos titulares, a implementação de mecanismos de segurança robustos como criptografia e controle de acesso e medidas ativas para prevenir viés algorítmico e discriminação, somadas às citadas na resposta anterior.

Além disso, destaca-se a vedação à exploração comercial dos dados sob pretexto de pesquisa, a obrigação de respeito à finalidade original do tratamento, a impossibilidade de repasse a terceiros não envolvidos diretamente na pesquisa e a necessidade de garantia de que os dados não serão usados para decisões pessoais, comerciais ou administrativas em relação aos titulares.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

A utilização das tecnologias de reconhecimento facial (Facial Recognition Technologies, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento.

Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

- 8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?**

O uso de tecnologias de reconhecimento facial para vigilância em espaços públicos e privados não pode ser normalizado sob pretexto genérico de segurança. A coleta

de dados biométricos em locais de circulação comum, como estações de metrô, ruas ou shoppings, não necessariamente ocorre para fins estritamente relacionados à segurança pública, exceção prevista pela LGPD.

Esse problema se intensifica quando infraestruturas privadas se apropriam da função de segurança pública, utilizando a vigilância biométrica como instrumento de gestão, sem a mediação ou qualquer controle estatal.

Diante desse vácuo regulatório, cabe à ANPD não apenas garantir a aplicação estrita da LGPD, mas também orientar o poder público e o setor privado sobre os limites legítimos da vigilância em espaços públicos e semipúblicos. Em contextos em que o uso de tecnologias invasivas avança mais rapidamente do que a regulamentação, é dever da Autoridade atuar de forma proativa, evitando a consolidação de práticas abusivas sob o argumento de que "já estão em uso". A ausência de regulação não deve ser confundida com permissão.

No uso de tecnologia de reconhecimento facial, é preciso garantir que o titular tenha conhecimento deste tratamento de dados pessoais e que existam medidas antidiscriminatórias ativas no tratamento e processamento desses dados pessoais.

Na prática, as câmeras ou outros mecanismos de captura de dados devem ser instalados em locais que permitam a obtenção do consentimento prévio dos titulares. Isso significa dizer que o titular deve ter a opção de não estar sujeito à coleta de sua imagem, sem que isso implique o cerceamento de outros direitos, como o de acesso a bens e serviços ou ao seu fácil deslocamento [1]. No metrô de São Paulo, a concessionária ViaQuatro instalou painéis publicitários equipados com câmeras que captavam imagens dos rostos dos passageiros para fins de análise de expressões faciais e direcionamento de anúncios. O caso ilustra uma prática que desrespeita a liberdade de escolha do titular, e a Justiça determinou que a coleta foi abusiva, diante da ausência de alternativas e da violação aos direitos de privacidade e autodeterminação informativa.

Uma vez coletadas as imagens e delas extraídas as características desejadas, as imagens devem ser permanentemente excluídas, de forma que não seja possível, nem pelos desenvolvedores do sistema, seu posterior resgate. Além disso, todos os dados armazenados permanentemente e/ou apresentados para os operadores do sistema devem ser anonimizados (por exemplo, somente devem ser expostos dados volumétricos, gráficos e similares).

Kieslich e Lünich (2024) [2] argumentam que a ausência de governança robusta sobre esses sistemas pode resultar em práticas abusivas e discriminações sistêmicas, especialmente no setor público e em espaços de circulação obrigatória. Para evitar discriminação, devem-se implementar medidas antidiscriminatórias ativas que previnam vieses algorítmicos e taxas de erro desiguais para grupos

vulneráveis, testando a acurácia do sistema e garantindo que a tecnologia não impeça o acesso a serviços essenciais ou leve à negação de bens/serviços, variação de preços ou condições desvantajosa. Um estudo do MIT mostrou que sistemas de reconhecimento facial tinham taxa de erro de 0,8% para homens brancos e até 34,7% para mulheres negras (Hardesty, 2018) [3].

Por fim, sem prejuízo do emprego de outras medidas de segurança, recomenda-se que todo armazenamento de imagens de rostos se dê em ambientes seguros e criptografados, separados logicamente dos ambientes onde os dados anonimizados são armazenados. Preferencialmente, o armazenamento de dados biométricos deve ocorrer em ambientes *offline*, com conexões criptografadas sempre que houver necessidade de acesso remoto. Como exemplo de boa prática, tem-se um exemplo no Face ID da Apple [4], que realiza o processamento local dos dados diretamente no dispositivo, sem transferência para servidores externos ou armazenamento em nuvem.

Referências

[1] Cf. Idec e InternetLab lançam guia para uso responsável do reconhecimento facial. <https://idec.org.br/noticia/idec-e-internetlab-lancam-guia-para-uso-responsavel-do-reconhecimento-facial>

[2] Kieslich, K., & Lünich, M. (2024). *Regulating ai-based remote biometric identification. investigating the public demand for bans, audits, and public database registrations*. In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (pp. 173-185). Disponível em: <https://arxiv.org/abs/2401.13605>. Acesso em 10 jul. 2025.

[3] Hardesty, L. *Study finds gender and skin-type bias in commercial artificial-intelligence systems*. MIT News Office, 11 fev. 2018. Disponível em: <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>. Acesso em 07 jul. 2025.

[4] Cf. Sobre a tecnologia avançada do Face ID <https://support.apple.com/pt-br/102381>

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Para responder esse questionamento, retomamos a Carta da campanha Tire Meu Rosto da Sua Mira:

"Independentemente das salvaguardas e correções que poderiam ser propostas para a criação de uma tecnologia alegada e supostamente "livre de erros", essa

vigilância constante, massiva e indiscriminada é – em si mesma – uma violação dos direitos e das liberdades das pessoas. Por estarmos falando de mecanismos aplicados de forma incompatível com os direitos humanos, pedimos pelo banimento, e não apenas por uma moratória, do reconhecimento facial no contexto da segurança pública"

Quando há sub-representação de determinados grupos, o sistema tende a falhar com eles, reproduzindo discriminações e desigualdades [1]. Durães (2024) relata que, em Sergipe, um homem negro foi preso por engano em um estádio após ser confundido por um sistema de reconhecimento facial. Em outro caso, uma mulher negra foi abordada três vezes em uma micareta, também por erro do sistema. Com receio de contribuírem para práticas discriminatórias e a escalada da violência institucional, intensificada pela repercussão internacional do assassinato de George Floyd, gigantes da tecnologia como IBM, Microsoft e Amazon decidiram interromper a venda dessas soluções a forças policiais e entidades governamentais (Idec, 2022). Esses exemplos evidenciam que, mesmo quando alegadamente "aperfeiçoados", os sistemas de reconhecimento facial operam em contextos que favorecem a reprodução de desigualdades estruturais.

Na prática, isso exige providências não somente daqueles que usam o sistema, mas também daqueles que o desenvolvem. Assim, devem ser adotadas medidas de controle, teste e correção dos algoritmos para averiguar se tais informações têm influência nos resultados do sistema, além de esforço e treinamento ativo de todos os envolvidos na cadeia de desenvolvimento e utilização do sistema.

Além disso, testes contínuos e avaliações independentes devem ser considerados indispensáveis. Os algoritmos devem ser validados por terceiros, com métricas auditáveis e em condições variadas, como diferentes níveis de luz, ângulos e resoluções de imagem. Métricas como a taxa de falsos positivos e falsos negativos devem ser monitoradas em tempo real, com atualização constante do sistema. Também é fundamental restringir o uso dessa tecnologia a contextos controlados e finalidades bem delimitadas. Ambientes estáveis, como sistemas de autenticação pessoal em áreas restritas, oferecem menos variáveis externas (como iluminação) e maior previsibilidade, o que favorece a precisão. Já a aplicação indiscriminada em espaços públicos aumenta substancialmente a margem de erro e os danos potenciais [2].

A confiabilidade de sistemas automatizados exige, ainda, que decisões com impactos significativos não sejam tomadas exclusivamente por máquinas. A LGPD estabelece em seu art. 20 que o titular tem direito à revisão de decisões automatizadas, o que impõe ao controlador a obrigação de incluir mecanismos de intervenção humana qualificada [3]. Quando ocorrem erros, é essencial que existam

canais de contestação acessíveis, procedimentos formais para revisão de casos e prazos claros para correção. Também devem ser previstos registros sistemáticos (*logs*) de todas as decisões automatizadas, inclusive das falhas, para garantir auditabilidade e responsabilização.

Referências

[1] Cf. <https://tiremeurostodasuamira.org.br/carta-aberta/>

DURÃES, U. *Reconhecimento facial: erros expõem falta de transparência e viés racista*. São Paulo, 28 abr. 2024. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/04/28/reconhecimento-facial-erros-falta-de-transparencia.htm>. Acesso em 03 jul. 2025.

IDEC. *Parlamentares de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos*. São Paulo, 20 jun. 2022. Disponível em: <https://idec.org.br/release/parlamentares-de-todas-regioes-do-brasil-apresentam-projetos-de-lei-pe-lo-banimento-do>. Acesso em 14 jul. 2025.

[2] Cf. *Idec e InternetLab lançam guia para uso responsável do reconhecimento facial*. <https://idec.org.br/noticia/idec-e-internetlab-lancam-guia-para-uso-responsavel-do-reconhecimento-facial>

[3] **Art. 20.** *O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.*

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Sim. Diferentemente de senhas, PINs ou endereços de e-mail que podem ser alterados após um vazamento, os dados biométricos são imutáveis e característicos de uma pessoa, agravando as consequências de um potencial vazamento causado por problemas de segurança da informação [1]. Logo, o uso dessas tecnologias deve ser evitado quando a coleta é obrigatória ou compulsória e não oferece alternativas menos intrusivas ao titular, violando o direito à liberdade de escolha e à proteção de direitos fundamentais do titular.

Isso porque, como já afirmado diversas vezes nesta contribuição, o reconhecimento facial expõe os titulares ao risco de discriminação ilícita ou abusiva, sobretudo contra grupos vulneráveis como pessoas negras, que apresentam maiores índices

de falha na verificação biométrica. Também é desaconselhável seu uso quando o reconhecimento de emoções é utilizado para tomada de decisões importantes que afetam a vida das pessoas, dada a questionável acurácia dessa funcionalidade [2].

Ambientes escolares, por exemplo, não configuram contextos apropriados para a aplicação dessa tecnologia. A assimetria de poder entre instituição e alunos, o caráter compulsório da presença e a formação ainda em desenvolvimento da personalidade indicam que o reconhecimento facial ali tende a ferir princípios como o da necessidade, da adequação e do livre consentimento. Um exemplo recente é o caso do Paraná, onde o Ministério Público ajuizou ação civil pública pedindo indenização de R\$15 milhões por supostas irregularidades na coleta de dados biométricos de estudantes da rede pública estadual, apontando violação à LGPD [3]. O mesmo raciocínio se aplica ao monitoramento de trabalhadores em tempo integral por meio de reconhecimento facial. A expectativa legítima de privacidade no ambiente de trabalho e o desequilíbrio na relação contratual tornam essa prática desproporcional.

Espaços públicos acessíveis à ampla circulação de pessoas, como praças, ruas e transporte coletivo, também impõem graves restrições. Um exemplo disso ocorreu no caso da Via Quatro, empresa responsável pela Linha 4-Amarela do Metrô de São Paulo, já relatado anteriormente [4]. A ação resultou em decisões judiciais favoráveis à proteção dos dados pessoais dos usuários.

O rastreamento massivo também pode ter efeito inibidor sobre a liberdade de expressão e reunião, fragilizando o tecido democrático. Na Eslovênia, recursos como reconhecimento facial e análise de atividades em redes sociais foram utilizados pelas autoridades para identificar e exercer pressão sobre participantes de manifestações pacíficas [5].

Por se tratar de atividade eminentemente sensível e de elevado risco social, alternativas menos invasivas que a biometria, mas ainda eficazes, podem ser adotadas. Tecnologias de autenticação multifatorial (como a combinação de senha com verificação via aplicativo [2FA] ou *token* físico) oferecem segurança em operações sensíveis sem recorrer a dados biométricos. Cartões de identificação com chips criptografados, controle de acesso com *QR codes* temporários e sensores de proximidade são exemplos viáveis em ambientes corporativos ou institucionais.

O Hospital Israelita Albert Einstein, por exemplo, adotou cartões RFID para controle de acesso e rastreamento de ativos, alegadamente reduzindo perdas operacionais e otimizando processos logísticos, sem depender da coleta de dados biométricos dos profissionais ou pacientes [6]. Tais mudanças foram implementadas após este mesmo Hospital sofrer com problemas de falta de controle de acesso e possíveis

acidentes de segurança, noticiados na mídia [7].

Referências

- [1] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. *Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas*. InternetLab/IDEC, São Paulo, 2020, p. 49. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf. Acesso em 14 jul. 2025.
- [2] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. *Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas*. InternetLab/IDEC, São Paulo, 2020, p. 10. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf. Acesso em 14 jul. 2025.
- [3] G1. *Ministério Público pede indenização de R\$15 milhões por supostas irregularidades no reconhecimento facial de alunos de escolas públicas no Paraná*. Curitiba, 29 abr. 2025. Disponível em: <https://g1.globo.com/pr/norte-noroeste/noticia/2025/04/29/mp-pede-indenizacao-supostas-irregularidades-reconhecimento-facial-de-alunos-pr.ghtml>. Acesso em 04. jul. 2025.
- [4] IDEC. *ViaQuatro é condenada por reconhecimento facial no Metrô de SP*. São Paulo, 11 mai. 2021. Disponível em: <https://idec.org.br/idec-na-imprensa/viaquatro-e-condenada-por-reconhecimento-facial-sem-autorizacao-no-metro-de-sp>. Acesso em 04 jul. 2025.
- [5] Cf. *European Digital Rights*. [*Biometric Mass Surveillance: What is it, and why does it need to be banned?*](#)
- [6] BAISI, A. *Hospital Albert Einstein tem redução de perdas com uso do RFID*. Disponível em: <https://www.mobiletime.com.br/noticias/21/09/2023/hospital-albert-einstein-tem-reducao-de-perdas-com-uso-do-rfid/>. Acesso em 10 jul. 2025.
- [7] O GLOBO. *Funcionário do Einstein vaza dados do Ministério da Saúde e expõe 16 milhões de pacientes com Covid-19*. Disponível em: <https://oglobo.globo.com/brasil/funcionario-do-einstein-vaza-dados-do-ministerio-da-saude-expoe-16-milhoes-de-pacientes-com-covid-19-24766745>. Acesso em 25 jul. 2025

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

O tratamento de dados biométricos exige uma abordagem cautelosa e estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos.

Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes.

Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados.

Com base nisso, questiona-se:

- 11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?**

Quando falhas ocorrem, os danos são profundos, duradouros e, muitas vezes, irreparáveis. Por isso, a prevenção deve ser encarada como núcleo estruturante de qualquer projeto que envolva dados sensíveis.

Para mitigar esses riscos, medidas de segurança técnicas indispensáveis incluem (i) criptografia robusta dos dados; (ii) controle de acesso estrito com o mínimo privilégio (por exemplo, um funcionário do financeiro só pode acessar o módulo de faturamento, sem permissão para visualizar dados de RH); (iii) a exclusão permanente dos dados biométricos após a extração das características desejadas [1]; (iv) e a realização de análises de vulnerabilidades e testes de intrusão/penetração (*pentest*) [2]. A lógica do "*zero knowledge proof*" (sistemas que

processam os dados sem necessidade de acessar sua forma bruta) também pode ser adotada para reforçar a segurança [3]. É igualmente fundamental implementar controles de acesso rigorosos, com autenticação multifatorial para administradores e *logs* automatizados de toda a atividade no sistema [4], garantindo rastreabilidade de acessos e operações.

No âmbito das medidas administrativas, pode-se falar também na elaboração de (i) Relatórios de Impacto à Proteção de Dados (RIPD) para tratamentos de alto risco; (ii) a manutenção de um Inventário de Registro de Operações de Tratamento de Dados (RoPA); (iii) a implementação de mecanismo eficiente de gestão de incidentes, tanto em termos de investigação quanto de notificação às autoridades e titulares; e, quando se tratar de tratamento em larga escala, (iv) a realização de auditorias independentes periódicas para tratamento em larga escala; e (v) a instituição de órgãos internos independentes para monitorar o uso da tecnologia e assegurar a responsabilização.

No caso do programa Smart Sampa, o Ministério Público de São Paulo recomendou à prefeitura medidas essenciais de governança e proteção de dados sensíveis. Entre elas, a criação de uma ouvidoria especializada para apurar denúncias de preconceito, discriminação e racismo vinculadas ao uso do sistema, além da implementação de um sistema eficaz de proteção de dados e critérios objetivos para o compartilhamento interinstitucional das informações coletadas [5]. O MP também defendeu a participação paritária de entidades com experiência em proteção de dados e direitos humanos nos espaços decisórios, a criação de instâncias permanentes de controle social e a divulgação periódica, em meio virtual, de dados sobre reclamações, estudos e melhorias do programa [5]. As recomendações evidenciam a necessidade de controle público, transparência e fiscalização cidadã frente ao uso massivo de tecnologias de vigilância.

Referências

[1] Cf. Cetic. *Proteção de dados pessoais: privacidade e confiança no ambiente digital*. Disponível em <<https://cetic.br/media/docs/publicacoes/6/20230727104116/psi-ano-xv-n-2-protecao-de-dados-pessoais.pdf>>

[2] DIAS, L. *Introdução aos Testes de Intrusão (Pentest)*, pp. 15-23. Disponível em: [https://semanacap.bcp.nic.br/files/apresentacao/arquivo/2147/Slides%20-%20Introdu%C3%A7%C3%A3o%20aos%20Testes%20de%20Intrus%C3%A3o%20\(Pentest\).pdf](https://semanacap.bcp.nic.br/files/apresentacao/arquivo/2147/Slides%20-%20Introdu%C3%A7%C3%A3o%20aos%20Testes%20de%20Intrus%C3%A3o%20(Pentest).pdf)

[3] Cf. *What Is a Zero-Knowledge Proof?*

<https://chain.link/education/zero-knowledge-proof-zkp>

[4] Cf. *O que são arquivos de log?* <https://aws.amazon.com/pt/what-is/log-files/>

[5] Cf. *Ministério Público recomenda criação de ouvidoria para programa de câmeras em São Paulo*.

Folha de São Paulo, 11 mar. 2024.

<https://www1.folha.uol.com.br/cotidiano/2024/03/ministerio-publico-recomenda-criacao-de-ouvidoria-para-programa-de-cameras-em-sao-paulo.shtml>

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

As boas práticas devem priorizar a liberdade de escolha do titular e a oferta de alternativas menos intrusivas para acesso ao serviço principal, como a validação por documentos de identificação.

Além disso, o controlador deve realizar avaliação prévia da real necessidade da biometria, adotando-a somente quando estritamente imprescindível para a funcionalidade específica [1]. Sempre que possível, recomenda-se limitar o uso da biometria a funções auxiliares ou complementares, que não comprometam o acesso básico ou essencial ao serviço, ou que haja alternativa à sua utilização.

Quanto à negativa do titular em fornecer seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, a restrição ao uso de determinadas funcionalidades pode ser justificada apenas se houver fundamentação técnica legítima e proporcional. Essa limitação deve ser comunicada antecipadamente, explicando-se de forma transparente quais funcionalidades ficarão inacessíveis e por qual motivo técnico. A proporcionalidade impõe que a restrição seja o mínimo necessário, sem prejuízo indevido ao usuário, e que não se estenda a direitos essenciais ou ao acesso pleno ao serviço principal.

Em contextos em que a biometria não for indispensável, a negativa do titular não pode gerar qualquer penalidade ou restrição relevante. Já em situações específicas, como segurança reforçada para operações financeiras ou acesso a dados sensíveis, a recusa pode legitimar limitações pontuais, desde que fundamentadas, proporcionais e respeitando os princípios da LGPD.

Referências

[1] IDEC. *Biometria Facial, Acesso à Saúde e Direito Fundamental à Proteção de Dados Pessoais: Nota técnica sobre o uso de dados biométricos em estabelecimentos de saúde suplementar*, p. 6. Disponível em: https://idec.org.br/sites/default/files/nt_biometria_facial_no_setor_de_saude_-_idec.pdf. Acesso em 14 jul. 2025

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

[Ver resposta 11]

Quando falhas ocorrem, os danos são profundos, duradouros e, muitas vezes, irreparáveis. Por isso, a prevenção deve ser encarada como núcleo estruturante de qualquer projeto que envolva dados sensíveis.

Para mitigar esses riscos, medidas de segurança técnicas indispensáveis incluem (i) criptografia robusta dos dados; (ii) controle de acesso estrito com o mínimo privilégio (por exemplo, um funcionário do financeiro só pode acessar o módulo de faturamento, sem permissão para visualizar dados de RH); (iii) a exclusão permanente dos dados biométricos após a extração das características desejadas [1]; (iv) e a realização de análises de vulnerabilidades e testes de intrusão/penetração (*pentest*) [2]. A lógica do “*zero knowledge proof*” (sistemas que processam os dados sem necessidade de acessar sua forma bruta) também pode ser adotada para reforçar a segurança [3]. É igualmente fundamental implementar controles de acesso rigorosos, com autenticação multifatorial para administradores e *logs* automatizados de toda a atividade no sistema [4], garantindo rastreabilidade de acessos e operações.

No âmbito das medidas administrativas, pode-se falar também na elaboração de (i) Relatórios de Impacto à Proteção de Dados (RIPD) para tratamentos de alto risco; (ii) a manutenção de um Inventário de Registro de Operações de Tratamento de Dados (RoPA); (iii) a implementação de mecanismo eficiente de gestão de incidentes, tanto em termos de investigação quanto de notificação às autoridades e titulares; e, quando se tratar de tratamento em larga escala, (iv) a realização de auditorias independentes periódicas para tratamento em larga escala; e (v) a instituição de órgãos internos independentes para monitorar o uso da tecnologia e assegurar a responsabilização.

No caso do programa Smart Sampa, o Ministério Público de São Paulo recomendou à prefeitura medidas essenciais de governança e proteção de dados sensíveis. Entre elas, a criação de uma ouvidoria especializada para apurar denúncias de preconceito, discriminação e racismo vinculadas ao uso do sistema, além da implementação de um sistema eficaz de proteção de dados e critérios objetivos para o compartilhamento interinstitucional das informações coletadas [5]. O MP também defendeu a participação paritária de entidades com experiência em proteção de

dados e direitos humanos nos espaços decisórios, a criação de instâncias permanentes de controle social e a divulgação periódica, em meio virtual, de dados sobre reclamações, estudos e melhorias do programa [5]. As recomendações evidenciam a necessidade de controle público, transparência e fiscalização cidadã frente ao uso massivo de tecnologias de vigilância.

Referências

- [1] Cf. Cetic. *Proteção de dados pessoais: privacidade e confiança no ambiente digital*. Disponível em <<https://cetic.br/media/docs/publicacoes/6/20230727104116/psi-ano-xv-n-2-protecao-de-dados-pessoais.pdf>>
- [2] DIAS, L. *Introdução aos Testes de Intrusão (Pentest)*, pp. 15-23. Disponível em: [https://semanacap.bcp.nic.br/files/apresentacao/arquivo/2147/Slides%20-%20Introdu%C3%A7%C3%A3o%20aos%20Testes%20de%20Intrus%C3%A3o%20\(Pentest\).pdf](https://semanacap.bcp.nic.br/files/apresentacao/arquivo/2147/Slides%20-%20Introdu%C3%A7%C3%A3o%20aos%20Testes%20de%20Intrus%C3%A3o%20(Pentest).pdf)
- [3] Cf. *What Is a Zero-Knowledge Proof?*
<https://chain.link/education/zero-knowledge-proof-zkp>
- [4] Cf. *O que são arquivos de log?* <https://aws.amazon.com/pt/what-is/log-files/>
- [5] Cf. *Ministério Público recomenda criação de ouvidoria para programa de câmeras em São Paulo*. Folha de São Paulo, 11 mar. 2024. <https://www1.folha.uol.com.br/cotidiano/2024/03/ministerio-publico-recomenda-criacao-de-ouvidoria-para-programa-de-cameras-em-sao-paulo.shtml>

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (smart cities), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

Em contexto de tratamento massivo de dados biométricos, como em cidades inteligentes, estádios ou espaços públicos, é indispensável a adoção de medidas que mitiguem os riscos inerentes à natureza sensível desses dados.

Primeiramente, os controladores devem realizar uma análise prévia de proporcionalidade e necessidade para determinar se o reconhecimento facial é estritamente necessário, priorizando alternativas menos invasivas e a transparência, como já amplamente debatido na contribuição.

Para além dos necessários mecanismos de segurança também já debatidos, reforça-se, nesse caso, a necessidade de implementação de medidas

antidiscriminatórias ativas.

Isso inclui a realização de avaliações de impacto algorítmico com recortes de raça, gênero, classe e território, tanto antes quanto durante o uso dos sistemas, com métricas construídas com participação social. Também é fundamental garantir auditorias independentes e obrigatórias, conduzidas por entidades autônomas com acesso irrestrito aos dados, códigos e critérios de decisão. A participação direta de grupos historicamente discriminados nas decisões sobre o desenvolvimento e uso de tecnologias, especialmente em políticas públicas, é essencial para a construção de sistemas mais justos. Além disso, deve-se proibir determinados usos discriminatórios, como o policiamento preditivo e uso de tecnologias de reconhecimento facial em espaços públicos. A transparência precisa ser radical, com mecanismos de explicabilidade, contestação e reversão acessíveis à população, bem como canais efetivos de denúncia e responsabilização. Por fim, a regulamentação deve estar orientada por princípios de justiça social e garantia de direitos, e não apenas por agendas de inovação e eficiência, assegurando sanções para práticas discriminatórias.

A comunicação sobre o tratamento de dados biométricos deve ser conduzida de forma clara, precisa e amplamente acessível ao público. Para isso, é necessário que as informações sejam disponibilizadas por diversos meios (como sinalização visível nos locais de coleta, aplicativos móveis, páginas institucionais e comunicados oficiais) e que incluam, de modo direto e transparente, os propósitos do tratamento, a base legal que o fundamenta, o prazo de retenção dos dados, as categorias envolvidas e os direitos assegurados aos titulares. A linguagem adotada deve ser acessível, livre de tecnicismos excessivos, permitindo que qualquer pessoa compreenda plenamente a natureza e a extensão do monitoramento realizado (Rodrigues et. al., 2024) [1].

Para garantir o controle dos titulares, mesmo em ambientes de difícil consentimento explícito, é essencial que existam mecanismos de *opt-out* claros e acessíveis. Pode-se disponibilizar, por exemplo, canais digitais e físicos para que os indivíduos solicitem exclusão de seus dados ou bloqueio de seu uso, sempre que possível. Tecnologias que permitam o mascaramento dinâmico ou a anonimização imediata dos rostos captados também podem minimizar o impacto da coleta (Matusek, 2024) [2].

Referências

[1] RODRIGUES, C; MENDONÇA, E; MENDONÇA, J; ZANATTA, R. *Contribuições da Data Privacy Brasil para a Tomada de Subsídios de Tratamento de Dados Pessoais de Crianças e Adolescentes da Autoridade Nacional de Proteção de Dados Pessoais*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024, pp. 33-35. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2024/08/Data-Privacy-Brasil.-Tomada-de-Subsidios-em-Direitos-de-Crianças.-ANPD.-2024.pdf>. Acesso em 07 jul. 2025.

[2] MATUSEK, F. *Demistifique o mascaramento de privacidade, edição e anomização de vídeo*. Genetec, 2024. Disponível em: <https://www.genetec.com/br/blog/produtos/mascaramento-de-privacidade-estatico-vs-dinamico>. Acesso em 07 jul. 2025.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Os agentes de tratamento devem adotar medidas que assegurem acesso fácil, transparente e contínuo às informações. O direito à informação clara exige que o titular seja informado, antes da coleta, sobre a natureza sensível dos dados, a finalidade específica do tratamento, os critérios da decisão automatizada, o tempo de retenção e os riscos envolvidos. Esse dever de transparência deve ser cumprido em linguagem acessível, sem termos técnicos ou vagos, e disponibilizado em canais

visíveis e compreensíveis (Rodrigues et. al., 2024) [1].

Já o direito de acesso e correção pressupõe que o titular possa verificar quais dados estão sendo tratados, inclusive resultados de sistemas automatizados de reconhecimento biométrico, e solicitar a correção de eventuais imprecisões. Isso implica que os sistemas devem ser auditáveis e que os controladores mantenham registros adequados, com possibilidade de revisão humana, quando necessário.

Quanto à revogação do consentimento, é necessário que o titular tenha meios simples e eficazes para retirar sua autorização sem prejuízo desproporcional. Isso inclui oferecer alternativas de autenticação sempre que possível, especialmente quando o tratamento biométrico não for imposto por obrigação legal. Os agentes devem ainda assegurar que a revogação seja efetiva, com exclusão dos dados ou anonimização segura, salvo se houver outra base legal que justifique a retenção [2].

Em qualquer hipótese, o tratamento automatizado deve respeitar os princípios da finalidade, necessidade, transparência, não discriminação e responsabilização, com salvaguardas técnicas que evitem decisões opacas, abusivas ou irreversíveis.

Referências

[1] RODRIGUES, C; MENDONÇA, E; MENDONÇA, J; ZANATTA, R. *Contribuições da Data Privacy Brasil para a Tomada de Subsídios de Tratamento de Dados Pessoais de Crianças e Adolescentes da Autoridade Nacional de Proteção de Dados Pessoais*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024, pp. 33-35. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2024/08/Data-Privacy-Brasil.-Tomada-de-Subsidios-em-Direitos-de-Crianças.-ANPD.-2024.pdf>. Acesso em 07 jul. 2025.

[2] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. *Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas*. InternetLab/IDEC, São Paulo, 2020, pp. 56-58. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf. Acesso em 14 jul. 2025.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

Para que esse tratamento seja legítimo, é indispensável garantir a participação informada, livre e específica dos pais ou responsáveis, mediante consentimento claro e destacado, precedido de informações acessíveis quanto à natureza dos dados coletados, finalidades, riscos, duração do tratamento e direitos assegurados ao titular.

Esse tipo de tratamento só será admissível quando estritamente necessário e proporcional à finalidade, observando-se, prioritariamente, o princípio do melhor interesse da criança ou do adolescente, conforme previsto no art. 14 da LGPD [1]. Isso significa que o tratamento deve proteger direitos fundamentais, promover o bem-estar do menor e jamais servir a interesses comerciais, de controle ou conveniência institucional sem base jurídica sólida. O Idec já enviou uma notificação para a operadora de planos de saúde Hapvida, após descobrir que a operadora coletava de maneira compulsória dados biométricos de seus pacientes [2]. Por conta disso, a empresa foi multada pelo Procon/AM e está impedida de utilizar a biometria facial pelo Procon/MA. Após toda essa pressão, a Hapvida respondeu ao Idec e disse que não usa mais biometria facial em crianças [3].

Em ambientes como escolas, clubes ou espaços recreativos, o uso de biometria só se justifica quando não houver alternativa menos invasiva que atenda à mesma finalidade (como controle de acesso, segurança ou autenticação) voltada ao melhor interesse das crianças e adolescentes. Ou seja, o tratamento dos dados biométricos ocorrerá, exclusivamente, quando for necessário priorizar os direitos desse público vulnerável. Nesses casos, os controladores devem oferecer medidas mitigadoras de riscos, como anonimização sempre que possível, limitação do acesso aos dados, não compartilhamento indevido e revisão periódica da necessidade da coleta.

A revogação do consentimento deve ser garantida a qualquer tempo, com alternativas viáveis para que a criança ou adolescente não seja privada de acesso a serviços essenciais em razão da recusa ao fornecimento do dado biométrico.

Referências

[1] **Art. 14.** *O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.*

[2] Cf. *Idec notifica Hapvida sobre biometria facial em pessoas do espectro autista*. <https://idec.org.br/release/idec-notifica-hapvida-sobre-biometria-facial-em-pessoas-do-espectro-autista-0>. Acesso em 31 jul. 2025

[2] Cf. *Mães e pais do Norte e Nordeste do Brasil denunciam abusos da Hapvida*. <https://idec.org.br/noticia/maes-e-pais-do-norte-e-nordeste-do-brasil-denunciam-abusos-da-hapvida>. Acesso em 31 jul. 2025

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Será admissível, nos termos da LGPD, quando houver consentimento específico e em destaque dado por pelo menos um dos pais ou responsáveis legais, ou quando for indispensável para cumprimento de obrigação legal, execução de políticas públicas ou para a proteção da vida ou da incolumidade física do menor.

A base mais comum em contextos escolares e recreativos é o consentimento, que deve ser precedido de informação clara, em linguagem acessível e compatível com a compreensão dos pais ou responsáveis, incluindo detalhes sobre a natureza dos dados biométricos, finalidade, duração do tratamento, riscos envolvidos e direitos garantidos.

Para garantir a participação informada, os responsáveis devem ter acesso a avisos de privacidade específicos para o público infantojuvenil, com canal de atendimento ativo e possibilidade de revogação do consentimento a qualquer tempo, sem prejuízo à criança ou ao adolescente. Além disso, os agentes de tratamento devem adotar medidas técnicas e organizacionais eficazes, como critérios rigorosos de controle de acesso aos dados, registro de operações, criptografia, segmentação de bancos de dados por faixa etária, anonimização sempre que possível, avaliações periódicas de impacto à proteção de dados e capacitação de profissionais que manuseiam esse tipo de dado.

Por fim, o tratamento deve ser continuamente revisado à luz do princípio do melhor interesse, evitando usos excessivos, desnecessários ou discriminatórios e assegurando que a coleta biométrica represente um benefício claro à segurança, dignidade e/ou bem-estar da criança ou adolescente. Considerando a garantia do melhor interesse e absoluta prioridade de seus direitos, não deve ser admitido o tratamento de dados prejudicial a esse público, ainda que com o consentimento dos pais e responsáveis. Afinal, as assimetrias informacionais entre controladores e pais e responsáveis permanecerão, de forma que o dever de assegurar a absoluta prioridade de crianças e adolescentes pertencerá, principalmente, aos agentes de tratamento de dados (art. 227, CF).

Em pesquisa conduzida pelo InternetLab [2], foi identificado que sistemas de reconhecimento facial implementados em escolas públicas estão sendo utilizados não apenas para controle de frequência, mas também para inferências subjetivas sobre o "estado emocional" dos alunos, como atenção, fadiga ou distração. Essas análises são feitas com base em expressões faciais captadas pelas câmeras, sem que os critérios técnicos para tais classificações sejam divulgados, auditados ou

validados cientificamente, e podem gerar classificações erradas e discriminatórias, sobretudo contra crianças negras ou neurodivergentes. O exemplo trata de uma forma de vigilância opaca e potencialmente coercitiva, que subordina o desenvolvimento infantil a classificações automatizadas sem base científica, operadas sob a aparência de neutralidade técnica.

Ao dispensar o consentimento informado, ignorar a diversidade emocional e impor padrões de comportamento idealizados por algoritmos, esses sistemas não apenas violam a legislação vigente, mas também comprometem a autonomia, a dignidade e o processo formativo das crianças, reduzindo sua experiência escolar a dados interpretáveis por modelos imprecisos e intransponíveis.

Referências

[1] **Art. 14.** *O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.*

[2] BOND, L. *Reconhecimento facial em escolas pode ameaçar privacidade*. Agência Brasil, 20 mar. 2023. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2023-03/reconhecimento-facial-em-escolas-pode-ameacar-privacidade>. Acesso em 21 jul. 2025.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

Por se tratar de dados sensíveis de hipervulneráveis, os agentes de tratamento devem demonstrar que a coleta é estritamente necessária para atingir a finalidade legítima e que não há alternativa menos invasiva que ofereça o mesmo grau de efetividade.

A compatibilização com o princípio da necessidade exige a coleta mínima de dados, preferencialmente com técnicas de estimativa que não armazenem imagens ou padrões biométricos de forma identificável. A Yoti, por exemplo, desenvolveu uma tecnologia de estimativa de idade facial que funciona sem armazenar imagens identificáveis. Em 2025, a rede britânica de lojas de departamentos John Lewis adotou essa solução para restringir a venda *online* de facas a menores de idade. Uma análise realizada pelo periódico *The Times* demonstrou que o sistema excluía as imagens automaticamente, alertava o entregador e exigia a apresentação de um documento físico no momento da entrega. Em um dos testes, a tentativa de compra

por um adolescente de 16 anos foi rejeitada, mesmo com o erro dentro da margem declarada [1].

Ainda assim, em situações que envolvam a retenção de dados, mesmo que temporária, devem ser adotadas medidas reforçadas de segurança, como criptografia, segregação de bases e limitação de acesso. Na prática, já vemos danos ocorrerem em razão da falta de adoção de processos de adequada governança, salvaguardas e fiscalização, como no incidente de segurança do Banco Neon [2] e de condomínios em Jundiaí/SP [3].

É fundamental que o processo seja transparente, com informação clara e acessível aos pais ou responsáveis, indicando a base legal utilizada, os critérios da análise biométrica, a duração do armazenamento e os direitos dos titulares.

Já o princípio do melhor interesse impõe que o tratamento promova a proteção da criança ou adolescente, sem sujeitá-los a riscos desnecessários ou discriminações. Sempre que possível, deve-se permitir formas alternativas de comprovação de idade e garantir que a estimativa não resulte em barreiras desproporcionais ao acesso de crianças a ambientes seguros.

Referências

[1] SELLMAN, M. *John Lewis introduces AI age checks to sell knives online*. The Times, 20 jan. 2025. Disponível em: <https://www.thetimes.com/uk/technology-uk/article/john-lewis-introduces-ai-age-checks-to-sell-knives-online-z6q9glqjr>. Acesso em 21 jul. 2025.

[2] Cf. *Banco Neon confirma vazamento de dados, mas nega 30 milhões de clientes afetados*. Disponível em: <https://www.infomoney.com.br/consumo/dados-de-mais-de-30-milhoes-de-clientes-do-banco-neon-foram-vazados-diz-site/> Acesso em 31 jul. 2025

[3] Cf. *Polícia Civil investiga se ataque a sistema de reconhecimento facial expôs dados de moradores de condomínios no interior de SP*. Disponível em: <https://g1.globo.com/sp/sorocaba-jundiai/noticia/2024/05/05/policia-civil-investiga-se-ataque-a-sistema-de-reconhecimento-facial-expos-dados-de-moradores-de-condominios-no-interior-de-sp.ghtml> Acesso em 31 jul. 2025

Curitiba/PR, 31 de julho de 2025

À Autoridade Nacional de Proteção de Dados (ANPD)
Setor de Coordenação-Geral de Normatização

Prezados senhores,

Atendendo ao Estatuto Social do Instituto Nacional de Proteção de Dados (INPD) e visando apoiar o desenvolvimento do ambiente nacional de proteção de dados pessoais, a observância dos direitos fundamentais de privacidade e de proteção de dados, o INPD vem, respeitosamente, em complemento às respostas à Tomada de Subsídios: Dados Pessoais Sensíveis – Dados Biométricos, realizada nesta data através do Portal Participa + Brasil, por intermédio do Login de sua Diretora Jurídica, Izabela Lehn, apresentar os seguintes estudos complementares:

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

De acordo com Jain et al. (2024) dado biométrico é aquele que se qualifica como qualquer característica fisiológica e/ou comportamental humana, desde que satisfaça os seguintes requisitos: **a) Universalidade:** cada pessoa deve apresentar tal característica (face, voz, impressão digital, DNA, entre outras); **b) Distintividade:** quaisquer duas pessoas devem ser suficientemente diferentes em termos da característica analisada; **c) Permanência:** a característica deve ser suficientemente invariável (em relação ao critério de correspondência) ao longo de um período de tempo; **d) Capturável ou Coletável ou Colecionável:** a característica pode ser medida quantitativamente. Deve-se considerar que os dados biométricos valem tanto para indivíduos vivos como mortos, considerando-se as variações e perdas existentes.

Há que se considerar que a biometria – ramo da identificação humana, de modo que a palavra possui origem grega, associando “bios” (vida) com “metron” (medida) - surgiu como área do conhecimento a partir de aplicações de cunho jurídico-legal: investigação criminal de suspeitos – impressão digital; determinação de paternidade – DNA; controle de aeroportos e

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

fronteiras – chegada e partida de pessoas – face, impressão digital; autorização de segurança para colaboradores da administração pública em atividades perigosas ou de caráter sigiloso – face, íris, impressão digital; sistemas de votação eletrônica (e-voting) – impressão digital; policiamento preditivo e identificação positiva de condenados e prisioneiros – face, impressão digital; perícia forense – escrita, voz, face, impressão digital, padrões de digitação, localização de pessoas desaparecidas – face; uso de aplicativos a exemplo do GOV.br – face; controle e vigilância de pessoas em áreas públicas – face; entre outros). Porém, vem se desenvolvendo e sendo aplicada em muitas aplicações civis: autorização de acesso em edifícios comerciais – face; sistemas de votação eletrônica em cooperativas (e-voting) – face, impressão digital; operações bancárias e financeiras – face; uso de dispositivos móveis – smartphones – face; hospitais e centros de saúde – face; controle de pessoas em áreas privadas, shopping centers, condomínios – face; entre outros.

Sendo assim, entende-se por biometria o reconhecimento automatizado de seres humanos com base nas suas características biológicas, como impressões digitais, formato do rosto, voz e íris ou comportamento, tais como jeito de andar ou falar (LI; JAIN, 2015. Corroborando com esse entendimento, o Radar Tecnológico da ANPD (número 2 de junho de 2024), a biometria é um campo de estudo que se baseia em métodos matemáticos e estatísticos para analisar e identificar indivíduos por meio de suas características fisiológicas e comportamentais. Entre as características fisiológicas mais comuns estão a impressão digital, a face, a íris, a geometria e vascularização da mão, o DNA e a voz. Já as características comportamentais incluem padrões únicos de voz, expressão facial, assinatura, modo de andar, entre outros. De acordo com a Lei Geral de Proteção de Dados (LGPD), os dados biométricos são classificados como dados pessoais sensíveis, pois estão diretamente vinculados à identidade única de cada indivíduo. A LGPD define dados sensíveis como aqueles que, se tratados de forma inadequada, podem representar riscos significativos à privacidade e aos direitos dos titulares. Por sua singularidade e potencial de identificação e personalização, os dados biométricos requerem um nível elevado de proteção, garantindo que seu uso seja seguro e alinhado às normas de privacidade e segurança da informação.

Utilizando como fonte o direito europeu, segundo o RGPD e o posicionamento das agências reguladoras, incluindo o European Data Protection Board (EDPB), destaca-se os seguintes critérios objetivos, para caracterização de um dado biométrico:

Origem do dado: O dado deve derivar de características físicas, fisiológicas ou comportamentais únicas do indivíduo, como impressões digitais,

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

reconhecimento de voz, facial, íris, geometria da mão, padrões de retina, assinatura, entre outros.

Tratamento específico: A informação para ser considerada biométrica está condicionada a derivar de um processo técnico específico que necessite de aplicação de tecnologia para extrair, registrar, analisar ou comparar essas características com o objetivo de identificação ou autenticação.

Potencial de identificação única: O dado biométrico deve permitir ou confirmar a identificação única de uma pessoa natural. Significa dizer que não basta que a característica seja física ou comportamental, ele precisar ser apta a identificar, de forma individual e inequívoca, o titular de dados.

Finalidade de identificação ou autenticação: O tratamento deve ter como finalidade a identificação ou autenticação do indivíduo, seja para controle de acesso, assiduidade, segurança, entre outros usos legítimos previstos em lei ou mediante consentimento explícito.

"A mera fotografia ou vídeo não os caracteriza como dados biométricos à luz do GDPR, a menos que sejam submetidos a tratamento específico para identificação única."

JAIN, A.; ROSS, A.; PRABHAKAR, S.. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, n. 1, p. 4 – 20, February, 2004. DOI: 10.1109/TCSVT.2003.818349.

Nota Técnica no. 17/2025/CON1/CGN/ANPD - Processo no. 00261.001953/2025-81

Andt.or.br, Calio. Pereira de Oliveira Neto, Reflexões Iniciais quanto ao Uso da Biometria nas relações de Trabalho: Do Paradigma Português às Projeções no Brasil

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

A transparência ativa no tratamento de dados biométricos, classificados como dados pessoais sensíveis pela LGPD (Lei nº 13.709/2018, art. 5º, II), é essencial para garantir que os titulares compreendam, de forma clara e acessível, como seus dados serão utilizados antes mesmo de fornecê-los.

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

Quadro Resumo: Boas Práticas em Conformidade com o GDPR e LGPD

Boas Práticas	Referências Legais
Política de Privacidade clara e específica	GDPR: arts. 12, 14 e 5 LGPD: arts. 6(VI), 9 e 41
Avisos no momento da coleta ou previamente	GDPR: arts. 13 e 14 LGPD: arts. 6(VI), 9, 18 e 41
Canal de atendimento ao titular	GDPR: arts. 15-22 LGPD: arts. 18 e 41
Registro de finalidades e bases legais	GDPR: arts. 5, 6 e 9 LGPD: arts. 6(I, II), 7, 11 e 37
Informação sobre compartilhamento e armazenamento	GDPR: arts. 13(1)(e) e 14(1)(e) LGPD: arts. 6(VI) e 48
Materiais educativos e linguagem acessível	GDPR: art. 12 LGPD: arts. 6(VI), 9 e 41



Nesse sentido:

A. Política de privacidade clara e acessível

A política deve conter linguagem simples, objetiva e estar disponível em canais acessíveis (sites, aplicativos, pontos de coleta). Deve informar: Finalidade do uso da biometria; Base legal utilizada, Período de retenção dos dados; Compartilhamento com terceiros; Direitos dos titulares. Gomes (2025) preconiza que a clareza da política de privacidade é um dos pilares da conformidade com a LGPD no uso de biometria.

B. Avisos de privacidade no ponto de coleta

Antes da coleta, o titular deve ser informado por meio de avisos visuais ou sonoros, com destaque para:

Que tipo de dado biométrico será coletado.

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

Se o consentimento é necessário ou se há outra base legal.

Como exercer seus direitos.

C. Consentimento informado (quando aplicável)

Nos casos em que o tratamento se baseia no consentimento (art. 11, I), este deve ser:

Livre, informado e inequívoco.

Destacado dos demais termos.

Registrado e documentado.

D. Canal de atendimento ao titular

Deve haver um canal funcional para que o titular possa:

Solicitar informações adicionais.

Revogar consentimento, quando esta for a base legal.

Exercer seus direitos (acesso, correção, exclusão etc.).

E. Relatórios de impacto e transparência institucional

A publicação de relatórios de impacto à proteção de dados (DPIA) e de boletins de transparência pode reforçar a confiança dos titulares e demonstrar accountability.

Fonte: Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo - Versão 2.0 EDPB Adotado em 29 de janeiro de 2020.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Ao que se refere à biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) em comparação à biometria tradicional (digital, íris, face), primeiramente é importante compreender as diferenças fundamentais no tratamento de dados biométricos convencionais, de natureza fisiológica, e os de natureza comportamental. A natureza dos dados pessoais do primeiro grupo são constituídos pelo rosto, impressão digital, íris, voz, etc...Já, os dados comportamentais se relacionam com dados

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

dinâmicos, tais como a maneira como o indivíduo segura um objeto, incluindo o ângulo, o uso da mão e a inclinação do mesmo, o ritmo, a velocidade e a pressão das teclas durante a digitação, dinâmica, pressão e andamento gráfico em assinatura ou escrita humana, maneira de caminhar, incluindo o ritmo, a velocidade e o padrão dos passos, entre outros. Em termos de coleta de dados, os métodos e técnicas se diferenciam principalmente pelo fato de que os dados do primeiro grupo, são estáticos, e no Segundo grupo, podem ser estáticos ou dinâmicos, configurando dados (variáveis) discretos ou contínuos. O European Data Protection Board (EDPB) recomenda medidas específicas para a biometria comportamental, tais como: i) minimização de dados; ii) anonimização; e, iii) controle do titular por meio do direito à explicação sobre algoritmos da análise comportamental. A Autoridade Bancária Europeia (EBA) orienta que para setores financeiros, a biometria comportamental deve ser complementar e não substitutiva aos métodos tradicionais.

A biometria comportamental, como padrões de digitação, reconhecimento de voz, movimento ocular ou dinâmica de uso de dispositivos, deve ser tratada com o mesmo grau de cautela que a biometria tradicional (impressão digital, íris, face). Porém, deve-se ter especial atenção às suas características específicas de variabilidade, contexto e inferência indireta. Riscos adicionais como o de profiling e vigilância constante podem trazer impactos graves à liberdade individual e riscos de decisões automatizadas injustas. Existem diferenças fundamentais entre biometria comportamental e a biometria tradicional, são elas:

A biometria comportamental pode gerar inferências que extrapolam a simples identificação, o que exige maior rigor na aplicação dos princípios da LGPD.

A biometria comportamental pressupõe o uso de camadas adicionais de proteção, dado seu potencial de vigilância contínua e inferência indireta de aspectos íntimos da personalidade. Em se tratando desse tipo de biometria boas práticas devem ser adotadas:

Consentimento reforçado: Quando aplicável, deve ser informado, granular e destacando a natureza contínua da coleta.

Limitação temporal e contextual: Evitar coleta permanente ou fora do contexto da finalidade.

Minimização e anonimização: Sempre que possível, utilizar dados agregados ou pseudonimizados.

Auditorias algorítmicas: Avaliar se há inferências indevidas ou discriminação algorítmica.

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

Transparência ativa: Informar claramente que o comportamento está sendo monitorado e para quê.

Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Sim, o uso de tecnologias biométricas, especialmente as mais recentes (biometria comportamental) impõe obrigações específicas aos controladores, com foco especial nos princípios da qualidade dos dados e da segurança, conforme previstos na Lei Geral de Proteção de Dados Pessoais (LGPD). Nesse sentido, as obrigações relacionadas à qualidade dos dados, exige que as informações sejam:

- Exatas, atualizadas e relevantes para a finalidade do tratamento.
- Coletadas de forma não excessiva e com base legal clara.
- Verificadas periodicamente, especialmente em sistemas automatizados que podem gerar falsos positivos.
- A qualidade dos dados é essencial para evitar decisões automatizadas injustas, especialmente em contextos como segurança pública ou crédito.

Quanto as obrigações relacionadas à segurança:

O controlador deve adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, vazamentos, destruição ou perda acidental. No caso da biometria, isso inclui:

- Criptografia e pseudonimização dos dados biométricos.
- Controle de acesso rigoroso aos sistemas que armazenam ou processam esses dados.
- Auditorias periódicas e testes de vulnerabilidade.
- Plano de resposta a incidentes, com notificação à ANPD e aos titulares (Art. 48).
- A segurança deve ser “proporcional ao risco”, o que significa que dados sensíveis como biometria exigem nível máximo de proteção.
- Avaliação de Impacto à Proteção de Dados (DPIA): obrigatória em casos de alto risco.
- Minimização de dados: coleta apenas do necessário para a finalidade específica.
- Treinamento contínuo de equipes: para evitar falhas humanas na manipulação de dados sensíveis.
- Auditoria de algoritmos: especialmente em sistemas de reconhecimento facial ou comportamental, para evitar vieses e discriminação.

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Segundo as instruções da Norma ISO/IEC 24745, devem ser observados os seguintes critérios técnicos e organizacionais para a adequada utilização da hipótese legal de prevenção à fraude, se não vejamos:

Justificativa da necessidade: A coleta biométrica só se justifica se a fraude representar um risco relevante à operação ou ao titular de dados e não houver meios menos intrusivos;

Avaliação de Impacto (RIPD): A ISO recomenda a realização de uma avaliação de riscos e impactos à privacidade para fundamentar o uso dos dados biométricos. Essa avaliação deve mapear os riscos de exposição ou uso indevido dos dados e identificar medidas técnicas para mitigação de riscos, como uso de templates não reversíveis e criptografia;

Mínima interferência: A ISO recomenda que seja coletado apenas o necessário, de acordo com a finalidade de prevenção à fraude, de acordo com princípio da necessidade (art. 6, III, da LGPD) e exige selecionar tecnologias biométricas com menor impacto, evitar armazenamento centralizado de dados.

Modelos de aplicação adequados: A norma apresenta modelos de aplicação biométrica (seção 8.2), entre os quais alguns oferecem maior segurança e menor risco à privacidade. São eles: **i)** Modelo local ou descentralizado, onde o armazenamento é realizado no cliente e é comparado com o cliente, minimizando o compartilhamento. Alguns exemplos: A impressão digital ou reconhecimento facial em iPhones (Face ID/Touch ID) e Androids e dispositivos de controle de acesso off-line, como fechaduras eletrônicas com leitor biométrico integrado, onde a digital do usuário é armazenada na memória local da fechadura. Nessa modalidade a comparação ocorre localmente, sem o envio de dados biométricos para a nuvem; e, **ii)** Modelo com uso de tokens com armazenamento distribuído, onde as informações biométricas são armazenadas e/ou processadas de forma dividida entre dois ou mais locais. Alguns exemplos desta modalidade são: a) a autenticação multifator em ambientes corporativos em que, a título

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

ilustrativo, um Smartcard armazena parte dos dados biométricos, enquanto um sistema local ou nuvem realiza a verificação final com base em dados complementares(token + endpoint + backend corporativo); b) soluções de acesso físico a locais de segurança crítica, como data centers, onde o token do usuário (cartão ou pendrive) contém uma parte criptografada da biometria, e a verificação só ocorre quando combinada com a parte armazenada localmente no servidor da sala restrita; e, **iii)** controle de passaporte eletrônico (ePassport), onde a imagem do titular é armazenada no chip RFID do passaporte e o processo de verificação pode ocorrer no servidor da autoridade migratória, comparando com a leitura local da câmara (token + servidor de imigração).

A escolha do modelo deve considerar a compatibilidade com o grau de risco da fraude a ser evitada e com a técnica da organização de proteger os dados.

Portanto, a aplicação da hipótese legal de “garantia da prevenção à fraude e à segurança do titular” (art. 11, II, “g”, da LGPD) para o tratamento de dados biométricos exige critérios rigorosos, dada a natureza sensível desses dados e os riscos associados ao seu uso indevido. São critérios para aplicação legítima da hipótese de prevenção à fraude:

Finalidade legítima, específica e proporcional: O tratamento deve estar diretamente vinculado à prevenção de fraudes, como autenticação de identidade em transações financeiras ou acesso a sistemas sensíveis. A coleta de dados biométricos não pode ser genérica ou preventiva sem justificativa concreta.

A finalidade deve ser “específica, explícita e legítima”, evitando usos genéricos que ampliem indevidamente o escopo do tratamento.

Demonstração de necessidade: A biometria deve ser estritamente necessária para atingir a finalidade de prevenção à fraude. Se houver meios menos invasivos (como senhas ou tokens), estes devem ser priorizados.

A “necessidade” deve ser avaliada com base em uma análise de proporcionalidade e minimização de dados.

Avaliação de impacto à proteção de dados (DPIA): É recomendável (e em muitos casos essencial) realizar uma DPIA para documentar os riscos e as medidas de mitigação adotadas.

Transparência e informação ao titular: Mesmo sem consentimento, o titular deve ser informado de forma clara sobre: a finalidade do uso da biometria; a base legal utilizada, bem como o acesso, a correção, a oposição etc.).

Segurança técnica e organizacional: A biometria exige medidas de segurança reforçadas, como criptografia, controle de acesso e anonimização.

Proibição de discriminação: O uso da biometria não pode resultar em tratamento discriminatório ou abusivo, especialmente contra grupos vulneráveis. Isso exige auditoria de algoritmos e revisão de vieses.

De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo?

A compatibilização entre o princípio da necessidade e o uso de dados biométricos para segurança da informação e acesso a serviços bancários exige uma abordagem baseada em proporcionalidade, minimização e justificativa técnica robusta.

Para tanto é se faz necessário: Justificativa técnica e funcional clara; Implementação com medidas de segurança reforçadas; Avaliação de Impacto à Proteção de Dados (DPIA); Transparência e opção ao titular.

A Justificativa técnica e funcional clara: o uso da biometria deve ser estritamente necessário para atingir a finalidade de segurança — como autenticação em transações de alto risco ou acesso a contas digitais. A adoção deve ser precedida de análise técnica comparativa, demonstrando que meios alternativos (como senhas ou tokens) não oferecem o mesmo nível de proteção. A biometria pode ser proporcional quando usada para mitigar riscos concretos de fraude, desde que sua adoção seja precedida de análise técnica e jurídica adequada.

A Implementação com medidas de segurança reforçadas: a biometria, por ser dado sensível, exige criptografia, controle de acesso, segregação de ambientes e anonimização sempre que possível. Isso reduz o impacto em caso de vazamento e reforça a legitimidade do tratamento.

A segurança técnica: é um dos pilares para justificar o uso de biometria em ambientes financeiros, especialmente diante do alto valor dos dados envolvidos Avaliação de Impacto à Proteção de Dados (DPIA). A realização de uma DPIA é essencial para demonstrar que o uso da biometria é necessário, proporcional e que os riscos foram mitigados. Isso também reforça a accountability do controlador.

Transparência e opção ao titular: mesmo quando o consentimento não é exigido (ex: prevenção à fraude), o titular deve ser informado de forma clara sobre: a base legal utilizada; a finalidade específica; seus direitos e formas de exercê-los.

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

Sempre que possível, deve-se oferecer alternativas menos invasivas para autenticação, respeitando a autodeterminação informativa.

Da privacidade à proteção de dados pessoais: fundamentos da Lei geral de proteção de dados. Danilo Doneda. ISBN: 9786559917969. 2021.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

A construção de sistemas eficazes exige:

Bases de dados com diversidade, significância estatística e representatividade populacional;

Avaliações de impacto algorítmico para prever e mitigar riscos;

Mecanismos de avaliação de conformidade são altamente recomendados.

Inobstante a relevância do Sistema de biometria para fins de autenticação do indivíduo, há que se reconhecer que apresentam riscos técnicos, sociais e jurídicos. Entre os principais:

Violação da privacidade e exposição indevida de dados sensíveis;

Discriminação algorítmica, especialmente em razão de raça, idade e gênero;

Falsos positivos e falsos negativos, comprometendo a confiabilidade.

Falta de transparência e explicabilidade algorítmica (Cebrian; Freitas, 2023);

Vigilância massiva e borramento entre espaços públicos e privados (Freitas; Rossi, 2020).

Esses riscos decorrem da complexidade dos modelos de IA e da qualidade dos dados utilizados. Portanto, recomenda-se:

Auditorias frequentes e independentes dos algoritmos.

Implementação de mecanismos de correção tempestiva de erros.

Governança algorítmica baseada em princípios éticos, sociais e técnicos.

Garantia do direito à revisão por humano em decisões automatizadas.

Consoante destaca Freitas (2025), o Direito tradicional, baseado em "coisas físicas", deve se adaptar à era das "não-coisas", exigindo novas estruturas

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

para lidar com tecnologias como a IA e seus impactos na privacidade, responsabilidade civil e justiça social.

Importante: fotos ou vídeos não são, por si sós, dados biométricos, a menos que tratados para realizar identificação pessoal automatizada.

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Diante do alto risco representado por uma eventual violação de dados biométricos — como o roubo de identidade, que pode ter consequências graves torna-se imprescindível que organizações adotem medidas técnicas e administrativas robustas, em consonância com os princípios da LGPD e com normas internacionais de boas práticas, como a ISO/IEC 24745:2011.

1. Medidas Técnicas e Administrativas Indispensáveis

Com base na ISO/IEC 24745 e na LGPD, destacam-se os seguintes pilares de segurança e privacidade:

a) Segurança da Informação (art. 46 da LGPD)

Confidencialidade: proteção contra acessos não autorizados aos dados biométricos.

Integridade: garantia de que os dados não serão alterados ou corrompidos de forma indevida.

Disponibilidade: os dados devem estar acessíveis apenas quando necessário e por pessoal autorizado.

Cancelamento e renovação: os dados biométricos devem ser revogáveis ou substituíveis sempre que necessário.

b) Proteção da Privacidade

Irreversibilidade: os templates biométricos devem ser protegidos contra a reconstrução da imagem original.

Desvinculação (unlinkability): impossibilidade de rastrear ou vincular registros biométricos entre bases distintas.

Confidencialidade das operações biométricas: proteção contra extração indevida de informações nos processos de autenticação ou identificação.

c) Governança e Gestão de Dados

Consentimento informado (art. 8º e art. 11 da LGPD): deve ser livre, específico, destacado e com finalidade claramente definida.

Transparência (art. 6º, VI): o titular deve ser informado sobre a finalidade, a base legal e os direitos associados ao tratamento.

Treinamento e conscientização: equipes internas devem ser capacitadas continuamente para o uso ético e seguro da biometria.

Regras claras sobre retenção e descarte (art. 15 da LGPD): os dados devem ser eliminados após o término do tratamento, salvo obrigação legal ou regulatória.

2. Parâmetros Mínimos de Avaliação de Riscos e Monitoramento

Para garantir a conformidade com a LGPD e a proteção integral dos dados biométricos, recomenda-se que as organizações implementem:

Relatório de Impacto à Proteção de Dados Pessoais (RIPD) – art. 38 da LGPD: obrigatório nos casos de alto risco, como tratamento de dados biométricos em larga escala, com detalhamento dos mecanismos de mitigação e justificativas legais.

Mapeamento de fluxos de dados biométricos: identificar todo o ciclo de vida do dado (coleta, uso, armazenamento, compartilhamento e descarte).

Auditorias regulares de segurança e compliance: verificação de conformidade com a LGPD, políticas internas e certificações.

Monitoramento contínuo de incidentes de segurança: com canais de resposta rápida, registro, investigação e notificação à ANPD e ao titular, nos termos do art. 48.

Política de minimização e limitação de acesso: assegurar que apenas pessoas autorizadas tenham acesso aos dados biométricos, de forma proporcional à finalidade do tratamento.

A proteção de dados biométricos exige uma abordagem integrada entre segurança da informação, governança de dados, avaliação de riscos e respeito aos direitos fundamentais dos titulares. A adoção de medidas técnicas alinhadas à ISO/IEC 24745, combinada com diretrizes legais da LGPD, representa o padrão mínimo necessário para prevenir violações e assegurar o uso ético e legítimo dessa tecnologia.

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O tratamento de dados biométricos de crianças e adolescentes, especialmente em contextos como escolas, espaços recreativos e plataformas educacionais, exige máxima cautela. Por envolver dados pessoais sensíveis de pessoas em condição peculiar de desenvolvimento, a Lei Geral de Proteção de Dados Pessoais (LGPD), no art. 14, estabelece que tal tratamento deve ser realizado sempre em observância ao melhor interesse da criança, conceito que vai além da privacidade e abrange aspectos como segurança, saúde, bem-estar, desenvolvimento e autonomia.

1. Participação informada dos pais ou responsáveis legais

Antes da implementação de qualquer sistema biométrico em ambiente escolar, deve-se garantir uma estratégia clara de conscientização e engajamento dos pais ou responsáveis, incluindo:

Campanhas informativas e reuniões prévias, conforme orienta o Guia da UNICEF (2021, p. 13), explicando a tecnologia, as finalidades do tratamento, os riscos envolvidos e os direitos dos titulares.

Consulta direta às crianças e adolescentes, especialmente se forem mais velhas, com linguagem acessível e proporcional à sua maturidade, conforme o padrão do Children's Code do ICO (UK).

Possibilidade de oposição ao tratamento, conforme previsto no Biometrics Guidance (UK, 2022, p. 10), que reconhece o direito de estudantes se recusarem a fornecer dados biométricos, mesmo com o consentimento dos responsáveis.

2. Base legal

Recomenda-se que o tratamento seja fundamentado em consentimento específico e destacado fornecido pelos pais ou responsáveis legais (art. 14, §1º, LGPD), salvo situações excepcionais que envolvam riscos à proteção dos estudantes ou estabelecimento e políticas públicas, como controle de evasão escolar. No entanto, o consentimento por si só não é suficiente: ele deve ser

precedido de uma avaliação concreta de necessidade, proporcionalidade e impacto, conforme exige a boa-fé e os princípios da lei.

3. Condições para conformidade com o princípio do melhor interesse

Para que o tratamento esteja alinhado ao melhor interesse da criança é fundamental que seja realizado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) com foco específico na criança (LGPD, art. 38), avaliando não apenas riscos à privacidade, mas também possíveis efeitos sobre: i) Autonomia e capacidade de escolha; ii) Direito de brincar, aprender e interagir livremente; iii) Desenvolvimento físico, emocional e psicológico; iv) Formação da identidade e expressão pessoal; v) O tratamento seja proporcional e realmente necessário, evitando coleta excessiva, retenção indevida ou uso secundário dos dados; vi) Haja políticas de exclusão de dados biométricos ao fim da necessidade, com garantias de que os dados não serão utilizados para finalidades de vigilância, controle excessivo ou discriminação.

Recomenda-se que instituições educacionais que pretendam adotar tecnologias biométricas:

- Realizem previamente uma DPIA (Data Protection Impact Assessment), com ênfase nos direitos da criança e nos impactos sociais e psicológicos, conforme o modelo da ICO.
- Criem canais claros de comunicação com famílias, inclusive para manifestação de oposição e exercício dos direitos previstos no art. 18 da LGPD.
- Implementem políticas de "Privacy by Design", que minimizem a coleta de dados sensíveis e priorizem o uso de tecnologias menos invasivas.
- Constituam comissões internas com participação da comunidade escolar (pais, professores e alunos) para acompanhar e fiscalizar o uso dessas tecnologias.
- Respeitem a autodeterminação informativa da criança, evitando práticas coercitivas ou restritivas à participação escolar baseadas na coleta de dados.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

O tratamento de dados biométricos de crianças e adolescentes, por envolver dados pessoais sensíveis de indivíduos em condição peculiar de desenvolvimento, está sujeito a requisitos legais e éticos rigorosos. A Lei

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

Geral de Proteção de Dados Pessoais (LGPD) estabelece, no artigo 14, que o tratamento de dados de crianças e adolescentes deve ser realizado com o consentimento específico e em atenção ao seu melhor interesse.

Hipóteses legais admissíveis

A principal base legal para o tratamento de dados biométricos de crianças é o consentimento específico e destacado dos pais ou responsáveis legais (art. 14, §1º, LGPD). Esse consentimento deve ser: i) Livre, informado e inequívoco; ii) Relacionado a uma finalidade clara, legítima e proporcional; e, iii) Recolhido antes do início do tratamento.

Em situações excepcionais que envolvam políticas públicas e que se faça necessário o uso da biometria para controle de evasão escolar em escolas públicas, ou, em ambientes adversos que representem ameaça a segurança do titular e ou do ambiente, é crível admitir-se a adoção da hipótese legal da política pública e prevenção à fraude no ambiente escolar.

É de extrema relevância a participação informada e o engajamento da comunidade escolar. A proteção efetiva dos direitos de crianças e adolescentes exige transparência e engajamento proativo dos pais, responsáveis e dos próprios estudantes. Entre as boas práticas destacam-se:

- Campanhas de conscientização junto aos responsáveis, com linguagem acessível, promovendo debates e consultas públicas sobre a adoção de sistemas biométricos;
- Informação clara e acessível sobre a finalidade, os riscos, a base legal e os direitos dos titulares, inclusive por meio de reuniões presenciais e materiais educativos;
- Consulta às próprias crianças e adolescentes, conforme sua faixa etária e grau de maturidade, respeitando sua autonomia progressiva.

Essas práticas estão em consonância com diretrizes internacionais como o Children's Code (UK) e o Guia UNICEF sobre proteção de dados em escolas, que orientam a escuta ativa dos menores e o envolvimento dos responsáveis desde as etapas iniciais da decisão.

Medidas técnicas e organizacionais para evitar abusos e vazamentos:

Para garantir a segurança e integridade dos dados biométricos tratados, recomenda-se a adoção das seguintes salvaguardas:

Realização de Relatório de Impacto à Proteção de Dados (RIPD), com foco específico nos impactos sobre os direitos da criança, incluindo aspectos como desenvolvimento, autonomia, segurança e privacidade;

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

Aplicação das diretrizes da ISO/IEC 24745:2011, que estabelecem requisitos de segurança para sistemas biométricos, com ênfase em:

Confidencialidade, integridade, disponibilidade e revogabilidade dos dados;

Irreversibilidade (não reconstrução da imagem original);

Desvinculação (unlinkability) de registros entre bases distintas;

Controle de acesso rigoroso, com autenticação multifator para operadores do sistema;

Retenção mínima e descarte seguro dos dados ao fim da finalidade;

Treinamento contínuo das equipes técnicas e pedagógicas envolvidas.

O tratamento de dados biométricos de crianças e adolescentes em escolas ou espaços recreativos requer a observância dos seguintes critérios: i) base legal válida, (ii) campanhas transparentes de informação aos pais e alunos, (iii) avaliação prévia dos riscos com foco no melhor interesse da criança, e (iv) implementação de medidas técnicas robustas e proporcionais à sensibilidade dos dados.

Essa abordagem assegura não apenas a conformidade legal, mas também o respeito à dignidade e aos direitos fundamentais de crianças e adolescentes, promovendo uma cultura de proteção de dados no ambiente escolar.

Permanecemos à disposição para contribuir com a regulação da proteção de dados biométricos no país.

Atenciosamente,

Instituto Nacional de Proteção de Dados

Martha Leal – Diretora Vice-Presidente

Izabela Lehn – Diretora Jurídica

Cinthia O. A. Freitas – Conselheira Consultiva

Matheus Passos - Conselheiro Consultivo

Daiane Dantas – Presidente da Comissão de Governança e Compliance

Rafael Mosele – Diretor Financeiro e Presidente da Comissão de Relações do Trabalho

Guilherme Gonçalves – Diretor de Capacitação Técnica

Adriana R. Quinelo - Associada

Adriana Neves Gomes de Azevedo - Fellow

Maysa González Rodriguez Dassie - Fellow

Classificação: INTERNA () CONFIDENCIAL () RESTRITO () PÚBLICO (x)

O [InternetLab](#) é um centro de pesquisa independente que, desde 2014, atua na interseção entre direito e tecnologia, com foco na produção de conhecimento qualificado para subsidiar políticas públicas.

No âmbito da Tomada de Subsídios sobre o tratamento de dados biométricos promovida pela ANPD, encaminhamos este documento como um complemento à nossa contribuição já registrada na plataforma Participa Mais Brasil. O documento aprofunda e expande alguns dos pontos, reunindo argumentos mais detalhados, referências e links. Optamos por responder apenas às perguntas que se conectam diretamente às nossas áreas de atuação, com o objetivo de oferecer subsídios técnicos e jurídicos que possam enriquecer o processo de construção de materiais orientativos e regulatórios, promovendo a proteção de dados pessoais e a inovação responsável.

BLOCO I - DEFINIÇÕES E PRINCÍPIOS

O tratamento de dados biométricos impõe a observância rigorosa dos princípios gerais de proteção estabelecidos na Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente os constantes em seu art. 6º. Por serem considerados dados pessoais sensíveis, os dados biométricos requerem uma abordagem cautelosa, baseada em fundamentos legais claros e em finalidades legítimas.

A LGPD não define diretamente o termo “dados biométricos”, mas a doutrina e o próprio Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que inspirou a legislação brasileira, descrevem dados biométricos como dados pessoais resultantes de tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a identificação única dessa pessoa. Exemplos incluem impressões digitais, reconhecimento facial, íris, geometria da mão, padrões de voz e até comportamentos como modo de digitar ou caminhar.

É imprescindível que os agentes de tratamento compreendam com precisão o conceito de dados biométricos e sua distinção em relação a outros dados, sensíveis ou não. Além disso, a operação de sistemas biométricos - que podem incluir sensores, câmeras, softwares de reconhecimento e algoritmos — deve ser avaliada à luz dos princípios da LGPD, como a finalidade, a necessidade, a transparência, a prevenção, a segurança e a não discriminação.

Diante desse contexto, pergunta-se:

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

De forma geral, é obrigação do controlador fornecer ao titular informações essenciais referentes ao tratamento de dados pessoais de forma clara e objetiva. No caso de dados biométricos, por se tratarem de dados sensíveis, tal obrigação deve ser realizada com redobrada atenção. Para além das obrigações gerais de transparência (art. 9, LGPD), o controlador deve se atentar para a comunicação dos riscos específicos daquele tratamento de dados pessoais. O acesso à informação é essencial para que o titular compreenda como seus dados são utilizados. Esse conhecimento possibilita o exercício de seus direitos e, quando necessário, a oposição a tratamentos de dados que violem a legislação. Um dos principais desafios, no entanto, está na comunicação eficaz.

Considerando que um dos principais obstáculos a uma comunicação efetiva sobre o tratamento de dados pessoais são documentos complexos e extensos, que dificultam o entendimento de fato sobre o fluxo de informações, entendemos que a comunicação com os titulares de dados deve prezar por uma linguagem e visual adequados, de fácil acesso. Isto é, para além de se pensar em políticas de privacidade e termos de uso, é importante que se tenha uma forma de se “resumir” ao titular de dados pessoais as informações contidas nesses documentos que de fato importam para sua tomada de decisão. Também é importante informar qual tecnologia está envolvida nessa coleta.

Não é possível - nem desejável - que um único modelo se aplique a todos os setores e controladores, mas entendemos que controladores que realizam tratamento de dados biométricos têm o dever de encontrar formas que se adequem às suas organizações e atividades.

[Experiências internacionais](#) providenciam alguns exemplos. Um deles, conhecido como Avisos *Just in Time* (JIT), nos quais se apresenta quadros breves e direcionados para a funcionalidade que irá coletar as informações no momento da coleta. Considerando que há uma tendência em não se ponderar o risco de fornecimento de dados biométricos, esses tipos de aviso podem ajudar o usuário a entender o impacto do fornecimento de seus dados pessoais, ao apresentar informações sobre privacidade relevantes e focadas na situação. Esses avisos são mais eficazes quando combinados com outras técnicas, permitindo que o usuário veja apenas o essencial ou clique para mais detalhes, seja expandindo a caixa. Assim, por exemplo, plataformas que demandam reconhecimento facial como autenticação de segurança, podem recorrer a esse mecanismo para notificar ao titular os riscos e demais informações, conforme a lei, sobre aquele tratamento de dados pessoais.

Outro exemplo é o aviso em camadas, apresentado no início ou em uma página central, com uma notificação concisa e resumida, seguida por camadas

sucessivas que oferecem diferentes níveis de detalhe. Esse formato permite que o titular acesse as informações de forma gradual e precisa, conforme seu interesse.

Considerando que o tratamento de dados pessoais envolvendo dados biométricos representa riscos significativos aos titulares, recomenda-se que os controladores não apenas mantenham Relatórios de Impacto à Proteção de Dados Pessoais (RIPDs) atualizados e completos, mas também desenvolvam versões acessíveis desses documentos para os próprios titulares. Essa adaptação deve ser pensada com base no entendimento do “cidadão comum” - ou seja, uma pessoa leiga em proteção de dados - e pode ser complementada com recursos visuais que facilitem a compreensão. O registro de atividades de tratamento (ROPA – art. 37) também deve ser mantido sempre atualizado, incluindo informações sobre o ciclo de vida dos dados pessoais em questão (i.e. por quanto tempo são armazenados, por qual finalidade, como são descartados e práticas de segurança implementadas ao longo desse período).

Por fim, entendemos que o papel do encarregado é fundamental nesse contexto. Um canal de comunicação eficiente, rápido e de fácil acesso e resposta é fundamental. Também é recomendável que seja disponibilizado mais de um canal que contemplem diferentes formas de comunicação - tanto escritas quanto orais - de modo a assegurar o pleno exercício dos direitos pelos titulares, inclusive por aqueles em situação de vulnerabilidade, como pessoas não alfabetizadas ou com limitações no letramento, ou por pessoas com deficiência.

BLOCO II – HIPÓTESES LEGAIS

As hipóteses legais para o tratamento de dados biométricos, assim como para o tratamento de quaisquer dados sensíveis, estão previstas no art. 11 da LGPD. A partir da biometria é possível identificar, de forma única, o indivíduo. Por essa razão, trata-se de uma tecnologia sensível que levanta questões complexas sobre privacidade, legalidade, proporcionalidade e segurança.

Assim, é fundamental que o agente de tratamento justifique a necessidade e a razoabilidade do tratamento desses dados, garantindo que seu uso seja proporcional e alinhado aos princípios gerais de proteção e aos direitos dos titulares.

O rol de hipóteses legais discriminado no art. 11 exige que o agente de tratamento fundamente a operação de dados biométricos em critérios objetivos e verificáveis, como consentimento específico e destacado, prevenção à fraude, ou finalidades de pesquisa, execução de políticas públicas, proteção da vida etc., garantindo respeito à proporcionalidade, necessidade e à autodeterminação informativa.

Diante disso, questiona-se:

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

O consentimento livre não pode estar condicionado à renúncia de um direito ou à restrição de uma liberdade. Por isso, principalmente em contextos envolvendo serviços essenciais, o consentimento dificilmente será uma base legal adequada, já que a recusa ao tratamento implicaria, na prática, a exclusão do titular do acesso ao serviço - isso indica que é necessário buscar uma outra hipótese legal mais adequada. Uma grande dificuldade em encontrar uma outra base legal adequada é um forte indício de que o tratamento de dados não deve ser realizado, pois viola o próprio regime de proteção da LGPD e os direitos fundamentais dos titulares. Embora essa recomendação seja especialmente relevante em contextos de serviços essenciais, sua lógica também se aplica a situações semelhantes, como [o controle acesso a determinados locais](#). Se a recusa ao consentimento resultar em impedimento de acesso, é provável que esse consentimento não seja verdadeiramente livre, o que pode indicar a ilegitimidade da base legal adotada. Nesses casos, é importante destacar que a coleta de dados biométricos só pode ocorrer após a obtenção de um consentimento válido, que deve ser prévio à coleta

propriamente dita. Por exemplo, no caso de captação de imagens, o consentimento deve ser obtido antes da gravação, por meio de uma ação clara do titular, como clicar em uma opção específica ou aceitar expressamente os termos do tratamento.

Um exemplo emblemático é o caso do Estado do Paraná, que autorizou a Companhia de Tecnologia da Informação e Comunicação do Paraná (Celepar) a coletar e tratar dados biométricos faciais de estudantes da rede estadual para controle de frequência escolar por meio de reconhecimento facial. A iniciativa foi alvo de Ação Civil Pública ajuizada pelo Ministério Público do Paraná (Processo 0004208-55.2025.8.16.0058), que apontou diversas violações a direitos fundamentais, em especial aos direitos de proteção de dados pessoais. Nesse caso, para além de outras problemáticas, a validade do consentimento foi claramente comprometida: os pais e responsáveis que não consentissem com o uso de TRF não teriam a vaga do aluno na instituição de ensino garantida. Essa vinculação retira do titular a possibilidade de escolha real, tornando o consentimento meramente formal. Quando o consentimento se transforma em requisito obrigatório, ele perde seu caráter voluntário e, conseqüentemente, sua validade jurídica nos termos da LGPD. Vale mencionar que a recusa do consentimento também não pode estar atrelada a uma justificativa.

O consentimento livre não pode estar vinculado a uma contrapartida financeira que compromete a capacidade do titular de avaliar criticamente os riscos envolvidos. A principal preocupação não está na existência de uma contrapartida financeira em si, mas nos efeitos que ela produz sobre o processo de tomada de decisão do titular. A oferta de pagamento em troca da coleta de dados biométricos pode comprometer a capacidade do titular de avaliar de forma crítica e informada os riscos envolvidos no tratamento. Esse tipo de incentivo reforça uma fragilidade estrutural do consentimento: a tendência generalizada de os titulares aceitarem os termos sem leitura ou compreensão adequada. Quando há uma recompensa imediata, essa etapa de ponderação é ainda mais negligenciada, o que "borra" o processo decisório e mina a autodeterminação informativa. Nessas circunstâncias, o consentimento, embora formalmente obtido, não pode ser considerado livre nem informado nos termos exigidos pela LGPD, especialmente diante da natureza sensível e de alto risco dos dados biométricos envolvidos.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

A aplicação da base legal da “garantia da prevenção à fraude” (art. 11, II, “g”,

LGPD) no tratamento de dados biométricos exige cautela redobrada. Trata-se de uma hipótese legítima, mas que não pode ser transformada em justificativa automática para qualquer uso de tecnologias invasivas sob o pretexto genérico de segurança. Sem critérios claros, corre-se o risco de essa base funcionar como válvula de escape para práticas abusivas, como o uso indiscriminado de reconhecimento facial em espaços públicos e privados.

Ainda que no [Guia sobre Legítimo Interesse](#) (2024) a autoridade tenha equiparado a sistemática necessária para aplicação da base legal prevenção à fraude e à segurança no caso de dados sensíveis àquela estipulada para aplicação do legítimo interesse, a operacionalização dessa equiparação não está suficientemente clara no guia disponibilizado. Isso porque o teste de balanceamento especificado no guia - necessário para justificar um tratamento legítimo com base no legítimo interesse - sopesa os direitos e liberdades fundamentais dos titulares com os *interesses do controlador ou de terceiro*. Assim, em sua própria raiz, o teste está modulado para a lógica pertencente à hipótese do legítimo interesse, que difere daquela aplicada à garantia da prevenção à fraude. Isso deixa zonas cinzentas relevantes para a efetiva concretização dos direitos e liberdades fundamentais dos titulares de dados. Por exemplo: ao aplicar o teste em caso de tratamento cuja finalidade é dita como segurança do titular, o que entra no lugar do legítimo interesse do controlador?

A dúvida sobre o que exatamente deve ser contraposto no teste de balanceamento, quando o tratamento de dados sensíveis se justifica com base na segurança do titular, revela uma lacuna conceitual crítica. No legítimo interesse tradicional, o teste pondera os direitos e liberdades do titular contra um interesse do controlador ou de um terceiro - algo externo à esfera do titular. No entanto, quando o fundamento jurídico alegado é a proteção da própria segurança do titular, como se daria essa ponderação? Nesse cenário, o tratamento é apresentado como supostamente favorável ao próprio titular, o que esvazia o conflito típico que o teste de balanceamento busca resolver. Além disso, como alguns casos conhecidos já [mostraram](#), esse mecanismo por si só não é suficiente para impedir a realização de golpes contra os titulares de dados.

Dessa forma, assim como ocorreu com a hipótese do legítimo interesse, que foi corretamente submetida a parâmetros rigorosos, a base da prevenção à fraude, quando utilizada para tratamento de dados biométricos, também deve vir acompanhada de um ônus argumentativo elevado para o controlador - específicos para esta hipótese legal. Ou seja, os controladores que dela se utilizarem, devem estar preparados para cumprir obrigações reforçadas, como: demonstração técnica e empírica da necessidade do dado para a finalidade pretendida, análise de proporcionalidade a partir de uma lente de riscos (principalmente em casos que a biometria pode implicar restrições de acesso a serviços essenciais), avaliação de alternativas menos intrusivas e apresentação de salvaguardas robustas.

Essa abordagem não impede o uso legítimo da base, mas atua como um freio

contra a banalização de soluções altamente invasivas.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares? (300 caracteres)

Nos casos em que o tratamento de dados biométricos se fundamenta no cumprimento de obrigação legal ou regulatória, os controladores – especialmente órgãos e entidades públicas – devem observar critérios rigorosos de necessidade, proporcionalidade e definição clara de finalidade. Normas de caráter genérico, como políticas públicas que incentivam o uso de tecnologias, não são suficientes, por si só, para legitimar o uso de dados sensíveis. É indispensável uma demonstração técnica e empírica de que o uso da tecnologia biométrica é estritamente necessário para o cumprimento do dispositivo legal, explicando como e por que o tratamento é essencial.

Um exemplo é o Plano Nacional da Educação (PNE), que já em 2014 incluiu várias metas voltadas ao incentivo ao uso de tecnologias na educação e à digitalização da gestão escolar. O novo PNE, ainda em discussão para o decênio 2024-2034, amplia ainda mais essas diretrizes. No entanto, essa previsão genérica de adoção de tecnologias não pode ser usada como salvo conduto para justificar automaticamente o uso de tecnologias - muitas vezes questionáveis, pelo grau de invasão, como reconhecimento facial - , em ambientes escolares.

A simples existência de uma meta de modernização tecnológica não supre a exigência legal de finalidade específica e proporcionalidade na coleta e tratamento de dados biométricos. Em outras palavras, há um salto entre uma diretriz ampla - como “fomentar o desenvolvimento de tecnologias para auxiliar as práticas de correção de fluxo, o acompanhamento pedagógico individualizado e a recomposição das aprendizagens” - e a efetiva necessidade do uso de uma tecnologia biométrica específica em um determinado contexto. Esse salto precisa ser tecnicamente preenchido com justificativas claras, baseadas em evidências, que demonstrem por que aquele tratamento é necessário, adequado e menos invasivo que outras alternativas possíveis.

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

A utilização das tecnologias de reconhecimento facial (Facial Recognition Technologies, ou FRTs) se destaca por sua aplicação em segurança pública, controle de acesso e autenticação digital, além de outros contextos que demandam identificação automatizada. A utilização de tecnologias emergentes, como alguns sistemas de inteligência artificial (IA), por exemplo, tem ampliado significativamente o uso de sistemas de reconhecimento facial em diversos setores da sociedade. Esses sistemas, ao capturar, processar e comparar características faciais únicas de indivíduos, realizam o tratamento de dados biométricos. Por conseguinte, a integração da IA nesses sistemas permite uma capacidade aprimorada de detecção, identificação e classificação de rostos em tempo real.

O tratamento de dados biométricos por meio de reconhecimento facial, especialmente se realizado de forma automatizada, levanta importantes preocupações jurídicas, éticas e sociais. Por um lado, a promessa de maior eficiência, segurança e personalização é atrativa; por outro, os riscos associados à vigilância em massa, reidentificação indevida e impactos desiguais sobre grupos vulneráveis tornam evidente a necessidade de salvaguardas robustas.

As tecnologias de reconhecimento facial, portanto, detêm alcance considerável, com a possibilidade de uma coleta massiva de dados biométricos, muitas vezes ultrapassando a quantidade de dados necessários à finalidade do tratamento.

Assim, é importante que a utilização das FRTs seja pautada pelos princípios e diretrizes da LGPD, como necessidade, proporcionalidade, transparência, prevenção e não discriminação, além de exigir justificativas claras para a sua adoção, especialmente quando há outras soluções menos intrusivas disponíveis, a fim de mitigar riscos ou ameaças aos direitos dos titulares de dados pessoais.

Nesse contexto, indaga-se:

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Parte-se aqui da premissa de que o ônus regulatório imposto aos controladores que optam pela adoção TRFs deve ser substancialmente mais

elevado do que aquele aplicável ao tratamento de outros dados pessoais. Trata-se de uma tecnologia intrinsecamente mais invasiva, com [potencial ampliado de vigilância, discriminação e erosão de direitos fundamentais](#). Por isso, a gravidade dos riscos envolvidos justifica a imposição de exigências normativas mais densas, tanto em termos de justificação quanto de transparência, governança e prestação de contas.

Assim, o uso de TRFs com o objetivo de, por exemplo, prevenir fraudes no caso de serviços essenciais - como [transporte, educação, programas de proteção social](#) - levanta preocupações importantes como riscos de exclusão e discriminação, por conta de falhas nos sistemas, desvios de finalidade, perda de controle dos dados e incidentes de segurança ([UNICEF, 2019, p. 16-17](#)). Portanto, sua adoção requer cautela.

A conformidade do uso de tecnologias de reconhecimento facial com os princípios da necessidade, proporcionalidade e transparência exige, como premissa básica, que o tratamento de dados esteja ancorado em uma finalidade legal e específica. Nos termos do art. 6º, I da LGPD, é essa definição precisa da finalidade que viabiliza a análise da pertinência do uso da tecnologia em relação ao problema que se pretende enfrentar, evitando, assim, o desvio funcional e a banalização da excepcionalidade do recurso tecnológico. A invocação de finalidades genéricas, como “segurança”, “eficiência”, “celeridade”, não satisfaz os critérios exigidos para demonstrar a efetiva contribuição da TRF ao objetivo declarado, tampouco permite aferir o respeito aos demais princípios da adequação, da necessidade e da minimização dos dados pessoais. Entendemos que eventual regulamentação do tópico deve considerar este ponto sobre finalidades genéricas de forma bastante rigorosa.

Mas não basta alegar uma finalidade específica, é necessário demonstrar a necessidade e a proporcionalidade da escolha. Isso implica justificar por que, dentre alternativas tecnológicas disponíveis, o reconhecimento facial é a medida mais adequada para alcançar o objetivo proposto e a menos invasiva possível para tal fim. Essa demonstração deve ser capaz de demonstrar uma relação lógica e empírica entre a finalidade almejada - pode, por exemplo, incluir uma comparação com outras soluções tecnológicas. Deve-se também justificar, com base no caso concreto, porque os dados coletados não excedem o estritamente necessário para a concretização de tal fim. Esse exame não se limita à eficiência técnica, devendo considerar especificamente os riscos associados ao uso de [dados biométricos](#). Ao se tratar de TRF para o público das crianças e adolescentes, esse exame deve, impreterivelmente, demonstrar além da finalidade legítima, adequação dos dados, sua necessidade e proporcionalidade da medida, o melhor interesse da criança.

Outro ponto central é a [limitação do tratamento à finalidade inicialmente declarada](#). A reutilização de dados biométricos para finalidades distintas daquelas que motivaram sua coleta viola o princípio da finalidade e compromete a legítima expectativa do titular sobre o uso de seus dados (art. 6º, V e X). Usos secundários

para fins de vigilância pública são especialmente problemáticos, visto que podem aumentar a vigilância desproporcional, discriminação estrutural e violar direitos fundamentais.

As informações fornecidas ao titular de dados são fundamentais para a efetivação do princípio da transparência. Assim como no caso da finalidade, o uso de termos vagos ou genéricos compromete a compreensão do titular e enfraquece sua capacidade de exercer seus direitos. Por exemplo, um sistema de reconhecimento facial que trata dados biométricos não está simplesmente coletando “imagens”, mas sim captando informações sensíveis que identificam de forma única a identidade física do indivíduo. No entanto, conforme [relatório](#) atualizado do Centro de Estudos de Segurança e Cidadania (CESeC, 2025), apesar dos 337 projetos ativos de reconhecimento para fins de segurança no Brasil, muitos dos estados não possuem nenhum tipo de aviso à população nos locais onde as câmeras integradas a tecnologias de reconhecimento facial foram instaladas (p. 20).

Nesse mesmo sentido, a imprecisão sobre os agentes de tratamento viola o direito à autodeterminação informativa. Para exercer protagonismo sobre seus próprios dados e concretizar os direitos previstos no artigo 18 da LGPD, o titular precisa saber quem toma as decisões sobre o tratamento, onde os dados estão armazenados e para onde direcionar suas solicitações. No caso das TRFs, esse problema se intensifica com a [fragmentação dos arranjos técnicos e comerciais](#), em que diferentes empresas fornecem equipamentos, processam imagens e armazenam dados, muitas vezes em parceria com o poder público. O resultado é uma cadeia de responsabilização opaca, especialmente grave em contextos de segurança pública, onde a assimetria entre Estado e cidadão torna ainda mais difícil o controle democrático dessas práticas. É essencial que haja definição clara e pública sobre quem responde por cada etapa do tratamento de dados, com informações acessíveis ao titular.

O compartilhamento de dados entre empresas e o poder público, ainda sem regulamentação específica, não é um mero detalhe técnico. Embora a LGPD vede o tratamento de dados pessoais com finalidade de segurança pública por pessoa jurídica de direito privado, salvo quando realizado sob responsabilidade de uma entidade pública, com comunicação à ANPD (cf. art. 4º, § 2º, LGPD), sabe-se que essa comunicação, na prática, não ocorre. (CESeC, 2025, p. 21). A ausência de regras claras compromete o controle democrático e precisa ser enfrentada no debate regulatório. Nesse contexto, sugerimos também que os critérios e instrumentos de contratação pública incorporem de forma explícita as exigências da LGPD, especialmente em processos que envolvam operadores responsáveis pelo tratamento de dados biométricos.

Vale ressaltar que a Lei de Acesso à Informação (Lei nº 12.527/2011 ou “LAI”) se aplica às atividades de tratamento de dados pessoais realizadas por órgãos e entidades públicas. Assim, os procedimentos estabelecidos pela LAI e seu

decreto regulamentador devem ser observados nesses casos. Por exemplo, a transparência ativa, no website dos órgãos competentes, de informações sobre a atividade realizada, os órgãos ou entidades responsáveis e os recursos e repasses financeiros envolvidos. No caso de parcerias com entes privados, justificativas genéricas de “segredo comercial” ou “sigilo empresarial” não são suficientes para negar o acesso à informação.

A transparência no uso das TRFs deve ser garantida não apenas por meio de informações fornecidas ao titular no momento da coleta, mas também pela produção de relatórios de avaliação de impacto (RIPD) públicos, redigidos em [linguagem acessível e acompanhados de mecanismos de controle social](#). O RIPD, conforme argumentamos na resposta à pergunta 2, não deve ser tratado como um documento burocrático ou interno, mas como um instrumento legítimo de controle social. Isso exige não apenas sua atualização contínua, mas também sua tradução para formatos compreensíveis ao cidadão comum, acompanhada de mecanismos efetivos de fiscalização e participação. O registro de atividades de tratamento (ROPA – art. 37) também deve ser mantido sempre atualizado, incluindo informações sobre o ciclo de vida dos dados pessoais em questão (i.e. por quanto tempo são armazenados, por qual finalidade, como são descartados e práticas de segurança implementadas ao longo desse período).

Sob o risco real de reforço de discriminações estruturais, especialmente contra populações historicamente vulnerabilizadas, é fundamental que qualquer implementação de TRFs seja antecedida por uma avaliação específica (e documentada) de riscos discriminatórios. É necessário, também, incorporar práticas regulares de auditoria dos sistemas, com foco específico na detecção de [vieses algorítmicos](#), com o objetivo de diminuir os riscos de discriminação. É preciso exigir bases de dados representativas e treinamento contínuo de operadores humanos para reduzir a desigualdade nos índices de erro que afetam, de maneira desproporcional, determinados grupos minorizados, como pessoas negras, indígenas, mulheres e a população trans.

As instituições que adotam TRFs devem, ainda, demonstrar que dispõem de estruturas internas voltadas à governança do uso da tecnologia, com capacidade para monitorar e prevenir riscos, revisar práticas, corrigir falhas e assegurar a responsabilização por eventuais abusos. O centro da política de mitigação de riscos deve se concentrar na prevenção de práticas discriminatórias e no controle do ciclo de vida dos dados biométricos.

Também nesse contexto, os canais de comunicação são de extrema importância. A função do encarregado é ser um ponto de contato direto com os titulares; ele deve fornecer respostas claras, acessíveis e tempestivas sobre o tratamento realizado, assegurando que os direitos previstos na LGPD sejam compreendidos e efetivamente exercidos. Assim, recomendamos que, para tratamentos que envolvam TRFs (e dados biométricos de forma geral) em contextos nos quais direitos fundamentais estejam particularmente em risco (como

segurança pública, saúde, benefícios sociais, educação), o prazo de resposta dos encarregados a solicitações de titulares seja regulamentado como menor do que quinze dias, tendo em vista a urgência da matéria e o risco inerente a este tipo de dado. Além disso, é imprescindível que sejam disponibilizados diversos canais de comunicação, tanto por meios escritos quanto orais, de modo a assegurar o pleno exercício dos direitos pelos titulares, inclusive por aqueles em situação de vulnerabilidade, como pessoas não alfabetizadas ou com limitações no letramento, e por pessoas com deficiência.

É igualmente importante que órgãos como controladorias, defensorias e conselhos especializados exerçam supervisão contínua sobre o uso dessas tecnologias, de modo a garantir o cumprimento de direitos fundamentais, princípios da LGPD e prevenir práticas abusivas.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

Embora não seja recomendável criar uma lista taxativa desses contextos, tendo em vista a rápida mudança das tecnologias e de seus usos, é possível identificar contextos em que o reconhecimento facial deve ser evitado. Entendemos que uma análise de proporcionalidade é um ponto de partida importante para definir situações nas quais os riscos e grau de intrusão não superam os supostos benefícios que advêm da tecnologia. Assim, situações nos quais direitos e liberdades fundamentais estão em cheque e podem ser gravemente comprometidos no caso de erros dos sistemas, indicam uma alta possibilidade de se banir esse tipo de tecnologia.

Alguns exemplos podem incluir: (i) TRFs em salas de aula e contextos escolares e (ii) uso de TRFs para finalidades preditivas (por exemplo: detecção de emoções e de comportamentos, indícios de evasão ou maior chances de reprovação em contextos escolares e policiamento preditivo).

Primeiramente, entendemos que [TRFs em contextos educacionais tendem a ser mais problemáticas](#). Como argumentamos em 2023, em [relatório](#) publicado pelo InternetLab sobre pesquisa que visava identificar como as escolas públicas brasileiras adotam políticas de reconhecimento facial, tais tecnologias podem ser consideradas, em última análise, tecnologias de vigilância aplicadas na educação. *“Nos casos analisados, nota-se que na implementação de reconhecimento facial, essas tecnologias têm sido compreendidas como tecnologias de educação e com finalidade pedagógica. Contudo, reconhecimento facial pode ser melhor enquadrado como uma tecnologia de vigilância, na medida em que não apresenta fins*

pedagógicos, e cuja finalidade principal está relacionada à segurança e controle de ambientes.” (p. 28). Nesse sentido, a decisão por sua aplicação deve ser precedida por um sopesamento rígido e robusto sobre a legitimidade da finalidade em questão, a necessidade da medida e dos dados coletados, sua adequação e proporcionalidade, sempre considerando o melhor interesse da criança e do adolescente.

Além disso, há riscos muito significativos no compartilhamento dessas informações com outras instituições públicas, principalmente quando utilizadas como concessão a demais serviços e benefícios: as TRFs possuem acurácia questionável para lidar com desafios de acesso a direitos. Por exemplo, é sabido que tais tecnologias possuem uma maior tendência a erro quando se trata de crianças (e grupos vulneráveis) - o que gera preocupações referentes a, por exemplo, maiores riscos de exclusão ([UNICEF, 2019, p. 16](#)). Nesse sentido, ao se utilizar dados biométricos para concessão de programas de [proteção social](#), salvaguardas robustas devem ser adotadas, como implementação de práticas que garantam a transparência, qualidade e livre acesso aos dados e a segurança dos dados em todo seu ciclo de vida.

No que tange ao segundo ponto - i.e. uso de TRFs para finalidades preditivas -, entendemos que a opacidade inerente às ferramentas de análises algorítmicas prejudicam um entendimento robusto e democrático sobre seu funcionamento e, portanto, de seus outputs, além do risco de resultados com baixa acurácia. Nesses casos, no entanto, erros podem ser extremamente comprometedores com relação aos direitos e impactos na vida das pessoas atingidas.

Por exemplo, na produção do [relatório](#) sobre tecnologias de vigilância na educação pública anteriormente mencionado, nos chamou atenção não só o fato de algumas empresas indicarem que oferecem serviços de previsão de quando um(a) estudante tem mais chances de reprovação, mas principalmente a falta de clareza sobre que tipo de uso dos dados são utilizados para fazer esse tipo de medição. Esse cenário é preocupante, visto que pode levar à estigmatização precoce de estudantes, rotulando-os como "propensos ao fracasso" antes mesmo de uma avaliação pedagógica humana. Um erro nesse tipo de classificação - seja por limitações do modelo, má qualidade dos dados ou generalizações estatísticas - pode comprometer oportunidades acadêmicas, afetar a autoestima dos estudantes e perpetuar ciclos de exclusão educacional.

Ainda no contexto educacional, vale mencionar o caso do Estado do Paraná, que autorizou a Companhia de Tecnologia da Informação e Comunicação do Paraná (Celepar) a realizar a coleta e o tratamento da biometria facial e de imagens dos estudantes da rede estadual de ensino para fins de registro de frequência escolar utilizando reconhecimento facial. Por conta de diversas violações a direitos fundamentais - principalmente aos direitos de proteção de dados pessoais -, o Ministério Público protocolou Ação Civil Pública (Processo 0004208-55.2025.8.16.0058) solicitando a remoção do ilícito e a indenização por

danos morais coletivos. Nesse caso, dentre as diversas problemáticas da implementação desse sistema diante de um público vulnerável (crianças e adolescentes), chama atenção as capacidades da tecnologia incluírem não só a identificação de gênero, mas também a detecção de emoções e atributos faciais para “[monitoramento comportamental e de emoções](#)”. Lembramos, neste ponto, que o [Parlamento Europeu](#) proibiu o reconhecimento de emoções no local de trabalho e nas escolas por meio do Regulamento de Inteligência Artificial.

Além disso, vale ressaltar que dados pessoais sobre crianças e adolescentes não poderão ser utilizados para quaisquer finalidades comerciais, incluindo qualquer forma de pesquisa de mercado, direcionamento de publicidade ou inteligência de negócios.

É importante destacar que, justamente pelos altos riscos de discriminação e vigilância massiva, entendemos também que o uso dessas tecnologias também para fins de segurança pública tende a ser ilegítimo. Não há evidências robustas de eficácia das TRFs nesse contexto - ao contrário, há indícios consistentes de altos índices de erro. Isso se soma a um elevado potencial de uso abusivo e discriminatório, sobretudo em contextos de policiamento ostensivo e controle populacional. Como apontam [Azevedo et al.](#) (2022, p. 145), as TRFs “promovem danos graves em razão de erros ou ‘funcionam bem’ e promovem vigilância em massa, além do reforço ao seletivismo penal”. Nesse contexto, o uso de TRFs muitas vezes se assemelha às chamadas *fishing expeditions* (práticas investigativas amplas e indiscriminadas, que buscam encontrar culpados a partir de uma vigilância generalizada, sem indícios prévios de delito). Isso contraria diretamente princípios fundamentais do Estado de Direito, como o princípio da presunção de inocência e o *in dubio pro reo*. O uso de TRFs, ao inverter essa lógica e tratar todos como suspeitos em potencial, subverte tais garantias constitucionais e promove um ambiente de desconfiança e repressão incompatível com os direitos fundamentais. Combinadas à inteligência artificial com fins preditivos, por exemplo, essas tecnologias podem reforçar a seletividade penal, gerar falsos positivos e discriminar populações vulneráveis, ao coletar massivamente dados biométricos para alimentar bancos de dados.

Nesse sentido, embora a disciplina da proteção de dados não regule diretamente a segurança pública, ela não só pode como deve desempenhar um papel crucial na prevenção desses riscos, especialmente por meio da regulamentação do compartilhamento de dados entre os setores público e privado nesta seara, conforme os parágrafos do art. 4º da LGPD. Isso porque grande parte das tecnologias utilizadas pelo poder público em contextos de segurança, como o reconhecimento facial, depende de tecnologias contratadas de empresas privadas (ou, ainda, no caso de uso de câmeras privadas contratadas por entes públicos por meio de convênios). Nesses casos, a ANPD poderia atuar de forma mais incisiva na fiscalização e regulamentação do compartilhamento de dados pessoais em contextos de segurança pública, emitindo opiniões técnicas obrigatórias e exigindo

RIPDs sempre que houver tratamento de dados sensíveis. Deve, ainda, acompanhar de perto situações em que há participação de entes privados.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

O tratamento de dados biométricos exige uma abordagem cautelosa e estruturada, considerando seu alto grau de sensibilidade e o potencial de identificação única dos indivíduos. A adoção de boas práticas e programas de governança voltados especificamente para esse tipo de dado é essencial para assegurar a conformidade com a LGPD e promover a proteção dos direitos fundamentais dos titulares.

O art. 46 da LGPD estabelece a obrigação de aplicação de medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas, o que se mostra ainda mais relevante quando se trata de dados que não podem ser alterados ou substituídos, como as características biométricas.

O art. 50 da LGPD, por sua vez, incentiva os agentes de tratamento a formularem regras próprias de boas práticas e de governança, incluindo diretrizes claras sobre responsabilidades, segurança da informação, gestão de riscos, mecanismos de resposta a incidentes e processos de atendimento aos direitos dos titulares. No caso dos dados biométricos, é especialmente recomendável que esses instrumentos também contemplem critérios rigorosos para coleta, armazenamento e uso, além de políticas internas que orientem avaliações constantes de proporcionalidade e riscos.

Nesse sentido, medidas de segurança, boas práticas e programas de governança no tratamento de dados biométricos devem estar alinhados aos valores da LGPD, incorporando uma lógica preventiva e transparente, garantindo, assim, o tratamento responsável por parte dos agentes.

Esse bloco visa identificar medidas técnicas e administrativas que devem ser implementadas para garantir a proteção integral dos dados biométricos, bem como os programas de governança em privacidade e boas práticas que devem ser adotados pelas organizações que tratam tais dados.

Com base nisso, questiona-se:

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

A exigência de autenticação biométrica em funcionalidades específicas de serviços não essenciais deve ser cuidadosamente analisada à luz dos princípios da LGPD, especialmente quando [há risco de discriminação ou exclusão indevida de titulares](#) que optem por não fornecer esse tipo de dado sensível.

O primeiro critério a ser considerado é a avaliação da essencialidade do dado biométrico para a [funcionalidade pretendida](#). O art. 6º, III da LGPD consagra o princípio da minimização, segundo o qual o tratamento de dados deve se restringir ao mínimo necessário para a realização de sua finalidade. Assim, a exigência da biometria só é juridicamente admissível quando houver uma justificativa técnica concreta de que essa forma de autenticação é indispensável ao funcionamento da funcionalidade oferecida. A ausência de alternativas viáveis, de igual eficácia e segurança, deve ser demonstrada de forma objetiva, e não presumida ou vinculada à mera conveniência operacional.

Nos casos em que, por exemplo, a [autenticação biométrica seja efetivamente indispensável](#) para o funcionamento seguro e eficaz de determinada funcionalidade, é fundamental que essa exigência seja acompanhada de uma explicação clara e acessível aos titulares. Deve-se informar, em linguagem simples, por que a biometria é necessária, quais etapas envolvem a coleta, o armazenamento, o uso e a eventual eliminação dos dados biométricos, e quais medidas de segurança estão implementadas para protegê-los. Além disso, deve-se deixar de forma evidente e transparente o nome e os canais de contato do encarregado pelo tratamento de dados, garantindo que os titulares possam exercer seus direitos de maneira plena e tempestiva, conforme previsto na LGPD.

Nos casos em que o tratamento de dados biométricos se baseia no consentimento do titular, a proporcionalidade entre a coleta e a finalidade é importantíssima. Antes de mais nada, vale ressaltar que nesses casos, a obtenção do consentimento deve ocorrer antes do início da coleta dos dados. O art. 8º da LGPD exige que o consentimento seja livre, informado e inequívoco. Se a negativa do titular implicar restrição significativa ao uso do serviço, especialmente quando não há outras formas de acesso, há risco de que o consentimento perca sua validade jurídica. A imposição de barreiras de acesso em razão da recusa ao fornecimento de dados biométricos, sem base técnica adequada, pode configurar violação não apenas à LGPD, mas também ao Código de Defesa do Consumidor - no

caso de se tratar de relações de consumo, na medida em que limita o acesso a serviços em condições de igualdade.

Por essa razão, uma [boa prática](#) fundamental é a oferta de meios alternativos de autenticação, sempre que técnica e financeiramente viáveis. O reconhecimento facial ou digital não pode se tornar a única via de acesso a funcionalidades que poderiam, com igual segurança, ser disponibilizadas mediante autenticação por senha, token, cartão ou múltiplos fatores. A adoção exclusiva da biometria pode, inclusive, agravar desigualdades de acesso, afetando pessoas idosas, com deficiência, ou pertencentes a grupos minorizados que sofrem com taxas maiores de falha em sistemas biométricos.

Adicionalmente, é essencial que a exigência da biometria seja justificada e documentada com transparência, em conformidade com os princípios da prestação de contas (art. 6º, X) e da boa-fé. A produção de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) é especialmente recomendável nesses casos e o registro de atividades de tratamento também deve ser mantido sempre atualizado, incluindo informações sobre o ciclo de vida dos dados pessoais em questão (i.e. por quanto tempo são armazenados, por qual finalidade, como são descartados e práticas de segurança implementadas ao longo desse período). Esses documentos devem analisar o contexto do tratamento, os riscos envolvidos e as medidas adotadas para mitigá-los. A publicação, em linguagem acessível, das razões pelas quais a funcionalidade depende tecnicamente da biometria é um instrumento de *accountability* importante para garantir o controle social sobre a prática.

Por fim, essas exigências devem estar inseridas em programas de governança em privacidade que contemplem não apenas a proteção técnica dos dados biométricos, mas também mecanismos contínuos de revisão da proporcionalidade das medidas adotadas. A revisão periódica das justificativas técnicas e jurídicas permite acompanhar o avanço de outras tecnologias de autenticação que possam, no futuro, substituir a biometria de forma menos invasiva, em linha com os princípios da precaução e da não discriminação.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

O tratamento de dados biométricos envolve riscos elevados à privacidade e à autodeterminação informativa, podendo afetar diretamente direitos previstos na LGPD, como o direito à informação clara e adequada (art. 6º, VI e art. 9º), o direito ao acesso aos dados (art. 18, II), o direito à correção (art. 18, III), o direito à eliminação de dados (art. 18, VI) e o direito de revisão a decisões automatizadas (art. 20).

As preocupações tornam-se ainda mais significativas quando os dados biométricos tratados se referem a grupos vulneráveis, como é o caso de crianças e adolescentes. A proteção dos dados biométricos desses indivíduos é de extrema importância, uma vez que tais grupos vulneráveis podem não possuir a plena capacidade de compreender as implicações nas quais estão expostos ao fornecerem ou terem seus dados biométricos coletados, estando suscetíveis a riscos, abusos e violações dos seus direitos.

Isso posto, a proteção de dados de crianças e adolescentes, assim como a proteção dos idosos na LGPD, é uma prioridade que reflete a responsabilidade de proteger os indivíduos mais vulneráveis na sociedade. A legislação estabelece uma base sólida para garantir que esses grupos tenham seus direitos respeitados e suas informações tratadas de maneira ética e segura. As organizações devem estar atentas a essas diretrizes e adotar práticas que assegurem a privacidade e a integridade de dados pessoais, promovendo um ambiente digital mais seguro e inclusivo para todos, especialmente para tais grupos.

Com base nessas questões, pergunta-se:

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

O tratamento de dados pessoais sensíveis de crianças deve observar critérios estritos de legalidade, transparência e proporcionalidade, com a identificação e mitigação de riscos, além da implementação de salvaguardas efetivas que garantam os seus direitos. As finalidades devem ser claras, específicas e justificadas, sempre compatíveis com o melhor interesse da criança. A coleta de dados biométricos não deve ser feita se a finalidade puder ser atingida por meios menos invasivos. Os dados tratados devem ser estritamente necessários, pertinentes e limitados ao propósito declarado, com a adoção de medidas robustas de segurança e confidencialidade ao longo de todo o ciclo de vida dos dados para prevenir acessos não autorizados e proteger a integridade e a privacidade das crianças. A implementação de governança interna facilita formalizando regras em documentos

como políticas e contratos, e, no caso de órgãos públicos, garantindo a publicidade dessas informações.

Considerando que a coleta de dados biométricos muitas vezes ocorre de forma desigual, especialmente em contextos de vulnerabilidade e dependência de [políticas públicas/programas de proteção social](#), expondo crianças a riscos como erro, vazamento, estigmatização e vigilância abusiva, os agentes de tratamento devem assegurar que:

1. Quando a base legal adotada for o consentimento, este deve ser livre, informado e inequívoco – o que significa que não pode estar condicionado à perda de qualquer benefício, serviço, ou, especialmente, de um direito (ver resposta 4). Caso contrário, trata-se de um consentimento meramente formal e, portanto, inválido à luz da LGPD. Além disso, é fundamental garantir informação clara, acessível e - quando possível - também adequada à faixa etária de crianças e adolescentes, especialmente considerando que, no caso de adolescentes entre 16 e 18 anos, o consentimento deverá ser colhido diretamente deles, além dos responsáveis, conforme os princípios da autodeterminação informacional e do desenvolvimento progressivo da capacidade.
2. Aplicação da Lei de Acesso à Informação (Lei nº 12.527/2011 ou “LAI”) às atividades de tratamento de dados pessoais realizadas por órgãos e entidades públicas - os procedimentos estabelecidos pela LAI e seu decreto regulamentador devem ser observados nesses casos. Por exemplo, a divulgação, no website dos órgãos competentes, de informações sobre a atividade realizada, os órgãos ou entidades responsáveis e os recursos e repasses financeiros envolvidos. No caso de parcerias com entes privados, justificativas genéricas de “segredo comercial” ou “sigilo empresarial” não são suficientes para negar o acesso à informação.
3. Canais para exercer os direitos dos titulares devem ser fáceis e ágeis - deve ser garantido canal eficaz, gratuito e acessível para que pais, responsáveis ou os próprios titulares, conforme sua capacidade progressiva, possam acessar os dados tratados, compreender como estão sendo usados e solicitar correções em caso de erros ou imprecisões - algo crítico principalmente em se tratando de sistemas automatizados, que frequentemente falham com mais intensidade nos grupos mais vulneráveis.
4. Os dados biométricos de crianças e adolescentes não estejam vinculados à finalidades comerciais - Tendo em vista seu melhor interesse e a legislação brasileira (Estatuto da Criança e do Adolescente, Resolução CONANDA nº 245/2024; Código de Defesa do Consumidor e Constituição Federal), ressalta-se que utilizar dados pessoais sobre crianças e adolescentes para quaisquer finalidades comerciais, incluindo qualquer forma de pesquisa de mercado, direcionamento de publicidade ou inteligência de negócios configura finalidade ilegítima e, portanto, tratamento ilegal. Conforme

explicitamos em nosso relatório "[O Direito das Crianças à Privacidade](#)", crianças são especialmente vulneráveis, por exemplo, à publicidade: até os 12 anos, não compreendem plenamente seu caráter persuasivo. Essa limitação cognitiva torna abusivas as estratégias mercadológicas voltadas a esse público. A publicidade baseada em dados e altamente segmentada agrava ainda mais essa vulnerabilidade, afetando crianças em todas as fases do desenvolvimento, dos 0 aos 18 anos.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

O princípio do melhor interesse, previsto no caput do art. 14 da LGPD, deve ser o eixo da análise. Isso exige que o agente de tratamento comprove, caso a caso, porque a biometria é necessária e como a opção adotada protege, de fato, a privacidade, a segurança e o desenvolvimento da criança.

Nesse sentido, entendemos que a utilização de dados biométricos sobre crianças e adolescentes em contextos escolares e espaços recreativos é, via de regra, contrária ao seu melhor interesse. Especificamente, entendemos que [TRFs em contextos educacionais tendem a ser mais problemáticas](#), tendo em vista sua desproporcionalidade, riscos de segurança, imprecisões e vieses discriminatórios é ilegítimo. Segundo [relatório da UNICEF](#), o uso indevido de dados biométricos de crianças pode gerar consequências graves e permanentes, como violações de privacidade e fraude de identidade. Embora essas tecnologias possam fortalecer sistemas de identificação, também apresentam o risco de cristalizar e limitar a identidade das crianças desde muito cedo (p. 19).

Se, no entanto, o tratamento de dados biométricos for comprovadamente necessário, a análise deve se guiar pelo risco dos tratamentos. Nesses casos, há uma sensibilidade dupla (dados sensíveis de um público vulnerável), que impõe salvaguardas técnicas e organizacionais mais robustas, como relatórios de impacto à proteção de dados pessoais (RIPD), protocolos robustos de segurança, formas de minimização de dados sensíveis coletados e revisão contínua das práticas adotadas por meio de auditorias. Os detalhes dessas diligências devem ser tornados públicos e disponíveis para revisão. No que tange ao consentimento dos pais e responsáveis, destacamos que todos requisitos para um consentimento válido se aplicam (ver resposta 4). Ressalta-se que esses dados pessoais biométricos sobre crianças e adolescentes não poderão ser utilizados para quaisquer finalidades comerciais, incluindo qualquer forma de pesquisa de mercado, direcionamento de publicidade

ou inteligência de negócios.

Embora o consentimento seja a hipótese mais comum para o tratamento de dados de crianças e adolescentes, existem outras hipóteses legais previstas no art. 11 da LGPD que poderiam justificar esse tipo de operação, como a proteção da vida ou da incolumidade física do titular ou de terceiros, a tutela da saúde quando realizada por profissionais ou serviços de saúde, a realização de estudos por órgãos de pesquisa, ou ainda o exercício regular de direitos em processos judiciais, administrativos ou arbitrais. Nessas situações, o tratamento precisa ser estritamente necessário e justificado para o fim proposto, e ainda assim deve passar por uma análise de risco mais rigorosa, por se tratar de dados de grupo vulnerável.

Aponta-se que o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (art. 11, II, b LGPD) é também uma hipótese legal possível para o tratamento de dados do público infanto-juvenil. Nesse caso, no entanto, reforça-se que o gestor público deve justificar o uso dos dados por meio de relatórios registrados e disponíveis para fiscalização, como pela ANPD. Em todos esses casos, deve ser garantido canal eficaz, gratuito e acessível para que pais, responsáveis ou os próprios titulares, conforme sua capacidade progressiva, possam acessar os dados tratados, compreender como estão sendo usados e solicitar correções em caso de erros ou imprecisões - algo crítico principalmente em se tratando de sistemas automatizados, que frequentemente falham com mais intensidade nos grupos mais vulneráveis. A hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD), ao ser aplicada para este público, exige um cuidado ainda maior (vide resposta 5). Por exemplo, o art. 158, XII, da Lei Geral do Esporte, ao restringir o cadastramento biométrico a maiores de 16 anos, e a [Nota Técnica nº 175/2023/CGF/ANPD](#), ao avaliar o projeto “Estádio Seguro”, parece indicar que essa justificativa, quando adotada sem salvaguardas adequadas, é incompatível com a proteção integral de crianças e adolescentes.

Comentários do ITI à Tomada de Subsídios da ANPD sobre Dados Biométricos

29 de julho de 2025

O Information Technology Industry Council (ITI) agradece a oportunidade de apresentar comentários à Tomada de Subsídios da Autoridade Nacional de Proteção de Dados (ANPD) sobre dados biométricos. O ITI é a principal voz, defensor e líder de pensamento do setor global de tecnologia da informação e comunicação. Nossos membros incluem as principais empresas de inovação do mundo, com sedes e cadeias de valor distribuídas em todo o mundo.

A privacidade e a confiança são fundamentais para os negócios e as operações globais de nossos membros. Juntamente com nossos membros, o ITI trabalha com governos, órgãos reguladores e partes interessadas em todo o mundo para fortalecer e alinhar as abordagens de proteção de dados e privacidade que protegem os direitos individuais e promovem a inovação.

I. DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

A LGPD não traz uma definição expressa do que se entende por "dado biométrico", limitando-se a incluí-lo como um dos tipos de dados pessoais sensíveis (art. 5º, II). Diante dessa lacuna conceitual, a interpretação adequada do que seja dado biométrico requer a combinação dos critérios estabelecidos na própria LGPD com referências internacionais consolidadas, especialmente o *General Data Protection Regulation* (GDPR), bem como posicionamentos de autoridades estrangeiras de proteção de dados e entidades especializadas.

Em primeiro lugar, é essencial considerar que, nos termos da LGPD, somente são considerados dados pessoais aqueles que permitem identificar ou tornar identificável uma pessoa natural. Esse critério é fundamental: características físicas ou comportamentais somente devem ser tratadas como dados pessoais quando estiverem direta ou indiretamente associadas à identidade de um determinado titular de dados e utilizadas para esse fim.

O Artigo 4.14 da GDPR define dados biométricos como o resultado de um "processo técnico específico" aplicado às características físicas, fisiológicas ou comportamentais de um indivíduo com o objetivo de identificação única dessa pessoa. O *Recital* 51 (Considerando 51) reforça que imagens, como fotografias ou vídeos, não são, por si só, dados biométricos, a menos que sejam tecnicamente tratadas para fins de identificação¹.

¹ *General Data Protection Regulation*. GDPR-text.com, 2018. Disponível em: <https://gdpr-text.com/read/recital-51/?col=2&lang1=pt&lang2=en&lang3=ru>. Acesso em 24 de jul. 2025

Esse entendimento é corroborado pelo Conselho Europeu de Proteção de Dados (EDPB)², que esclarece que o mero registro de imagens não constitui por si só o tratamento de dados biométricos. Isso só ocorre quando essas imagens são tratadas por algoritmos ou técnicas que extraem medidas biométricas - como vetores faciais ou mapas dactiloscópicos - e as utilizam com a finalidade de identificar ou autenticar indivíduos.

As autoridades nacionais europeias adotaram critérios semelhantes. A Autoridade de Proteção de Dados do Reino Unido (ICO)³, por exemplo, sustenta que os dados biométricos devem (i) referir-se a características físicas, fisiológicas ou comportamentais, (ii) estar sujeitos a tratamento técnico específico e (iii) ter a finalidade de permitir a identificação exclusiva de uma pessoa. A autoridade dos Países Baixos segue uma linha semelhante, afirmando que os dados biométricos são dados que (i) se referem a características pessoais que são geralmente permanentes; (ii) resultam de tratamento técnico comparando medidas biométricas com uma referência; e (iii) têm a finalidade de estabelecer ou confirmar a identidade de um indivíduo.⁴

Nos Estados Unidos, os legisladores estaduais aderiram a essas normas globais (tratando a biometria como sensível somente quando usada para identificação) ao aprovarem leis abrangentes de privacidade do consumidor, as quais estão presentes em 20 estados diferentes.

Portanto, é possível extrair três critérios objetivos que devem ser observados cumulativamente para que determinados dados sejam considerados dados sensíveis nos termos da LGPD:

1. Referência a características físicas, fisiológicas ou comportamentais inerentes a uma pessoa natural (e.g., impressões digitais, características faciais, voz e o andar);
2. Submissão a tratamento técnico específico, por meio do uso de tecnologias que extraem, codificam ou convertem essas características em medidas ou modelos;
3. Finalidade de identificação ou autenticação individual, ou seja, o uso de dados com a finalidade de permitir ou confirmar quem é o titular dos dados.

Portanto, não basta somente que uma tecnologia capture características do corpo humano para que ela esteja tratando automaticamente com dados sensíveis. A identificação (ou identificabilidade) do titular dos dados é um elemento indispensável para determinar dados como biométricos. Sendo assim, as tecnologias que apenas detectam presença, inferem atributos sem identificação ou realizam rastreamento anônimo não devem, por si só, serem classificadas como tratamento de dados biométricos.

Alguns exemplos de usos importantes da biometria que não envolvem identificação incluem:

- Distinção entre uma pessoa e um objeto em um depósito. Esse é um mecanismo de segurança crucial para proteger pessoas de serem lesionadas por máquinas automatizadas.
- Automação de funções de rotina, como o uso de vozes humanas para transcrever registros de reuniões ou auxiliar pessoas com deficiências físicas.

² *Guidelines 3/2019 on processing of personal data through video devices*. Edpb.europa.eu, 2020. Disponível em: <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en> Acesso em 24 de jul. 2025

³ *Key data protection concepts*. Ico.org.uk. Disponível em: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/key-data-protection-concepts/>. Acesso em 29 de jul. 2025

⁴ *Rules for the use of biometrics*. Autoriteitpersoonsgegevens.nl. Disponível em: <https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/biometrics/rules-for-the-use-of-biometrics>. Acesso em 29 de jul. 2025

- Contagem do número de pedestres que usam serviços locais, como trilhas para caminhadas ou transporte público.
- Uso de Inteligência Artificial (IA) para descrever imagens em texto ou áudio para, por exemplo, ajudar usuários com baixa visão.
- Foco de câmera em rostos humanos em vez de objetos de fundo.

Em conclusão, a Autoridade Nacional de Proteção de Dados (ANPD) deve adotar uma abordagem cuidadosa e tecnicamente orientada, de acordo com as melhores práticas internacionais. Isso significa reconhecer que o conceito de dados biométricos sensíveis não deve ser aplicado de forma ampla ou imprecisa, mas somente quando os três critérios mencionados acima estiverem presentes. Essa postura é essencial para garantir a segurança jurídica, evitar distorções interpretativas e permitir o uso responsável de tecnologias que operam com dados biométricos, mas que não necessariamente expõem os titulares dos dados a riscos significativos de identificação. Ao se concentrar no uso da biometria como um método de identificação - onde ela é mais sensível - garante-se que o foco regulatório permaneça nos cenários com maior potencial de dano.

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

Os três critérios principais (explicados na resposta à pergunta 1) devem ser aplicados aos dados biométricos comportamentais da mesma forma que os dados biométricos tradicionais. A mera coleta ou análise desses comportamentos não é suficiente para caracterizá-los como dados sensíveis nos termos da LGPD.

Outro elemento importante para essa análise é o conceito de imutabilidade relativa, abordado pelo European Parliamentary Research Service (EPRS)⁵. Segundo o estudo, o termo "biométrico" pressupõe certo grau de permanência: são características que os indivíduos não podem alterar voluntariamente, como o rosto ou a impressão digital. Portanto, as técnicas que analisam gestos, assinaturas, voz ou marcha - apesar de envolverem comportamento - podem ser consideradas biométricas, pois se baseiam em padrões corporais relativamente constantes. Por outro lado, comportamentos voluntários e amplamente modificáveis, como preferências de navegação, hábitos de consumo ou conteúdo de comunicação, não se qualificam como dados biométricos, pois não refletem uma característica física ou comportamental estável intrínseca ao corpo da pessoa.

Em resumo, a mera natureza comportamental dos dados não é suficiente para classificá-los automaticamente como dados biométricos. É essencial avaliar o método de tratamento técnico e a finalidade do uso. Essa abordagem evita uma interpretação excessivamente ampla e desproporcional da categoria de dados biométricos e garante um equilíbrio entre a proteção de direitos e a inovação tecnológica, em linha com os princípios da LGPD.

II. HIPÓTESES LEGAIS

⁵ *Biometric Recognition and Behavioural Detection. Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*. European Parliament, August 2021. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf). Acesso em 29 de jul. 2025

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

Para que o consentimento para o tratamento de dados biométricos seja considerado livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD, é essencial que o titular dos dados tenha clareza sobre a finalidade do tratamento, compreenda suas implicações e possa expressar sua vontade de forma autônoma, sem coerção ou engano.

A exigência de que o consentimento seja dado livremente não implica necessariamente a ausência de quaisquer condicionamentos. O que a LGPD proíbe é a coerção, a falta de transparência ou a imposição de desvantagens excessivas ao titular dos dados. A mera oferta de um serviço vinculado ao tratamento de dados pessoais - inclusive dados biométricos - não invalida, por si só, o consentimento. A mera oferta de um serviço em troca de consentimento não o invalida, desde que:

- Haja transparência com relação à necessidade dos dados para a prestação do serviço; e
- O titular dos dados não seja obrigado a consentir sob pena de sofrer desvantagens desproporcionais ou discriminatórias;

É importante reconhecer que o titular dos dados tem a liberdade de determinar quais serviços deseja usar, e pode ou não consentir com o tratamento de seus dados, com base em informações claras e suficientes fornecidas a ele pelos agentes de tratamento. O ecossistema digital, caracterizado pelo alto dinamismo, competitividade e pluralidade de soluções, oferece aos titulares de dados meios concretos para exercer essa autodeterminação informativa, escolhendo os serviços que melhor se alinham às suas preferências e expectativas. Assim, o consentimento pode ser livre, mesmo que sua recusa resulte na indisponibilidade de um determinado serviço, desde que não seja um serviço essencial ou de acesso obrigatório.

O consentimento pode não ser uma hipótese legal adequada em situações de desequilíbrio estrutural entre as partes, como nas relações entre o governo e os cidadãos, ou em contextos em que a recusa do consentimento cause danos desproporcionais ao titular dos dados, comprometendo assim sua liberdade de escolha. Nesses casos, deverão ser utilizadas outras bases legais previstas na LGPD, sempre com a devida observância dos princípios da minimização, necessidade e finalidade.

Dada a relevância do consentimento como base legal para o tratamento de dados pessoais sensíveis, é essencial que a ANPD reconheça, em suas diretrizes e interpretações regulatórias, as particularidades envolvidas na avaliação do livre consentimento, especialmente no contexto da economia digital. Esse reconhecimento é essencial para evitar abordagens excessivamente restritivas que possam comprometer a viabilidade legal e econômica de modelos de negócios legítimos amplamente utilizados na prestação de serviços digitais. Ao considerar a liberdade dos titulares de dados de escolher, com base em informações claras, quais serviços desejam utilizar e com quais práticas de tratamento de dados concordam, a ANPD contribuirá para a consolidação de um ambiente regulatório equilibrado que, ao mesmo tempo, proteja os direitos dos titulares de dados e garanta a sustentabilidade da inovação e da competitividade no ambiente digital brasileiro.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De

que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

O uso de dados biométricos para fins de prevenção à fraude deve ser analisado à luz da LGPD, ponderando, de um lado, os direitos fundamentais à privacidade e à proteção de dados e, de outro, o interesse coletivo na segurança, na estabilidade econômica e na prevenção de atos ilícitos. Trata-se de uma típica aplicação do princípio da proporcionalidade, que exige a verificação da adequação, necessidade e proporcionalidade da medida em sentido estrito. No contexto brasileiro, marcado por altos índices de fraudes bancárias, golpes digitais e uso indevido de identidades falsas, o tratamento de dados biométricos para fins de autenticação é, muitas vezes, a medida mais segura, eficaz e menos invasiva disponível para proteger os usuários e o sistema financeiro como um todo.

Vale ressaltar que, segundo a Serasa, somente em janeiro de 2025, foram registradas 1,24 milhão de tentativas de fraude no Brasil, um aumento de 41,6% em relação ao ano anterior - o equivalente a uma tentativa de golpe a cada 2,2 segundos. Dados da Serasa Experian⁶ mostram que, em 2024, as tentativas de fraude contra bancos e cartões cresceram 10,4% em relação a 2023, representando 53,4% de todas as fraudes registradas no ano. Essas fraudes, evitadas pelo uso de mecanismos de autenticação de usuários, poderiam ter causado um prejuízo estimado em R\$ 51,6 bilhões.

A base legal para prevenção de fraudes, expressamente prevista no artigo 11, II, "g" da LGPD, reflete esse equilíbrio e representa um avanço regulatório em relação ao GDPR europeu, que não trata especificamente desse cenário. A ausência dessa base legal na legislação europeia tem criado dificuldades práticas, levando as empresas a se valerem de outras bases legais.

No Brasil, o reconhecimento legal da prevenção à fraude como base legal para o tratamento de dados sensíveis deve ser interpretado como uma expressão dos princípios constitucionais da segurança jurídica e da ordem econômica, previstas no art. 170 da Constituição Federal, bem como compatível com o princípio da necessidade previsto na LGPD. O uso da biometria, desde que acompanhado de salvaguardas técnicas e organizacionais adequadas - como minimização de dados, medidas robustas de segurança, governança e avaliação de impacto - não é apenas proporcional, mas socialmente desejável. Além de proteger o titular dos dados, a biometria pode atuar como um mecanismo de inclusão digital, permitindo o acesso seguro a serviços essenciais, especialmente para populações vulneráveis.

Portanto, dada a realidade nacional e a necessidade de proteção contra ameaças sistêmicas, o tratamento de dados biométricos para fins de prevenção de fraudes deve ser reconhecido como legítimo, necessário e proporcional, dentro de uma interpretação equilibrada da LGPD que garanta tanto os direitos individuais quanto a segurança das relações sociais e econômicas.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e

⁶ Prevenção à Fraude. Mais da metade dos brasileiros já foi vítima de fraude e 20% deles perderam até R\$ 5 mil, revela estudo inédito da Serasa Experian. Experian, 25 de março de 2025. Disponível em:

<https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/mais-da-metade-dos-brasileiros-ja-foi-vitima-de-fraude-e-20-deles-perderam-ate-rdollar-5-mil-revela-estudo-inedito-da-serasa-experian/>

Acesso em 30 de jul. 2025

órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

Quando o tratamento de dados biométricos for realizado para o cumprimento de uma obrigação legal ou regulatória, é essencial que os controladores observem os princípios previstos na LGPD e adotem salvaguardas adequadas para mitigar riscos e garantir os direitos dos titulares dos dados. Os princípios de finalidade, necessidade e minimização de dados devem orientar todas as atividades de tratamento. Isso significa que:

- **Finalidade:** o tratamento deve estar claramente vinculado à obrigação legal ou regulatória, sendo vedada a utilização de dados biométricos para fins diversos daqueles expressamente previstos em lei;
- **Necessidade:** deve ser comprovado que os dados biométricos são estritamente necessários para o cumprimento da obrigação e que a finalidade não pode ser alcançada por meios menos invasivos;
- **Minimização:** somente as informações biométricas indispensáveis para o cumprimento da obrigação devem ser coletadas e tratadas, evitando-se a coleta excessiva ou desproporcional.

Além disso, é essencial que os controladores adotem medidas técnicas e administrativas robustas para garantir a segurança dos dados biométricos.

III. TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRT) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

Embora o uso de tecnologias de reconhecimento facial esteja amparado por hipóteses legais na LGPD, sua aplicação deve observar estritamente os princípios da necessidade, proporcionalidade, transparência e não discriminação. Em particular, é importante reconhecer que, em determinados contextos - como a prevenção de fraudes no sistema financeiro ou em serviços digitais -, o uso da biometria pode ser não apenas legítimo, mas essencial para proteger os direitos dos usuários e garantir a integridade das operações. Nesses casos, o reconhecimento facial pode ser a única ferramenta viável para impedir a fraude de identidade e o acesso não autorizado, desde que seu uso seja proporcional à gravidade do risco e cercado de salvaguardas adequadas.

Mesmo assim, a proteção contra riscos à privacidade e à dignidade dos titulares de dados continua sendo fundamental. O princípio da necessidade exige que o uso dessa tecnologia seja restrito ao mínimo necessário para atingir o objetivo de prevenção de fraudes, sem qualquer desvio para outros fins não autorizados. A proporcionalidade, por outro lado, exige uma avaliação clara de que os benefícios, especialmente em termos de interesse coletivo em segurança, estabilidade econômica e prevenção de crimes, superam os impactos sobre os direitos dos titulares dos dados. A transparência, por sua vez, impõe o dever de fornecer informações claras sobre a coleta, o uso e o armazenamento de tais dados, garantindo o exercício dos direitos previstos na LGPD.

Em resumo, o reconhecimento facial pode desempenhar um papel legítimo e relevante na prevenção de fraudes, desde que seu uso seja cuidadosamente orientado por critérios técnicos, legais e éticos

que garantam a proteção dos direitos fundamentais e evitem abusos.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Os sistemas de reconhecimento facial devem ser projetados e implementados desde o início com base no princípio da privacidade desde a sua concepção (*privacy-by-design*), adotando salvaguardas técnicas e organizacionais que garantam a alta precisão e minimizem os riscos aos direitos dos titulares dos dados. Para garantir eficácia e confiabilidade, é essencial que esses sistemas sejam treinados com bancos de dados amplos e diversificados que sejam representativos da população, a fim de reduzir a parcialidade e minimizar os erros de identificação, como falsos positivos (identificação incorreta) e falsos negativos (não identificação daqueles que deveriam ser reconhecidos).

O tratamento de dados biométricos que não permitem a identificação de uma pessoa física - ou seja, dados que não constituem dados pessoais nos termos da LGPD - é essencial para o treinamento e o aprimoramento dos sistemas de reconhecimento facial. Quando anonimizados ou utilizados de forma a não permitir a reidentificação do titular dos dados, esses dados são indispensáveis para garantir a eficácia, justiça e precisão desses sistemas, especialmente para reduzir o viés e melhorar o desempenho técnico dos algoritmos. É fundamental que a ANPD reconheça expressamente essa premissa, conferindo segurança jurídica para o desenvolvimento tecnológico responsável e compatível com os princípios de proteção de dados, sem impor restrições desproporcionais ao uso de informações que não constituam dados pessoais.

IV. SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Dado o alto potencial de danos resultantes de violações de dados biométricos, como roubo de identidade, é essencial adotar medidas técnicas e administrativas robustas para mitigar esses riscos. O setor de tecnologia tem sido proativo nesse sentido, incorporando mecanismos avançados de segurança da informação - como criptografia, segmentação de banco de dados, anonimização, controle de acesso e rastreabilidade - desde os estágios iniciais do desenvolvimento de produtos e sistemas.

Além disso, muitas empresas já implementam práticas sofisticadas de *privacy by design* e *by default*, tratando dados biométricos de forma parametrizada, com o objetivo de identificar padrões ou calibrar sistemas, sem identificar ou reidentificar uma pessoa física, o que reduz significativamente os riscos à privacidade.

Para garantir a conformidade com a LGPD, é fundamental que as organizações adotem parâmetros

mínimos para avaliação contínua de riscos por meio de relatórios de impacto à proteção de dados (RIPDs) e monitoramento de possíveis vieses ou falhas de segurança. A definição de políticas internas claras, o treinamento das equipes e a governança ativa sobre o ciclo de vida dos dados também são medidas fundamentais para garantir o tratamento responsável e proporcional desses dados sensíveis. Esse conjunto de ações, já amplamente adotado por empresas do setor, demonstra que é possível combinar inovação tecnológica com proteção abrangente aos titulares dos dados.

V. DIREITOS DE INDIVÍDUOS E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Os agentes de tratamento, especialmente no setor de tecnologia, fizeram progressos significativos na implementação de práticas que garantem o respeito aos direitos dos titulares de dados, inclusive em contextos complexos, como o tratamento automatizado de dados biométricos. As empresas de tecnologia vêm adotando medidas técnicas e organizacionais que facilitam o exercício dos direitos previstos na LGPD - como o direito à informação clara, ao acesso, à correção dos dados e à revogação do consentimento - por meio de interfaces amigáveis, políticas de privacidade mais acessíveis e canais digitais eficientes de suporte ao titular dos dados.

Além disso, o setor tem investido em soluções inovadoras para promover maior transparência, como painéis de controle de dados, logs de acesso e recursos que permitem aos titulares visualizar, corrigir ou excluir dados de forma independente. No caso específico da biometria, várias empresas já incorporaram salvaguardas, como *privacy-by-design*, uso de dados pseudonimizados para treinamento do sistema e fornecimento de mecanismos para revisão humana de decisões automatizadas, quando necessário. Esses esforços demonstram um compromisso com o uso ético e seguro de tecnologias avançadas, promovendo a proteção de dados pessoais sem comprometer a funcionalidade e a inovação.



/Biometría, Derecho Administrativo y Datos

/Este estudio se enmarca dentro de la Cátedra ENIA
UAM-Veridas en IA Responsable.



Financiado por
la Unión Europea
NextGenerationEU



MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA



Plan de Recuperación,
Transformación y Resiliencia



VeriDas

Los autores de este estudio son:

- **Julián Fiérrez Aguilar**, Catedrático de Universidad, Director del Grupo de Reconocimiento Biométrico de la Universidad Autónoma de Madrid (<https://biometrics.eps.uam.es/>) y director de la Cátedra ENIA UAM-Veridas en IA Responsable.
- **Rubén Tolosana Moranchel**, Profesor Permanente Laboral en la UAM y co-director de dicha Cátedra ENIA.
- **Leire Arbona Puértolas**, Directora de Legal y Cumplimiento de Veridas.
- **Mikel Sánchez Yoldi**, Director de Ingeniería de Soluciones de Veridas.
- **Francisco Zamora Martínez**, Director de Tecnologías Core de Veridas.

Todos los derechos reservados. Este documento contiene información confidencial, propiedad de Veridas Digital Authentication Solutions, S.L., y no puede ser reproducido, copiado ni divulgado a terceros sin la autorización expresa y por escrito de Veridas. La información contenida en este documento debe mantenerse en secreto y utilizarse exclusivamente en beneficio de Veridas.

/Índice

01

/Introducción

Caminar de la mano hacia una
identidad digital privada y segura _____ 04

02

/De las contraseñas a los RBRs

La importancia de la identidad digital
segura y confiable _____ 06

Las contraseñas: un método
insostenible _____ 08

Las técnicas biométricas originarias:
riesgos y limitaciones _____ 12

Referencias Biométricas Renovables:
una tecnología segura y privada por
diseño y defecto _____ 16

RBRs vs. Plantillas Biométricas _____ 24

03

/Ejercicio práctico

Parte 1: Construcción de RBRs _____ 29

Parte 2: Construcción de Plantillas
Biométricas _____ 34

Parte 3: RBRs vs. Plantillas
Biométricas _____ 40

04

/Conclusiones

¿Es posible comprometer un RBR? _____ 42

Una Nueva Era en Identidad Digital:
El Potencial de las Referencias
Biométricas Renovables (RBRs) _____ 44

01 / Introducción

/ Caminar de la mano hacia una identidad confiable en los espacios físicos y digitales

En 1992, Europa dio un paso histórico con la creación del **Mercado Único Europeo**, un hito que no solo unió economías, sino que demostró el poder de la **colaboración entre naciones, reguladores y empresas** para lograr un entorno más próspero y seguro. Este éxito consolidó a Europa como un referente mundial en **derechos individuales, progreso económico y bienestar social**.

En esa misma línea, Europa se ha posicionado a la vanguardia de la **protección de datos personales**, destacando con la aprobación en 2016 del **Reglamento General de Protección de Datos (RGPD)**¹, que reafirma su compromiso con la privacidad y seguridad en el entorno digital. **Para los desarrolladores de tecnología, cumplir con el RGPD no solo permite el acceso a mercados europeos, sino también les permite contar con diferenciales valorados por la ciudadanía para competir en todo el mundo.** La demanda de soluciones que generen confianza ha convertido esta regulación en un **estándar reconocido internacionalmente**.

A lo largo de los últimos años, vivimos inmersos en una **nueva revolución industrial** impulsada por la digitalización y el avance de la **Inteligencia Artificial**. **En este escenario**

global, las autoridades de protección de datos en Europa han identificado con claridad los desafíos que plantea la digitalización y han sabido regularlos de forma precisa.

Estas regulaciones, como el RGPD, han sido **claves para marcar el rumbo a los desarrolladores**, quienes están logrando soluciones tecnológicas creadas para finalidades y requisitos específicos que no solo cumplen con la normativa, sino que van más allá en la protección de los ciudadanos, **promoviendo una confianza fundamentada** en el uso adecuado de estas tecnologías.

En el año 2012, el entonces Grupo de Trabajo del Artículo 29, hoy Comité Europeo de Protección de Datos (CEPD), analizó los sistemas de identificación basados en Plantillas Biométricas y advirtió sobre los riesgos para la privacidad y seguridad. Aunque fue una evaluación acertada para su época, los **nuevos desarrollos tecnológicos han cambiado por completo las reglas del juego.**

La llegada de la **Inteligencia Artificial con Redes Neuronales Profundas** aplicada a la biometría ha permitido que las **Referencias Biométricas Renovables (RBRs)** se expandan y asienten, transformando por completo la gestión de datos biométricos y logrando que la **seguridad y la privacidad**, antes vistas como opuestas, ahora se potencien mutuamente.

La velocidad a la que se están produciendo estas innovaciones tecnológicas **requiere una reacción rápida** por parte de los reguladores. Si Europa no acompaña este ritmo, perderá su actual posición de liderazgo global de la identidad digital. En su dictamen de 23/05/2024² sobre el flujo de pasajeros

en aeropuertos, el Comité Europeo de Protección de Datos recalca: **“Cualquier conclusión en esta opinión queda sujeta a futuros desarrollos tecnológicos”**. Este enfoque deja claro que las normativas deben evolucionar constantemente para **reflejar los avances en biometría y otras tecnologías.**

No se trata de revisar las decisiones del pasado, que fueron correctas para las tecnologías de su tiempo, sino de **certificar** las nuevas soluciones con rapidez, **monitorear** sus efectos y **adaptarlas** de forma continua. En el campo de las soluciones de software es imprescindible referirse a soluciones certificadas para dar seguridad en lo que constituye el objeto de la regulación. Esta dinámica requiere la **colaboración constante entre las autoridades de Protección de Datos, Inteligencia Artificial, Ciberseguridad, las organizaciones de defensa de los Derechos Digitales y los propios desarrolladores.**

Por último, las soluciones a todos estos problemas las debemos seguir buscando en el **Derecho. Los miedos, las presunciones o los prejuicios no pueden servir de base para limitar los derechos fundamentales de las personas y la libre iniciativa empresarial.**

Estas limitaciones solamente las pueden establecer las leyes que deben ser elaboradas en base a **hechos, certezas y diálogo.**

¹ <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

² https://www.edpb.europa.eu/system/files/2024-05/edpb_opinion_202411_facialrecognitionairports_en.pdf

02 / De las contraseñas a los RBRs

/La importancia de la identidad digital privada y segura

En la actualidad, la vida de las personas transcurre tanto en **espacios físicos** como en **entornos digitales**, y en ambos contextos es fundamental utilizar la **identidad de manera confiable**.

Una primera regla para lograr esa confiabilidad es la de que, **por defecto, solamente debemos acreditar nuestra identidad cuando haya una razón que lo justifique. Evitar que nuestra identidad sea suplantada sin nuestro consentimiento es la razón principal** a la que se unen otras de evitación de fraudes, cumplimiento de requisitos normativos o conveniencia.

En el mundo físico, la identidad personal se verifica mediante documentos oficiales como el DNI, pasaporte o permiso de conducir. Sin embargo, en el ámbito digital, la **gestión de la identidad** presenta mayores desafíos. A medida que la **digitalización avanza** y nuestras actividades se trasladan al entorno online, la **confianza en la autenticidad de la identidad** se convierte en un pilar esencial para el funcionamiento seguro de la sociedad.

Aunque el entorno físico ha sido tradicionalmente considerado más confiable, hoy esa garantía ya no existe. La **IA generativa** permite la creación de **documentos de identidad falsos** con apariencia auténtica, que se usan tanto en entornos presenciales como digitales. Esto convierte al mundo físico en un entorno **tan vulnerable, o incluso más**, que el digital, aunque en este último, los fraudes pueden alcanzar dimensiones mucho mayores.

Existe, además, una descompensación notable en la **percepción de la gravedad** de la suplantación de identidad en ambos espacios. En el mundo físico, se considera un **delito**, mientras que en el digital ha comenzado a **normalizarse**. Esta diferencia, junto con la falta de **mecanismos efectivos** de verificación de identidad, ha generado un déficit de confianza en las interacciones online. Según Europol y la Agencia de la Unión Europea para la Ciberseguridad (ENISA), más del **60% de los incidentes de cibercrimen** en 2023 estuvieron relacionados con **ataques de phishing**³.

La Carta de los Derechos Fundamentales⁴ de la Unión Europea protege la privacidad de los ciudadanos, garantizando el derecho al respeto de la vida privada (artículo 7) y el derecho a la protección de datos personales (artículo 8). El **Reglamento General de Protección de Datos (RGPD)** y toda la legislación en materia de protección de datos está también enfocada a la minimización del tratamiento de datos personales, es decir, de esa información que identifica o hace identificable a una persona.

Es por ello que cualquier proceso que requiera la acreditación de la identidad de los usuarios debe estar adecuadamente analizado, con el objetivo de ofrecer las **máximas garantías de privacidad y seguridad**. Este análisis implica no solo la fundamentación legal, sino también la búsqueda de los medios más pertinentes para lograr el fin perseguido, protegiendo a los usuarios de posibles intentos de suplantación al tiempo que su privacidad no se ve mermada.

En España, **la Carta Española de Derechos Digitales⁵** reconoce el derecho al **pseudoni-**

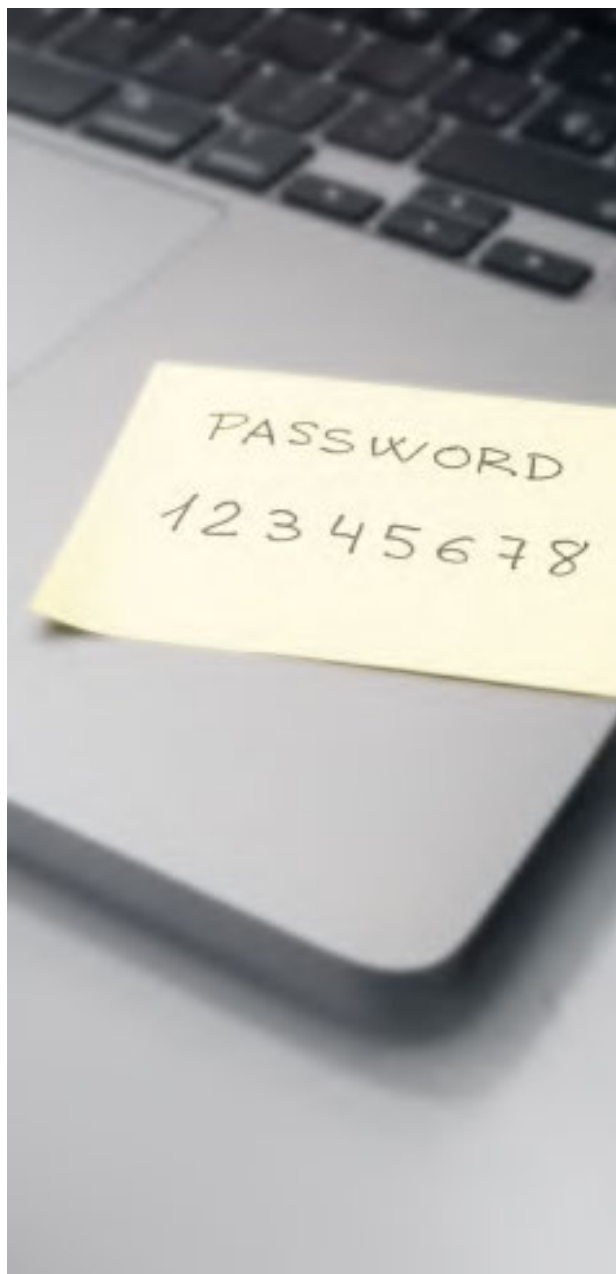
mato, lo que permite a los individuos usar un seudónimo siempre que no se generen perjuicios a terceros. Sin embargo, este derecho está sujeto a la condición de que, en caso necesario, la identidad real pueda ser acreditada ante una autoridad judicial.

En definitiva, el pseudonimato, cimentado en una **verificación de la identidad previa**, permite mantener el equilibrio entre la **privacidad y la responsabilidad legal**, al permitir que se preserve la identidad de un individuo salvo en situaciones en las que debe ser revelada. Este sistema previo de verificación es el que permite autenticar al usuario cuando sea necesario, proporcionando así una capa adicional de **seguridad en el entorno digital**. Los métodos actuales, como las contraseñas, han demostrado ser vulnerables y poco eficaces por sí solos, lo que hace que la adopción de **tecnologías avanzadas** sea indispensable para consolidar un entorno digital seguro, privado y alineado con los **derechos individuales**.

³ <https://www.europol.europa.eu/publications-events/main-reports/iocta-report>

⁴ https://www.europarl.europa.eu/charter/pdf/text_es.pdf

⁵ https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf



/Las contraseñas: un método insostenible en solitario

Desde su invención en los años 60 para proteger sistemas informáticos primitivos, las contraseñas se han mantenido como la principal herramienta de autenticación digital. Sin embargo, hoy en día, su **efectividad global ha quedado en entredicho** debido a la creciente sofisticación de los **ciberataques** y los desafíos de seguridad que presentan. En lugar de ser un pilar fiable de seguridad, las contraseñas han pasado a ser vistas como un método **vulnerable, costoso e insostenible**, y además, constituyen uno de los principales elementos de la **brecha digital**, ya que su gestión compleja genera desigualdades en el acceso seguro a los servicios digitales.

Hackeabilidad: riesgo teórico y real

En teoría, las contraseñas que combinan letras, números y símbolos ofrecen una resistencia razonable frente a los ciberataques. Sin embargo, los datos son alarmantes y sugieren que la realidad difiere notablemente de la teoría:

⁶ <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

⁷⁸⁹ <https://www.ibm.com/reports/data-breach>

¹⁰ <https://www.weforum.org/agenda/2021/12/passwords-safety-cybercrime/>

¹¹ <https://krontech.com/33-password-statistics-you-need-to-know-for-your-cyber-security>

El número de violaciones de datos ha aumentado significativamente a nivel mundial. Un ejemplo claro es Estados Unidos, donde se pasó de 447 violaciones en 2012 a más de **3.200 en 2023** ⁶, con un costo promedio de **4,81 millones de dólares por brecha** ⁷, reflejando el alarmante incremento de este tipo de incidentes.

El phishing y el robo de credenciales se han consolidado, por segundo año consecutivo, como la principal puerta de entrada para los ciberataques. Las credenciales comprometidas es el tipo de fraude más común, suponiendo el **16%** de todas las violaciones de datos ⁸.

Las violaciones relacionadas con el robo o compromiso de credenciales son las que más tiempo tardan en ser identificadas y contenidas, con un promedio de **292 días** desde la infiltración hasta la resolución ⁹.

Al preguntar cómo los usuarios gestionan sus contraseñas, el **18%** admite usar la misma contraseña para todos sus servicios online, el **39%** las anota en un papel, el **10%** las guarda en un archivo en su ordenador, y solo el **28%** utiliza un gestor de contraseñas seguro.

Una contraseña de **8** caracteres solo con letras minúsculas puede ser hackeada **instantáneamente**. Si se añade una mayúscula y un número, el tiempo de hackeo se extiende a **1 hora**, y si además se incluye un símbolo, puede tardar hasta **8 horas** ¹⁰.

El **49%** de los profesionales de seguridad informática y el **51%** de los usuarios admiten compartir sus contraseñas con otras personas, incluso para acceder a cuentas empresariales, lo que expone gravemente las redes internas a ataques e imposibilita la trazabilidad de responsabilidades ¹¹.

De las **20** contraseñas más comunes a nivel mundial, **17** pueden descifrarse en **menos de un segundo**, siendo la combinación “12345” la más utilizada ¹². Concretamente, el 24% de los estadounidenses usa variaciones de contraseñas extremadamente débiles como: “abc123”, “Password”, “123456”, “Iloveyou”, “111111”, “Qwerty”, “Admin” y “Welcome” ¹³.

¹² <https://www.cnn.com/2023/11/16/most-common-passwords-70percent-can-be-cracked-in-less-than-a-second.html>

¹³ <https://www.comparitech.com/blog/information-security/password-statistics/>

¹⁴ <https://www.digitalguardian.com/blog/uncovering-password-habits-are-users%E2%80%99password-security-habits-improving-infographic>



¹⁵ <https://www.pewresearch.org/internet/2017/05/17/tech-adoption-climbs-among-older-adults/>

¹⁶ <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/is-cybersecurity-incompatible-with-digital-convenience>

Brecha digital: contraseñas y desigualdad de acceso

El uso de contraseñas complejas y su correcta gestión requieren de un cierto nivel de **alfabetización digital**. Sin embargo, muchas personas, especialmente de sectores más vulnerables, con discapacidades o con menos acceso a la educación tecnológica, están más expuestas a los ciberataques por la dificultad que les supone su correcta gestión.

El reciente estudio¹⁵ sobre la adopción de tecnología entre los adultos mayores revela que las personas de mayor edad suelen tener dificultades para **gestionar de manera segura** sus credenciales digitales. En particular, el informe indica que muchos adultos mayores (63%) se ven obligados a escribir sus contraseñas en papel, lo que aumenta el riesgo de que sean robadas o comprometidas. Además, el estudio destaca que 49% de los adultos mayores no tienen confianza en su capacidad para realizar tareas en línea de forma segura, lo que perpetúa las malas prácticas de seguridad como la reutilización de contraseñas y el uso de contraseñas débiles.

Por tanto, es crucial complementar las soluciones actuales de identificación con otras que sean más **intuitivas y accesibles** para todos, independientemente de su nivel de educación o experiencia tecnológica. Solo así podremos garantizar que la **identidad digital esté protegida** y que todos tengan la oportunidad de participar plenamente en la economía digital.

Insostenibilidad del modelo de contraseñas

A pesar de su larga historia como método de autenticación, las contraseñas han demostrado ser un **modelo insostenible** en el entorno digital actual, especialmente si no se combinan con otras alternativas de autenticación basadas en posesión o **inherencia**, como tokens o biometría. La creciente **sofisticación de los ciberataques** y la vulnerabilidad inherente a las prácticas de gestión de contraseñas han llevado a un aumento en las violaciones de seguridad.

Por si fuera poco, el uso de contraseñas también implica un **coste elevadísimo** para las empresas y los individuos. Según McKinsey¹⁶, las organizaciones pueden gastar hasta **70 dólares por empleado al año** en la gestión de contraseñas, incluyendo el tiempo dedicado a restablecimientos y asistencia al cliente. Además, un **50% de los empleados** ha reportado una sobrecarga laboral debido a la necesidad de asegurar sus credenciales, lo que repercute negativamente en su productividad.

La realidad es que el modelo de contraseñas, además de ser vulnerable, es costoso y poco eficiente en la gestión de identidades digitales. Con el aumento de las amenazas cibernéticas y la creciente complejidad de la tecnología, es imperativo que las organizaciones complementen sus defensas con soluciones de autenticación más sostenibles y eficaces.

/Las técnicas biométricas originarias: riesgos y limitaciones

El **reconocimiento facial** como tecnología biométrica comenzó a desarrollarse en la década de 1990, cuando los avances en el procesamiento digital de imágenes permitieron la captura y **análisis automatizado** de los rasgos faciales.

Pero no fue hasta los años 2000, cuando comenzó a ganar tracción con su implementación en aeropuertos, instalaciones gubernamentales y empresas para **mejorar la seguridad y funcionalidad**. Durante esa década, la tecnología avanzó rápidamente, impulsada por el aumento de la capacidad de procesamiento de las computadoras y el desarrollo de algoritmos de reconocimiento cada vez más precisos.

A medida que esta tecnología se fue perfeccionando, se integró en **sistemas de autenticación digital** y dispositivos móviles, como los smartphones, donde actualmente permite desbloquear el teléfono o acceder a aplicaciones mediante el simple reconocimiento del rostro. Estos avances han hecho que el reconocimiento facial sea una de las tecnologías biométricas más utilizadas a nivel global.

¿Cómo funciona esta tecnología?

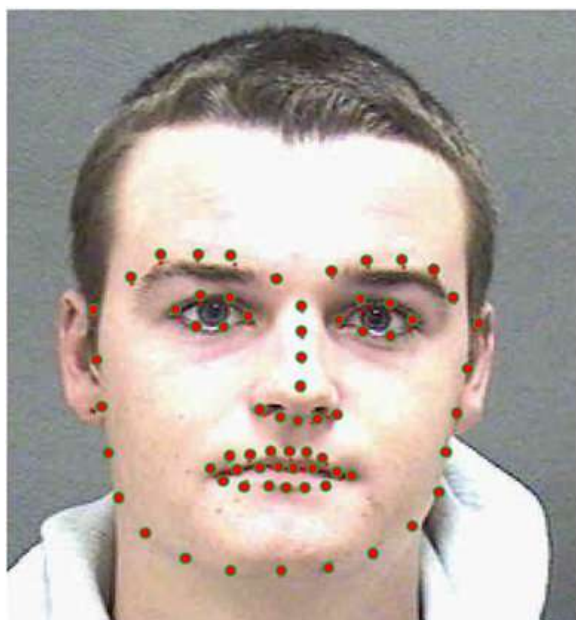
Las **Plantillas Biométricas** son representaciones matemáticas de los rasgos faciales de una persona. A diferencia de una imagen tradicional, la plantilla biométrica no guarda una foto del rostro, sino un conjunto de coordenadas que describen la relación entre distintos **landmarks faciales**.

Estos landmarks, también conocidos como “puntos característicos”, pueden incluir la distancia entre los ojos, la forma de la nariz, o la proporción de la boca respecto a otros elementos del rostro.

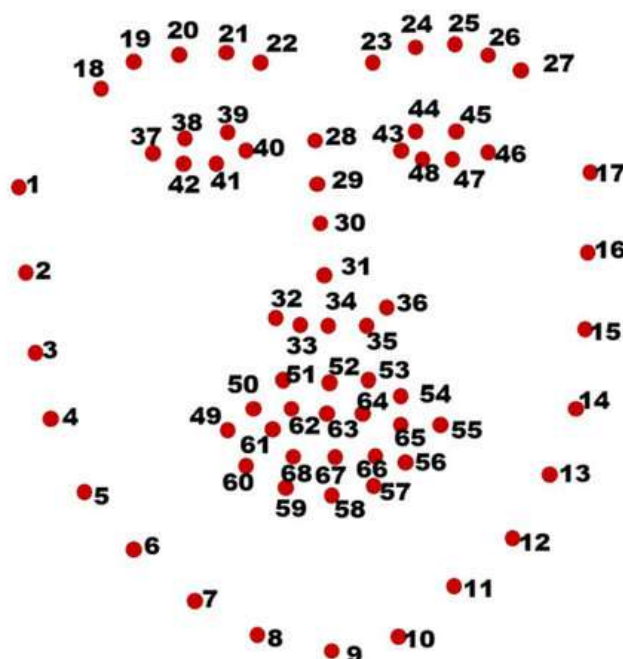
El proceso comienza con la **captura de una imagen facial** mediante una cámara. Esta imagen es analizada para identificar entre 60 y 80 puntos clave en el rostro. Los sistemas de reconocimiento facial tradicionales convierten estos puntos en una serie de datos numéricos, lo que constituye la **Plantilla Biométrica**. Esos datos se utilizan después para comparar nuevas imágenes faciales que se capturen en futuros intentos de autenticación.

Durante la autenticación, se genera una nueva plantilla basada en la imagen actual del rostro y se compara con las plantillas almacenadas. Si los rasgos faciales coinciden dentro de un **margen aceptable**, se confirma la identidad de la persona. Este método convierte los rasgos faciales en datos que permiten identificar de manera precisa a un individuo, y por ello su uso se comenzó a extender ampliamente en aplicaciones como el control de acceso, la verificación de identidad en sistemas bancarios, y la seguridad en aeropuertos.

Este enfoque tecnológico tiene sus limitaciones, que serán abordadas más adelante en el documento cuando lo comparemos con las **Referencias Biométricas Renovables (RBRs)**, que han avanzado en términos de privacidad y seguridad que ya se aplican en los sistemas empleados en los casos de uso señalados.



(a)



(b)

Fuente imagen. 'A framework for facial age progression and regression using exemplar face templates' por Ali Ahmed Elmahmudi and Hassan Ugail¹⁷

¹⁷ https://www.researchgate.net/publication/343699139_A_framework_for_facial_age_progression_and_regression_using_exemplar_face_templates

¿Cuáles son sus riesgos y limitaciones?

A pesar de los avances que trajo consigo el reconocimiento facial basado en **Plantillas Biométricas**, esta tecnología plantea **importantes riesgos para la privacidad y la seguridad**, como quedó reflejado en el **Dictamen 3/2012 del Comité Europeo de Protección de Datos (CEPD)**. Este dictamen fue uno de los primeros estudios en Europa que abordó de manera exhaustiva los problemas asociados al uso de las Plantillas Biométricas, señalando varios riesgos clave:

/Unicidad: Cada persona genera una única plantilla biométrica a partir de sus rasgos faciales irrepetibles. Esto significa que, si la plantilla es comprometida, no puede ser modificada o reemplazada, porque los rasgos que representa son únicos. Este riesgo convierte a las Plantillas Biométricas en un recurso sensible a largo plazo, ya que una vez que los datos son vulnerados, la persona queda permanentemente expuesta.

/Reversibilidad: A partir de una Plantilla Biométrica almacenada, es posible reconstruir la información original y, por ende, el rostro de la persona. Esto se debe a que la Plantilla Biométrica representa puntos específicos y característicos del rostro de una persona en el caso de la biometría facial. Conociendo cómo se construye esta plantilla, es posible identificar dichos puntos y, en cierta medida, reconstruir la estructura facial que representan. El impacto de este riesgo es especialmente elevado cuando las plantillas se almacenan en bases de datos centralizadas, que pueden ser objetivo de ataques y brechas de seguridad. Si un atacante accede a estas bases de datos, podría reconstruir los rasgos faciales originales de los usuarios, comprometiendo su privacidad.

/Interoperabilidad: Las Plantillas Biométricas, una vez creadas, pueden ser reutilizadas en distintos sistemas para múltiples fines. De hecho, en algunos ámbitos, especialmente en la biometría de huellas dactilares, ya existían estándares internacionales establecidos al respecto. Esta capacidad aumenta el riesgo de que, si una plantilla se ve comprometida en un sistema, el atacante pueda acceder a otros servicios utilizando la misma plantilla.

/Irrevocabilidad: A diferencia de las contraseñas, que pueden ser cambiadas en caso de compromiso, las Plantillas Biométricas no se pueden modificar ni revocar, porque en esencia son una representación “escrita” de sus rasgos. Esto implica que, si los datos biométricos de una persona son vulnerados, esa persona no tiene la capacidad de cambiar su identidad digital. La irrevocabilidad de las plantillas deja a los usuarios expuestos de manera indefinida si su información es comprometida.

El Dictamen 3/2012 subrayó que estos riesgos asociados a las Plantillas Biométricas tradicionales presentan un **alto nivel de amenaza para la privacidad y la seguridad** de los individuos. Como consecuencia, las autoridades de protección de datos europeas, incluida la AEPD, han cuestionado y restringido el uso de esta tecnología en ciertos contextos, particularmente cuando se almacenan en **bases de datos centralizadas**. Este dictamen se ha convertido en una referencia clave para el desarrollo de soluciones biométricas en la última década. Es por ello que los científicos y desarrolladores entendieron que sólo aquellas tecnologías que logran un diseño simultáneamente privado y seguro, sin comprometer ninguno de estos valores, podrán **escalarsse** de forma sostenible en Europa y, por extensión, en el mundo.

/Referencias Biométricas Renovables: una tecnología segura y privada por diseño y defecto

Las **Referencias Biométricas Renovables (RBRs)** representan una evolución tecnológica crucial para la protección de la identidad digital. Desarrolladas como respuesta a las limitaciones y riesgos de las plantillas biométricas tradicionales, las RBRs están definidas en el **estándar ISO/IEC 24745:2022**. Este estándar describe las propiedades de las RBRs que, analizadas desde una perspectiva de protección de datos y seguridad, permiten asegurar una privacidad por defecto y desde el diseño (**privacy by default and by design**), abordando las preocupaciones expresadas por las autoridades de control en relación con las plantillas biométricas tradicionales.

Cabe destacar que el estándar ISO no especifica una fórmula técnica única para convertir una referencia biométrica en una RBR, lo cual **fomenta el desarrollo** continuo de soluciones innovadoras que mejoran la privacidad y la seguridad. Esta flexibilidad solo es posible gracias a una **regulación tecnológicamente neutra**.

A continuación, se explora una de las metodologías más comunes para crear y operar con RBRs: la aplicación de **Inteligencia Artificial (IA)** y **Redes Neuronales Profundas (DNNs)** en modelos biométricos. Estas tecnologías permiten que el dato resultante posea, desde su propia concepción, todas las características de una RBR, transformando radicalmente la gestión de la biometría en favor de una mayor privacidad y seguridad. Además de mejorar la precisión, este enfoque garantiza una mayor protección de los datos biométricos al evitar su exposición directa.



La Inteligencia Artificial y el Reconocimiento Facial: el cerebro humano como base

La extensión de las RBRs es posible gracias a los avances en Inteligencia Artificial y el desarrollo de Redes Neuronales Profundas. Estas redes, inspiradas en la **estructura del cerebro humano**, consisten en capas de nodos interconectados que simulan cómo las neuronas procesan y aprenden de la información. Desde los años 40, cuando Warren McCulloch y Walter Pitts comenzaron a modelar las primeras redes neuronales, hasta la actualidad, las DNNs han evolucionado enormemente. Gracias a los avances computacionales de los últimos 20 años, las redes neuronales modernas son capaces de analizar cientos de rasgos biométricos con una precisión superior a la del reconocimiento humano, como ha sido ampliamente demostrado¹⁹.

El cerebro humano es una máquina increíblemente sofisticada para el **reconocimiento facial**. Este proceso involucra varias áreas del cerebro, particularmente la **corteza fusiforme**²⁰, que está especializada en la identificación de rostros. El cerebro no guarda una imagen exacta de cada rostro que ve; en su lugar, emplea estrategias complejas para recordar, distinguir y reconocer a las personas. A continuación, exploramos tres mecanismos clave que utiliza el cerebro, y cómo estos se reflejan en la tecnología de RBRs:

Cerebro vs. tecnología de RBRs

/Procesamiento de rasgos diferenciales: El cerebro no almacena un “mapa” exacto del rostro. En su lugar, se enfoca en los rasgos más distintivos que hacen único a cada individuo. Estos rasgos pueden ser la forma de los ojos, el tamaño de la nariz o la proporción entre diferentes partes del rostro. Esta técnica de codificación diferencial permite al cerebro identificar rápidamente a una persona incluso en condiciones cambiantes, como bajo diferentes ángulos de visión o expresiones faciales.

De manera similar, las RBRs no almacenan una imagen completa del rostro, sino que analizan entre 500 y 600 características distintivas que definen a una persona. Esto no solo permite una mayor precisión que el cerebro humano, sino que también evita la necesidad de almacenar un “molde” fijo del rostro, lo que mejora la seguridad y la privacidad.

¹⁹ <https://arxiv.org/pdf/1404.3840>

²⁰ <https://www.sciencedirect.com/science/article/abs/pii/S0028393214001869>

/Procesamiento basado en prototipos: Otra técnica que emplea el cerebro es la creación de un “rostro promedio” a partir de los rostros que ha visto a lo largo de la vida. Este “prototipo” sirve como una referencia general para comparar nuevos rostros. Cuando el cerebro observa un rostro, lo compara automáticamente con esta imagen promedio, destacando los rasgos que se desvían más de esa norma para facilitar la identificación.



Las RBRs utilizan una técnica similar, pero a una escala mucho mayor. Los algoritmos de Inteligencia Artificial se entrenan en grandes bases de datos que contienen millones de rostros, muy por encima de la cantidad de caras que nuestro cerebro llega a conocer y reconocer. Esto permite que las RBRs operen con un nivel de exactitud que supera al del cerebro, especialmente en escenarios donde hay pequeñas variaciones o características difíciles de discernir.

/Plasticidad y flexibilidad: El cerebro humano es altamente plástico, lo que significa que puede adaptarse a cambios en la apariencia física de las personas. Con el paso del tiempo, el cerebro ajusta sus patrones de reconocimiento a medida que una persona envejece o cambia su aspecto (pérdida de cabello, uso de gafas, etc.). Esta capacidad de adaptación permite que sigamos reconociendo a las personas incluso después de muchos años o cambios físicos.



En el caso de las RBRs, esta capacidad se refleja en la forma en que los algoritmos de IA no dependen de puntos faciales estáticos o landmarks fijos para identificar a una persona. En lugar de eso, los algoritmos aprenden a identificar los rasgos más relevantes y estables, que presentan pocas variaciones a lo largo del tiempo, lo que permite reconocer al usuario incluso cuando su apariencia cambia de manera significativa.

El proceso de reconocimiento facial del cerebro humano es increíblemente sofisticado, basado en la diferenciación de rasgos, la comparación con prototipos y la flexibilidad para adaptarse a los cambios. Las RBRs, impulsadas por las redes neuronales profundas, imitan estos mecanismos, pero con la ventaja de poder procesar y analizar grandes volúmenes de datos con mayor rapidez y precisión.

¿Cuáles son sus características principales?

Las Referencias Biométricas Renovables (RBRs) representan una evolución en comparación con las tecnologías biométricas tradicionales, al abordar de manera directa los riesgos identificados por el Comité Europeo de Protección de Datos (CEPD) y otros reguladores. Las RBRs son representaciones abstractas y matemáticas de los rasgos biométricos de una persona, que no almacenan datos directos de estos rasgos, lo que impide la reconstrucción de la información original.

Algunas de las características clave de las RBRs, que las hacen especialmente útiles para su uso en procesos de acreditación de identidad, incluyen las siguientes:

/Multiplicidad: Por la forma en la que se generan, cada sistema establece una forma de representar las características biométricas creando así RBRs. Es decir, de una misma imagen facial, cada sistema genera RBRs distintas que resulta imposible comparar entre sí; y de distintas imágenes faciales de una misma persona, incluso el mismo sistema genera RBRs distintas, que sí podrán ser comparadas dentro de ese sistema concreto.

En definitiva, nuestro rostro es único, pero las representaciones (RBRs) que se pueden hacer del mismo son múltiples, casi infinitas, adaptándose al contexto o aplicación en la que se usen. Esto significa que no se cuenta con una única referencia que por tanto, si se comprometiera, no pondría en riesgo todos los sistemas ni la característica biométrica (el rostro, que sí es único) de la persona. (Ver las características de No interoperabilidad y Revocabilidad).

/Irreversibilidad: Según se ha explicado respecto a su creación, muy relacionada con la forma en la que los seres humanos reconocemos y asociamos caras, las RBRs no guardan detalles específicos del rostro, lo que significa que no se puede reconstruir la imagen facial original a partir de ellas. Estas referencias están basadas en una representación abstracta de los rasgos del usuario y se codifican de manera que no puedan revertirse para recuperar los rasgos originales.

El sistema funciona por asociación de características respecto de los rostros conocidos en el entrenamiento, estableciendo referencias posicionales que son lo que, entre otras cuestiones, reflejan las RBRs. La RBR no almacena rasgos específicos del rostro que puedan ser empleados por un atacante para reconstruir el rostro o la identidad física de la persona, estando diseñadas desde el inicio para respetar y proteger la privacidad del usuario.

/No interoperabilidad: La representación abstracta y matemática que de un rostro realiza cada sistema o modelo biométrico es distinta, por lo que las RBRs solo pueden ser posteriormente interpretadas por el sistema que entiende esa representación. Eso implica que, a diferencia de las plantillas biométricas tradicionales, que pueden funcionar en distintos sistemas, las RBRs están diseñadas para ser utilizadas solo en un contexto o sistema específico. Cada RBR se adapta a una aplicación concreta y no es reutilizable en otros sistemas sin autorización, limitando su uso a un contexto específico. Así, incluso si un atacante obtiene acceso a una RBR en un sistema, no podrá utilizarla en otro, reforzando la seguridad de la identidad del usuario²¹.

/Revocabilidad: Como se ha explicado previamente, cada sistema establece una forma de representar las características biométricas para crear RBRs, y precisamente cada sistema podría también cambiar a futuro, si así fuese necesario o conveniente, ese “método”. La consecuencia de eso sería que el nuevo sistema (entendiéndose también como una nueva versión del mismo sistema) ya no utiliza ni “interpreta” las RBRs antiguas, sino que genera y emplea otras nuevas para la comparación. Así, partiendo de una misma característica biométrica (rostro), las RBRs pueden “resetearse” o revocarse si se sospecha que una referencia ha sido comprometida (aún después de entender que el riesgo ante accesos no autorizados a RBRs es mínimo) de una forma tan sencilla como cambiando algún pequeño parámetro de configuración del sistema.

Esto significa que, en caso de duda sobre la seguridad de una referencia biométrica, se puede generar una nueva dejando inservible la anterior, sin necesidad de cambiar las características biométricas originales del usuario. Esto resuelve la preocupación habitual al comparar los sistemas biométricos con las contraseñas, dado que las RBRs permiten una actualización tan rápida y eficaz como las de las contraseñas si fuese necesario (o incluso más porque la responsabilidad de regeneración recaería sobre el operador y no sobre el usuario).

La suma de todas estas características brinda un nivel de protección sin precedentes hasta la fecha, evidenciado por la **ausencia total de violaciones de datos reportados ante las Autoridades Nacionales de Ciberseguridad**. Su diseño permite cumplir con las normativas de protección de datos, tales como el RGPD en Europa, que promueven la minimización y protección de datos sensibles. Esto las convierte en una tecnología ideal para los mercados que buscan soluciones seguras y respetuosas con la privacidad, permitiendo su escalabilidad y sostenibilidad en el ámbito global.

²¹ Hoy en día es habitual encontrar dos grandes categorías de ataques a los sistemas con el objetivo de suplantar identidades: ataques de presentación, consistentes fundamentalmente en engañar al sistema en la captura de los datos de partida (por ejemplo, que el rostro no pertenezca a una persona real que se encuentra físicamente ante el dispositivo, sino que se trata de una fotografía, un vídeo, una máscara, etc.), y ataques de inyección, consistentes en introducir en el sistema datos saltándose los procesos de captura normales y los controles de seguridad. Ante cada uno de estos ataques se responde con distintas medidas de seguridad y tecnológicas, existiendo estándares y certificaciones independientes al respecto. Sin embargo, la característica de No Interoperabilidad refleja que aunque alguien consiguiera inyectar una RBR en un sistema distinto del original que la creó, saltándose todos los controles de seguridad establecidos, esa RBR va a ser inservible en ese sistema.



RBRs y el cumplimiento normativo: Un enfoque hacia la protección de datos

Las Referencias Biométricas Renovables (RBRs) abordan eficazmente las preocupaciones planteadas por las autoridades de protección de datos en relación con la **gestión y protección de datos biométricos**. Su diseño innovador garantiza que se cumplan los principios de privacidad por diseño y por defecto, ofreciendo un marco que permite la **protección de la identidad digital** de los usuarios sin comprometer sus derechos.

Es crucial que la atención no se centre únicamente en la tecnología en sí, sino en su **aplicación y en los contextos de uso**. La regulación debe enfocarse en los escenarios específicos en los que se implementan las RBRs, asegurando que se utilicen de manera que prioricen la privacidad y la seguridad del individuo.

La calidad de la tecnología es fundamental. Las RBRs han demostrado ser precisas en comparación con **estándares establecidos**, como los del National Institute of

Standards and Technology (NIST) de los Estados Unidos, y ofrecen capacidades avanzadas para la detección de ataques de suplantación e inyección, así como la mitigación de sesgos. Esto no solo asegura la eficacia de la identificación, sino que también contribuye a generar **confianza en su uso** por parte de las organizaciones.

Además, el **control del usuario sobre sus datos** es un aspecto esencial en el cumplimiento normativo. Los usuarios deben tener acceso a información clara y comprensible sobre cómo se utilizan sus datos biométricos, otorgar su **consentimiento siempre** que sea posible y contar con el poder de disposición sobre su información. Este enfoque centrado en el usuario es clave para fomentar la confianza y garantizar un marco de **uso responsable de la tecnología biométrica**.

/RBRs vs. Plantillas Biométricas

Diferentes en su esencia y en sus características

A continuación, se detallan las principales ventajas de las RBRs comparadas con las Plantillas Biométricas tradicionales:

	Plantillas Biométricas	Referencias Biométricas Renovables (RBRs)
Unicidad vs. Multiplicidad	Cada rostro de cada persona se corresponde con una única plantilla biométrica ya que ésta contiene rasgos que le son únicos . Si una plantilla se utiliza en múltiples sistemas, se convierte en un único punto de fallo , permitiendo a un atacante acceder a todos esos sistemas si logra comprometerla.	Si bien el rostro de cada persona es único, las representaciones que los sistemas biométricos hacen de él, en forma de RBRs , pueden ser múltiples . De esta forma, se generan distintas RBRs para cada contexto o sistema que emplea un usuario, y en caso de compromiso de una de ellas no se ponen en riesgo otros sistemas ni los rasgos de la persona.
Reversibilidad vs. Irreversibilidad	Las Plantillas Biométricas almacenan datos que pueden ser utilizados para reconstruir la imagen original . Por ejemplo, si una plantilla facial almacena características específicas del rostro (como la distancia entre los ojos, la forma de la nariz, etc.), un atacante que obtenga acceso a esa plantilla puede utilizar esos datos para recrear una imagen del rostro original, al estilo de un retrato robot.	Las RBRs, en lugar de una representación fija del rostro, crean una referencia matemática posicional de los rasgos de una persona dentro del conjunto de imágenes con las que la red ha sido entrenada. Esta referencia no puede ser utilizada para reconstruir la imagen original del rostro, lo que garantiza que, incluso si un atacante accede a la referencia, no podrá obtener la identidad real del usuario.

Plantillas Biométricas

Referencias Biométricas Renovables (RBRs)

Interoperabilidad vs. No interoperabilidad

Las Plantillas Biométricas pueden ser reutilizadas en **múltiples sistemas y aplicaciones**, lo que aumenta el riesgo de que, si una plantilla se ve comprometida, el atacante pueda acceder a otros servicios utilizando la misma plantilla. Esta característica genera preocupaciones sobre la exposición de datos biométricos, ya que una violación en un sistema puede tener repercusiones en varios otros, comprometiendo la identidad del usuario en múltiples contextos.

Las RBRs están diseñadas para un uso controlado y específico. Cada sistema crea RBRs distintas a las de otros sistemas, y **su uso queda limitado al sistema que las creó** dado que sólo este puede entender las referencias posicionales que representan. Esta característica implica que cada RBR **se adapta a un contexto particular**, limitando así su reutilización en diferentes sistemas. La falta de interoperabilidad entre las RBRs refuerza la seguridad de la identidad digital del usuario, garantizando que ésta se maneje de manera aislada, sirviendo al mismo tiempo como mecanismo de control para el usuario sobre sus propios datos.

Irrevocabilidad vs. Revocabilidad

Las Plantillas Biométricas son **permanentes** puesto que describen rasgos que son perdurables en el tiempo. Si esta plantilla se ve comprometida, el usuario no tiene la capacidad de cambiarla; quedan indefinidamente expuestos a riesgos de suplantación de identidad o acceso no autorizado.

Las RBRs están diseñadas para permitir la **revocación** de referencias biométricas. Si una RBR es comprometida, el sistema puede generar rápidamente una **nueva referencia** y dejar inutilizada de facto la anterior sin necesidad de alterar los rasgos del usuario.

Un proceso de creación con similitudes y diferencias estructurales

Tanto las Plantillas Biométricas como las Referencias Biométricas Renovables (RBR) ofrecen enfoques estructurados para la gestión de datos biométricos, aunque **difieren fundamentalmente** en la forma en que gestionan los riesgos para la privacidad y la seguridad. La siguiente tabla ofrece un desglose claro de los pasos clave de cada proceso, haciendo hincapié en las características específicas de cada tecnología y su impacto en la **seguridad, la privacidad y el cumplimiento** de las normas reglamentarias.

Fase del proceso	Plantillas Biométricas	Referencias Biométricas Renovables (RBRs)
1. Captura de la imagen facial	Se captura una imagen del rostro mediante una cámara estándar o infrarroja. <i>Nota: Este paso puede complementarse con un proceso de verificación de identidad para asegurar que la imagen capturada corresponda a una identidad real, verificable y autenticada. Este proceso incluye el análisis de un documento de identidad oficial, la comparación biométrica entre la foto del documento y el selfie del usuario, así como una prueba de vida para prevenir cualquier intento de fraude o suplantación.</i>	
2. Análisis de los rasgos faciales	El sistema de reconocimiento facial identifica una serie de puntos en el rostro, normalmente entre 60 y 80 landmarks, que definen las proporciones y relaciones espaciales entre las distintas partes del rostro, como la distancia entre los ojos o la posición de la nariz. Estos landmarks son puntos faciales predeterminados y comunes en todos los rostros humanos, lo que permite que el sistema sea universalmente aplicable.	Los algoritmos mezclan miles de características del rostro en un conjunto de entre 500 y 600 valores numéricos. Estas características incluyen no solo las relaciones espaciales entre los rasgos faciales, sino también patrones más profundos derivados del análisis de la imagen. Esta mayor cantidad de información permite generar una representación abstracta del rostro pero que, al mismo tiempo, dentro de la interpretación del sistema específico, es más detallada y precisa que las plantillas biométricas tradicionales. Al no depender de puntos faciales fijos, las RBRs son altamente resistentes a variaciones en la apariencia del rostro y no pueden revertirse para reconstruir el rostro original.

Fase del proceso	Plantillas Biométricas	Referencias Biométricas Renovables (RBRs)
3. Generación de la Plantilla/ RBR	Los landmarks detectados en el rostro se convierten en una representación matemática de las relaciones espaciales entre estos puntos clave. Esta Plantilla Biométrica es un conjunto de datos numéricos que describe las proporciones y las distancias entre las distintas partes del rostro, como los ojos, la nariz y la boca. El resultado es una plantilla estática vinculada de manera directa a los puntos fijos del rostro, lo que puede generar vulnerabilidades si se comprometen.	Las RBRs no almacenan información específica del rostro. En su lugar, crean una representación posicional de los rasgos biométricos en un sistema de coordenadas multidimensional, que determina cómo estos rasgos se relacionan con los de otros individuos en el sistema (ej. un número asignado en una escala de claridad de ojos indica la posición relativa de una persona en comparación con las otras, pero no refleja el color exacto de sus ojos), sin que sea posible identificar esa relación a partir de la RBR.

4. Encriptación	El proceso de encriptación en tecnologías biométricas consiste en transformar los datos biométricos generados (ya sean plantillas o referencias biométricas renovables) en un formato ilegible mediante un algoritmo criptográfico. De esta forma, los datos solo pueden ser descifrados y leídos con una clave de descryptación adecuada, garantizando la seguridad y confidencialidad de la información almacenada o transmitida. <i>Nota: La diferencia principal no radica tanto en el proceso de encriptación en sí, sino en lo que se está encriptando. Mientras que en las plantillas biométricas se encriptan datos específicos sobre los puntos faciales fijos, en las RBRs se encripta una representación abstracta y posicional que, por su diseño, ya ofrece mayor resistencia a ataques y no puede ser revertida para reconstruir el rostro.</i>

03 /Ejercicio Práctico

A continuación, presentaremos una serie de ejercicios sencillos diseñados para profundizar en la comprensión de qué es una Referencia Biométrica Renovable (RBR) y cómo se construye. **Es fundamental destacar que estos ejercicios representan una simplificación extrema del proceso real de creación de una RBR.** Su propósito es reforzar conceptos clave que nos ayudarán a comprender por qué esta tecnología es privada y segura por diseño y por defecto.

/Parte 1. Construcción de Plantillas Biométricas

Ejercicio 1: Aquí se han construido las Plantillas Biométricas de tres personajes públicos, utilizando tres rasgos biométricos simples. Los criterios se detallan en la tabla.



Pilar Rubio



Adrien Brody



Barack Obama

Color de la piel Se ha elegido entre: /Piel muy clara /Piel clara /Piel clara intermedia /Piel olivácea /Piel oscura /Piel muy oscura	Piel olivácea	Piel clara	Piel oscura
*Tamaño de nariz Se ha elegido entre: Grande, mediana o pequeña.	Pequeña	Grande	Grande
*Volumen de labios Se ha elegido entre: Gruesos, medianos o finos.	Gruesos	Finos	Medianos

Ejercicio 2: En esta tabla se ha añadido una nueva identidad que complementa las del Ejercicio 1. Utilizando los mismos rasgos biométricos analizados previamente, se han creado las Plantillas Biométricas para estas cuatro identidades.



Pilar Rubio



Adrien Brody



Barack Obama



Emma Stone

Color de la piel: Se han ordenado según el color de su piel: Muy clara, piel clara, piel clara intermedia, piel olivácea, piel oscura o piel muy oscura.

Fila de ejemplo	Fila de ejemplo	Fila de ejemplo	Fila de ejemplo
Piel olivácea	Piel clara	Piel oscura	Piel muy clara

Tamaño de nariz: Se han ordenado según el tamaño de su nariz: Grande, mediana o pequeña.

Pequeña	Grande	Grande	Pequeña

Volumen de labios: Se han ordenado según el tipo de labios: gruesos, medianos o finos.

Gruesos	Finos	Medianos	Medianos

Ejercicio 3: Comparando los resultados de los Ejercicios 1 y 2, observamos que las plantillas biométricas de los tres personajes son las mismas en ambos ejercicios.



Pilar Rubio

EJERCICIO 1	EJERCICIO 2
Piel olivácea	Piel olivácea
Pequeña	Pequeña
Gruesos	Gruesos



Adrien Brody

EJERCICIO 1	EJERCICIO 2
Piel clara	Piel clara
Grande	Grande
Finos	Finos



Barack Obama

EJERCICIO 1	EJERCICIO 2
Piel oscura	Piel oscura
Grande	Grande
Medianos	Medianos

/Parte 2. Construcción de RBRs

Ejercicio 1: En este ejercicio, se han creado RBRs de los mismos tres personajes públicos utilizando tres rasgos biométricos simples. Se ha seguido un criterio de ordenación específico para cada rasgo. Este proceso muestra cómo las RBRs se generan de forma única para cada contexto, reforzando la seguridad y personalización de las referencias biométricas.



Pilar Rubio



Adrien Brody



Barack Obama

Color de la piel Se han ordenado según el tono de su piel, en orden ascendente, comenzando desde el tono más claro hasta el más oscuro.	2	1	3
Tamaño de nariz ordenado por tamaño de nariz en orden ascendente, desde la nariz más pequeña hasta la más grande.	1	3	2
Volumen de labios Se han clasificado por volumen de labios en orden ascendente, de los labios más finos a los más gruesos.	3	1	2

Ejercicio 2: En la tabla a continuación, se ha añadido una nueva identidad para complementar las presentadas en el Ejercicio 1, utilizando los mismos rasgos biométricos analizados previamente para crear las RBRs.



Pilar Rubio



Adrien Brody



Barack Obama



Emma Stone

Color de la piel: Se han ordenado según el color de su piel, en orden ascendente de tono de piel más claro a más oscuro.

3	2	4	1

Tamaño de nariz: Se han ordenado según el tamaño de su nariz, en orden ascendente de nariz más pequeña a más grande.

2	4	3	1

Volumen de labios: Se han ordenado según el tamaño de los labios, en orden ascendente de labios más finos a más gruesos.

4	1	3	2

Ejercicio 3: Al comparar los resultados de los Ejercicios 1 y 2, observamos que los RBRs no contienen datos identificables de manera directa. Podría incluso plantearse la pregunta de si el RBR constituye un dato personal por sí mismo.



Pilar Rubio

EJERCICIO 1	EJERCICIO 2
2	3
1	2
3	4



Adrien Brody

EJERCICIO 1	EJERCICIO 2
1	2
3	4
1	1



Barack Obama

EJERCICIO 1	EJERCICIO 2
3	4
2	3
2	3

/Parte 3. RBRs vs. Plantillas Biométricas

Ejercicio 1: Con lo analizado en los ejercicios, podrías adivinar a qué personalidad pertenece de las mostradas previamente sin mirar a los resultados obtenidos anteriormente.

¿Quién soy? _____

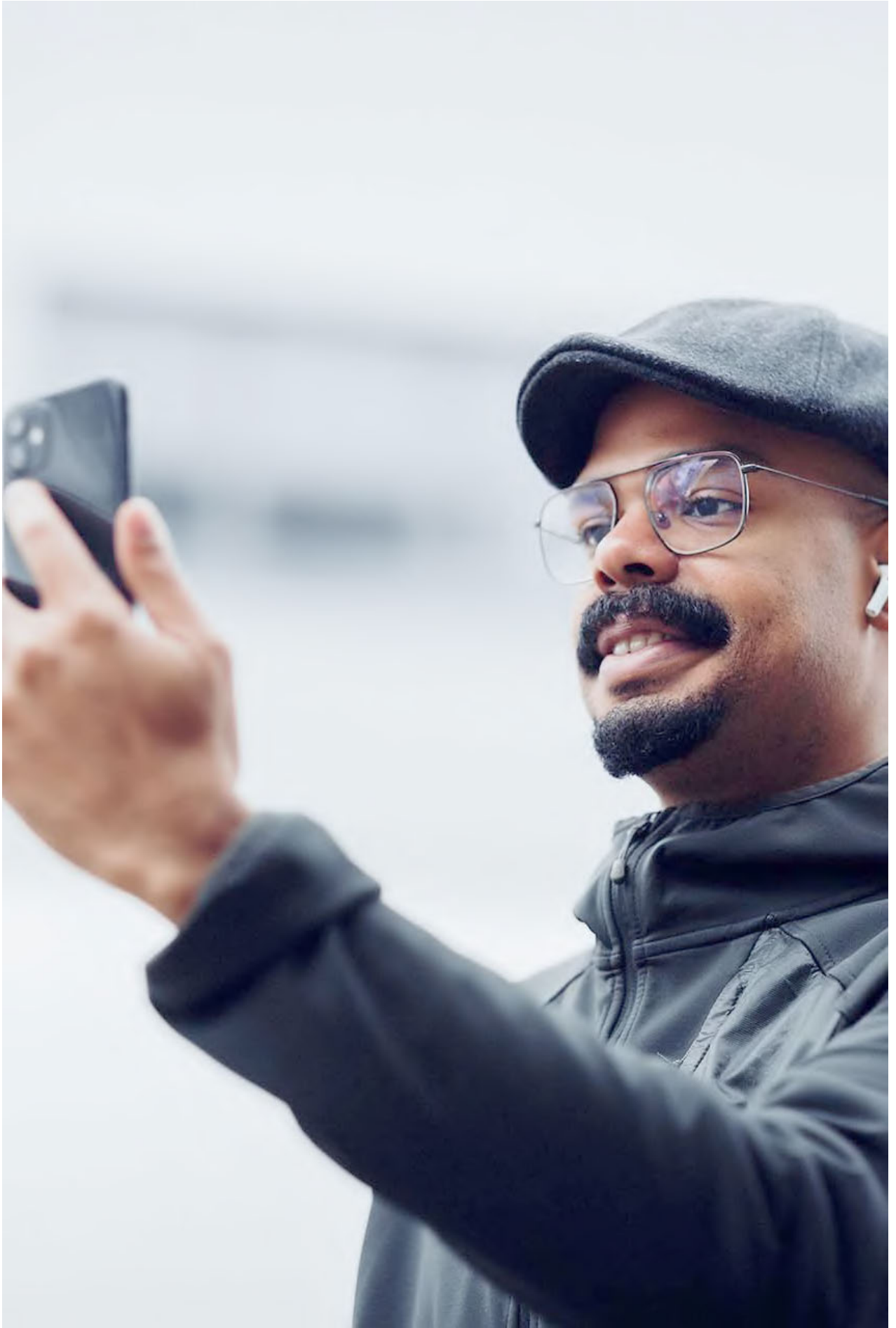


RBR



Plantilla Biométrica

Color de la piel	3	Piel clara
Tamaño de nariz	2	Grande
Volumen de labios	4	Finos



04 / Conclusiones

/¿Es posible comprometer un RBR?

Vulnerar una Referencia Biométrica Renovable (RBR) y deducir la identidad de la persona que representa implicaría un proceso de una complejidad teórica tan enorme, que a día de hoy debemos calificar como imposible. Hasta la fecha, **no se han reportado ataques** exitosos a sistemas basados en RBR, un contraste notable frente a otras tecnologías más vulnerables, como las contraseñas.

Este nivel de protección se basa en la avanzada estructura de datos y en múltiples capas de seguridad que hacen de las RBRs una tecnología altamente segura para la gestión de la identidad digital. Para intentar vulnerar una Referencia Biométrica Renovable (RBR) y determinar el rostro que representa, un atacante debería tener acceso a una serie de **datos críticos y confidenciales**:

/Conjunto de imágenes faciales de entrenamiento y sus Referencias Biométricas Renovables (RBRs): Para intentar deducir datos físicos de un individuo a partir de una RBR, sería imprescindible disponer de una base de datos de cientos de miles o millones de imágenes faciales como sus correspondientes referencias biométricas. Este conjunto de imágenes y RBRs proporciona una referencia masiva y detallada, sobre la cual el modelo biométrico establece patrones complejos y múltiples características faciales.

/Detalle de los rasgos biométricos analizados: Los sistemas de RBR analizan entre 500 y 600 valores biométricos, combinando una variedad de rasgos. Estos rasgos incluyen detalles faciales mucho más complejos que puntos comunes como la distancia entre ojos o el tamaño de la nariz, ya que son una combinación de una multiplicidad de rasgos que, en conjunto, caracterizan a una persona. Sin acceso a esta información detallada sobre los rasgos específicos seleccionados y su ponderación, cualquier intento de deducir una identidad sería impreciso.

/Relación y peso de los rasgos analizados:

Además de identificar rasgos individuales, el sistema de RBRs analiza cómo se relacionan entre sí estos valores numéricos. La relación entre los rasgos se establece a partir de una matriz multidimensional en la que cada posición tiene un peso específico dentro del conjunto total de valores. Esta relación, que es específica para cada modelo biométrico, determina cómo se “codifican” los valores en una RBR, lo que añade una capa extra de complejidad y dificulta aún más cualquier intento de revertir la referencia biométrica para reconstruir el rostro original.

/Modelo de encriptación: La encriptación avanzada de cada RBR garantiza que su representación no pueda revertirse para recuperar los datos faciales originales sin una clave específica de desencriptación. Esto asegura que, incluso si se accede a una RBR, sin el modelo de encriptación y la clave de acceso adecuada, sería imposible reconstruir la identidad de la persona.

Obtener toda esta información, ya de por sí un reto prácticamente imposible, requeriría además la aplicación de **técnicas estadísticas avanzadas y modelos computacionales de última generación** para establecer correlaciones precisas entre las imágenes faciales originales y sus rasgos biométricos específicos. A esto se suma la dificultad adicional de aplicar esta información en futuros intentos de autenticación, dado el uso de tecnologías avanzadas de prevención de suplantación, como las **pruebas de vida**, y de sistemas de detección de **ataques de inyección**.

Estos factores hacen que la probabilidad de reconstruir un rostro a partir de una RBR y emplearlo para suplantación de identidad sea **extremadamente baja o directamente imposible**. Sería necesario contar con una infraestructura avanzada, acceso no autorizado a datos protegidos y conocimientos técnicos significativos.

En cambio, la **ingeniería social** representa un método más accesible y directo para suplantar identidades. Esta práctica incluye

la búsqueda de datos personales publicados en redes sociales u otras fuentes online. Por ejemplo, un atacante puede encontrar con enorme facilidad fotografías de un individuo en internet o datos personales que faciliten el acceso a sus cuentas. A diferencia de un ataque a una RBR, donde el nivel de dificultad es extremo, obtener información visual de una persona y utilizarla en un ataque de suplantación en el entorno digital es cada vez más habitual y requiere pocos recursos. De hecho, el **phishing y el acceso a información pública de los usuarios** son los métodos de ataque más comunes, con una tasa de éxito considerablemente alta en la vulneración de cuentas.

Este contraste subraya que, mientras la tecnología RBR es una solución avanzada y resistente a los ataques, la exposición de datos personales en internet y los ataques de ingeniería social presentan una **amenaza y significativa para la seguridad de la identidad digital**.

/Una nueva era en identidad digital: El potencial de las Referencias Biométricas Renovables (RBRs)

Las Referencias Biométricas Renovables (RBRs) representan un **salto tecnológico decisivo** en la protección de la identidad, al combinar una seguridad avanzada con principios de privacidad integrados desde su diseño. Esta tecnología supera las limitaciones y vulnerabilidades de las plantillas biométricas tradicionales, consolidándose como una alternativa robusta para la gestión segura de identidades digitales.

Principios clave como la **irreversibilidad, multiplicidad, no interoperabilidad y revocabilidad** aseguran que las RBRs brinden un nivel de privacidad sin precedentes, cumpliendo con los **estándares regulatorios más exigentes**, como el Reglamento General de Protección de Datos (RGPD) en Europa.

La arquitectura de las RBRs demuestra cómo la **privacidad por diseño y por defecto** puede integrarse en la tecnología biométrica, ofreciendo una solución adaptable, segura y conforme a las normativas actuales. A diferencia de los métodos tradicionales, las RBRs promueven la soberanía y el control del usuario sobre sus datos personales y son altamente resistentes ante amenazas avanzadas, desde filtraciones de datos hasta fraudes de identidad.

De cara al futuro, las RBRs establecen un estándar para las tecnologías de identidad que priorizan la **seguridad y privacidad del usuario y el cumplimiento normativo**, posicionándose como una solución ideal para organizaciones comprometidas en fortalecer la

confianza digital en un mundo cada vez más interconectado.

Este documento es solo el inicio de un camino hacia una **mayor explicabilidad de las soluciones tecnológicas** en biometría y para fomentar una confianza sólida en el uso de estas tecnologías cuando estas cuentan con las oportunas establecidas por los reguladores. Lograr este objetivo requiere esfuerzos tanto de los desarrolladores, que deben comprometerse a hacer sus tecnologías comprensibles, como de los reguladores, que deben avanzar en su conocimiento técnico y comprensión de estas soluciones. Estas actitudes de ambas partes son esenciales para que Europa logre ser referencia en la utilización privada y segura de las soluciones biométricas en beneficio y bajo la soberanía de sus ciudadanos y para que sus empresas expandan estas soluciones a escala mundial.

A/C

Coordenação-Geral de Normatização

Autoridade Nacional de Proteção de Dados - ANPD

São Paulo, 1º de agosto de 2025

Ref.: Tomada de Subsídios sobre dados pessoais sensíveis - dados biométricos.

Prezados Senhores,

A Zetta, associação sem fins lucrativos que reúne empresas de tecnologia atuantes no mercado financeiro e de meios de pagamento, inscrita no CNPJ/MF sob o nº 37.253.906/0001-28, com sede na Avenida Paulista, 1765, Andar 7, Bela Vista, São Paulo/SP, CEP 01.311-930, vem, respeitosamente, **apresentar material complementar às suas contribuições para a Tomada de Subsídios da Autoridade Nacional de Proteção de Dados (“ANPD”) sobre dados pessoais sensíveis - dados biométricos**, onde oferece considerações melhor detalhadas e quadros exemplificativos que enriquecem suas considerações enviadas pela Plataforma Participa + Brasil.

BLOCO I – DEFINIÇÕES E PRINCÍPIOS

1. Quais critérios objetivos devem ser observados para caracterizar um dado como biométrico nos termos da LGPD?

Para apoiar a definição de critérios objetivos para caracterizar o dado biométrico nos termos da LGPD, destaca-se o entendimento da Autoridade de Proteção de Dados do México (“INAI”)¹, do Comitê Europeu para a Proteção de Dados (*European Data Protection Board* ou “EDPB”)² e do art. 16 ter da Lei de Proteção de Dados Chilena³.

Tais parâmetros consideram “dados biométricos” aqueles que, cumulativamente, atendam aos seguintes critérios: **(a)** estejam vinculados a características físicas, fisiológicas, comportamentais ou traços de personalidade de um titular de dados; **(b)** resultem de um tratamento específico (em regra, uma forma de medição); e **(c)** que a finalidade seja identificar / autenticar de maneira única o titular.

Nesse sentido, imagens captadas em vídeo, fotografias, gravações de voz ou dados semelhantes não devem ser, em si mesmos, considerados dados biométricos. Isso porque, o dado biométrico é apenas aquele resultante do tratamento dos dados brutos originários com a finalidade de identificação única do indivíduo.

¹ https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf

² https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

³ <https://www.diariooficial.interior.gob.cl/publicaciones/2024/12/13/44023/01/2583630.pdf>

Esse é o entendimento do EDPB: *“The video footage of an individual **cannot however in itself be considered as biometric data** under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual”*.

A definição proposta busca refletir a distinção entre **dados brutos com potencial biométrico** e **dados biométricos em si**, conforme interpretação adotada pelo EDPB. Essa distinção é fundamental no contexto da LGPD, especialmente para garantir segurança jurídica e evitar a extensão do regime de dados sensíveis a tratamentos que não envolvem riscos equivalentes.

No setor financeiro, por exemplo, uma fotografia do rosto capturada para compor um cadastro - sem processamento técnico adicional - não deve ser considerada, por si só, um dado biométrico sensível. Por outro lado, quando essa imagem é submetida a um algoritmo de reconhecimento facial pela extração e comparação de padrões únicos como vetores faciais para identificar e autenticar de forma única o titular, tal como é feito no momento do login no aplicativo, aí sim ocorre o tratamento biométrico nos termos do art. 5º, II da LGPD.

O elemento determinante, portanto, não é a natureza do dado em si (ex: uma imagem facial), mas o tratamento técnico aplicado a ele com a finalidade específica de identificação ou autenticação biométrica. Assim, imagens ou vídeos não são dados biométricos “em si”, salvo se tecnicamente processados com essa finalidade. Tal distinção preserva a proporcionalidade regulatória e evita impactos desnecessários em operações de baixo risco, como armazenamento de imagens em bases de dados não sujeitas a mecanismos automáticos de reconhecimento.

Na prática, imagine que uma instituição financeira use sistema de reconhecimento facial para validar a identidade de clientes. Nesse processo, são extraídas características biométricas únicas (como a distância entre os olhos e formato do maxilar)⁴ do titular e comparadas à *selfie* tirada na hora. Ao aplicar o entendimento do EDPB, nota-se que os dados biométricos seriam esses pontos específicos extraídos, não as fotos em si. Portanto, se houver vazamento apenas da imagem do cliente, a exposição será de dado pessoal (fotografia) e não de dado sensível biométrico.

No mercado financeiro, dados como a biometria facial são utilizados para fins de autenticação e prevenção à fraude, mas o tratamento técnico desses dados ocorre de duas formas distintas:

1. **Para desbloqueio do aplicativo:** são empregados mecanismos de segurança do dispositivo do próprio titular (ex.: Face ID ou Touch ID). Nesse processo, o aplicativo da instituição apenas solicita ao sistema operacional do dispositivo do titular que confirme sua identidade. O sistema do aparelho trata os dados biométricos do titular e retorna para a instituição apenas uma resposta

⁴ <https://blog.zapsign.com.br/en/reconhecimento-facial/>

binária (Verdadeiro ou Falso), sem que a esta tenha acesso à imagem ou à impressão digital do titular.

2. **Para verificação de identidade e prevenção à fraude:** em situações como o cadastro inicial, ativação de novos aparelhos, ou em análises de segurança (ex: suspeita de invasão de conta, roubo de dispositivo ou atualização de dados cadastrais), a instituição financeira realiza verificações ativas. Nesses casos, são processadas tecnicamente pela instituição financeira a imagem do rosto do titular para confirmação de identidade de forma segura.

2. Quais práticas de transparência ativa podem ser exigidas dos controladores que realizam tratamento de dados biométricos, para permitir que titulares tenham informações claras sobre o tratamento antes de fornecerem seus dados?

Para a Autoridade de Proteção de Dados do Reino Unido (“ICO”), a forma mais eficiente de transparência aos titulares sobre uso de dados biométricos deverá considerar fatores como: **(i)** o caso de uso; **(ii)** a natureza de relacionamento com o titular; e **(iii)** os dados envolvidos na atividade de tratamento⁵.

Com base nisso, quanto mais evidente for o tratamento de dados para o titular, considerando as práticas comuns do setor e a relação prévia com o indivíduo, **menor será a exigência de medidas adicionais de transparência.**

Quando o reconhecimento biométrico é utilizado para confirmar a identidade do titular em uma transação conhecida - como **acessar conta, solicitar crédito ou chargebacks** - o contexto muda substancialmente. Nesses casos, o tratamento é realizado dentro de um ambiente autenticado e sob relacionamento ostensivo como o titular, geralmente em conformidade com as exigências do Banco Central do Brasil, como as previstas na Resolução CMN nº 4.893/21, que impõem controles de segurança e mecanismos robustos de autenticação para operações com contas digitais. Trata-se de prática exigida pelo regulador e esperada pelos usuários. Nesses casos, é suficiente indicar a Política de Privacidade ao longo da jornada do cliente ou prestar explicações sobre o tratamento, quando solicitadas (por exemplo, nos casos em que o reconhecimento facial é necessário para ativar um determinado serviço, indicar na tela antes de obter o reconhecimento às finalidades para as quais ocorrerá o tratamento).

3. De que forma a biometria comportamental (por exemplo, reconhecimento de voz, padrões de digitação, movimento ocular) deveria ser tratada em comparação à biometria tradicional (digital, íris, face)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios da qualidade dos dados e da segurança?

⁵

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>

A legislação vigente não traz distinção conceitual entre biometria comportamental e tradicional e, como consequência, não estabelece obrigações diferentes com base nessa distinção. Assim, eventuais normas infralegais não podem impor exigências distintas sem respaldo legal, sob pena de ferir o princípio da legalidade. Portanto, embora o INAI (México) e o ICO (Reino Unido)⁶⁻⁷⁻⁸ façam distinções conceituais entre dados biométricos físicos/fisiológicos e biométricos comportamentais, nenhuma das duas autoridades impõe deveres específicos ou diferenciados de acordo com tal classificação. Dessa forma, ambas as categorias estão sujeitas às mesmas obrigações legais, inclusive em relação aos princípios de qualidade dos dados e segurança da informação.

Adicionalmente, no contexto do sistema financeiro, regulamentos como a Resolução Conjunta nº 6/23 e a Resolução CMN nº 4.893/21 reforçam a necessidade de mecanismos robustos de prevenção à fraude, baseados em dados íntegros, relevantes e completos (princípios da qualidade e segurança). Isso vale para qualquer tipo de dado biométrico utilizado como fator de autenticação ou detecção de risco, desde que sejam observadas as regras de governança e uso legítimo das informações, atendendo a propósitos específicos e informados, e também com salvaguardas de auditoria e performance dos modelos.

Segundo o Grupo de Trabalho do Artigo 29 (WP29), fabricantes relataram que a adoção de tecnologias biométricas comportamentais no setor financeiro aumentou as taxas de detecção de fraudes e proporcionou maior agilidade na resolução de reivindicações legítimas. A Autoridade de Proteção de Dados de Singapura (PDPC) também reconheceu o uso da biometria comportamental como medida voltada à segurança, especialmente em aplicações voltadas à prevenção de fraudes.

BLOCO II – HIPÓTESES LEGAIS

4. Como garantir que o consentimento para o tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco, conforme exigido pela LGPD? Em quais contextos o consentimento não deve ser considerado uma hipótese legal adequada para o tratamento desses dados?

É imperativo que a futura orientação/regulamentação reconheça, de forma explícita, que o consentimento não é, e não deve ser, a única base legal para o tratamento de dados biométricos, especialmente no setor financeiro, no qual há uma primazia da segurança e da higidez do funcionamento do sistema financeiro nacional.

⁶ https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf

⁷ <https://home.inai.org.mx/wp-content/uploads/GuiaBiometricos-Dic2024.pdf>

⁸

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/>

A hipótese do art. 11, II, “g” da LGPD - que autoriza o uso destes dados para garantia da prevenção à fraude e à segurança do titular - é fundamental a legitimação do uso de dados biométricos para autenticação e validação de identidade e para subsidiar tarefas de prevenção, resposta e investigação de incidentes de fraude. É o caso, por exemplo:

- abertura de contas;
- recuperação de acesso ou de senha;
- acesso e visualização de informações financeiras sensíveis;
- autorização de transações financeiras relevantes ao contexto do titular;
- atualizações cadastrais;
- autenticação em canais de atendimento;
- operações de prevenção, resposta e investigação de fraudes em si (elaboração de relatórios, cooperação técnica, acompanhamento de casos);
- autenticação em processos de contestação comercial e recuperação de crédito;
- dentre outras situações.

Ademais, existe a hipótese do art. 11, II “a” da LGPD, que autoriza o tratamento de dados biométricos quando indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador. As autoridades supervisoras do Sistema Financeiro Nacional - por meio de suas normas específicas - exigem das instituições reguladas a adoção de medidas adequadas e aptas para garantir a segurança de suas atividades (requisitos de segurança da informação e segurança cibernética) e a validação efetiva da identidade de seus clientes e a autenticidade e legitimidade de suas transações (ex.: processos de KYC e AML/CFT - conhecer clientes e prevenção à lavagem de dinheiro e o financiamento ao terrorismo).

Ainda nestes casos de dispensa do consentimento, o controlador deve dar a devida transparência ao titular dos dados e garantir-lhe o exercício de seus direitos. Isso porque a aplicação de outras bases legais que não o consentimento, a exemplo das mencionadas acima, não isenta o controlador do cumprimento dos demais dispositivos da LGPD, com destaque para os referentes à autodeterminação informativa, aos princípios de tratamento de dados pessoais e aos direitos dos titulares desses dados.

Quando o consentimento é a base legal pertinente para o tratamento de dados biométricos, o controlador deve seguir os requisitos da LGPD para a coleta de manifestação de vontade válida. Para negócios digitais, o titular manifesta um consentimento informado ao visualizar informações como a finalidade do tratamento, a existência da coleta e uso de dados biométricos, o checkbox de opt-in e, por meio de um botão “saiba mais”, o titular pode ser dirigido a uma segunda camada com detalhes adicionais, como a política de privacidade e o termo de consentimento específico.

5. Quais critérios devem ser observados para a adequada aplicação da hipótese legal de “garantia da prevenção à fraude” (art. 11, II, “g”, LGPD) nos casos de tratamento de dados biométricos? De que maneira é possível compatibilizar o princípio da necessidade do tratamento de dados biométricos, com a finalidade de prover a segurança das informações e

o acesso a soluções bancárias e financeiras, por exemplo? Quais salvaguardas podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais?

Como respondido na **Pergunta 4** desta Tomada de Subsídios, o uso de dados biométricos no setor financeiro encontra respaldo legal principalmente no art. 11, II, “a” e “g” da LGPD. No caso específico da garantia da prevenção à fraude e à segurança do titular, assim como em outros, os critérios para o tratamento de dados biométricos devem ser:

- finalidade específica e restrita, ou seja, o tratamento deve estar circunscrito apenas às atividades necessárias para a consecução da finalidade;
- proporcionalidade, ou seja, o benefício da segurança deve ser proporcional ao risco à privacidade, e a criticidade das atividades descritas anteriormente está em linha com esse princípio da proporcionalidade;
- segurança, ou seja, a natureza sensível dos dados biométricos exige do controlador a adoção de medidas técnicas e administrativas aptas a garantir a proteção das informações contra riscos de exposição interna, vazamentos etc;
- transparência, ou seja, ainda que não seja necessário o consentimento do titular, é fundamental prover informações claras e acessíveis a respeito do uso dos dados e também os canais para exercício de direitos básicos de privacidade.

A elaboração de relatório de impacto pode ser desejável, especialmente a nível setorial, que consigne a relevância, proporcionalidade e necessidade do uso de tais dados e recomendações de práticas de segurança e medidas de mitigação de riscos.

O uso de dados biométricos no setor financeiro, para as atividades descritas na **Pergunta 4** desta Tomada de Subsídios, é compatível com o princípio da necessidade. Tais dados não são apenas essenciais, mas também proporcionais e adequados para as finalidades de promoção da segurança, da inclusão e da boa experiência do titular.

A dimensão do problema de fraudes no Brasil justifica a urgência e a necessidade de mecanismos de segurança robustos. Dados da Serasa Experian revelam que 51% dos brasileiros já foram vítimas de fraude. Segundo a TransUnion, a perda financeira média por golpe é de US\$ 1.032, e uma pesquisa do DataSenado aponta que 24% dos cidadãos perderam dinheiro com crimes cibernéticos no último ano. Apenas em 2025, o país já registrou mais de 2,8 milhões de tentativas de fraude, com um prejuízo potencial superior a 40 bilhões de reais.

Diante deste cenário, a biometria permite identificar e autenticar pessoas com mais eficácia do que métodos tradicionais, como senhas e tokens que são mais suscetíveis a ataques de phishing, engenharia social e vazamento de dados, protegendo contra fraudes e ampliando o acesso a serviços financeiros. Isto é uma realidade especialmente para quem enfrenta barreiras com senhas, documentos e mecanismos tecnológicos complexos para autenticação de múltiplos fatores, como é o caso de boa parte da população brasileira.

O uso da biometria para as situações mencionadas anteriormente, portanto, é proporcional ao benefício usufruído e a segurança esperada das aplicações de serviços financeiros digitais.

Quanto às medidas de mitigação dos riscos decorrentes do tratamento de dados biométricos, recomenda-se adotar salvaguardas técnicas e organizacionais destacadas por autoridades como o ICO⁹, o INAI¹⁰ e a PIPC¹¹, agrupadas abaixo em dois conjuntos:

- **Medidas prioritárias:** (i) controles rigorosos de acesso aos dados biométricos; (ii) realização periódica de testes de invasão (*pentests*); (iii) elaboração e aplicação de política robusta de segurança da informação; (iv) criptografia dos dados biométricos, tanto em trânsito quanto armazenados; (v) execução de varreduras de vulnerabilidades nos sistemas envolvidos, com ações corretivas quando necessário; (vi) registro de *logs* das interações e acessos aos dados biométricos; (vii) armazenamento segregado dos dados biométricos das outras informações pessoais; e (viii) condução de *due diligence* em fornecedores envolvidos no tratamento.
- **Medidas complementares:** (i) o armazenamento apenas do *template* biométrico (como vetores matemáticos), evitando guardar a imagem completa da impressão digital; e (ii) a adoção dos controles previstos em normas internacionais relevantes, como ISO/IEC 24745:2022, que trata da proteção de informações biométricas.

6. Em determinadas ocasiões, o tratamento de dados biométricos pode ser realizado para o “cumprimento de obrigação legal ou regulatória” (art. 11, II, “a”, LGPD). Quais critérios e salvaguardas devem ser observadas nestes casos pelos controladores, especialmente entidades e órgãos públicos, visando à mitigação de riscos e garantia de direitos dos titulares?

No contexto do sistema financeiro nacional, existem diversas legislações e normas infralegais que servem como fundamento jurídico para o tratamento de dados biométricos, em linha com o permissivo estabelecido pelo art. 11, II, “a”, da LGPD. Essas normas geralmente visam à prevenção à fraude, segurança nas transações e identificação inequívoca do titular dos dados. Os critérios, portanto, devem ser: (i) a existência de obrigação legal ou regulatória específica que, para seu cumprimento, faça-se necessário o tratamento de dados pessoais de forma proporcional ao risco a ser mitigado; (ii) a adequação, ou seja, a coleta e o tratamento dos dados biométricos deve ser proporcional ao fim pretendido, ou seja, o grau de sensibilidade e risco deve justificar o uso da biometria e também não existam meios menos intrusivos com igual eficácia; (iii) finalidade, ou seja, o uso dos dados deve estar limitado aos fins da obrigação legal ou regulatória, como, por exemplo, prevenção à lavagem de dinheiro, autenticação de identidade em sistemas financeiros, dentre outras finalidades possíveis estabelecidas em norma). Isso compreende, inclusive, decisões administrativas ou judiciais que produzem efeitos normativos, como é o caso de ordens judiciais para divulgação de dados biométricos.

9

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

¹⁰ https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf

¹¹ <https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do#none>

A norma deve estabelecer de forma clara a necessidade de identificação ou autenticação robusta, ou mesmo a adoção de medidas de segurança qualificadas e proporcionais ao risco a ser mitigado, ainda que o comando legal não mencione o termo "biometria" explicitamente.

Citamos como exemplo de obrigações legais ou regulatórias: (i) Lei nº 9.613/1998 (Prevenção à Lavagem de Dinheiro - PLD/FT), que exige dos regulados a identificação e manutenção de registros dos clientes, sendo a biometria hoje considerada uma das medidas de segurança mais seguras e robustas para tanto; (ii) Lei nº 12.865/2013, que exige das instituições a adoção de medidas de segurança para o atendimento das necessidades dos usuários; (iii) Circular BCB nº 3.978/2020 (PLD/CFT), que exige das instituições a identificação e verificação da identidade dos clientes, com procedimentos e medidas compatíveis com o risco; (iv) Resolução CMN nº 4.893/2021 (Política de Segurança Cibernética), que exige das instituições a adoção de políticas, medidas e controles para proteção de dados e segurança cibernética; (v) a Resolução Conjunta nº 1/2020 (Open Finance), que exige da instituição a adoção de procedimentos e controles para a autenticação de clientes; (vi) Resolução Conjunta nº 6/2023, que exige a adoção de procedimentos e controles para abertura e manutenção de contas; (vii) Resolução BCB nº 142/2021, que exige a adoção de procedimentos e controles para prevenção de fraudes na prestação de serviços pelas instituições autorizadas a funcionar pelo BCB; (viii) Instrução Normativa nº 138/2022, que exige biometria para a contratação de empréstimo consignado, dentre outras normas;

As salvaguardas a serem adotadas para mitigar os riscos decorrentes do tratamento de dados biométricos devem seguir os mesmos padrões indicados para os agentes que se utilizam da base legal de "prevenção à fraude", como detalhado na **Pergunta 5**. Isso porque as medidas técnicas e organizacionais de proteção de dados devem ser proporcionais aos riscos inerentes à operação de tratamento, independentemente da base legal invocada. Tal entendimento é compatível com a orientação do ICO¹², que não diferencia medidas de segurança conforme a base legal adotada, mas a partir da natureza e sensibilidade dos dados, e do impacto potencial sobre os titulares.

Some-se a isso o fato de que a jurisprudência do STJ tem caminhado no sentido de exigir das instituições financeiras mecanismos eficazes para impedir transações fora do perfil do cliente, como no caso do REsp 2.052.228/DF, reforçando as diretrizes de muitas das normas supracitadas.

7. Quais os limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa (art. 11, II, "c", LGPD), mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior? Quais salvaguardas adicionais seriam eventualmente necessárias a fim de salvaguardar os interesses e direitos dos titulares nesses casos?

¹².

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

Conforme orientação da ANPD em seu Guia sobre o tratamento de dados para fins acadêmicos e realização de estudos e pesquisas¹³, **a anonimização não é requisito obrigatório** para o uso de dados pessoais nesses contextos. A ANPD esclarece que:

“Em conjunto, esses dispositivos legais indicam que a anonimização ou a pseudonimização de dados pessoais não foram instituídas pela LGPD como medidas de segurança impositivas, isto é, que devem ser adotadas em todo e qualquer caso de estudos e pesquisas. Da mesma forma, a LGPD não estabeleceu a anonimização ou a pseudonimização como condição técnica para a divulgação pública ou para o compartilhamento de dados pessoais para fins de realização de estudos e pesquisas, devendo-se reconhecer, inclusive, que, em alguns casos, a identificação dos titulares pode ser imprescindível para os objetivos da pesquisa. A leitura mais adequada – e que decorre, em especial, do uso da expressão “sempre que possível” tanto nos arts. 7º e 11 quanto nos arts. 13 e 16 – é a de que a LGPD optou por um modelo mais flexível, que busca equilibrar a proteção de dados pessoais com as peculiaridades e os propósitos de realização dos mais diversos estudos e pesquisas.”

Assim, o termo “necessária”, quando vinculado à anonimização, não se aplica como exigência mandatória. Consequentemente, **não é juridicamente exigível a adoção de medidas adicionais exclusivamente com base na potencialidade de reidentificação**, nos termos da LGPD.

Contudo, como apontam a Autoridade de Proteção de Dados de Hong Kong¹⁴ e ICO¹⁵, em muitos casos, os dados biométricos sequer podem ser efetivamente anonimizados. Isso porque, mesmo quando não estão diretamente vinculados a titular identificável, podem permitir a inferência de dados sensíveis (como etnia, características físicas específicas, condições de saúde, entre outras) que permitem a reidentificação do indivíduo. Assim, medidas adicionais de anonimização devem ser consideradas, baseadas no risco de reidentificação. De acordo com o Estudo Preliminar sobre Anonimização da ANPD¹⁶, **o risco de reidentificação está sempre presente**, por isso, a avaliação deve se concentrar no grau do risco e nas medidas adotadas para reduzi-lo a nível aceitável.

Portanto, eventuais salvaguardas implementadas devem ser **proporcionais ao risco concreto de reidentificação** e podem incluir, entre outras: **(i)** técnicas que assegurem a irreversibilidade dos *templates* biométricos, dificultando a reconstrução da imagem do titular; **(ii)** mecanismos que assegurem a irreversibilidade e não vinculabilidade (*unlinkability*) entre várias bases ou sistemas, como destaca o ICO¹⁷; e **(iii)** restrições de acesso, segmentação de bases e políticas de uso e de compartilhamento que limitem os efeitos de eventuais violações ou usos indevidos.

¹³

<https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf>

¹⁴ https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

¹⁵

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

¹⁶ <https://www.gov.br/participamaisbrasil/blob/baixar/37060>

¹⁷

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

BLOCO III – TECNOLOGIAS DE RECONHECIMENTO FACIAL (FRTS) E APLICAÇÃO DE TECNOLOGIAS EMERGENTES E INOVADORAS NO TRATAMENTO DE DADOS BIOMÉTRICOS

8. Como garantir que o uso de tecnologias de reconhecimento facial, ainda que amparado por uma hipótese legal da LGPD, observe os princípios da necessidade, proporcionalidade, transparência e de forma a evitar discriminação ilícita ou abusiva sobre determinados grupos sociais? Quais salvaguardas técnicas, jurídicas e institucionais devem ser implementadas para mitigar esses riscos?

A tecnologia de reconhecimento facial representa, para o ecossistema de serviços financeiros digitais, uma ferramenta fundamental não de vigilância, mas de segurança, conformidade regulatória e inclusão financeira. Seu uso é essencial para proteger os consumidores e a integridade do sistema contra fraudes cada vez mais sofisticadas.

Transparência ativa e contextual no setor financeiro

- O princípio da transparência deve ser aplicado de forma contextual. Existe uma diferença entre o uso de biometria em espaços públicos, onde o titular pode não ter ciência e nem a expectativa de tratamento dessa natureza, e o seu uso em uma jornada de contratação de um serviço financeiro. No contexto das plataformas de serviços financeiros digitais, o tratamento biométrico é uma etapa esperada e claramente comunicada ao usuário, e ela ocorre quando o cliente ativamente busca abrir uma conta, contratar um produto ou autorizar uma transação. O titular nesse contexto percebe a biometria como uma camada de proteção para seus próprios recursos e interesses.
- Assim, entendemos que o dever de transparência é plenamente atendido pela disponibilização de um Aviso de Privacidade claro, objetivo e acessível durante a jornada do usuário, no momento do cadastro ou antes da primeira autenticação biométrica. Essa abordagem contextual é mais eficaz do que avisos genéricos, pois informa o titular no momento exato em que a informação é mais relevante.

Necessidade e proporcionalidade no contexto financeiro

- O princípio da necessidade no setor financeiro deve ser analisado sob a ótica da mitigação de riscos de segurança, fraudes e do cumprimento de deveres regulatórios. Assim, métodos tradicionais, como senhas ou tokens por SMS, podem ser mais vulneráveis a ataques de engenharia social, phishing e SIM swapping. A biometria facial, combinada com ‘prova de vida’ (*liveness checks*), é hoje o meio mais eficaz e proporcional para garantir, de forma remota e escalável, que a pessoa do outro lado da tela é de fato quem alega ser. Trata-se de uma exigência imposta pelo cenário de fraudes e pelas regulações do Banco Central do Brasil em matéria de segurança cibernética.
- Pode ser preciso manter a amostra original (a foto) e o *template* biométrico, pois a fotografia original constitui parte de conjunto probatório jurídico que é fundamental para atividades de prevenção e combate à fraudes e crimes financeiros. Tais dados combinados também são importantes em situações de litígios, investigações e para demonstração de conformidade. Portanto, a base legal do exercício regular de direitos

em processo judicial, administrativo e arbitral pode ser válida para a retenção das informações.

- Minimização e finalidade específica: o setor privilegia o sistema de verificação (1:1), que compara o dado apresentado com o *template* previamente cadastrado pelo titular. Portanto, técnicas de identificação (1:N), que buscam em uma base de dados para descobrir quem é o titular, não são práticas comumente adotadas. Essa é uma salvaguarda que limita o tratamento ao mínimo necessário para a finalidade pretendida.
- A biometria facial é utilizada para fins de identificação e autenticação. Não há tratamento para inferência de outros dados sensíveis, como condições de saúde.

Mitigação de vieses discriminatórios

- O setor possui como prática a contratação de fornecedores - inclusive aqueles que venham a prover serviços de reconhecimento facial - que tenham passado por qualificações prévias demonstrando conformidade com padrões de qualidade e segurança em seus serviços.
- Ademais, para o desenvolvimento interno de soluções que usam dados biométricos, são relevantes as orientações do ICO¹⁸⁻¹⁹: (a) assegurar que a base de dados para treinar modelos contenha representação adequada de diferentes etnias e gêneros; (b) realizar testes e avaliações para identificar a existência de vieses discriminatórios; (c) empregar ferramentas disponíveis no mercado para analisar a estrutura e métricas da IA; (d) testar a acurácia estatística do sistema de IA utilizado; e (e) implementar processos para manejo de erros, especialmente os que minimizam os impactos ao titular, como mecanismos para questionar os resultados do reconhecimento facial.

9. Como os sistemas de reconhecimento facial podem ser projetados desde sua concepção e implementados de modo a garantir alta eficácia e confiabilidade, minimizando erros de identificação, como falsos positivos e negativos? Quais mecanismos devem ser adotados para corrigir tempestivamente essas falhas, em especial quando o tratamento de dados pessoais por reconhecimento facial é utilizado por tecnologias de tratamento automatizado?

Todas as ações para assegurar alta eficácia e confiabilidade dos sistemas de reconhecimento facial (melhoria do desempenho) devem ser proporcionais aos riscos específicos do seu uso. Por exemplo, sistema usado para monitorar espaços públicos e identificar pessoas procuradas pela justiça, em geral, requer nível de desempenho mais rigoroso do que solução para autenticar indivíduos que acessam prédio empresarial, considerando potenciais prejuízos decorrentes da identificação incorreta. Assim, as recomendações abaixo devem ser entendidas como sugestões a serem avaliadas conforme o risco do sistema em questão, e não como obrigações universais.

¹⁸

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-fairly/>

¹⁹

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/>

Como sistemas de reconhecimento facial são aplicações de IA, para garantir o seu desempenho, são indicadas as mesmas práticas recomendadas para modelos de IA. Com base no Guia de IA e Proteção de Dados do ICO²⁰ e o *toolkit* de riscos²¹, sugerimos considerar os seguintes controles:

- **Etapas de planejamento:** é aconselhável definir, para os objetivos da solução, o nível mínimo de acurácia estatística requerido;
- **Etapas de seleção e coleta de dados:** deve-se assegurar, considerando o público-alvo da IA, que os dados usados para fins de treinamento sejam representativos, completos, precisos e rotulados, e que os riscos de *overfitting* e *underfitting* tenham sido avaliados e mitigados;
- **Etapas de testes e validação:** recomenda-se realizar testes documentados para: (i) verificar a acurácia estatística da solução globalmente e quanto aos grupos relevantes, assegurando o cumprimento do nível mínimo definido; (ii) identificar eventuais problemas de *overfitting* e *underfitting*; e (iii) implementar correções, como retreinamento ou ajuste de parâmetros, se forem detectadas falhas;
- **Etapas de implantação e monitoramento:** é recomendável (i) fornecer aos usuários afetados mecanismos para questionar os resultados da solução; (ii) aplicar monitoramento contínuo ou testes periódicos para garantir a manutenção da acurácia estatística; e (iii) manter cópias das versões anteriores dos modelos de IA que continuam aprendendo após o lançamento, possibilitando o retorno a versões anteriores caso ocorram degradações no desempenho.

10. É possível identificar contextos e situações concretas em que o uso de tecnologias de reconhecimento facial não é recomendado? Se sim, quais e por quê? Quais tecnologias alternativas podem ser utilizadas por controladores, de forma eficaz, em substituição ao reconhecimento facial, visando à garantia de maior segurança em suas operações e com menor impacto sobre a proteção de dados de titulares?

O reconhecimento facial não deve ser utilizado se existirem métodos adequados e proporcionais para alcançar o mesmo resultado sem o uso de biometria, especialmente se houver formas de tratamento significativamente menos invasivas que possam atender à finalidade desejada. Em outras palavras, o reconhecimento facial deve ser evitado sempre que alternativas capazes de garantir nível equivalente, ou suficiente diante dos riscos envolvidos, estiverem disponíveis.

Por exemplo, o uso de reconhecimento facial para o controle de presença/ausência em escolas pode representar monitoramento excessivo, afetando negativamente o direito à educação. Em locais públicos, a aplicação da tecnologia sem justificativa clara e proporcional pode configurar vigilância em massa. Em processos seletivos e contratações, seu uso para análise de expressões faciais durante entrevistas traz risco concreto de discriminação e reforço de vieses algorítmicos,

20

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/>

²¹https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fico.org.uk%2Fmedia%2Fkr3mveig%2Fai_and_data_protection_risk_toolkit_v11.xlsx&wdOrigin=BROWSELINK

comprometendo a justiça do processo. Em eventos políticos ou manifestações, a tecnologia é ainda mais complexa, pois pode ser usada para identificar e até perseguir manifestantes.

Quanto a tecnologias alternativas, há outras informações que podem ser usadas com intuito de apoiar ou substituir o reconhecimento facial, conforme o contexto específico. Por exemplo, a PIPC²², em seu Guia sobre Dados Biométricos, apresenta os seguintes exemplos: **(i)** para acesso a instalações físicas ou dispositivos, recomenda-se a utilização de dados baseados na digital do indivíduo, cartões de acesso ou senhas complexas; e **(ii)** para acesso a aplicativos, sugere-se: **(a)** autenticação via serviços de resposta automática, onde o usuário recebe uma ligação telefônica automática e deve seguir instruções para confirmar a identidade; ou **(b)** uso de *tokens* ou senhas temporárias enviadas por SMS, e-mail ou aplicativos autenticadores previamente validados.

Outra ferramenta útil na prevenção de fraudes são os dados de telecomunicações. As soluções baseadas nesses dados permitem, por exemplo, verificar se o telefone e outras informações de contato correspondem a registros das operadoras, confirmar se a localização da transação bate com a localização do dispositivo do titular, e identificar indícios de fraudes, como o *SIM swap*. A Anatel destaca o uso desses dados por instituições financeiras para prevenir fraudes e informa que as prestadoras disponibilizam informações para os bancos, permitindo que adotem medidas preventivas relativas às movimentações financeiras vinculadas ao celular em troca de chip.²³

Para que organizações como instituições financeiras possam, quando adequado e considerando os riscos envolvidos, adotar alternativas ao reconhecimento facial, **é fundamental que a ANPD fomente a criação de ambiente regulatório que incentive a pesquisa e o desenvolvimento de soluções seguras e eficazes**. A falta de regulamentação que estimule a inovação e a adoção de métodos alternativos de prevenção a fraudes tende a levar as organizações a optarem pelo uso excessivo de biometria facial, até em situações em que os riscos não justificariam o tratamento de dados biométricos, devido à ausência de opções viáveis e juridicamente seguras.

BLOCO IV – SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

11. Dado o impacto significativo de uma violação de dados biométricos, como roubo de identidade, quais medidas de segurança técnicas e administrativas devem ser consideradas indispensáveis para mitigar esses riscos? Além disso, quais parâmetros mínimos de avaliação de riscos e monitoramento devem ser exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral desses dados sensíveis?

Conforme mencionado na **Pergunta 5**, com base em orientações do ICO, INAI e PIPC, destacamos as seguintes medidas de segurança que consideramos fundamentais para a proteção dos dados biométricos: **(i)** controle rigoroso de acesso aos dados; **(ii)** realização de

²² <https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do#none>

²³ <https://www.gov.br/anatel/pt-br/assuntos/dicas-contras-fraudes/golpes-atuais-mais-comuns>

testes de penetração; **(iii)** implementação de políticas de segurança da informação; **(iv)** criptografia de dados pessoais, tanto durante a transmissão quanto em armazenamento; **(v)** varreduras (*scans*) regulares a fim de identificar vulnerabilidades nos sistemas que processam dados biométricos, com adoção de medidas corretivas quando necessário; **(vi)** registro em logs de todos os acessos realizados aos dados biométricos; **(vii)** armazenamento segregado dos dados biométricos em relação a outras informações; e **(viii)** se houver contratação de terceiros, a realização de *due diligence* adequada e estabelecimento de cláusulas contratuais robustas em relação às obrigações de segurança a serem adotadas.

Quanto aos parâmetros mínimos para a mensuração e monitoramento dos riscos de segurança, não há diferenças entre a metodologia aplicada à biometria facial e as práticas utilizadas para outros riscos relativos à cibersegurança. Assim, com base na ISO/IEC 27005:2023²⁴, destacamos os seguintes passos básicos:

- a) **Definição de critérios de risco:** estabelecer, conforme o apetite de risco da organização, as regras e parâmetros para aceitação dos riscos;
- b) **Identificação dos riscos:** identificar os ativos envolvidos; ameaças potenciais a esses ativos; controles existentes; e vulnerabilidades. Quanto às ameaças específicas à biometria facial, ressaltamos os ataques típicos apontados pelo Guia do Centro Nacional de Cibersegurança do Reino Unido (NCSC)²⁵, tais como: **(i)** ataques de apresentação (comuns, em que artefatos, como fotografias, são usados para falsificar a validação da identidade; **(ii)** interceptação dos resultados dos sensores (ataque que visa modificar ou interceptar os dados captados pelos sensores, como fotos ou leituras biométricas, para burlar e/ou comprometer o sistema; **(iii)** subversão da integridade da inscrição (isto é, inserir dados biométricos de outra pessoa no cadastro de alguém, fraudando assim o reconhecimento facial); **(iv)** ataques aos bancos de dados (alteração de dados durante a transmissão ou armazenamento); **(v)** ameaças internas (ações maliciosas executadas por profissionais com acesso legítimo ao sistema); **(vi)** ataques aos sistemas de TI (típicos ataques de segurança direcionados à infraestrutura tecnológica); **(vii)** ataques de negação de serviço (com objetivo de tornar o sistema indisponível, podendo forçar a operação em redes menos seguras; por isso, a infraestrutura de contingência deverá ter segurança equivalente ao sistema biométrico).
- c) **Análise dos riscos:** avaliação das possíveis consequências e da probabilidade de ocorrência dos riscos, para definir o nível do risco;
- d) **Tomada de decisão:** com base nos critérios estabelecidos, avaliar se o risco é aceitável e decidir se deve ser mitigado, aceito, compartilhado ou evitado. Conforme tal decisão, pode ser necessário elaborar e executar plano de ação específico; e

²⁴ <https://www.normas.com.br>

²⁵ <https://www.ncsc.gov.uk/collection/biometrics>

- e) **Monitoramento:** é fundamental acompanhar continuamente os elementos identificados na análise de risco para incorporar alterações, como o surgimento de novas ameaças, e ajustar a avaliação conforme necessário.

Por fim, no que se refere ao primeiro questionamento (as boas práticas que devem ser adotadas para assegurar que a limitação não configure discriminação ilícita ou abusiva), destacam-se os pontos já apresentados na **Pergunta 8**.

12. Considerando que há serviços não essenciais cujas funcionalidades específicas podem depender tecnicamente da autenticação biométrica, quais boas práticas devem ser observadas para garantir que essa limitação não configure discriminação ilícita ou abusiva? Em que contextos a negativa do titular ao fornecimento de seus dados biométricos, especialmente quando o tratamento se baseia no consentimento, pode justificar, de forma proporcional e transparente, a restrição ao uso de determinadas funcionalidades?

Em complemento às orientações apresentadas na **Pergunta 8**, é essencial considerar o princípio da acessibilidade no uso de ferramentas biométricas, especialmente no caso de indivíduos com deficiência visual, que podem enfrentar dificuldades significativas no uso dessa solução²⁶.

Diante disso, é importante que as organizações avaliem esse desafio de maneira responsável e implementem mecanismos que mitiguem barreiras identificadas. Por exemplo: quando for possível confirmar a existência de deficiência visual, é recomendável, em caráter excepcional, viabilizar os métodos alternativos de autenticação, mesmo que esses não ofereçam o mesmo nível de proteção.

Sobre o uso da base legal do consentimento, é legítimo que a recusa do titular em consentir com o tratamento de dados biométricos leve à indisponibilidade de funcionalidades específicas que, de fato, dependam desse tipo de dado. Por exemplo, nas instituições financeiras que oferecem a possibilidade de confirmação de transações por biometria ou senha, recusar o consentimento pode implicar, legitimamente, na não disponibilização da funcionalidade biométrica ao titular; já as academias podem disponibilizar o acesso às suas dependências tanto por biometria facial quanto por senha associada ao número de matrícula²⁷. Nesse cenário, caso o titular opte por não fornecer o consentimento, o acesso via biometria facial poderá ser validamente negado.

Contudo, destaca-se que o não fornecimento do consentimento **não deve**, em hipótese alguma, inviabilizar o acesso a serviços ou funcionalidades cuja operação **não dependa necessariamente** da coleta de dados biométricos.

²⁶ <https://www.vice.com/en/article/facial-recognition-apps-are-leaving-blind-people-behind/>

²⁷ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/>

Nos outros casos em que não se adota a base do consentimento, a recusa do titular em fornecer a biometria deve ser tratada como exercício legítimo do direito de oposição. Aqui, a negativa de acesso à funcionalidade, serviço ou produto poderá ser considerada lícita desde que **(i)** seja tecnicamente inviável ofertar a funcionalidade sem tratamento de dados biométricos, conforme os mesmos parâmetros aplicáveis à hipótese de consentimento; ou **(ii)** os direitos ou interesses legítimos da organização, relativos à exigência do dado biométrico, não sejam superados pelo direito do titular de não a ofertar (há razão pela qual a validação biométrica é necessária, como a existência de bem protegido relevante)²⁸.

13. Quais seriam as boas práticas específicas a serem adotadas pelos controladores para conferir uma proteção eficaz no tratamento de dados biométricos? Como garantir que os dados biométricos coletados sejam utilizados de forma transparente e responsável, evitando, por exemplo, a discriminação ilícita e abusiva em face dos usuários?

Retomando as orientações já apresentadas nas **Perguntas 2, 5, 8 e 11**, destacamos os seguintes pontos adicionais:

- **Medidas de proteção e segurança:** além da necessidade de realizar avaliação estruturada de riscos de cibersegurança, conforme detalhado na **Pergunta 11**, reforçamos a importância de implementar controles técnicos e organizacionais indicados na Pergunta 8. Tais controles estão alinhados com as boas práticas recomendadas por autoridades de proteção de dados como o ICO (Reino Unido), o INAI (México) e a PIPC (Coreia do Sul).
- **Medidas de transparência:** a obrigação legal de transparência no uso de dados biométricos está no art. 9º da LGPD, que determina a necessidade de informar ao titular os elementos essenciais da operação de tratamento. Contudo, a forma como tais informações devem ser apresentadas ao titular deve considerar fatores como a finalidade específica da atividade de tratamento, a natureza do relacionamento entre a organização e o titular e ainda o contexto de uso da tecnologia. Como indicado nas **Perguntas 2 e 8**, com base na abordagem do ICO, quanto mais clara e compreensível for a atividade de tratamento para o titular (por exemplo, em casos de uso amplamente difundidos e esperados pelo público), menor será a exigência por práticas ativas de comunicação. Em contrapartida, usos menos usuais ou mais sensíveis exigem transparência proativa e reforçada, com comunicações específicas.
- **Risco de discriminação:** em relação à prevenção de discriminações ou vieses, reiteramos as medidas já detalhadas na **Pergunta 8**, com base nas orientações do ICO.

14. Como os controladores podem assegurar o respeito à autodeterminação informativa dos titulares em contextos de tratamento contínuo e massivo de dados biométricos – como em iniciativas de cidades inteligentes (*smart cities*), monitoramento de grandes multidões, como em estádios e espaços públicos? Quais medidas concretas devem ser adotadas para garantir

que os titulares sejam devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

No que se refere ao direito à informação, e como já abordado na **Pergunta 2**, quando os titulares não possuem expectativa sobre a coleta de informações biométricas (em especial em situações em que não há vínculo anterior com o controlador), é necessário empenho adicional para garantir a transparência do tratamento.

Para cumprir essa exigência, é possível, por exemplo, instalar sinalizações visíveis nos locais de coleta contendo informações básicas sobre o tratamento realizado, bem como indicar os canais pelos quais os titulares podem acessar dados mais completos e exercer seus direitos. Também é recomendável o uso de QR Codes posicionados em estruturas fixas, como paredes, painéis ou telas, que direcionem para o Aviso de Privacidade da organização, onde devem constar todas as informações exigidas pela legislação.

A ANPD já avaliou situação análoga e considerou adequadas as medidas mencionadas acima de prestação de informação, conforme Nota Técnica nº 29/2024/FIS/CGF/ANPD (§ 6.1.4)²⁹.

BLOCO V - DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

15. De que forma os agentes de tratamento podem garantir o respeito aos direitos dos titulares, em especial o direito à informação clara, o direito ao acesso e à correção de dados e o direito à revogação do consentimento, como, por exemplo, em contextos de tratamento automatizado de dados biométricos?

Além das medidas de transparência já abordadas em **Perguntas anteriores**, é essencial garantir o exercício dos direitos dos titulares, levando em conta as particularidades inerentes à utilização de tecnologia biométrica.

Quanto ao **direito de acesso**, o ICO³⁰ reconhece que existem limitações técnicas para fornecer diretamente dados biométricos, pois eles normalmente se apresentam como representações matemáticas complexas e não inteligíveis para os seres humanos. Essas representações - ou *templates* - não possuem valor informativo direto para o titular e, se fornecidas, poderiam expor o sistema a riscos de engenharia reversa ou outros vetores de ataque. Por isso, recomenda-se que o controlador forneça:

- A confirmação da existência do tratamento e a finalidade específica (ex.: “seus dados biométricos faciais são utilizados para autenticação de login e para autorização de transações acima de R\$ 1.000,00, visando prevenir fraudes e proteger sua conta”).
- O tipo de dado biométrico tratado, tais como biometria facial, impressão digital etc.

²⁹ https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-29_2024.pdf

³⁰

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>

- A fonte dos dados, informando que o *template* foi gerado a partir da foto (“selfie”) ou imagem fornecida pelo próprio titular durante o processo de cadastro.
- A possibilidade de fornecer a amostra original que deu origem ao *template* (ex.: a foto de rosto enviada no cadastro), caso esta ainda seja armazenada pelo controlador.
- Outras informações vinculadas ao processo, como data e hora das últimas autenticações bem-sucedidas ou falhas, e o identificador da conta associado (como o CPF).

Essa abordagem fornece transparência significativa e útil ao titular, sem criar vulnerabilidades de segurança para o ecossistema financeiro.

O **direito à correção**, conforme pontuado pelo próprio ICO³¹, não é aplicável ao resultado estatístico de uma comparação biométrica. A decisão de autenticar ou não um usuário é baseada em um cálculo de probabilidade (*match score*), e não em um dado cadastral passível de simples retificação. O direito à correção, no entanto, é aplicável aos seguintes casos:

- Erro na associação: quando há um erro no processo de cadastro que vinculou a biometria de um indivíduo ao CPF de outro.
- Necessidade de atualização: mudanças físicas relevantes no titular (ex.: envelhecimento, acidentes etc.) podem degradar a qualidade da autenticação. Para garantir o acesso contínuo e seguro do cliente, as plataformas devem oferecer um fluxo de recadastramento biométrico, permitindo que o *template* antigo seja descartado e substituído por um novo e mais acurado³².

O direito à **revogação do consentimento** deve ter sua aplicação ponderada com as demais bases legais que legitimam o tratamento de dados no setor financeiro, em especial o cumprimento de obrigação legal ou regulatória e a garantia da prevenção à fraude e à segurança do titular. No mercado financeiro, o uso da base legal do consentimento para o tratamento de dados biométricos é residual e geralmente está amparado nas duas bases legais anteriormente mencionadas. Mas, quando cabível, a revogação do consentimento deve ensejar procedimento que leve a inutilização ou exclusão do *template* biométrico, impedindo com que o dado seja utilizado para autenticações futuras. É importante destacar que a revogação do consentimento não pode implicar a eliminação automática e irrestrita de registros de validações biométricas já realizados. As instituições financeiras e de pagamento possuem obrigações impostas pelo BCB, CVM e outros supervisores do SFN, algumas delas amparadas em legislações de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, que exigem a manutenção dos registros históricos de transações e da identificação do cliente por períodos determinados. Tais registros são essenciais para:

- Auditorias regulatórias e de segurança.
- Investigações de fraudes e disputas de transações (*chargebacks*).

³¹

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/>

³²

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/>

- Comprovação do cumprimento de deveres perante os órgãos reguladores.

A revogação, nestes casos específicos, cancela o uso futuro da biometria, mas os registros devem ser mantidos pelo prazo exigido na regulamentação setorial aplicável.

16. Diante da sensibilidade dos dados biométricos de crianças e adolescentes, especialmente em contextos como escolas e espaços recreativos, como garantir a participação informada dos pais ou responsáveis e em quais hipóteses legais esse tipo de tratamento seria admissível? Quais condições devem ser observadas para que esse tratamento esteja alinhado ao princípio do melhor interesse, nos termos do art. 14 da LGPD?

De acordo com o Enunciado CD/ANPD nº 1/2023³³, a ANPD reconhece que o tratamento de dados pessoais de crianças e adolescentes pode ser realizado com base em qualquer uma das hipóteses legais previstas nos arts. 7º e 11 da LGPD, desde que seja garantido o atendimento ao melhor interesse do menor. Dessa forma, desde que os requisitos legais para a base escolhida sejam cumpridos e fique comprovado que a atividade de tratamento está voltada para o melhor interesse da criança ou do adolescente, o uso de dados biométricos desses indivíduos pode se apoiar em qualquer das bases legais previstas na LGPD

No que diz respeito à **transparência** e ao **envolvimento dos pais ou responsáveis legais**, embora a legislação britânica (*Protection of Freedoms Act 2012*) estabeleça abordagem distinta, exigindo consentimento dos responsáveis para tratamento de dados biométricos de menores, o Guia do Governo do Reino Unido³⁴ apresenta recomendações que podem ser utilizadas como referência, desde que adaptadas ao arcabouço jurídico brasileiro. Assim, além de incluir informações sobre o tratamento de dados biométricos no Aviso de Privacidade, é recomendável, quando possível: **(i)** enviar comunicações formais aos pais ou responsáveis, contendo explicações claras sobre os objetivos e fundamentos do tratamento; **(ii)** informar os canais de atendimento destinados ao exercício de direitos dos titulares e obtenção de mais detalhes sobre o tratamento; e **(iii)** quando aplicável, disponibilizar mecanismos que permitam a oposição ao tratamento, com orientações visíveis e acessíveis sobre como exercer essa prerrogativa.

Por último, a análise do melhor interesse da criança deve ser feita com base nas circunstâncias concretas de cada caso, levando em conta, em especial: **(i)** o bem jurídico que se busca proteger (em especial o próprio interesse da criança ou adolescente), o que permite verificar se o impacto sobre a privacidade do titular é justificado e proporcional ao objetivo pretendido; **(ii)** a existência de alternativas menos invasivas que permitam alcançar o mesmo resultado, com desempenho semelhante; e **(iii)** a possibilidade de mudanças relevantes em certas características biométricas durante o desenvolvimento físico da criança ou adolescente, como é

³³

<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf>

³⁴ https://assets.publishing.service.gov.uk/media/62d7d76c8fa8f50c012d14df/Biometrics_Guidance_July_2022.pdf

o caso das feições faciais na puberdade, o que pode interferir na eficácia do tratamento, especialmente se ele precisar perdurar por longos períodos³⁵.

17. Em quais hipóteses legais esse tipo de tratamento seria admissível, e como garantir a participação informada dos pais ou responsáveis, além da adoção de medidas técnicas e organizacionais eficazes para evitar abusos, vazamentos ou acessos indevidos?

Sobre bases legais aplicáveis e a necessidade de participação informada de pais ou responsáveis, valem as observações já feitas na **Pergunta 16**:

- **Bases legais:** conforme previsto no Enunciado CD/ANPD nº 1/2023, a ANPD admite que o tratamento de dados pessoais de crianças e adolescentes seja realizado com fundamento em qualquer das hipóteses previstas nos arts. 7º e 11 da LGPD, desde que esteja assegurado, como prioridade, o melhor interesse da criança ou do adolescente. Sendo assim, o uso de dados biométricos de menores de idade é permitido, desde que haja base legal devidamente fundamentada e o tratamento tenha como finalidade proteger os interesses dos menores.
- **Transparência:** além de incluir as informações no Aviso de Privacidade, é recomendável, se possível, realizar a comunicação direta aos pais e/ou responsáveis, com explicações sobre a operação de tratamento e os meios disponíveis para o exercício dos direitos dos titulares.

Por fim, quanto às medidas de segurança a serem adotadas, aplicam-se os mesmos parâmetros já indicados nas **Perguntas 5 e 11**.

18. Em casos de verificação ou estimação de idade por meio de fornecimento de dados biométricos para acesso a plataformas digitais e jogos, por exemplo, quais critérios devem ser observados no tratamento dos dados de crianças e adolescentes? Como compatibilizar tal prática com o princípio da necessidade e do melhor interesse?

A escolha por mecanismos de verificação de idade deve considerar 3 (três) fatores principais: **(i)** o contexto em que essa verificação se dá; **(ii)** o nível de precisão da tecnologia escolhida; e **(iii)** a disponibilidade de alternativas menos invasivas que consigam alcançar o mesmo resultado de forma adequada.

- **Contexto de verificação:** a definição do método mais adequado dependerá diretamente da finalidade e da criticidade do serviço prestado. Nesse sentido, é fundamental compreender o princípio da necessidade não apenas como a limitação ao menor volume de dados possível, mas como o uso dos dados essenciais para atingir finalidades legítimas, permitindo uma ponderação cuidadosa entre a privacidade e outras obrigações, como a garantia do melhor interesse de crianças e adolescentes. Em certos casos, a coleta de um dado

³⁵https://quno.org/sites/default/files/resources/QUNO_Briefing%20Paper_Biometric%20data%20of%20PACTO_SEP2020.pdf

específico pode ser a medida mais adequada para proteger este grupo vulnerável. Essa análise é crucial para garantir que a coleta de dados biométricos esteja de acordo com o princípio da necessidade e respeite o melhor interesse da criança ou adolescente. Conforme orientações do ICO, a técnica adotada para confirmar a idade deve ser proporcional aos riscos oferecidos pelo serviço e pelo tratamento de dados aos menores de idade.

Exemplo: Uma plataforma de serviço financeiro digital pode utilizar a biometria facial para verificar a idade, especialmente se o serviço envolver funcionalidades restritas a maiores de idade (como alguns produtos de crédito e de investimentos). Ao combinar a biometria com a verificação de um documento de identidade digital, busca-se confirmar com mais segurança e dentro do melhor interesse do menor se a pessoa que está tentando abrir uma conta ou acessar um investimento é realmente o titular do documento, prevenindo fraudes. Trata-se de camada adicional de verificação, na medida em que o documento comprova a identidade registrada e a biometria reforça que quem está usando o dispositivo/serviço é de fato aquela pessoa.

- **Acurácia da tecnologia:** deve-se considerar o grau de confiabilidade e precisão da tecnologia adotada, pois tecnologias que estimam a idade com biometria frequentemente apresentam margem de erro considerável³⁶⁻³⁷ e métodos que combinam a verificação documental (como análise do documento de identidade) com a confirmação visual costumam ser mais eficazes.
- **Soluções alternativas menos invasivas:** É igualmente necessário avaliar se existem métodos menos intrusivos que, no contexto analisado, sejam capazes de atingir nível de acuracidade semelhante, ou minimamente satisfatório, em face do risco efetivo de acesso indevido de menores. Exemplos de alternativas incluem³⁸⁻³⁹: declaração de idade feita diretamente pelo usuário, mediante fornecimento da data de nascimento (ou a autodeclaração); confirmação via cartão de crédito, com cobrança simbólica (R\$ 0,01) para verificar titularidade e idade; análise de comportamento digital, inferindo a idade a partir do padrão de uso e conteúdos acessados; verificação presencial de documentos oficiais antes de conceder o acesso; e até a obtenção de consentimento do responsável legal, desde que a sua identidade e autoridade possam ser confirmadas de maneira confiável.

Em suma, a utilização de biometria facial para fins de verificação etária deve ser cuidadosamente avaliada em cada situação concreta, com base no princípio do melhor interesse da criança e do adolescente, levando em conta os riscos específicos e os impactos potenciais associados ao uso de dados biométricos.

³⁶ [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA\(2023\)739350_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf)

³⁷ <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>

³⁸ [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA\(2023\)739350_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf)

³⁹ <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>

Zetta

À sua consideração,
Zetta