Agência Nacional de Proteção de Dados
Coordenação-Geral de Normatização
Coordenação de Normatização 1

Nota Técnica nº 23/2025/CON1/CGN/ANPD

1. INTERESSADO

1.1. Conselho Diretor, Secretaria-Geral, Gabinete do Diretor-Presidente.

2. ASSUNTO

2.1. Consolidação das contribuições recebidas na Tomada de Subsídios.

3. REFERÊNCIAS

3.1. Processo SEI/ANPD nº 00261.004105/2024-42.

3.2. Processo SEI/ANPD nº 00261.001953/2025-81 (Tomada de Subsídios).

4. RELATÓRIO

4.1. Trata-se do projeto regulatório que dispõe sobre o Item 5 da Agenda Regulatória da Autoridade Nacional de Proteção de Dados (ANPD) para o biênio 2025-2026, aprovada pela Resolução nº 23, de 09 de dezembro de 2024 (SEI/ANPD nº 0160131), *Dados Biométricos - Dados Sensíveis.*

4.2. O processo iniciou-se em 11/6/2024, com o envio do Ofício nº 205/2024/CON1/CGN/ANPD (SEI/ANPD nº 0126497) às áreas técnicas para indicação de membros para composição da equipe de projetos conforme art. 11, da Portaria ANPD nº 16/2021.

4.3. Logo após, na data de 27/06/2024, foi firmado o Termo de Abertura de Projeto (TAP) (SEI/ANPD nº 0128230) que assim dispõe:

> [..]
>
> A ANPD entende ser necessário, no que tange ao tratamento de dados sensíveis - dados biométricos, assegurar que o tratamento desses dados estão sendo feitos com observância às diretrizes da LGPD, ou seja, respeitando o direito de privacidade, a inviolabilidade da intimidade, da honra e da imagem e, ao mesmo tempo, fomentando a livre iniciativa e a livre concorrência, o desenvolvimento econômico e tecnológico, garantindo transparência e consentimento informado, e protegendo contra a discriminação e

uso indevido dos dados.

Será necessário aprofundar estudos e pesquisas sobre o tema, bem como realizar tomada de subsídios, encontros com especialistas e *benchmarking* internacional.

4.4. Diante disso, a fim de verificar a perspectiva da sociedade sobre o tema – que inclui titulares, agentes de tratamento de diferentes setores e modelos de negócios –, esta Coordenação-Geral optou por realizar Tomada de Subsídios - Nota Técnica nº 17/2025/CON1/CGN/ANPD (SEI/ANPD nº 0187746) -, nos termos dos arts. 18 a 22, da Portaria nº 16, de 08 de julho de 2021, que aprova o processo de regulamentação no âmbito da Autoridade. *In verbis:*

> Art. 18. A Tomada de Subsídios visa obter insumos para o processo de regulamentação e pode ser realizada a qualquer momento, a critério da Equipe de Projeto.
>
> § 1º A Tomada de Subsídios não representa o posicionamento final da ANPD.

4.5. Assim, foi comunicada a referida Tomada, por meio do Despacho SEI/ANPD nº 0188805, a ser realizada entre os dias 02 de junho e 02 de julho, com prorrogação para até o dia 01 de agosto de 2025 (Despacho SEI/ANPD nº 0193884).

4.6. Para isso, foram elaboradas 18 (dezoito) perguntas, divididas em 5 (cinco) blocos temáticos, da seguinte forma (SEI/ANPD nº 0187788):

a. **Bloco 1** – Definições e princípios;

b. **Bloco 2** – Hipóteses Legais;

c . **Bloco 3**– Tecnologias de reconhecimento facial e aplicação de tecnologias emergentes e inovadoras no tratamento de dados biométricos;

d. **Bloco 4** – Segurança, boas práticas e governança;

e. **Bloco 5** – Direitos dos titulares e grupos vulneráveis.

4.7. Ato contínuo, foi publicada a Consulta à Sociedade em formato de Tomada de Subsídios e disponibilizada para contribuições por meio da Plataforma Participa Mais Brasil.

4.8. É o relatório.

5. ANÁLISE

Das Contribuições Recebidas

5.1. No âmbito da Plataforma, foram recebidas 83 (oitenta e três) manifestações de contribuintes, das quais 30 (trinta) receberam complementações, e outras 5 (cinco) manifestações que foram integralmente encaminhadas em formato ".pdf", pelo correio eletrônico institucional normatizacao@anpd.gov.br. Tal situação se deu em razão do limite de caracteres disponível no "Opine Aqui" da Plataforma Participa Mais Brasil, fato que impossibilitou a submissão integral da contribuição. Todas as contribuições foram devidamente analisadas pela Equipe de Projeto e

juntadas ao processo, conforme Certidão SEI/ANPD nº 0213041.

5.2. Ressalta-se que as manifestações em formato ".pdf" foram anexadas ao processo em epígrafe (SEI/ANPD nº 0212868, 0212869, 0212878, 0212880, 0212887, 0212888, 0212889, 0212890, 0212892, 0212894, 0212895, 0212897, 0212899, 0212901, 0212903, 0212904, 0212905, 0212906, 0212907, 0212908, 0212909, 0212910, 0212911, 0212912, 0212913, 0212914, 0212915, 0212917, 0212918, 0212919, 0212920, 0212921, 0212922, 0212923, 0212924), assim como as manifestações provenientes da Plataforma Participa Mais Brasil - "Opine Aqui" (SEI/ANPD nº 0212926).

5.3. Considerando que foram formuladas 18 (dezoito) perguntas e que houve 88 (oitenta e oito) manifestações de contribuintes, o número global de contribuições recebidas e analisadas pela CGN foi de **1.594 (mil quinhentos e noventa e quatro)**, considerando que cada resposta equivale a uma contribuição.

5.4. Quanto ao perfil dos contribuintes, cerca de 68 (sessenta e oito) representaram algum agente de tratamento, o que equivale a, aproximadamente, 78% (setenta e oito porcento). Os demais, se pronunciaram em nome próprio.

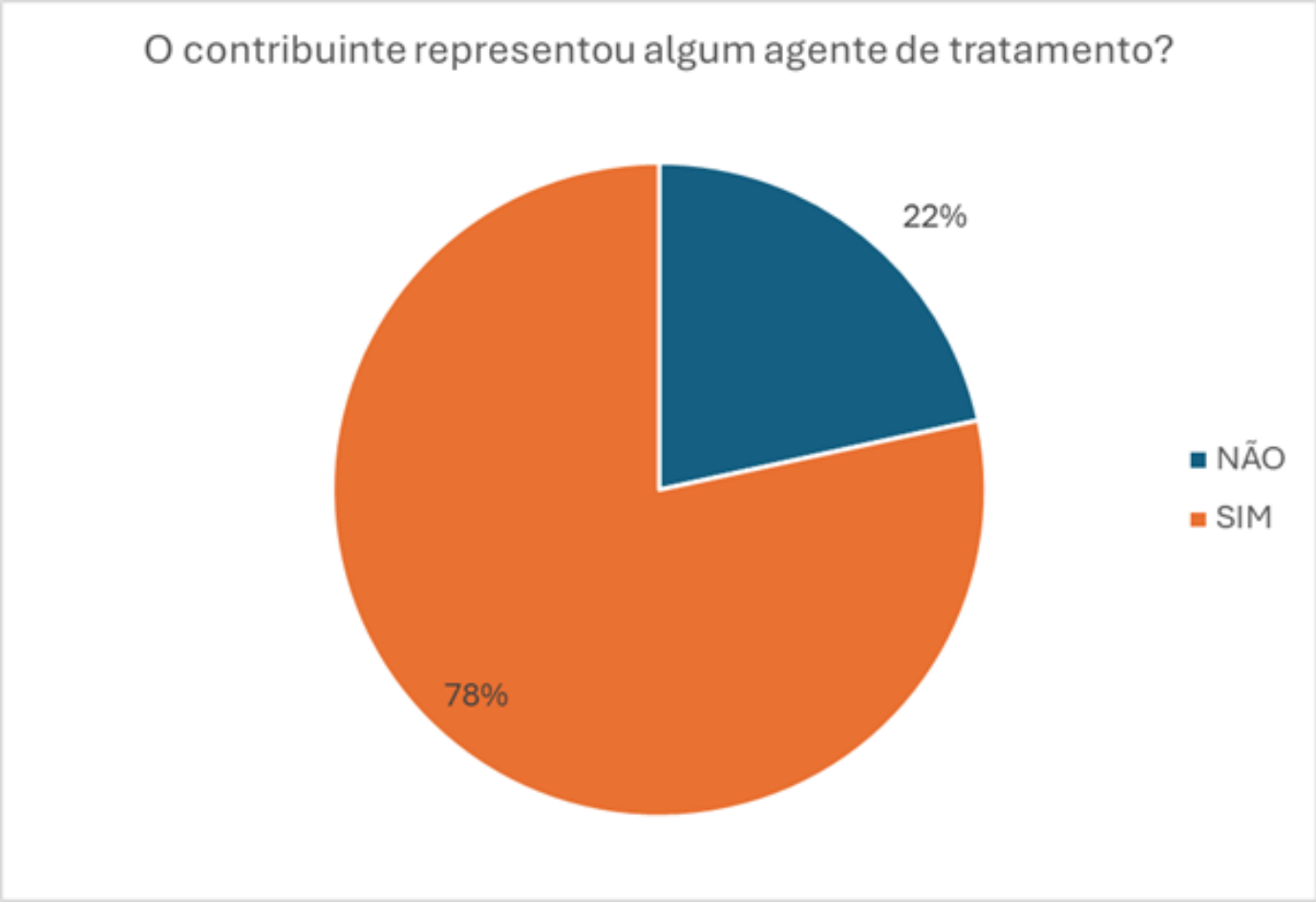

Gráfico 1 - Contribuintes que responderam ao questionário em nome de algum agente de tratamento

5.5. No que se refere à nacionalidade dos participantes, a maioria é brasileira - 98% (noventa e oito por cento). A participação de estrangeiros foi em um número pequeno. Veja o Gráfico 02:

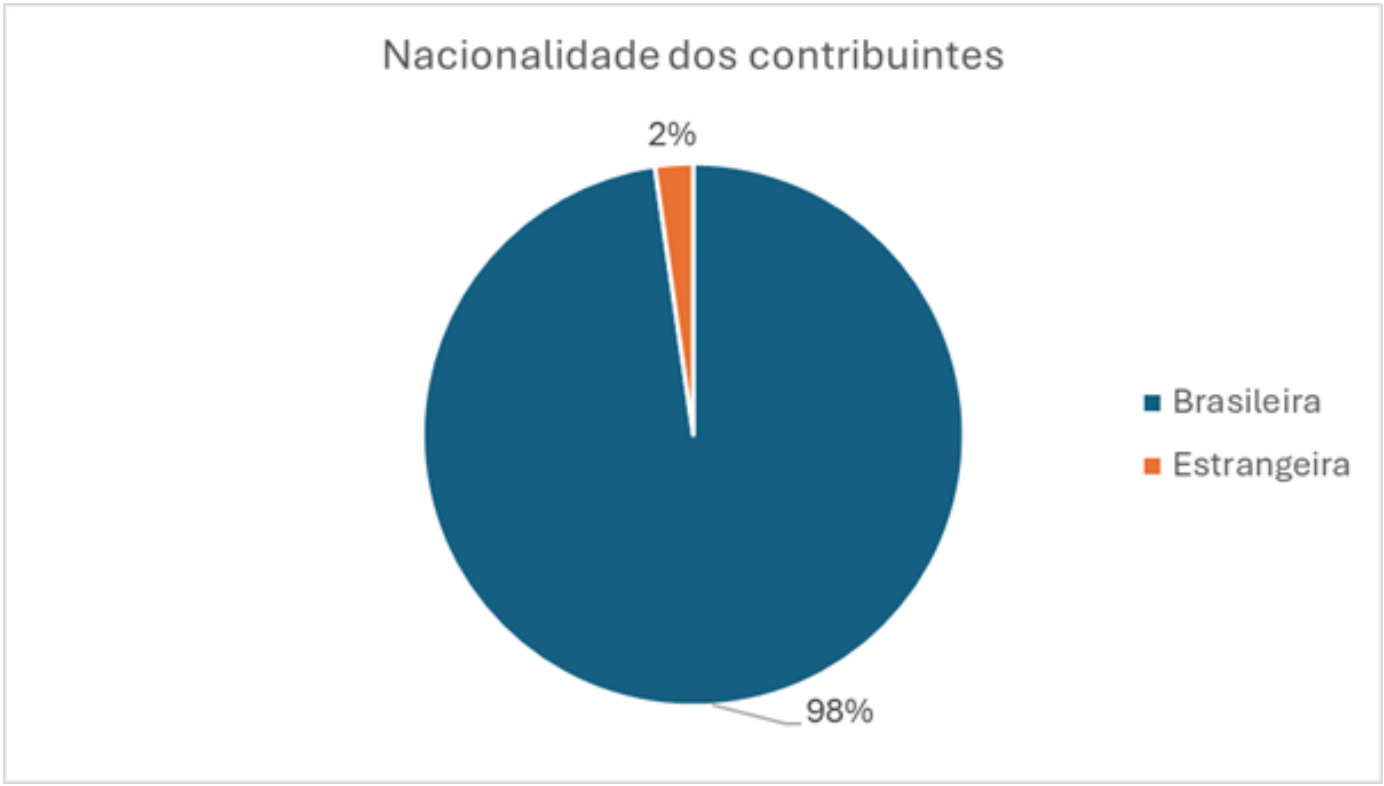

Gráfico 2 - Nacionalidade dos contribuintes

5.6. No que tange à região do Brasil de origem dos contribuintes, o Sudeste obteve o maior índice de representatividade, com 78% (setenta e oito porcento), conforme o Gráfico 03:

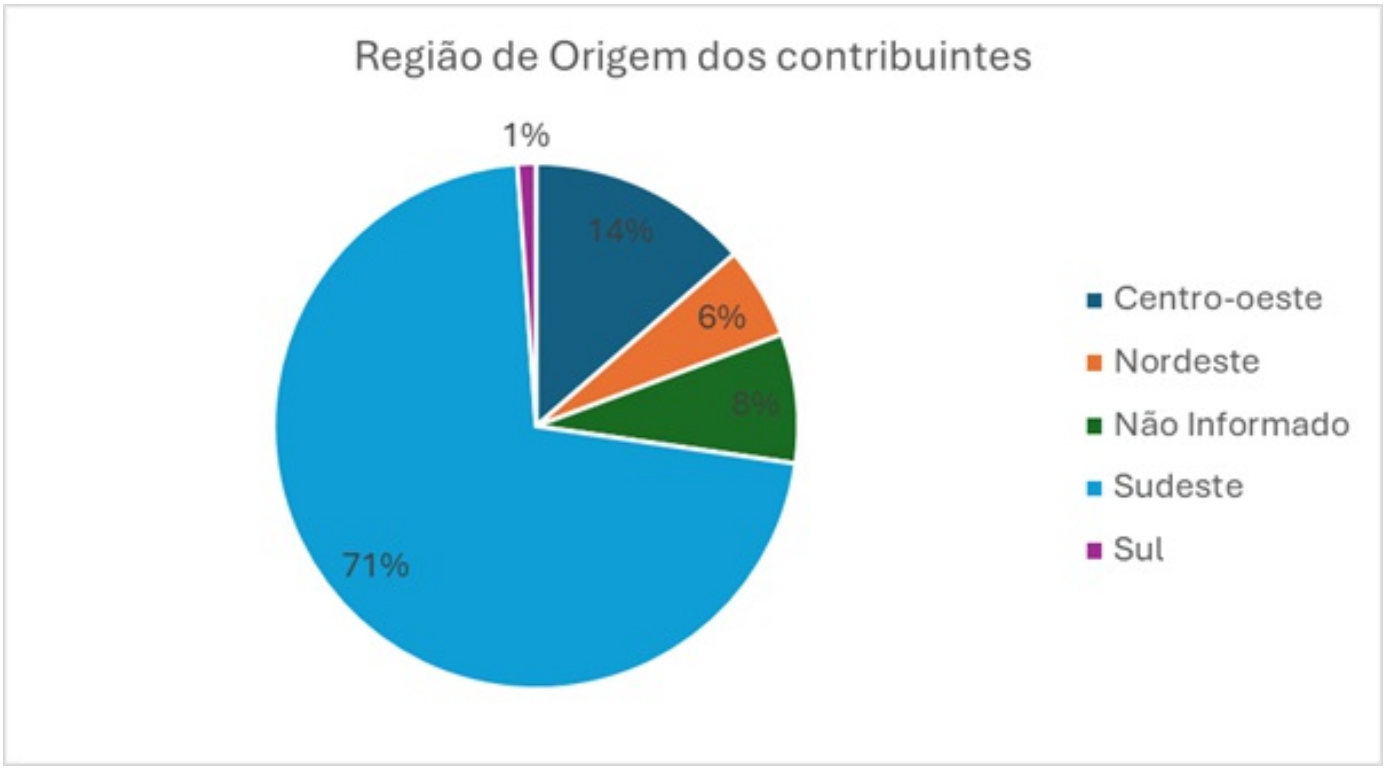

Gráfico 3 - região de origem dos contribuintes

5.7. Quanto às profissões dos contribuintes, houve prevalência da carreira advocatícia, com a maioria de 55% (cinquenta e cinco por cento), seguido do setor da engenharia, correspondendo a 20% (vinte por cento), conforme gráfico 04:

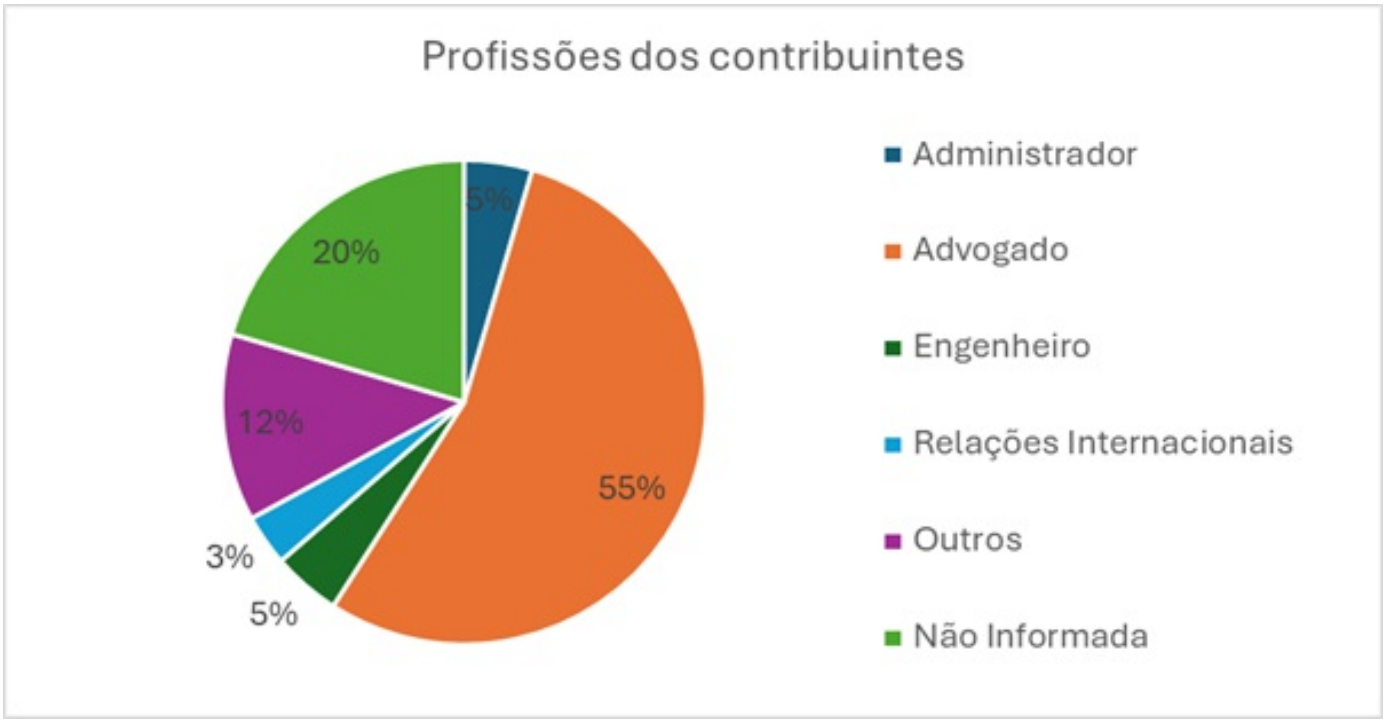

Gráfico 4 - profissão dos contribuintes

5.8. Por fim, quanto ao tipo de contribuinte, as pessoas físicas tiveram prevalência, com cerca de 47% (quarenta e sete porcento das contribuições). A iniciativa privada consubstanciou 32% (trinta e dois porcento), conforme o Gráfico 05:

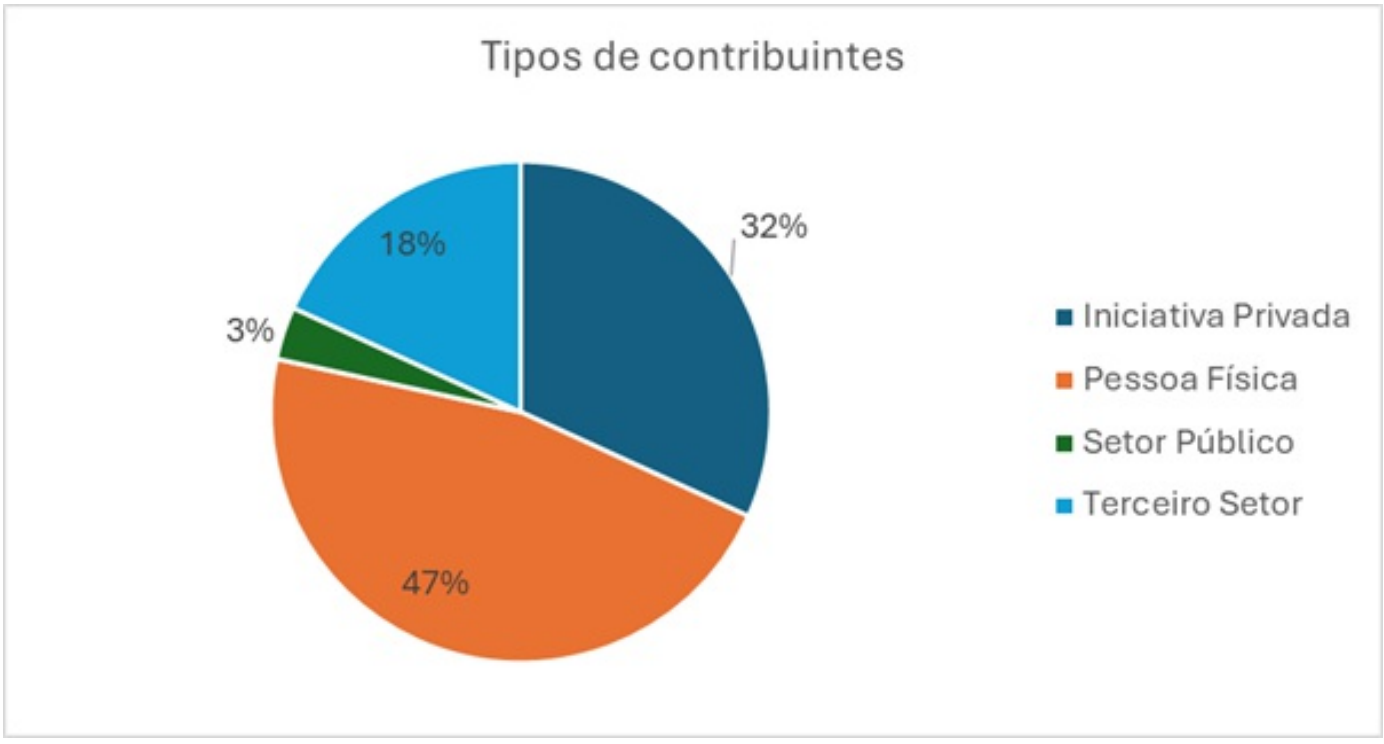

Gráfico 5 - Tipos de contribuintes

<u>Metodologia da Análise</u>

5.9. Mesmo não se tratando de Consulta Pública de normativo, nos termos da legislação aplicável, as análises foram realizadas de forma similar com o objetivo de favorecer a transparência e a participação social.

5.10. Assim, foi realizado primeiro o descarte das contribuições repetitivas, em conformidade com o parágrafo único do art. 19 do Decreto nº 10.411/2020 e com o § 6º do art. 62, do Regimento Interno da ANPD (RIANPD), aprovado pela Portaria nº 1, de 8 de março de 2021.

5.11. Cabe destacar que o juízo de admissibilidade das contribuições considerou a pertinência em relação ao escopo do Projeto e a ausência de duplicidade em relação às análises previamente realizadas.

5.12. Para fins de análise pela equipe de projeto, as contribuições foram consolidadas em 18 (dezoito) arquivos, que correspondem a cada questão submetida à Tomada de Subsídios. Esses arquivos consolidam as contribuições submetidas tanto por e-mail institucional, em formato ".pdf", quanto as recebidas no âmbito da Plataforma Participa Mais Brasil.

6. CONSOLIDAÇÃO DAS CONTRIBUIÇÕES: CONVERGÊNCIAS E DIVERGÊNCIAS

6.1. A análise das contribuições nesta Nota Técnica foi organizada de modo a delinear um cenário no qual se verificam pontos de convergências e divergências em relação ao questionamento formulado.

6.2. Assim, optou-se por destacar tais pontos em formato de tópicos gerais, seguidos por breves descrições. Essa estratégia permite facilitar a análise de mérito das contribuições por parte da equipe de projeto e, com isso, eventualmente utilizá-las como parâmetro na elaboração dos produtos relativos ao projeto regulatório. Além disso, permite também sistematizar as contribuições recebidas com a finalidade de proporcionar uma leitura fluída do documento. O produto desta análise consolidada será apresentado ao longo deste documento.

6.3. Sem prejuízo disso, tanto as contribuições provenientes da Plataforma Participa Mais Brasil (SEI/ANPD nº 0212926) quanto as manifestações recebidas por e-mail institucional foram anexadas ao Processo em epígrafe na íntegra e estão disponíveis para acesso e consulta.

6.4. A seguir, apresenta-se cada uma das 18 (dezoito) questões, com as respectivas convergências e divergências.

BLOCO I - PRINCÍPIOS DA LGPD

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

6.5. As contribuições sobre esse questionamento apresentam diferentes perspectivas quanto aos critérios a serem observados para a caracterização de um dado pessoal como biométrico nos termos da LGPD. De modo geral, destaca-se a relevância de parâmetros claros que orientem essa definição, ao mesmo tempo em que surgem entendimentos distintos sobre sua aplicação prática.

Pontos Convergentes:

6.6. Dentre os elementos que convergem quanto os critérios objetivos estão os seguintes:

- **Natureza do dado biométrico:** Há um consenso de que os dados biométricos devem estar vinculados a características físicas, fisiológicas ou comportamentais inerentes a uma pessoa natural. São mencionados com frequência exemplos tradicionais como impressões digitais, íris, reconhecimento facial, voz, forma de andar e padrões de digitação (OP-968689, OP-969488, OP-1000400).
- **Tratamento técnico específico:** A mera existência de uma característica física ou comportamental não configura um dado biométrico. É crucial que essa característica seja capturada e processada por meios técnicos específicos, como *softwares* de reconhecimento facial, sistemas de autenticação por voz, algoritmos, sensores ou outras tecnologias que extraiam padrões ou modelos matemáticos únicos, também chamado de *templates* biométricos. Assim, uma foto simples ou gravação de voz, por exemplo, não é biométrica por si só, mas pode se tornar se utilizada por um sistema de reconhecimento com a finalidade de extrair características identificadoras (OP-1003891, OP-1005106, OP-1005106).
- **Finalidade de identificação ou autenticação única:** O dado só deve ser classificado como biométrico quando processado com a finalidade de identificar ou autenticar de forma inequívoca uma pessoa. Assim, usos de características físicas ou comportamentais para fins estatísticos, analíticos ou de pesquisa, sem a respectiva individualização, não configura tratamento de dados biométricos (OP-1006162, OP-1006297, OP-1006120).
- **Alinhamento com Normativas Internacionais:** muitas contribuições sugerem que a ANPD alinhe a interpretação da LGPD, em especial no que se refere à caracterização de dados biométricos como dados pessoais sensíveis, com parâmetros internacionais, como o Regulamento Geral de Proteção de Dados da União Europeia (RGPD), as diretrizes do *Information Commissioner's Office* (ICO) do Reino Unido, o *European Data Protection Board* (EDPB) e normas ISO, como a ISO/IEC 2382-37:2022 e a ISO/IEC 24745:2022 (OP-967732, OP-969104, dentre outras).

<u>Pontos Divergentes:</u>

6.7. Por outro lado, as contribuições também apresentaram divergências relevantes, especialmente no que se refere a:

- **Unicidade individual como critério obrigatório:** A maioria das contribuições considera a unicidade individual — entendida como a capacidade de identificar de forma única, singular ou inequívoca — critério fundamental e, em muitos casos, cumulativo para caracterizar um dado como biométrico. Nessa visão, a biometria se aplica apenas a elementos capazes de distinguir uma pessoa de todas as demais, como impressões

digitais, padrões de íris ou reconhecimento facial. Em contraponto, outras contribuições questionam a exigência desse critério, sustentando que qualquer dado pessoal vinculado a uma característica física, imaterial ou comportamental é de plano biométrico, ainda que utilizado apenas para classificações genéricas ou coletivas. Outros ampliam essa discussão ao apontar que o potencial de individualização também deveria ser observado, pois, mesmo quando a finalidade declarada não é a de identificar pessoas, a mera possibilidade técnica de vinculação à identidade já seria suficiente para caracterizar o dado como biométrico, independentemente do uso pretendido (OP-1002202, OP 1006211, OP-1006211).

- **Classificação de Dados Biométricos como Dados Sensíveis (com RBRs):** Houve divergência entre os participantes quanto à natureza sensível dos dados biométricos. Algumas contribuições defendem que, com o uso de Referências Biométricas Renováveis (RBRs), que incorporam características como:

o **Multiplicidade:** possibilidade de gerar várias credenciais biométricas a partir da mesma característica original.

o **Irreversibilidade:** impossibilidade de reconstruir a imagem original (por exemplo, o rosto ou a íris) a partir da referência armazenada.

o **Não interoperabilidade:** a credencial criada em um sistema não pode ser usada em outro, evitando reutilização indevida.

o **Revogabilidade:** caso ocorra uma violação, a referência pode ser "cancelada" e substituída por outra, assim como ocorre com senhas.

6.8. Nesse sentido, deve a ANPD avaliar se, nesses casos, os dados ainda devem ser considerados como sensíveis. Por outro lado, a posição predominante sustenta que os dados biométricos são intrinsecamente sensíveis, em razão de sua singularidade e imutabilidade. Argumenta-se que, mesmo quando tratados por RBRs ou templates biométricos revogáveis, a característica original permanece única, e um eventual vazamento configuraria dano irreversível ao titular, justificando a necessidade de proteção reforçada. (OP-969104, OP-969154 OP-969488, OP-977469, OP-979836, OP-1005260, OP-1006232, entre outras).

- **Contexto do Risco:** Algumas contribuições sustentam que os dados biométricos não devem ser vistos como intrinsecamente perigosos ou automaticamente de alto risco. Segundo essa perspectiva, o risco não está no dado em si, mas no contexto em que ele é utilizado, ou seja, depende da finalidade, da escala do tratamento e das medidas de segurança adotadas. Assim, em cenários com salvaguardas adequadas, o tratamento de dados biométricos pode ter riscos significativamente reduzidos. Isso pode ocorrer, por exemplo, quando do emprego de tecnologias inovadoras como as RBRs, uma vez que, diferentemente da biometria tradicional, que

muitas vezes é fixa e permanente (como a digital de uma pessoa), as RBRs possuem características e mecanismos que aumentam a segurança, descaracterizando o dado bruto. Assim, a classificação deve apoiar-se em uma análise de risco que considere as condições concretas do tratamento e as salvaguardas aplicadas, e não apenas o tipo de dado em si (OP-969154, OP-1006220, OP-1006158, dentre outras).

- **Conteúdos Gerados por Inteligência Artificial (IA):**Há contribuição que levanta a hipótese de que conteúdos gerados por IA, como vozes ou rostos sintéticos, não deveriam ser automaticamente enquadrados como dados biométricos para fins da LGPD, ainda que possam ter origem em pessoas reais. Três são os pontos principais: (i) a ruptura do vínculo identificador entre o dado sintético e a pessoa natural, (ii) a ausência de mensurabilidade biológica direta, já que não há coleta da característica física original, e (iii) a falta de confiabilidade na identificação reversa, que inviabiliza a associação inequívoca com um titular específico. Trata-se de uma ponderação voltada às tecnologias emergentes, que busca diferenciar dados efetivamente biométricos daqueles produzidos artificialmente a partir de modelos de IA (OP-1006158, OP 969154).

6.9. As contribuições revelaram consenso quanto à necessidade de critérios objetivos para a caracterização de dados biométricos, destacando-se a vinculação à características físicas, fisiológicas ou comportamentais de uma pessoa natural, a exigência de tratamento técnico específico e a finalidade de identificação ou autenticação única, além da importância de alinhamento com referências internacionais como RGPD, diretrizes europeias e normas ISO. Por outro lado, surgiram divergências relacionadas à obrigatoriedade da unicidade individual, à análise contextual do risco, ao enquadramento de conteúdos gerados por inteligência artificial, à classificação automática de todos os dados biométricos como sensíveis diante de inovações tecnológicas e à adoção do potencial de individualização como critério, ainda que a finalidade não seja identificar diretamente o titular.

Pergunta 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?

6.10. Em relação ao questionamento sobre as práticas de transparência ativa exigíveis dos controladores que realizam o tratamento de dados biométricos, os contribuintes apresentaram diferentes perspectivas. Foram registradas manifestações de consenso, bem como divergências quanto às formas consideradas mais adequadas para assegurar que os titulares recebam informações claras antes da coleta de seus dados.

Pontos Convergentes:

6.11. Dentre os elementos comuns identificados nas contribuições,

verificam-se entendimentos convergentes quanto a:

- **Sinalização Visual e Avisos no Ponto de Coleta:** Necessidade de avisos visíveis e compreensíveis nos locais onde ocorre a coleta de dados biométricos, tanto em ambientes físicos quanto digitais. Quanto ao **conteúdo**, a maioria das contribuições indicam que os controladores devem disponibilizar as principais informações contidas nas políticas de privacidade, tais como, a finalidade do tratamento, a hipótese legal utilizada, o tipo de dado coletado, o período de retenção, os critérios de descarte, as medidas de segurança adotadas, as hipóteses de compartilhamento com terceiros e os direitos dos titulares (OP-968762, dentre outras). Quanto à **forma**, os avisos podem assumir diferentes formatos, como placas, cartazes, folhetos, pop-ups, banners, QR Codes ou televisores. Devem, sobretudo, indicar de forma clara a realização da coleta e disponibilizar acesso ao aviso completo ou à política de privacidade na sua integralidade, preferencialmente antes do início da coleta (OP 1003891, OP-968689, dentre outras).
- **Transparência sobre Riscos e Alternativas:** Há concordância quanto à necessidade de fornecer informações claras sobre os riscos associados ao tratamento de dados biométricos, incluindo eventuais impactos à privacidade e à segurança. Também se destacou a importância de oferecer, sempre que possível, alternativas ao uso da biometria, permitindo que o titular exerça sua escolha de forma consciente e informada (OP-966760, OP-1005679, OP-1005612).
- **Canais de Atendimento e contato com o Encarregado pelo tratamento de dados pessoais:** As contribuições ressaltam a necessidade de disponibilizar canais de comunicação que permitam aos titulares esclarecerem dúvidas e exercer seus direitos. Destacam, também, que a identificação do Encarregado pelo tratamento de dados pessoais e o respectivo canal de contato devem ser apresentados de forma clara e acessível. (OP-966032, OP-969104, OP-1003688).
- **Disponibilização de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD):**Contribuintes sugerem a publicação de versões simplificadas ou a disponibilização de *links* acessíveis para o Relatório de Impacto à Proteção de Dados Pessoais, especialmente em situações de alto risco ou no âmbito de políticas públicas, de modo a permitir que titulares e sociedade compreendam a análise de riscos envolvida (OP-1005260, OP994148, OP-1006256).

Pontos Divergentes:

6.12. As contribuições também apresentaram as seguintes divergências relevantes:

- **Práticas de transparência específicas em contraponto à possibilidade de**

eleição (flexibilidade e proporcionalidade): Algumas contribuições sugerem que a ANPD deveria estabelecer práticas específicas e padronizadas de transparência. A maioria, entretanto, entende que não existe uma metodologia única aplicável a todos os casos. Para essa visão, as práticas de transparência devem considerar fatores como a finalidade da coleta, a natureza do relacionamento com o titular e o tipo de dado sensível tratado, no caso, os dados biométricos. Nessa perspectiva, recomendam que as medidas sejam proporcionais ao porte da empresa, ao contexto do tratamento e aos riscos envolvidos, permitindo que cada controlador adote os meios mais adequados à sua realidade operacional, em vez da imposição de práticas fixas e taxativas (OP-1005635, dentre outras).

- **Nível de transparência aos detalhes técnicos (Taxas de Erro, Vieses) em contraponto à proteção de segredos de negócio e segurança operacional:** Os participantes divergem quanto ao nível de detalhamento a ser exigido. Parte defendeu a divulgação de informações técnicas sobre o desempenho da tecnologia, incluindo taxas de erro (falsos positivos e negativos) e riscos de vieses que possam afetar grupos vulneráveis. Outras contribuições alertam para a necessidade de equilibrar a transparência com a proteção de segredos comerciais e informações confidenciais. No contexto de segurança pública ou prevenção à fraude, destacou-se que a exposição excessiva de algoritmos ou bases de dados poderia comprometer investigações e a segurança dos sistemas, recomendando-se, nesses casos, a comunicação em termos gerais, sem revelar detalhes operacionais sensíveis (OP-969104, OP-979836, OP-1006120).
- **Transparência para o treinamento de algoritmos de Inteligência Artificial (IA):** Foram apresentadas posições diferentes sobre o uso de dados biométricos no treinamento de algoritmos de IA. Algumas contribuições defendem a exigência de um consentimento específico e separado, não incluído em termos de serviço genéricos. Também sugerem que os titulares sejam informados previamente sobre a impossibilidade de eliminação total dos dados já utilizados no treinamento, em razão das limitações do *machine unlearning* (técnicas que buscam "desaprender" informações já incorporadas a um modelo de inteligência artificial, mas que não garantem a exclusão completa dos dados pessoais coletados). Propôs-se, ainda, a criação de interfaces padronizadas de consentimento para evitar os chamados *dark patterns* (padrões de design que induzem ou manipulam o usuário a consentir sem plena consciência) (OP-996562, OP-997897).

6.13. De modo geral, as contribuições apontam convergência quanto à necessidade de avisos claros e acessíveis, políticas de privacidade específicas, canais de atendimento, consentimento informado, divulgação de relatórios de impacto e transparência sobre riscos e alternativas. Por outro lado, persistem divergências relevantes em temas como a definição de práticas de transparência ativa específicas ou flexíveis, o nível de detalhamento técnico a ser divulgado, e o uso de dados biométricos no treinamento de algoritmos de inteligência

artificial. Observou-se, assim, um núcleo de consenso em torno das práticas mínimas de transparência ativa, acompanhado por debates abertos em pontos sensíveis que ainda demandam maior amadurecimento regulatório.

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, face, íris)? Existem obrigações específicas que podem derivar dessas novas tecnologias, detidamente especial observância aos princípios de qualidade dos dados e da segurança?

6.14. As contribuições sobre esse questionamento apresentaram diferentes perspectivas quanto ao tratamento da biometria comportamental em comparação à biometria tradicional. Foram registradas manifestações de consenso em alguns aspectos centrais, bem como divergências relevantes sobre a extensão e as formas mais adequadas de aplicação prática.

Pontos Convergentes:

6.15. As contribuições sugerem os seguintes elementos comuns em relação a entendimentos convergentes:

- **Natureza sensível e proteção reforçada:** Existe um consenso de que tanto a biometria comportamental quanto a tradicional devem ser tratadas como dados pessoais sensíveis pela LGPD. Isso exige a adoção de salvaguardas jurídicas e técnicas mais rigorosas em todas as etapas do tratamento, assegurando um nível de proteção compatível com sua natureza (OP-1006162, OP-1005106).
- **Ênfase nos Princípios da Qualidade dos Dados e da Segurança:**Houve consenso sobre a necessidade de aplicar com rigor os princípios da qualidade dos dados no tratamento da biometria comportamental, assegurando a integridade e a confiabilidade das informações. Além disso, destacou-se a importância de serem adotadas medidas de segurança adequadas à essa natureza, fato que sugere a aplicação de medidas mais estritas. Porém, nas contribuições encaminhadas não foram identificadas menções a medidas específicas. As sugestões apontam para as medidas originárias da segurança da informação (OP-1006230, OP-1005901, OP-1005718).
- **Necessidade de Transparência e Consentimento Reforçado:** Houve consenso de que a biometria comportamental exige maior transparência e consentimento reforçado. Destacou-se que a coleta contínua, muitas vezes passiva ou imperceptível, gera a necessidade de informar claramente o titular sobre a coleta, a finalidade e as inferências possíveis no contexto da biometria comportamental, de modo a garantir a compreensão adequada antes da coleta (OP-1005901, OP-1005718, OP-1006230).

- **Recomendação de Relatório de Impacto à Proteção de Dados (RIPD):** As contribuições convergem quanto à importância da elaboração do RIPD em projetos que envolvem biometria comportamental, em razão da complexidade e dos riscos potenciais associados ao seu tratamento. Observa-se que, embora o Relatório também seja citado em outros blocos como medida administrativa de caráter geral, neste ponto ele é mencionado especificamente em relação à biometria comportamental, sem que tenham sido identificadas diferenças significativas em comparação às medidas aplicáveis à biometria tradicional (OP-1006162, OP-1006232).
- **Governança algorítmica e validação contínua:** Há consenso para a necessidade de mecanismos permanentes de validação, monitoramento de falsos positivos e negativos e auditorias regulares dos algoritmos de biometria comportamental. Ressalta-se também a importância de uma governança técnica estruturada, capaz de acompanhar a complexidade desses sistemas e garantir a consistência de seus resultados. (OP-1006297, OP-969154).
- **Riscos de Reidentificação, Perfilamento e Discriminação:** As contribuições convergem para a necessidade de atenção especial aos riscos de reidentificação, perfilamento e discriminação algorítmica no uso da biometria comportamental. Destacou-se a possibilidade de que esses dados permitam inferir características pessoais sensíveis e influenciem decisões automatizadas que possam afetar os titulares de maneira desigual (OP-999971, OP-1005627, OP-1002202).

Pontos Divergentes:

6.16. As contribuições também apresentaram divergências relevantes:

· **Diferenciação legal e obrigações específicas:** As contribuições divergem quanto à necessidade de estabelecer distinções específicas para a biometria comportamental. Algumas delas defendem o tratamento uniforme, ou seja, sem que haja distinção entre biometria tradicional e biometria comportamental, argumentando que a LGPD não prevê diferenciações entre tipos de biometria e que criar distinções em norma infralegal afrontaria o princípio da legalidade. Para esse grupo, a regulação deve se basear no risco e no contexto de uso, independentemente do tipo de biometria. Em contrapartida, outras contribuições sustentam que a biometria comportamental exige regras mais rigorosas de segurança, transparência e governança em relação à biometria tradicional, uma vez que geram riscos adicionais de erro e de invasividade. Há contribuições que relacionaram a biometria comportamental à categoria de "alto risco prevista no Ato Europeu de Inteligência Artificial (AI Act)" (OP-1006217, OP-969104, OP-1005673).

> "O Ato Europeu de Inteligência Artificial corresponde ao Regulamento (UE) 2024/1689, aprovado em junho de 2024 pela

> União Europeia. Trata-se do primeiro marco regulatório abrangente sobre inteligência artificial no continente, que classifica os sistemas de IA por níveis de risco e impõe requisitos mais rigorosos para aqueles considerados de alto risco, incluindo aplicações de identificação biométrica, categorização de pessoas e reconhecimento de emoções."

- **Definição de dado biométrico comportamental como dado sensível:** Para um grupo de participantes, a simples coleta de comportamentos não é suficiente para se classificar o dado comportamental como dado sensível, sendo necessário avaliar critérios objetivos, como a finalidade e o tratamento técnico voltado à identificação ou autenticação inequívoca. Nessa perspectiva, comportamentos voluntários, facilmente modificáveis ou utilizados apenas em análises agregadas sem intenção de individualização não configurariam biometria comportamental (OP-1005679). Por outro lado, algumas contribuições defendem que qualquer dado biométrico, quando utilizado para identificar uma pessoa, deve ser automaticamente considerado sensível, independentemente do contexto ou da técnica empregada (OP-1005106, OP-1005679, OP-1006221).
- **Contextos de uso e restrições setoriais:** Houve divergência quanto à possibilidade de utilização da biometria comportamental em determinados setores. Algumas contribuições defendem a restrição ou mesmo a proibição em contextos como educação, saúde, trabalho e segurança pública, bem como em aplicações associadas à inferência emocional ou ao controle de produtividade. Por outro lado, outra abordagem reconhece potencial em usos setoriais específicos, notadamente no setor financeiro, para prevenção de fraudes, e na área da saúde, para monitoramento clínico. Para esses casos, destacam a importância de adoção de medidas de transparência e controles rigorosos como forma de mitigação de riscos (OP-1006068, OP-969104, OP-1006232).

6.17. Permanecem divergências específicas quanto ao tratamento da biometria comportamental. O debate concentra-se na legalidade de estabelecer distinções regulatórias, na definição de critérios objetivos para sua caracterização como dado sensível e nas formas mais adequadas de gerir os riscos decorrentes de sua natureza dinâmica que proporciona a possibilidade de inferências e que, muitas vezes, não é perceptível.

BLOCO II - HIPÓTESES LEGAIS

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?

6.18. A LGPD impõe cuidados especiais no tratamento de dados

biométricos, exigindo que o consentimento seja livre, específico, destacado, informado e inequívoco. Contudo, em certos contextos, o consentimento pode não ser a hipótese legal mais adequada, sendo necessário recorrer a outras hipóteses previstas na lei. Essa questão procurou compreender a percepção dos agentes de tratamento referente ao tema.

Pontos Convergentes:

6.19. Dentre os elementos comuns identificados nas contribuições verificam-se as principais convergências:

- **Garantia para que o Consentimento para tratamento de dados biométricos seja livre, específico, destacado, informado e inequívoco:**
    - **Observância aos princípios de proteção de dados:** Há consenso de que a informação fornecida ao titular deve observar os princípios da LGDP no sentido de que haja transparência e clareza da informação, com detalhamento integral do tratamento e respectivos riscos, com consentimento especificado para cada finalidade de tratamento, através de uma ação afirmativa explícita e inequívoca do titular, sem pré-seleção, e não podendo ser presumido por omissão ou silêncio (OP-1006225, OP-1006256, OP-1006098, OP-967752, OP-1005635, OP-1005718, OP-1006225, OP-1006073, dentre outras).
- **Consentimento Informado, Específico e com Opção de Recusa (quando aplicável):** Houve consenso de que, quando o consentimento for utilizado como base legal, ele deve ser obtido de forma destacada, livre, específica e inequívoca. É necessário informar se a coleta é obrigatória ou facultativa, bem como as consequências da recusa. Ao titular deve ter assegurada a possibilidade de não fornecer os dados biométricos sem sofrer prejuízo indevido. O consentimento precisa ser registrado de forma segura e auditável (OP-1005104, OP-1005673, OP-1006155).
- **Contextos em que o consentimento não deve ser considerado uma hipótese legal:** Houve consenso de que, em determinadas situações, o consentimento não é uma hipótese legal adequada.
    - **Natureza do Consentimento e Assimetria de Poder:** Muitas manifestações consideram que o consentimento não é adequado quando há desequilíbrio de poder entre o titular e o controlador, situações em que a recusa implicaria prejuízo desproporcional ou impossibilidade de acesso (OP-100040, OP-967368, OP-1000400, dentre outras).
    - **Prevenção à fraude e segurança do titular:** O consentimento não deve ser considerado a hipótese legal adequada quando a coleta de dados biométricos decorre de necessidade legítima de segurança, como a prevenção de fraudes e a autenticação do usuário em cadastros bancários ou aplicações digitais. Nessas situações, a

finalidade do tratamento está diretamente vinculada à proteção do próprio titular e à garantia da integridade das operações, não se tratando de uma escolha facultativa, mas de uma exigência para assegurar confiabilidade e segurança. (OP-1005963, OP-1006052, OP-1006155, OP-1006217, dentre outras).

- **Obrigação legal ou regulatória:** O consentimento não deve ser considerado adequado quando a possibilidade de recusa pelo titular inviabilizaria o cumprimento de obrigação legal ou regulatória. Algumas contribuições argumentam que, nesses casos, não há manifestação verdadeiramente livre, pois o tratamento é condição indispensável para a prestação do serviço ou para atender exigências normativas, como ocorre em processos de autenticação destinados à prevenção de fraudes, como o acesso seguro a um aplicativo bancário ou a verificação de identidade exigida por lei. (OP-967368, OP-1005627, OP-1005963, OP-1006187, dentre outras).

Pontos Divergentes:

6.20. Por outro lado, as contribuições apresentaram as seguintes divergências relevantes:

- **Natureza do consentimento e assimetria de informações**: As respostas indicam entendimentos distintos sobre a validade do consentimento como base legal no tratamento de dados biométricos nessas situações. Parte reconheceu sua aplicação, mas destacou que, em relações jurídicas assimétricas, a presunção de livre escolha pode ser limitada, mencionando riscos de "fadiga" ou "ficção" do consentimento e reforçando que o silêncio do titular não pode ser interpretado como anuência. Outros observaram que, mesmo em processos de autenticação considerados tecnicamente seguros, não há garantia de que o consentimento seja efetivamente livre, apontando situações de indução fraudulenta e possíveis fraudes em sistemas de autenticação facial (OP-968762, OP-1005260, OP-1005673, OP-1004895).
- **Hierarquia entre bases legais:** Muitos contribuintes avaliam que não há hierarquia entre as hipóteses legais, ou seja, qualquer hipótese pode legitimar o tratamento de dados pessoais sensíveis, ao passo que há quem defenda que o consentimento deve ser privilegiado em detrimento das demais pela natureza sensível e invasiva dos dados biométricos (OP-100510, OP-1005901, OP-1006211, dentre outras).
- **Influência de compensação financeira/incentivos:** Algumas manifestações consideram que os incentivos podem afetar a avaliação dos riscos, comprometendo a plena liberdade do titular, enquanto outras compreendem que não há invalidação, desde que a voluntariedade da decisão seja preservada (OP-1005635, OP-100510, OP-977469, OP-1006256, dentre outras).

- **Atuação da ANPD**: Algumas contribuições consideram que a ANPD deve reconhecer as nuances do consentimento livre na economia digital, evitando abordagens restritivas, apenas detalhando as diretrizes de uso legítimo. Outros entendem que a ANPD deve declarar explicitamente a inadequação do consentimento em contextos específicos e exigir avaliação de impacto e alternativas menos invasivas (Claro, OP-1005679, OP-977469, OP-969104, dentre outras).

6.21. Embora o consentimento represente um pilar fundamental para o tratamento de dados pessoais sob a LGPD, sua validade depende da observância rigorosa de requisitos como liberdade, clareza e especificidade. Nesse sentido, há convergências quanto à observância aos requisitos e princípios, inclusive quanto à sua inaplicabilidade em situações que o consentimento não seria a hipótese legal mais adequada, como, por exemplo, o cumprimento de obrigações legais ou finalidades ligadas à segurança e prevenção de fraudes. Contudo, há divergências quanto à adequação do consentimento em situações de assimetria de informações; à existência de hierarquia do consentimento em relação às demais hipóteses; à influência de compensação financeira ou incentivos na validade do consentimento; e ao papel da ANPD em relação ao reconhecimento do consentimento em contextos específicos.

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?

6.22. A utilização de dados biométricos envolve desafios quanto à aplicação da hipótese legal de prevenção à fraude. Dada a natureza sensível desses dados e o seu potencial impacto sobre as liberdades e os direitos fundamentais, torna-se indispensável refletir sobre os critérios de aplicação dessa hipótese legal, a compatibilização com o princípio da necessidade e as salvaguardas adequadas para reduzir risco.

Pontos de Convergência:

6.23. Dentre os elementos comuns identificados nas contribuições verificam-se as principais convergências:

- **Critério a ser observado para a adequada aplicação da hipótese legal de garantia da prevenção à fraude no tratamento de dados biométricos:**
    - **Observância dos princípios de proteção de dados:** Há um consenso de que o tratamento de dados biométricos deve ser transparente,

com uso estritamente necessário e proporcional ao risco de fraude, para finalidade específicas e legítimas, e não a propósitos genéricos, evitando o excesso e limitando a coleta ao mínimo indispensável (OP-1005713, OP-100623, OP-1005982, OP-1003688, OP-979836, OP-1004793, OP-1006256, OP-1005673, OP-969282, OP-966032, OP-1006217, dentre outras).

- **Compatibilização entre 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.**
    - **Comprovação de risco concreto:** O controlador deve demonstrar, por análise de risco, a existência de ameaças significativas que justifiquem o uso da biometria em relação ao risco identificado e seu impacto na segurança. (OP-100561, OP-969104, OP-1005725, dentre outras).
    - **Relatório de Impacto a Proteção de Dados (RIPD):** É recomendado que se realize um RIPD previamente para documentar riscos, justificar o uso da biometria, mapear possíveis vieses e definir medidas de mitigação eficazes (OP-966029, OP-994148, OP-1002117, OP-1003688, dentre outras).
    - **Exigência de alternativas menos invasivas**: Uma corrente significativa defende que o uso da biometria só se justifica se não houver meios alternativos e menos invasivos que atinjam a mesma finalidade de forma satisfatória, exigindo a prova da indispensabilidade da biometria (OP-966029, OP-1002202, OP-1003891, OP-1006256, dentre outras).
- **Salvaguardas que podem ser implementadas para mitigar os riscos às liberdades e aos direitos fundamentais:**
    - **Biometria como mecanismo mais seguro:** Muitos contribuintes apontam que a tecnologia biométrica oferece maior certeza na verificação de identidade e é comprovadamente mais segura que outros métodos (como senhas ou documentos de posse), sendo essencial para proteger usuários e o sistema financeiro contra fraudes sofisticadas e indispensável para autenticação (OP-1003688, OP-1006132, OP-1005679, OP-100623, OP-1006225, OP-1006297, OP-1005718, dentre outras).
    - **Medidas técnicas fortes:** A implementação de criptografia forte, pseudonimização/anonimização, biometria temporária ou transformada em *hash* irreversível, autenticação multifator, segregação de dados, e controles de acesso rigorosos, uso de tecnologias de privacidade, armazenamento local (*on-device)*, Referências Biométricas Renováveis, *templates* biométricos (em vez de imagens brutas), registros detalhados de *"logs"* de todas as operações de tratamento, monitoramento contínuo do ambiente em

busca de vulnerabilidade e realização periódicas de auditorias são salvaguardas amplamente citadas como essenciais (OP-994148, OP-1003891, OP-967368, OP-1003688, OP-1003891, OP-1006162, OP-968689, OP-966032, OP-966029, OP-1006198, OP-1006297, OP-96915, OP-977469, OP-969154, OP-1005625, OP-1005260, OP-1006217, OP-1005673, dentre outras).

Pontos divergentes:

6.24. Por outro lado, as contribuições apresentaram as seguintes dissonâncias relevantes:

- **Aplicação de Teste de Balanceamento:** Algumas contribuições afirmam que a realização prévia do Teste de Balanceamento não é uma medida legalmente obrigatória para a licitude da atividade ao passo que outros indicam que é fundamental demonstrar a necessidade (OP-1005635, OP-1006225, OP-1006256, dentre outras).
- **Abrangência da Hipótese Legal:** Enquanto uns argumentos sugerem que a interpretação deve ser ampla, outros, por sua vez, alertam que a hipótese legal não pode ser um "cheque em branco" ou um pretexto genérico para coleta biométrica indiscriminada (OP-1005679, OP-1002202, OP-969104, OP-1006256, dentre outras).
- **Exigência de alternativas não biométricas:** Muitas contribuições afirmam que a biometria é a solução mais segura, enquanto outras destacam que é indispensável prever alternativas não biométricas. (OP-1003688, OP-1006211, OP-1004895, OP-1006297).
- **Dados financeiros como dados sensíveis:** No contexto da hipótese legal de "garantia de prevenção à fraude" (art. 11, II, "g", da LGPD), uma contribuição propõe a inclusão dos dados financeiros no rol de dados sensíveis, com o objetivo de conferir maior clareza quanto à sua aplicabilidade. Essa proposta busca assegurar a identificação plena do titular e reforçar a proteção tanto do indivíduo quanto das instituições envolvidas. (OP-950124).

6.25. Há convergência quanto à necessidade de observância dos princípios de proteção de dados. Nesse sentido, a aplicação da hipótese legal de prevenção à fraude no tratamento de dados biométricos deve observar a necessidade, a proporcionalidade e a finalidade legítima, utilizando tais dados apenas quando indispensáveis. Além disso, há consenso sobre a adoção de salvaguardas fortes. Embora também haja consenso sobre a segurança trazida pela biometria na verificação de identidade, contribuintes discordam sobre a necessidade de aplicação de testes de balanceamento, a abrangência dessa hipótese legal, a exigência de alternativas não biométricas e a classificação de dados financeiros como sensíveis.

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?

6.26. O tratamento de dados biométricos para o cumprimento de obrigações legais o regulatórias exige que órgãos e entidades públicas adotem critérios claros e salvaguardas adequadas, garantindo a proteção dos titulares e a mitigação de riscos.

Pontos Convergentes:

6.27. Dentre os elementos comuns identificados nas contribuições verificam-se as principais convergências:

- **Observância dos princípios da LGPD:** Há um consenso de que, mesmo amparado por uma obrigação legal, o tratamento de dados biométricos deve rigorosamente observar os princípios da LGPD, especialmente os da necessidade, finalidade e proporcionalidade, garantindo transparência ativa, fornecendo informações claras, precisas, acessíveis e destacadas aos titulares sobre a finalidade, a base legal, a obrigatoriedade do tratamento, como seus dados serão usados, prazos de retenção, armazenamento, medidas de segurança, compartilhamento e como exercer seus direitos (OP-969282, OP-1003891, OP-1006217, OP-968762, OP-1006220, dentre outras).
- **Previsão legal ou normativa expressa e específica:** Muitas manifestações consideram que o tratamento de dados biométricos deve ser fundamentado em uma norma legal ou regulatória expressa, clara, específica e válida. A mera generalidade normativa, diretrizes amplas ou objetivos de modernização tecnológica não são suficientes para justificar o uso massivo de dados sensíveis ou tecnologias invasivas (OP-969104, OP-966032, dentre outras).
- **Medidas técnicas e de Governança:** A implementação de medidas técnicas e administrativas eficazes e adequadas aos riscos é crucial para a segurança de dados sensíveis, tais como, criptografia, controle de acesso, rastreamento das operações realizadas, limitação de retenção e descarte seguro dos dados. Com relação a salvaguardas específicas, identificou-se a citação dos padrões técnicos internacionais, como as ISO/IEC JTC 1/SC 37 e ISO/IEC 24745:2022 (OP-967368, OP-1005718, OP-1006217, OP-1005080, dentro outros).
- **Foco Aprimorado em Órgãos Públicos:** A atuação pública deve ser ética, segura e alinhada à legalidade, proporcionalidade e aos valores constitucionais, como dignidade, autodeterminação informativa e intimidade (OP-1006049, OP-100562, OP-1002202, dentre outras).

Pontos divergentes:

6.28. Por outro lado, as contribuições apresentaram poucas dissonâncias relevantes:

- **Conceito de obrigação legal**: Alguns argumentam que a hipótese legal de obrigação legal ou regulatória se aplica apenas quando a lei ou regulamento expressamente exigir a coleta de dados biométricos e, ainda assim, de forma excepcional. Por outro lado, há manifestações que entendem que essa hipótese pode ser utilizada como meio legítimo de conformidade mesmo sem previsão específica. Parte das manifestações, portanto, considera que sua aplicação deve ocorrer apenas em casos em que a lei ou regulamento imponham de forma clara a coleta, enquanto outras a reconhecem como fundamento mais amplo de legitimidade. (OP-1006232, OP-1006297, dentre outras).

6.29. De modo geral, houve consenso de que tratamento de dados biométricos para fins legais ou regulatórios deve apoiar-se em previsão normativa expressa, observar os princípios da LGPD e adotar salvaguardas para garantir a proteção dos titulares e a proporcionalidade da atuação dos órgãos públicos.

Pergunta 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?

6.30. O tratamento de dados biométricos para pesquisa exige cuidados especiais, mesmo com anonimização, devido ao risco de reidentificação. A questão teve por objetivo identificar e compreender quais são os limites que o tratamento de dados biométricos deve respeitar quando da utilização desses dados, ainda que anonimizados, para a realização de estudos e pesquisas e, também, se há necessidade de salvaguarda adicionais e, se sim, quais.

Pontos Convergentes:

6.31. Dentre os elementos que convergem quanto os critérios objetivos estão os seguintes:

- **Limites do tratamento de dados biométricos para a realização de estudos por órgãos de pesquisa, mesmo nos casos em que há a anonimização dos dados, considerando o cruzamento de bases de dados e a eventual possibilidade de reidentificação posterior:**
    - **Observância aos princípios da LGPD:** Há consenso de que os princípios da LGPD devem ser observados, sobretudo o **princípio da**

minimização, ou seja, coletar e usar apenas os dados estritamente necessários para o objetivo da pesquisa, e da **transparência,** que pressupõe que seja completa e acessível, sobretudo, quanto aos objetivos do estudo e metodologia da pesquisa. Mencionam, também, a necessidade de códigos de conduta e ética em pesquisa e, por fim, a descrição das formas de eliminação ou descarte seguro dos dados biométricos ao final do ciclo de estudo (OP-1006230, OP-1005080, OP-1005260, OP-1005080, OP-1005673, OP-977469, OP-1005080, OP-1005673, OP-97746, OP-1005260, OP-1005718, OP-1006211, OP-1006220, dentre outras).

- **Alto Risco de reidentificação:** Há consenso generalizado de que, mesmo com a anonimização, dados biométricos carregam um risco significativo de reidentificação, especialmente devido ao cruzamento de bases de dados e ao avanço tecnológico, exigindo salvaguardas adicionais, porém não foram identificadas menções explícitas a técnicas específicas, sendo sugeridas as medidas técnicas costumeiramente aplicadas à biometria tradicional advindas do campo da segurança da informação. (OP-1003891, OP-1006232OP-968762, OP-969104, OP-1005625, dentre outras).

- **Salvaguardas adicionais seriam eventualmente necessárias a fim de resguardar os direitos dos titulares:**
  - **Finalidade Exclusiva para Pesquisa:** É amplamente aceito que o tratamento de dados biométricos deve ter finalidade exclusivamente científica, acadêmica, histórica ou estatística, de interesse público, com proibição explícita de fins comerciais, promocionais ou de controle individual, aplicando salvaguardas e uso em ambientes controlados (OP-967752, OP-1002202, OP-1003891, OP-1005718, dentre outras).
  - **Obrigatoriedade de Avalição de Impacto:** Muitas contribuições apontam necessidade de avaliações prévias de impacto do tratamento dos dados biométricos (OP-967752, OP-977469, OP-1002202, OP-1003688, dentre outras).
  - **Controle Rigoroso de Acesso:** A restrição de acesso aos dados a pesquisadores autorizados e qualificados, sujeitos a confidencialidade, bem como a segregação de bases de dados são salvaguardas essenciais mencionadas por diversos contribuintes (OP-1003891, OP-1005080, OP-968689, OP-968762, dentre outras).

<u>Pontos Divergentes:</u>

6.32. Por outro lado, as contribuições apresentaram poucas dissonâncias relevantes:

- **Obrigatoriedade da anonimização:** Muitos contribuintes enfatizam que a

anonimização deve ser feita para descaracterizar o dado como pessoal e reduzir riscos. Alguns, no entanto, afirmam que a anonimização não é obrigatória e dependerá do tipo de metodologia de pesquisa e da base de dados (OP-1006049, OP-1006110, OP-1006155, OP-1006198, dentre outras).

- **Necessidade de consentimento:** Algumas manifestações entendem que o tratamento de dados biométricos para pesquisa pode ser feito sem o consentimento, desde que respeitados os princípios legais e com as devidas salvaguardas, outros defendem que o consentimento é obrigatório (OP-969488, OP-977469, OP-996562, OP-1005625, dentre outras).
- **Restrição específica para grupos vulneráveis:** As manifestações apresentaram entendimentos distintos sobre a coleta e o uso de dados biométricos de menores de 18 anos e indivíduos em situação de vulnerabilidade social, econômica ou cultural, como comunidades indígenas e quilombolas. Parte dos contribuintes defende restrições mais rígidas, chegando a propor a limitação ou até mesmo a proibição do tratamento nesses casos, salvo quando houver previsão legal específica e salvaguardas excepcionais que justifiquem a prática. Outros, porém, não apoiam uma vedação absoluta, mas ressaltam a necessidade de aplicar salvaguardas gerais consistentes a todos os titulares, garantindo também a proteção desses grupos, sem criar regras exclusivas ou restritivas (OP-969104, OP-945269, OP-1006232, OP-1005718).
- **Definição jurídica de "órgãos de pesquisa":** Uma contribuição alerta para a necessidade de definir juridicamente à luz da LGPD o conceito de "órgãos de pesquisa" a fim de excluir a possibilidade de acesso, por empresas privadas com interesses comerciais, aos dados biométricos obtidos em razão dessa hipótese legal de modo a evitar dúvidas sobre usos secundários (OP-969154).

6.33. Há consenso sobre a necessidade de que o tratamento de dados biométricos por órgãos de pesquisa, mesmo quando submetido a processos de anonimização, deve observar limites rigorosos, considerando o risco inerente de reidentificação e a sensibilidade dessa categoria de dados, devendo ser aplicadas as devidas salvaguardas. No entanto, os contribuintes discordam sobre a obrigatoriedade de anonimização, a necessidade de obter consentimento e sobre haver uma restrição específica para determinados públicos. Além disso, aponta-se a necessidade de definição jurídica da expressão "órgãos de pesquisa".

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

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?

6.34. As contribuições apresentaram diferentes perspectivas sobre o uso de Tecnologias de Reconhecimento Facial (TRF) no âmbito da LGPD. Observou-se consenso quanto à necessidade de salvaguardas técnicas, jurídicas e institucionais, mas também divergências quanto ao grau de transparência exigido, às soluções técnicas propostas, à aplicação em segurança pública e aos critérios de classificação de risco a serem definidos pela ANPD.

Pontos convergentes:

6.35. Dentre os elementos que convergem quanto os critérios objetivos estão os seguintes:

- **Necessidade e proporcionalidade:** As contribuições convergem que o uso das TRFs deve se restringir ao estritamente necessário, com coleta mínima de dados, por período determinado e apenas para a finalidade declarada. Destaca-se, ainda, que a conveniência operacional inerente ao modelo de negócio não justifica seu uso, sendo essencial demonstrar a inexistência de alternativas menos invasivas e assegurar tratamento adequado, proporcional e devidamente fundamentado (OP-1003688, OP-967368, OP-977469).
- **Transparência:** As manifestações convergem quanto à necessidade de garantir transparência no uso das TRFs. Há também consenso sobre a relevância do Relatório de Impacto à Proteção de Dados Pessoais como instrumento essencial de transparência no contexto da TRF, devendo ser elaborado em linguagem acessível e disponibilizado ao público. Além disso, enfatiza-se a necessidade de canais de comunicação eficazes que possibilitem ao titular exercer seus direitos, questionar decisões automatizadas e relatar situações de uso indevido ou discriminatório (OP-967368, OP-1006212, OP-966032, OP-969104).
- **Relatório de Impacto à Proteção de Dados:** A realização de Relatório de Impacto à Proteção de Dados é uma salvaguarda essencial e frequentemente recomendada ou exigida, especialmente para tecnologias invasivas como reconhecimento facial, em espaços públicos e em casos de risco relevante ou elevado (OP-967368, OP-1003688, OP-1004793, OP-1006162, dentre outras).
- **Prevenção de discriminação ilícita ou abusiva:** As contribuições convergem quanto à necessidade de prevenir discriminação no uso das TRFs, destacando o treinamento de algoritmos com bases diversificadas e representativas para reduzir vieses. Há consenso sobre a realização de testes de viés e auditorias independentes, bem como sobre a importância da revisão humana das decisões automatizadas. (OP-1005718, OP-968529, OP-1004811).

- **Salvaguardas técnicas específicas aplicadas às TRFs:** Há consenso quanto à necessidade de adotar salvaguardas no tratamento de dados biométricos. Usualmente, as contribuições sugerem a adoção de medidas originárias do campo da segurança da informação como, por exemplo, criptografia, anonimização, controle de acesso, entre outras. Especificamente para as TRFs, algumas contribuições mencionam as seguintes:
    - **Detecção de Vivacidade (*Liveness Detection*)**: Tecnologia de segurança biométrica capaz de verificar se uma pessoa está viva e fisicamente presente durante uma autenticação que utilize seus dados biométricos, prevenindo, assim, fraudes por falsificação, como o uso de fotos, vídeos ou máscaras (OP-1006155 e OP-1005612). Em menor grau, há quem defenda que uso dessa ferramenta deve ser obrigatório para garantir a presença do titular do dado biométrico quando da sua autenticação (OP-1005612)
    - **Mecanismos *anti-spoofing:*** Aplicação de técnicas capazes de detectar tentativas de fraude por fotos, vídeos ou impressões digitais artificiais, aliadas à prova de vida (OP-1006132, OP-1006220).
- **Salvaguardas jurídicas aplicadas às TRFs:** As contribuições convergem ao destacarem a necessidade quanto à correta definição da hipótese legal prevista na LGPD e a necessidade de observância de legislações antidiscriminatórias, em complemento à LGPD, para prevenir práticas discriminatórias. (OP-966032, OP-1005718, OP-968762).
- **Salvaguardas institucionais aplicadas às TRFs:** Houve convergência quanto à necessidade do estabelecimento de mecanismos de governança, com a criação de comitês multidisciplinares, com o objetivo de promover o uso ético e responsável das TRFs (OP-1004811, OP-1005679, OP-966032, OP-1006158).

Pontos Divergentes:

6.36. As contribuições também apresentam as seguintes divergências relevantes:

- **Nível de transparência:** As contribuições apresentam entendimentos distintos. Em contextos nos quais a TRF já é amplamente utilizada, como no setor de telecomunicações e financeiro, alguns consideram suficientes os avisos de privacidade disponibilizados no ponto de coleta. Por outro lado, há manifestações que defendem a adequação da transparência ao local de uso, destacando, no caso de espaços públicos, a necessidade de sinalização visível e acessível, além de posições que sugerem ampliar o escopo da transparência, com acesso público a informações sobre contratos, finalidades, softwares e hardwares empregados. (OP-1006297, OP-1006211, OP-969154, OP-1006120).
- **Referências Biométricas Renováveis – RBRs:** As contribuições indicam que

as RBRs, embora sejam um tipo de TRF, aparecem em dois contextos distintos. De um lado, são apresentadas como elemento que redefine a própria caracterização de dados biométricos, pois, ao introduzir propriedades como irreversibilidade e revogabilidade, reduzem os riscos associados ao dado original, o que leva parte dos participantes a questionar sua classificação automática como dado sensível. De outro lado, são citadas como medida de segurança específica aplicada às TRFs, especialmente por seguirem o princípio do *privacy by design* e possibilitarem o uso de criptografia avançada, garantindo que a representação biométrica não seja revertida sem a chave de desencriptação adequada (OP-969154 e OP-1006098);

6.37. De forma geral, observa-se que, embora exista ampla convergência quanto à necessidade de salvaguardas eficazes para garantir o uso responsável das TRFs, permanecem divergências relevantes sobre o grau de transparência exigido, a adoção de soluções técnicas específicas, os limites para sua aplicação em segurança pública e espaços públicos e os critérios de classificação de risco a serem adotados pela ANPD. Esses pontos representam os principais desafios identificados nas contribuições, indicando a importância de que eventuais parâmetros regulatórios considerem, de forma equilibrada, a proteção de direitos fundamentais, a segurança jurídica e os impactos sobre a inovação tecnológica.

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?

6.38. A questão trata de como os sistemas de reconhecimento facial devem ser projetados para garantir eficácia e confiabilidade com o objetivo de evitar erros de identificação e possibilitar a correção de falhas. As manifestações indicam consenso quanto à necessidade de incorporar salvaguardas técnicas e organizacionais desde a concepção *(privacy by design),* ao mesmo tempo em que revelam divergências sobre o alcance da LGPD, a aplicação em espaços públicos e a utilização de alternativas tecnológicas.

Pontos Convergentes:

- ***Privacy by Design*:** As análises apontam convergência quanto à necessidade de que os sistemas de reconhecimento facial sejam desenvolvidos, por padrão e desde a sua concepção, observando as medidas de segurança, técnicas e administrativas conforme dispõe o art. 46, § 2º, da LGPD. Ressalta-se a importância de que tais práticas assegurem precisão, proteção e mitigação de riscos, sendo igualmente necessário que

o controlador mantenha evidências documentadas da adoção do *Privacy by Design* desde a fase do projeto da solução até a sua execução (OP-963578, OP-1000400, OP-1006098).

- **Bases de Dados diversificadas e representativas:** As contribuições convergem quanto à necessidade de que os algoritmos embarcados nas TRFs sejam treinados com bases de dados amplas, diversificadas e representativas da população no contexto de aplicação. Essa diversidade deve contemplar variáveis demográficas, como etnia, gênero e idade, bem como diferentes condições de iluminação e ângulos de captura. (OP-965486, OP-1003688, OP-1005718).
- **Testes rigorosos e validação Contínua:** As contribuições convergem quanto à necessidade de que os sistemas de reconhecimento facial sejam submetidos a testes rigorosos antes da implementação, com validação da precisão a partir de bases de dados diversificadas e simulações de cenários reais para assegurar maior eficácia. Após a implantação, ressalta-se a importância da realização de validações periódicas e contínuas, contemplando métricas de erro, além da aferição da acurácia por diferentes grupos demográficos (OP-1002117, OP-1003891, OP-1002202).
- **Monitoramento contínuo e auditorias:** Há convergência quanto à necessidade de monitorar continuamente o desempenho dos sistemas de reconhecimento facial, utilizando recursos como alertas automáticos e relatórios periódicos capazes de identificar anomalias e padrões de erro em tempo real. Destaca-se também a importância da realização de auditorias regulares, internas e independentes, como instrumento para assegurar conformidade com normas de segurança e privacidade, detectar vieses e promover melhorias contínuas (OP-967368, OP-1002202, OP-977469).
- **Mecanismos de *feedback* e revisão humana:** Há consenso quanto à necessidade de incorporar mecanismos de *feedback* contínuo, aliados à revisão humana em situações de baixa confiança estatística, decisões críticas ou falhas no processo automatizado. Ressalta-se que essa revisão deve ser tempestiva, efetiva e acessível, realizada por pessoa qualificada e com autoridade para alterar ou corrigir a decisão automatizada (OP-963578, OP-999971, OP-1005673).
- **Canais acessíveis de contestação e correção de falhas:** As contribuições indicam alinhamento quanto à necessidade de disponibilizar canais acessíveis e eficazes para que os titulares possam contestar resultados provenientes do uso das TRFs, solicitar revisão humana e corrigir dados pessoais. Destaca-se também a importância do registro detalhado da rastreabilidade das decisões, de modo a possibilitar auditoria e garantir mecanismos de responsabilização (OP-968689, OP-969104.
- **Transparência, explicabilidade e governança:** As contribuições convergem quanto à necessidade de assegurar transparência em contextos que

envolvam as TRFs de forma a garantir que os usos da tecnologia e as decisões automatizadas a ela associadas sejam rastreáveis e acompanhadas de justificativas claras e compreensíveis. Ressalta-se, ainda, a importância do estabelecimento de mecanismos de governança específicos para sistemas de IA que se utilizem das TRFs, contemplando a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) e a adoção de referenciais internacionais, como o NIST AI Risk Management Framework (*National Institute of Standards and Technology – EUA*), as normas ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*) e as diretrizes do IEEE (*Institute of Electrical and Electronics Engineers*) (OP-968689, OP-1004793, OP-1005104).

Pontos divergentes:

6.39. As contribuições também apresentam as seguintes divergências relevantes:

- **Ponderação entre erros toleráveis e dano real:** Há divergência quanto à forma de lidar com os erros nos sistemas de reconhecimento facial. Algumas contribuições sugerem que o erro técnico não pode ser considerado uma "falha tolerável", mas sim um dano real aos direitos fundamentais, de modo que a ausência de controles rigorosos configura violação direta aos princípios da LGPD. Em sentido diverso, outras manifestações reconhecem que não é possível eliminar integralmente os erros, defendendo a necessidade de equilibrar critérios como precisão, *recall*, equidade, discriminação e necessidade (OP-969104, OP-1006110, OP-1005627).
- **Alternativas às TRFs:** As contribuições divergem quanto à centralidade do uso da TRF. Enquanto a maior parte das manifestações se concentra em propor melhorias para a biometria facial, algumas respostas sugerem alternativas menos invasivas ou complementares, como autenticação multifator (senhas, tokens ou biometria de menor impacto, como impressões digitais), biometria comportamental, cartões inteligentes ou QR Codes dinâmicos. (OP-1005625, OP-1006232, OP-999971).
- **Regulação do uso de dados biométricos anonimizados para eficácia e redução de vieses em TRFs:** As respostas apresentam divergência quanto ao papel dos dados biométricos não identificáveis no aprimoramento das TRFs. Uma manifestação destaca que o processamento de dados anonimizados, por não serem considerados dados pessoais à luz da LGPD, é fundamental para melhorar a eficácia dos sistemas e reduzir vieses, propondo que a ANPD reconheça expressamente essa premissa para oferecer maior segurança jurídica ao desenvolvimento tecnológico (OP-1005679, OP-1006220).

6.40. Em geral, as manifestações evidenciam a importância de estruturar

as TRFs com salvaguardas a serem adotadas desde a concepção *(privacy by design),* assegurando maior precisão, confiabilidade e transparência. Ao mesmo tempo, permanecem divergências quanto à aplicabilidade da LGPD em contextos de segurança pública, no uso em espaços públicos, à aceitação de erros técnicos e à adoção de alternativas menos invasivas. Esses pontos demonstram que, embora haja avanços em torno de práticas comuns, o debate regulatório ainda exige definições claras capazes de equilibrar inovação tecnológica, segurança jurídica e a proteção dos direitos fundamentais.

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?

6.41. Com base nas contribuições recebidas, identificam-se pontos de convergência e divergência sobre os contextos em que a utilização das TRFs não é recomendada, as justificativas associadas e as tecnologias alternativas que podem ser utilizadas. De forma geral, os participantes apontam situações específicas de não adoção das TRFs, os motivos que sustentam essa posição e as soluções alternativas de modo a preservar a eficácia e com menor impacto sobre a proteção de dados pessoais.

Pontos Convergentes:

6.42. Dentre os elementos comuns identificados nas contribuições, verificam-se entendimentos convergentes quanto a:

- **Aplicação das TRFs em contextos de ambientes educacionais:** As manifestações convergem quanto à inadequação do uso das TRFs em escolas, especialmente para controle de frequência. Destaca-se a vulnerabilidade de crianças e adolescentes, que estão mais suscetíveis a riscos e práticas discriminatórias (OP-967752, OP-968529, OP-969104, OP-1004811).
- **Aplicação das TRFs em contextos de saúde:** As contribuições indicam consenso ao apontar que locais de tratamento médico e hospitais são ambientes sensíveis, nos quais o uso da TRFs é considerado inadequado, salvo exceções legais fundamentadas e controladas previamente pela autoridade de proteção de dados (OP-1005673, OP-1004811, OP-1004811).
- **Vigilância massiva e indiscriminada:** Verifica-se convergência quanto à necessidade de atenção especial ao uso das TRFs para que não se configure contextos de vigilância em massa com a utilização de forma indiscriminada. São citados cenários como estações de transporte, eventos de grande porte, vias públicas, centros comerciais e estádios, nos quais o

risco de monitoramento permanente e abrangente é mais evidente (OP-967368, OP-969104).

- **Ausência de necessidade real e proporcionalidade:** Há convergência quanto ao entendimento de que a tecnologia de reconhecimento facial não deve ser utilizada sem uma necessidade específica e uma justificativa clara e proporcional, sobretudo quando o mesmo objetivo pode ser alcançado por meios menos intrusivos. Essa vedação inclui usos atualmente considerados triviais, como programas de pontos, descontos em supermercados ou controle de acesso em academias e condomínios (OP-966029, OP-950124, OP-963578, OP-1006098).
- **Processos com alto risco de erro, viés ou discriminação:** As contribuições convergem no sentido de que as TRFs não são adequadas para serem utilizadas em processos seletivos, análises de crédito, policiamento preditivo ou reconhecimento de emoções, devido ao risco de reprodução de vieses algorítmicos e decisões discriminatórias. Destaca-se a preocupação com a maior incidência de erros em grupos que possam estar sub-representados nas bases de dados biométricos. (OP-1005612, OP-1005713, OP-1005718).

Pontos divergentes:

6.43. As contribuições também apresentaram divergências relevantes:

- **Proibições absolutas vs. avaliação contextual:** As manifestações divergem quanto à adoção das TRFs. Uma parte defende a proibição total em determinados contextos, como escolas e hospitais, ou o banimento do uso em tempo real em espaços públicos e semiabertos, citando como referência o *AI Act* da União Europeia e recomendações de autoridades de proteção de dados, como o EDPB e a ANPD. Em contrapartida, outra parte argumenta que não devem existir proibições genéricas, sustentando que a avaliação do uso das TRFs deve ser feita caso a caso, com base em critérios como viabilidade técnica, eficácia, riscos envolvidos e, sobretudo, no contexto da aplicação, em conformidade com os princípios da LGPD, incluindo necessidade, minimização e não discriminação. (OP-1006198, OP-969154, OP-1004811, OP-969104).
- **Aplicação das TRFs no Setor Financeiro contra Fraudes:**As manifestações divergem quanto ao papel das TRFs no setor financeiro. Parte dos participantes, especialmente representantes desse segmento, afirmam que as TRFs são indispensáveis, pois funcionam como barreira antifraude, por serem capazes de cruzarem variáveis dinâmicas que outras soluções não possuem. Já outras manifestações, embora reconheçam sua relevância na prevenção a fraudes, sustentam que alternativas menos invasivas devem ser consideradas, sobretudo quando a finalidade de segurança não justifica limitar direitos e liberdades fundamentais dos titulares (OP-

1006132, OP-1005635, OP-1005901).

- **Aplicação das TRFs em contextos de Segurança Pública:**As contribuições divergem quanto à possibilidade ou não de utilização das TRFs:
    - **TRFs mediante lei específica:** Algumas contribuições sustentam que a atividade de segurança pública está excluída do escopo da Lei Geral, conforme o art. 4º, III, "a", devendo, portanto, observar regime próprio em que o consentimento não se aplica, prevalecendo o interesse público. Nesse sentido, o tratamento de dados biométricos e, por consequência, a utilização de qualquer tecnologia deve ser disciplinada por lei específica que estabeleça critérios adequados e proporcionais ao risco da atividade, justamente para evitar a ocorrência de discriminação, vieses e falsos positivos. Em havendo lei específica, há, ainda, quem compreenda pela necessidade de autorização judicial prévia para o tratamento de dados biométricos em investigações mais invasivas e pela necessidade desse tratamento ser acompanhado de avaliações de impacto sobre direitos fundamentais, de caráter obrigatório e público. Seria necessário, também, desenvolver mecanismos que impeçam a atuação autônoma de entes privados e garantir fiscalização rigorosa da ANPD. Por fim, há a proposta de vedação do uso de reconhecimento facial em tempo real para fins de segurança pública, admitindo-se apenas a análise retrospectiva sob condições estritas. (OP-1006120, OP-1006120, OP-1002202, OP-1005705).
    - **TRFs com base na LGPD:**Em sentido contrário, outras manifestações entendem pela aplicabilidade da LGPD em qualquer contexto, incluindo a segurança pública e, portanto, a utilização das TRFs deve observar os princípios da Lei Geral. Desse modo, em situações específicas, a utilização das TRFs pode ser essencial para identificar foragidos, localizar desaparecidos ou prevenir crimes em áreas críticas, desde que empregada com finalidade legítima e com proporcionalidade. (OP-969154, OP-1006256).
- **Aplicação das TRFs em espaços públicos:**As contribuições apresentam posições divergentes sobre a utilização da TRF em espaços públicos. Parte defende que seja classificada como atividade de alto risco, exigindo auditorias prévias e independentes, isentas de vieses e dotadas de acurácia, cabendo ao controlador comprovar a conformidade, em linha com o *AI Act* da União Europeia. Também há propostas no sentido de que, em âmbito nacional, o tema seja disciplinado por lei específica. Por outro lado, alguns participantes sustentam a proibição ou restrição, apontando riscos como vigilância indiscriminada, violação da presunção de inocência e dificuldades para garantir proporcionalidade. Outros não propõem vedação, mas defendem ajustes ao contexto urbano e de segurança pública, além da possibilidade de correções posteriores em casos de falsos positivos. Sugere-se, ainda, a criação de um *sandbox* regulatório para

permitir testes controlados e aperfeiçoamento da tecnologia sob supervisão da ANPD (OP-979836, OP-996562, OP-997897, OP-969104, OP-1005104, OP-1006211, OP-1006120).

- **Grau de intrusão dos tipos de biometria:** As manifestações divergem quanto ao nível de intrusão entre diferentes tipos de biometria. Enquanto parte se concentra em alternativas não biométricas, outros apontam que modalidades como a impressão digital ou a voz podem ser consideradas menos intrusivas do que a biometria facial em determinados contextos (OP-1003688, OP-1006256, OP-1002202).

6.44. De modo geral, as contribuições evidenciam uma preocupação recorrente com a proteção da privacidade, a prevenção de práticas discriminatórias e a observância do princípio da proporcionalidade no uso das TRFs, sobretudo, em espaços públicos, ambientes educacionais e em relação a grupos vulneráveis. Ao mesmo tempo em que se identifica uma tendência favorável à adoção de alternativas menos intrusivas, persiste o debate sobre a pertinência de eventual proibição absoluta e sobre o papel específico das TRFs em setores considerados críticos, como o financeiro e a segurança pública.

BLOCO IV - SEGURANÇA, GOVERNANÇA E BOAS PRÁTICAS

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 conformidade com a LGPD e a proteção integral desses dados sensíveis?

6.45. As contribuições quanto a esse questionamento tratam das medidas de segurança, técnicas e administravas indispensáveis a serem aplicadas ao tratamento de dados biométricos em razão dos riscos próprios a essa atividade. Há consenso quanto à necessidade de se adotar medidas de segurança em aspecto amplo, com destaque para aquelas originárias do campo da segurança da informação, e, ao mesmo tempo, apresentam divergências notáveis, como, por exemplo, a ponderação entre a flexibilidade *versus* a rigidez das medidas "indispensáveis" a mitigar o risco do tratamento.

Pontos Convergentes:

6.46. Quanto às medidas de segurança indispensáveis à atuação do controlador, tem-se:

- **Criptografia forte**: Consenso em relação à necessidade de adoção de uma criptografia forte como, por exemplo, o padrão criptográfico *256-bit Advanced Encryption Standard* - AES-256 ou superior para proteger os dados biométricos, tanto em relação ao armazenamento quanto no que se refere à transmissão, incluindo o uso de chaves criptográficas gerenciadas em ambientes seguros como a utilização dos Módulos de Segurança de Hardware ou *Hardware Security Modules – HSMs,*que respondem por

dispositivos físicos projetados para proteger e gerenciar de forma segura chaves criptográficas (OP-996562, OP-997897, OP-10005652, OP-967368, entre outras).

- **Controle rigoroso de acesso**: A medida de controle de acesso rigoroso é amplamente citada, com a indicação da autenticação multifator – MFA e controle de acesso baseado em função, ou seja, *Role-Based Access Control* – RBAC, cujo acesso é atribuído com base em responsabilidades definidas e, desse modo, recai unicamente na função em que o usuário desempenha dentro da organização para limitar quem pode visualizar ou manipular os dados biométricos (OP-1005725, OP-968529, OP-100366, OP-963578, OP-1003688, entre outras).
- **Uso de *templates* biométricos ao invés dos dados brutos**: O armazenamento de *templates* biométricos no lugar de imagens ou dados brutos, e com a utilização de criptografia com *hashing* seguro e "*salt*" único por usuário para evitar ataques de comparação em massa em caso de vazamento teve citação ampla (OP-979836, OP-999971, OP-1000400, OP-1006098, entre outras). Há, também, posições que recomendam que o armazenamento do *template* biométrico ocorra em dispositivo próprio do titular ou que esse seja criptografado com chave sob sua posse (OP-1006230 e OP-1006068) ou, ainda, em menor extensão, recomendam a proibição do armazenamento do dado biométrico bruto (OP-996562 e OP-997897).
- **Segregação de redes e armazenamento seguro**: A **segregação de redes** que lidam com informações biométricas das demais redes corporativas (OP-1006225, OP-1005104, entre outras) é uma medida técnica de citação recorrente, acompanhada da utilização de *firewalls* e sistemas de detecção de intrusão (OP-967368) muitas vezes com ênfase em ambientes seguros e isolados (OP-1005104). Ainda, algumas contribuições sugerem a **segregação das bases de dados,** cujos controles de acesso devem ser rigorosos (OP-1005612, OP-1006220, OP-1003688, entre outras), e, além disso, a segregação dos dados sensíveis (OP-1006073).
- ***Privacy by design*:** Sugere-se que regulamentação deve permitir o emprego de estratégias de *privacy by design* ajustadas ao papel do agente de tratamento, diferenciando obrigações de fabricantes de *hardware* e plataformas (OP-1006297).
- **Registro de *"logs"* e rastreabilidade**: A manutenção de registros detalhados dos *"logs"* em todas as etapas do tratamento, desde os acessos, é citada, além da necessidade de registro de operações, alterações e decisões automatizadas a fim de possibilitar a rastreabilidade e auditabilidade (OP-969104, OP-999971, OP-1003688, OP-1005673, OP-1006211, dentre outras).
- **Auditorias regulares, periódicas e independentes:** Realização de ações de auditorias internas de segurança periódicas, bem como externas que

permitam avaliar se os controles internos e as operações de tratamento estão em conformidade com os preceitos da LGPD, os direitos dos titulares e o nível de segurança adequado às bases de dados biométricos também são medidas citadas. (OP-967752, OP-969104, OP-1000400, OP-1003891, entre outras).

- **Testes de segurança:** A serem desempenhados de forma rotineira e preventiva para identificar e corrigir falhas. Diversas foram as medidas mencionadas, tais como:
    - **Medidas de detecção de vulnerabilidades,** (OP-945269, entre outras) com a utilização dos **Testes de Segurança de Aplicativos** ou *Application Security Testing - AST*, como, o teste de segurança estático - SAST, teste de segurança dinâmico - DAST e teste de segurança interativo – IAST (OP-1005625);
    - **Testes de intrusão ou *pentests*:** Para a identificação de falhas e vulnerabilidades antes que hackers as encontrem, por meio de simulação de ataques cibernéticos realizados por profissionais em sistemas de informação, redes e aplicações (OP-967368, OP-968689, OP-1005901);
- **Monitoramento contínuo a ameaças:** Estabelecimento de procedimentos e rotinas de monitoramento contínuo de ameaças, como por exemplo, o *Security Information and Event Management – SIEM*(OP-1005625), foi citado;
- **Detecção de anomalias em tempo real:** Algumas contribuições apontam o uso de ferramentas automatizadas de detecção de anomalias para identificar possíveis ataques (OP-967752, OP-1000400 e OP-1005080);
- **Anonimização e Pseudonimização**: Medidas para **anonimizar ou pseudonimizar** dados biométricos sempre que possível são recomendadas para reduzir riscos do tratamento (OP-966032, OP-969104, OP-994148, OP-999971, OP-1004090, OP-1005679, OP-1005901, OP-1006225, entre outras);
- **Tecnologias de Aprimoramento da Privacidade – PETs**: Utilização das PETs que garantem privacidade desde a concepção - *privacy by design* e possuem atributos como irreversibilidade, não interoperabilidade e revogabilidade dos dados biométricos conforme a ISO/IEC nº 24745:2022 (OP-977469, OP-1005106, OP-1000513, OP-1006068, OP-1006098) foi apontada em algumas contribuições. Em sentido semelhante, a utilização das PETs como ferramenta para identificar os *templates* biométricos que necessitam de revogação (OP-1006198);

6.47. No que tange às medidas administrativas a serem consideradas indispensáveis, tem-se:

- **Política de Segurança da Informação e Proteção de Dados**: As contribuições revelaram consenso quanto à necessidade de se estabelecer

Política de Segurança da Informação e Proteção de Dados, com algumas variações quanto ao seu conteúdo e extensão. Temos:

- **Recomendação geral para uma Política de Segurança da Informação e de Proteção de Dados:** As contribuições mencionam a necessidade de se estabelecer políticas de segurança da informação e de proteção de dados claras como medida essencial para atender aos preceitos da LGPD (OP-967368, OP-999971, OP-1003688, OP-1004811, OP-1005652, OP-1005679, OP-1005725, OP- 100-5871);
- **Política de Segurança da Informação e Proteção de Dados Pessoais que aborde conteúdo específico:** Algumas contribuições detalham tipos, procedimentos, diretrizes e ou elementos específicos que a Política de Segurança da Informação e de Proteção de Dados deve abordar. Assim, temas como Políticas de Controle de Acesso, procedimento de Backup dos dados (OP-966029), diretrizes internas voltadas ao uso ético dos dados (OP-995585), políticas claras de governança (OP-969104), políticas claras sobre tratamento e retenção dos dados (OP-1000400), políticas claras sobre coleta e uso dos dados (OP-1002117) e desenvolvimento de políticas e procedimentos internos sobre o tratamento de dados biométricos (OP-1006217) devem fazer parte de uma política de segurança da informação e de proteção de dados pessoais;
- **Estabelecimento de um Programa de Segurança da Informação:** Algumas contribuições propõem que a Política de Segurança da Informação e de Proteção de Dados é parte integrante de um programa mais amplo de segurança da informação ou de uma estrutura sólida de governança organizacional (OP-963578, OP-1005106, OP-1006068 e OP-1006225).
- **Gestão de Riscos para conformidade com a LGPD:**Há contribuições que relacionam diretamente a Política de Segurança da Informação e de Proteção de Dados à avaliação de riscos, ao monitoramento e à garantia de conformidade com a LGPD, sendo tal política parâmetro mínimo de avaliação contínua da conformidade e dos riscos com o desenvolvimento dos indicadores-chave de risco (OP-1005104 e OP-1005225). Algumas contribuições enfatizam que a avaliação/análise dos riscos deve seguir os parâmetros trazidos pelas ISO/IEC 27005:2023, que contempla o gerenciamento de risco em segurança da informação (OP-1005635, OP-1006297), a ISO/IEC 27001:2022, que cuida do sistema de gestão da segurança da informação, e, por fim, a ISO IEC 24745:2022, que trata da proteção da informação biométrica (OP-01006220).

- **Plano de Resposta a Incidentes de segurança**: Diversas contribuições enfatizam a importância dessa medida como necessária ao cumprimento da LGPD. As contribuições também variaram quanto ao conteúdo e

extensão.

- **Recomendação geral e indispensabilidade:** Apontado como medida mínima indispensável à conformidade com a LGPD. A ampla maioria das contribuições mencionou o plano de forma abrangente (OP-966032, OP-968529, OP-968689, OP-1002117, OP-1006230, entre outras). Há quem entenda que o plano tem por objetivo mitigar incidentes (OP-1006220), outros, porém, que o instrumento deve fazer parte de uma política de governança organizacional (OP-1006198 e OP-1006217);
- **Conteúdo específico:** Algumas contribuições mencionam elementos específicos que o Plano de Resposta a Incidentes deve abordar como, por exemplo, definição de papeis, procedimentos de contenção e comunicação (OP-967368); Plano de Respostas a Incidentes específicos para tratar dos incidentes que envolvam a violação de dados biométricos (OP-1000400); Plano que determine a ação rápida e eficaz (OP-1005612), que detalhe os protocolos de contenção, investigação e notificação à ANPD e comunicação com os titulares (OP-1006073) e, ainda, que implemente mecanismo eficiente de gestão dos incidentes (OP-1006211);
- **Integração com a Gestão da Segurança da Informação e Governança:** Há contribuições que relacionam o Plano de Resposta a Incidentes a programas mais amplos como a Política de Segurança da Informação, governança organizacional e gestão de riscos (OP-995585, OP-1005673 e OP-1006217).

- **Treinamento e conscientização contínuos**: O treinamento contínuo e periódico de conscientização em segurança para funcionários que lidam com dados biométricos foi amplamente recomendado. (OP-968368, OP-968762, OP-999971, OP-1005673, OP-1005679, dentre outras). Há contribuições que sugerem conteúdos específicos às ações de treinamento e capacitação, como: conscientização na temática da segurança da informação, temáticas relacionadas ao uso ético dos dados pessoais (OP-995585 e OP-1005104), proteção de dados em geral (OP-1000400), e abordagem específica sobre minimização de dados biométricos - cultura da minimização na organização (OP-1006198). Ainda, algumas contribuições indicaram como público-alvo todos os colaboradores da organização (OP-967368), outras somente colaboradores que lidam diretamente com dados biométricos (OP-995585, OP-9999971, OP-1005104, entre outras) e, em menor extensão, terceiros e profissionais responsáveis pelas equipes de segurança da informação (OP-1004811 e OP-10062220).
- ***Due Diligence* e revisão contratual com fornecedores**: A realização de processos adequados de *Due Diligence* e a inclusão de cláusulas contratuais rigorosas junto a fornecedores e terceiros foram apontados como essenciais para garantir a conformidade com a LGPD (OP-1005871,

OP-1006217, OP-1006220, entre outras). Ainda, algumas contribuições citam expressamente a necessidade de revisão contratual rigorosa específica junto a fornecedores e/ou terceiros (OP-1005718, OP-1006162, OP-1006230, OP-1005080, entre outras). Há, também, contribuição que especificamente ressalta a necessidade de procedimento de avaliação prévia de fornecedores relacionados à segurança da informação e proteção de dados (OP-1006217).

- **Retenção e descarte seguros dos dados biométricos**: Definição de políticas claras de retenção e descarte seguro dos dados biométricos, limitando o prazo de armazenamento à finalidade específica.
    - **Políticas claras para a retenção de dados biométricos:** Necessidade de estabelecimento de políticas claras para a retenção e descarte dos dados biométricos com a indicação de prazos para a retenção e revisão periódica de necessidade de guarda destes e minimização da coleta (OP-995585, OP-969104, OP-1000400, OP-977469, OP-1003891, OP-1006162, dentre outras).
    - **Critérios e métodos para descarte:** Há contribuição que sugere que a evolução tecnológica deve ser critério para descarte de dados biométricos vulneráveis (OP-966260), outra indaga, por exemplo, qual o procedimento para que uma pessoa possa ser excluída do banco de dados biométricos (OP-1005104) e, por fim, há quem defenda a exclusão permanente dos dados biométricos coletados após a extração das características desejadas, ou seja, quando exaurida a finalidade que motivou a coleta (OP-1006211);
    - **Gestão do ciclo de vida dos dados:** Em menor extensão, algumas contribuições mencionam a necessidade de compatibilizar as etapas do tratamento com o ciclo de vida dos dados biométricos. Assim, primordial efetuar mapeamento dos fluxos dos processos organizacionais que se utilizem de dados biométricos para identificar o ciclo de vida destes, além de se realizar a gestão ativa do ciclo (OP-1003891, OP-1004215 e OP-1006225).

6.48. Ainda, quanto aos parâmetros mínimos de **avaliação de riscos e monitoramento** a serem exigidos das organizações para garantir a conformidade com a LGPD e a proteção integral dos dados sensíveis, os seguintes parâmetros foram amplamente citados:

- **Governança e *Accountability***: Inúmeras contribuições ressaltam a necessidade do estabelecimento da governança e adoção dos princípios da *accountability* para a efetiva proteção dos dados biométricos (OP-969104, OP-1004895, OP-1005679, OP-1006198, dentre outras). De forma mais específica, algumas contribuições citam a necessidade do fortalecimento d a **governança em privacidade,** incluindo a definição de papéis e responsabilidades e documentação pertinente para fins de

responsabilização (OP-977469, OP-1006220, OP-1004895 e 1005725, dentre outras). Ainda, outras contribuições enfatizam os conceitos do *privacy by design* e *by default* necessários a serem observados e intrínsecos à governança (OP-1006225, OP-979836). Por fim, houve menção de que a LGPD apoia a adoção de **boas práticas** como elementos fundamentais para a conformidade (OP-1005963 e OP-967732);

- **Avaliação de impacto à proteção de dados:** Há consenso quanto à indispensabilidade da elaboração e atualização periódica do Relatório de Impacto à Proteção de Dados (RIPD) como instrumento que compõe a governança e necessário ao tratamento de alto risco. O estabelecimento de parâmetros mínimos para a avaliação de risco, como análises de impacto e avaliação de legítimo interesse (LIA), é medida amplamente citada (OP-1004895, OP-967752, OP950124, entre outras);
- **Documentação e Registro de Operações (RoPA):** Algumas contribuições salientam a importância de documentar as operações de tratamento dos dados pessoais a fim de garantir a rastreabilidade e, por conseguinte, a *accountability* (OP-1006217, OP-1006211, OP-1005106, entre outras);
- **Análise de Viés e Impactos em Grupos Vulneráveis** Há uma crescente preocupação com a **análise de viés e impactos** sobre grupos vulneráveis no uso de biometria, sendo um parâmetro sugerido para avaliação de riscos (OP-969104, OP-1005679, OP-1006225). Uma contribuição afirma ser preciso considerar a distinção entre grupos vulneráveis e tipos de serviços para ponderar entre o risco e o benefício da coleta do dado biométrico (OP-994148).

<u>Pontos de Divergência:</u>

6.49. Os seguintes pontos apresentaram visões distintas ou abordagens menos convencionais ao cenário atual. São elas:

- **Referências a Avaliações Internacionais:** As contribuições também apresentaram divergências sobre a relevância de padrões técnicos internacionais. Um grupo enfatizou a importância de alinhar a regulação nacional a parâmetros já consolidados, citando avaliações conduzidas *pelo "National Institute of Standards and Technology* – NIST (EUA)", que realiza testes de desempenho, precisão e vieses em sistemas biométricos, bem como a norma "ISO/IEC 30107-3:2023", que define metodologias para verificar a resistência de sistemas biométricos a ataques de apresentação (*spoofing*), ou seja, tentativas de fraude mediante uso de artefatos como fotos, gravações de voz ou impressões digitais artificiais. Outro grupo, entretanto, não atribuiu a mesma relevância a essas referências, concentrando suas análises em aspectos internos de governança e mecanismos de controle organizacional.
- **Flexibilidade vs. rigidez das Medidas de Segurança "Indispensáveis"**:

- **Abordagem flexível e proporcional com base no risco e no contexto do tratamento**: Muitos contribuintes argumentam que as medidas de segurança devem ser flexíveis, proporcionais ao contexto do tratamento, ao porte da organização, ao volume dos dados tratados e aos riscos reais envolvidos, a fim de evitar a adoção de requisitos de segurança excessivamente rígidos e únicos que possam ser excessivos ou inadequados (OP-1005627, OP-1006297, entre outras). Uma contribuição menciona que eventual definição de medidas de segurança deve observar as boas práticas de cibersegurança evitando exigências padronizadas e rígidas (OP-1005627). Outra, ainda, que a ANPD deveria evitar um rol taxativo ou "padrão mínimo único" para preservar a neutralidade tecnológica (OP-1006132).
- **Abordagem da rigidez e medidas mínimas indispensáveis:** Por sua vez, inúmeras contribuições enfatizam a necessidade do estabelecimento de medidas de segurança fortes, mínimas e até mesmo mandatórias, devido à natureza sensível e irreversível dos dados biométricos (OP-963578, OP-9694888, OP-969488, OP-977469. OP-979836, OP-1006162, entre outras).

6.50. Nessa esteira, há contribuições que afirmam que as medidas de segurança a serem consideradas como mínimas são: criptografia no nível do modelo com a utilização de "*hash*" seguro, controle de acesso com segregação estrita de funções e *"logs"* de auditoria, anonimização, testes de vulnerabilidade, avaliações de risco periódicas, Relatório de Impacto à Proteção de Dados, monitoramento contínuo de vulnerabilidades e plano de resposta à incidentes (OP-966032, OP-967752). Duas contribuições citaram que o *privacy by design* deveria ser medida obrigatória de segurança (OP-996562, OP-997897).

6.51. Por fim, há, também, contribuição que conclui que proteger dados biométricos é proteger direitos fundamentais, fato esse que exige rigor técnico, jurídico e institucional. Enfatiza, nesse ponto, que a maioria dos projetos públicos que utilizam o reconhecimento facial no Brasil carecem de salvaguardas mínimas (OP-969104).

6.52. À luz das abordagens evidenciadas, é possível destacar que os pontos de discordância recaem na ponderação entre:

(I) Universalidade em contraponto à especificidade das medidas: Há dissonância quanto à universalidade das medidas a serem consideradas indispensáveis ou mínimas que deveriam ser aplicadas para todo e qualquer tratamento de dados biométricos em contraponto à argumentação de que a imposição de um rol taxativo ou rígido seria contraproducente, oneroso e inadequado, pois não considera as particularidades de cada organização e, sobretudo, o contexto de uso.

(II) Natureza do Risco: Há divergência quanto ao entendimento sobre

se o dado biométrico por si só possui um “risco intrínseco elevado”. Isso porque algumas contribuições argumentam que o risco é inerente à imutabilidade do dado e, portanto, exige medidas de proteção máxima; em contraponto, outras contribuições expressam que o risco é variável e depende do contexto, escala e finalidade da coleta e, por essa razão, as medidas de segurança a serem adotas variam.

(III) Custo e adequação: A abordagem acerca da flexibilidade das medidas ainda ressalta que medidas rígidas podem gerar custos desnecessários para pequenas empresas, enquanto a abordagem da rigidez prioriza a proteção máxima devido ao dano irreversível, uma vez que ajusta a medida de segurança ao risco do tratamento, assim, eventuais custos para a implementação dessas devem ser suportados pelo agente de tratamento para garantir a proteção dos dados biométricos.

- **Armazenamento em Nuvem**:
    - **Proibição do armazenamento em nuvem**: Uma contribuição afirma, de forma taxativa, "nunca armazenar em nuvem (no país ou no estrangeiro)". Assim, independentemente da nacionalidade do provedor ou da localização dos servidores, o armazenamento em nuvem dos dados biométricos deve ser evitado por completo, ou seja, proibido (OP-966760)
    - **Abordagem não proibitiva quanto ao armazenamento em nuvem.** A maioria dos contribuintes não fazem menção específica à proibição de armazenamento em nuvem, no sentido oposto, focam na necessidade de estabelecer medidas de segurança, técnicas e administrativas rigorosas, na necessidade de avaliação de risco e adoção dos conceitos do *privacy by design.* Ou seja, uma vez adotadas as salvaguardas necessárias à proteção dos dados biométricos, esses podem ser armazenados em qualquer ambiente, incluindo o ambiente de nuvem, desde que seguro (OP-1006098, OP-1005635).
- **Custódia dos Dados Biométricos:**
    - **Custódia do Titular**: Algumas contribuições defendem que o cenário ideal seria que os dados biométricos estivessem sob a custódia do próprio titular (OP-1006068)**.** Adicionalmente, tal abordagem sugere o controle da chave de criptografia pelo titular do dado biométrico (OP-1006098), ainda, a utilização de armazenamento local (*on-device*), sob o controle do titular (OP-1006198), e, ainda, sugere-se que seja utilizado o *template* biométrico e que esse fique, também, armazenado no dispositivo do titular ou criptografado com a chave sob sua posse (OP-1006230).

- **Custódia do Controlador com medidas de segurança fortes:** Abordagem mais recorrente nas contribuições reconhece que os dados biométricos podem ser custodiados pelo controlador, desde que se adotem medidas de segurança extremamente rigorosas. Assim, deve-se adotar, por exemplo: bases biométricas descentralizadas e armazenadas em locais seguros (OP-968529), ainda, adotar medidas como a segregação de redes que lidam com dados biométricos das demais redes corporativas, além do armazenamento segregado em módulos de segurança específicos (OP-1000400), entre outras medidas de segurança;
- **Custódia pelo Estado:** Uma contribuição sugeriu que a custódia da identidade fosse atribuída exclusivamente ao Estado, afastando o acesso por outros agentes. Essa posição, minoritária entre as manifestações, destacou preocupações com a segurança da criptografia e com o risco de comercialização indevida dos dados, que poderia resultar em fraude de identidade. Trata-se de uma visão distinta, uma vez que a maioria das contribuições se concentrou em práticas de transparência adotadas pelos controladores (OP-944113).

- **Responsabilidade pela Avaliação de Impacto (RIPD)**:
  - **Estrutura institucional independente**: Um contribuinte sugere que a avaliação de impacto deveria ser feita por uma estrutura institucional independente, como, por exemplo, por uma agência governamental, e não pelo próprio controlador (OP-1004895).
  - **Responsabilidade do Controlador**: A maioria das contribuições aponta que a realização do RIPD é de responsabilidade do controlador, ou seja, da própria organização, sendo requisito obrigatório quando do tratamento de dados sensíveis ou em situações de alto risco (OP-963578, OP-963578, OP-966029, entre outras).
- **Uso de Dados Sintéticos Gerados por IA**:
  - **Medida Complementar em Testes/Treinamentos**: No contexto do desenvolvimento de sistemas de IA e de decisões automatizadas, uma contribuição menciona o **uso de dados sintéticos gerados por modelos generativos de IA** como medida complementar para mitigar riscos em testes e treinamentos.

6.53. As contribuições versaram sobre a adoção de medidas de segurança, técnicas e administrativas indispensáveis a mitigar os riscos quando do tratamento dos dados biométricos. Em síntese, houve um alinhamento quanto à necessidade do estabelecimento de medidas de segurança fortes, havendo a indicação específica de diversas delas. Todavia, existem divergências significativas quanto aos seguintes pontos: estabelecimento de um rol mínimo e obrigatório de medidas a serem aplicadas a todos os tratamentos de dados

biométricos; existência de um risco excessivo inerente ao tratamento desse tipo de dado; custódia dos dados. Há, ainda, contribuições pontuais que defendem a proibição do armazenamento em nuvem, a obrigatoriedade de elaboração do RIPD por instituição independente e a utilização de dados sintéticos gerados por modelos generativos de IA como medida complementar.

Pergunta 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?

6.54. As contribuições recebidas exploram eventual restrição de acessos a serviços não essenciais que dependam de dados biométricos em caso de negativa do titular. Buscou-se compreender se a indisponibilidade por esse motivo não configura restrição ilícita ou abusiva. Ainda, quando o tratamento for realizado com base no consentimento em que contextos a negativa do titular pode justificar eventual restrição de uso de determinadas funcionalidades.

Pontos Convergentes:

6.55. Dentre os elementos comuns identificados nas contribuições, verificam-se entendimentos convergentes quanto a:

- **Alternativas não biométricas:** Há consenso de que as organizações devem sempre oferecer métodos alternativos de autenticação além da biometria. Essas alternativas podem incluir senhas tradicionais, tokens, cartões de acesso, autenticação multifatorial (MFA), QR Codes ou PINs. O objetivo primordial é garantir a acessibilidade e evitar a discriminação ou exclusão indevida, especialmente de grupos vulneráveis ou pessoas com deficiência (OP-966032, OP-1006073, OP-1006217, dentre outras).
- **Transparência das informações:** Amplamente considerada uma boa prática que os controladores sejam plenamente transparentes e informem os titulares de forma clara e prévia sobre a necessidade do uso dos dados biométricos, a finalidade, os benefícios, as alternativas disponíveis e as consequências exatas de sua recusa ao titular. Há, ainda, em menor escala, quem defenda o acesso público a informações sobre contratos, softwares e hardwares utilizados no tratamento. Muitos defendem que a comunicação deve ser acessível e detalhada, reforçando a confiança e o compromisso com a LGPD (OP-967368, OP-967752, OP-1006187, OP-1006230, OP-1006297, OP-1006211, OP-969154, OP-1006120, dentre outras).

- **Necessidade e proporcionalidade da biometria:** Quase a totalidade das contribuições concordam que o uso da biometria e qualquer restrição decorrente de sua recusa devem observar os princípios da LGPD, especialmente os princípios da necessidade, adequação e proporcionalidade. Assim, a biometria só deveria ser exigida ou justificar uma restrição quando for tecnicamente indispensável para a funcionalidade específica, e não houver alternativa igualmente eficaz e segura (OP-966032, OP-969282, OP-977469, OP-994148, dentre outras).
- **Recusa não deve impedir o acesso ao serviço principal:** É amplamente aceito que a recusa do titular em fornecer dados biométricos não pode resultar em exclusão total do serviço ou impedir o acesso às funcionalidades básicas. Nesse sentido, as restrições devem ser limitadas às funcionalidades que dependem tecnicamente da biometria e cuja indisponibilidade não comprometa direitos fundamentais do titular (OP-966760, OP-967368, OP-968529, OP-977469, OP-1006220, dentre outras).
- **Biometria para segurança reforçada e prevenção à fraude:** Muitos contribuintes concordam que a biometria é legitimamente essencial para funcionalidades que exigem alto nível de segurança, como transações financeiras de alto valor, acesso a dados sensíveis, assinatura eletrônica qualificada, ou para a prevenção de fraudes. Nesses cenários de alto risco, a restrição de funcionalidades em caso de recusa biométrica é mais frequentemente considerada justificada e proporcional (OP-950124, OP-968689, OP-995585, OP-1000400, dentre outras).
- **Consentimento Livre, Informado e Revogável:**Quando o tratamento biométrico tiver por hipótese legal o consentimento, as contribuições apontam que é crucial que este seja livre, informado, inequívoco, específico e revogável. Assim, negar o serviço pela falta de consentimento pode ser considerado uma prática abusiva se não houver liberdade real de escolha ou alternativas viáveis. Apontam, ainda, que o titular deve ter o direito de "*opt-out*" de forma simples e acessível, sem que isso implique restrições desproporcionais (OP-966029, OP-966032, OP-969154, OP-1005625, dentre outras).
- **Avaliação de Impacto à Proteção de Dados (RIPD/DPIA)**Muitos contribuintes recomendam a realização de Relatórios de Impacto à Proteção de Dados (RIPD) ou Avaliações de Impacto (DPIA) como uma boa prática para justificar a necessidade da biometria, analisar os riscos envolvidos no tratamento, buscar alternativas e documentar as decisões, especialmente se a biometria for um requisito exclusivo ou envolver alto risco de discriminação ou exclusão (OP-969104, OP-969154, OP-1002117, OP-1006256, dentre outras).

<u>Pontos Divergentes:</u>

6.56. Em relação aos pontos divergentes, as contribuições sinalizam

para dois aspectos, **possibilidade de recusa** e **extensão da restrição** em caso de recusa. Na ponderação entre os aspectos, as seguintes abordagens são identificadas:

- **Restrição legítima sob condições rígidas:** A maioria das contribuições sinaliza a possibilidade de restrição de funcionalidades *apenas* se a biometria for tecnicamente indispensável e comprovadamente inviável oferecer a funcionalidade sem a sua coleta (OP-966032, op-967368, dentre outras). Além disso, em menor grau, algumas contribuições justificam a possibilidade de restrição se os direitos e interesses protegidos pela exigência da biometria (como segurança e prevenção a fraudes) prevalecerem sobre o direito do titular de não a fornecer, desde que seja proporcional e transparente (OP-1005635, OP- 1006225, OP-1006297).

- **Impossibilidade de haver restrição ou restrição mínima:** Outra corrente defende que nenhuma funcionalidade deve ser restringida em caso de negativa do titular, ou que a recusa nunca deve gerar penalidades ou restrições desproporcionais. Argumentam que o usuário não deve ser "refém do mundo digital" e que sempre deve haver uma contingência ou alternativa para garantir o acesso pleno aos serviços (OP-944113, OP-945269, OP-966760, OP-1006220, dentre outras).

- **Autonomia Empresarial:** Algumas poucas contribuições enfatizam a autonomia que a organização possui a partir do modelo de negócio em face da oferta do serviço para determinar quando a biometria é tecnicamente necessária e para fazer escolhas tecnológicas que protejam usuários e operações, especialmente em contextos de segurança e prevenção à fraude (OP-1005627, OP-1006052).

6.57. No geral, identificaram-se convergências sobre: a necessidade de oferecer alternativas não biométricas, quando possível; a transparência quanto ao tratamento, em menor ou maior grau; a necessidade de observância dos princípios da LGPD tanto para o tratamento de dados biométricos, como para eventuais restrições devido à recusa de fornecer os dados; a recomendação de elaboração de RIPD; a impossibilidade de a recusa de fornecer os dados importar em restrição de acesso à funcionalidade principal. Houve divergência, no entanto, sobre a possibilidade de recusa e a extensão da restrição. Algumas justificam a possibilidade de restrição se os direitos e interesses protegidos pela exigência da biometria prevalecerem sobre o direito do titular, outras defendem a impossibilidade de qualquer restrição e há, ainda, algumas que enfatizam a autonomia empresarial.

Pergunta 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?

6.58. A questão procurou identificar se há boas práticas específicas a serem observadas quando do tratamento de dados biométricos e, também, quais os mecanismos específicos de transparência para que os dados biométricos coletados sejam utilizados em acordo a LGPD, a fim de evitar discriminação ilícita e abusiva.

Pontos convergentes:

6.59. A maioria das contribuições sugere que seria uma boa prática a adoção de um conjunto forte de medidas de segurança, técnicas e administrativas, compreendidas como medidas organizacionais e de governança, como meio de proteção eficaz ao tratamento dos dados biométricos e, por consequência, aptos a garantirem o seu uso responsável. Nesse sentido, verifica-se:

- **Medidas de segurança:** Há consenso de que a proteção eficaz dos dados biométricos tem por pilar a implementação de fortes salvaguardas de segurança, como por exemplo, a adoção da criptografia, controle de acesso rigoroso com autenticação multifator, minimização dos dados, utilização de *templates* biométricos em detrimento do uso dos dados brutos e a anonimização e a pseudoanonimização foram amplamente citadas como medidas necessárias, ou seja, estruturantes à proteção dos dados biométricos (OP-966032, OP-967368- OP-1006211, OP-1006297, OP-1005963, dentre outras); para além das medidas comumente citadas, há contribuições que indicam explicitamente as seguintes:
    - **Técnicas Avançadas e de Aprimoramento de Privacidade (PETs):** Fazem parte deste grupo, as Referências Biométricas Renováveis (RBRs), as *Biometric PETs* (B-PETs) e as técnicas de criptografia avançada, tais como criptografia homomórfica, computação multipartidária segura (SMPC) e *Zero Knowledge Proofs* (ZKP), que permitem realizar operações e verificações sobre dados criptografados sem a necessidade de revelá-los (OP-1005635, OP-1006068, OP-106098, OP-1006162);
    - **Arquitetura de processamento local (*On-Device*):** Adotar arquitetura de sistema, sempre que possível, em que a captura, o processamento e a verificação do dado biométrico sejam efetuados no dispositivo do próprio usuário, sem que o dado biométrico bruto seja transmitido para um servidor centralizado. Isso minimizaria drasticamente o risco de eventual interceptação e acesso indevido (OP-977469, OP-1003891, OP-1006220).
    - **Adoção de padrões internacionais de certificação:** Algumas contribuições sugeriram que as soluções biométricas fossem avaliadas conforme normas internacionais de referência, como os testes do NIST, a certificação ISO/IEC 30107-3:2023, voltada à detecção de ataques de falsificação (*spoofing*), e a ISO/IEC 24745:2022, que dispõe sobre requisitos específicos de proteção à

informação biométrica (OP-969154).

- **Medidas administrativas (organizacionais e de governança):** Há convergência acerca da importância de se estruturar a governança organizacional voltada à privacidade e à proteção de dados pessoais, ou seja, governança da privacidade ou, ainda, governança de dados biométricos, para além de medidas como àquelas advindas do campo da segurança da informação. Assim, as contribuições elencam as seguintes medidas: Relatório de Impacto à Proteção de Dados (RIPD) a ser realizado antes do início do tratamento dos dados biométricos, especialmente em operações classificadas como de alto risco; necessidade de garantir mecanismos de transparência ao titular com o fornecimento de informações claras e acessíveis sobre a finalidade da coleta, com especial destaque à hipótese legal e aos riscos envolvidos; período de retenção e os direitos do titular; desenvolvimento e adoção de políticas internas claras; capacitação contínua das equipes que atuam na organização; realização de testes periódicos de autorias; e, por fim, a incorporação dos conceitos do *privacy by design* e *privacy by default* foram recomendações recorrentes (OP-963578, OP-966032, OP-967368, OP-1005718, OP-1006187, OP-1006225, OP-1006230, dentre outras);
- **Medidas técnicas para evitar a discriminação e vieses:** As contribuições indicam que há preocupação com o uso indevido e discriminatório dos dados biométricos como ponto central de convergência. Foram sugeridas as seguintes práticas específicas capazes de mitigar eventual uso discriminatório dos dados biométricos:
    - **Auditoria de algoritmos e mitigação de vieses:** Muitas contribuições destacam a necessidade de testar e auditar os algoritmos para identificar e corrigir vieses (OP-966032, OP1005104, OP-1006220, OP-1006232, OP-1006230, OP-1003891, dentre outras)
    - **Revisão humana:** A implementação de mecanismos de supervisão ou revisão humana em decisões automatizadas baseadas em biometria foi frequentemente sugerida para prevenir erros e discriminação (OP-999971, OP-1000400, OP-1006155, OP-1006232, OP-1003688, dentre outras).
    - **Uso de bases de dados diversificadas:** Algumas contribuições indicam que, para treinar os algoritmos de forma justa, é essencial utilizar bases de dados que sejam amplas, atualizadas e representativas da diversidade da população (OP-968689, OP-995585, OP-999971, OP-1000400, OP-1006187, OP-1005963, dentre outras);
    - **Canais de Contestação:** Garantir que os titulares tenham canais acessíveis para questionar, contestar e corrigir decisões tomadas com base em seus dados biométricos é uma prática recomendada (OP-1004811, OP-1005080, OP-1000400, OP-1002117, dentre outras).

Pontos divergentes:

6.60. As divergências indicam dissonância quanto aos seguintes aspectos:

- **Nível e forma da transparência:** Apesar da concordância sobre a necessidade de transparência (art. 9º da LGPD), há nuance acerca da extensão e profundidade da informação que deve ser fornecida de forma ativa ao titular dos dados biométricos. Algumas contribuições defendem que, **quanto mais evidente e comum for a atividade de tratamento, menor a exigência de práticas ativas de transparência** (OP-1006297, OP-1005871). Em contrapartida, há a defesa de adoção de práticas de transparência mais sólidas e ativas, como a publicação de relatórios de impacto e a documentação pública de decisões técnicas e legais sem a vinculação ao tipo ou à complexidade do tratamento realizado (OP-1003688);

- **Abordagem Regulatória vs. Inovação:** Uma divergência sutil recai em eventual abordagem que pondere entre **regulação** e **inovação**. Um contribuinte alerta que exigências excessivas em projetos experimentais ou de pesquisa, onde o risco é mínimo, podem comprometer a inovação (OP-1006297);

- **Governança dos Dados Biométricos Integrada vs. Específica:** Há uma diferença na abordagem de como as políticas de governança devem ser estruturadas. Uma fonte recomenda integrar a governança de dados biométricos nas políticas gerais de proteção de dados já existentes para evitar burocracia e custos adicionais (OP-1005627). Outras, no entanto, mencionam a adoção de "políticas internas específicas para biometria", sugerindo a necessidade de um tratamento documental separado e mais detalhado (OP-1003891, OP-1006220). Há, também, contribuição que sugere política específica para dados sensíveis (OP1005725).

6.61. No geral, as contribuições apresentaram consenso em relação à necessidade de adoção de medidas de segurança, técnicas e administrativas para os dados biométricos por parte dos agentes de tratamento. Nessa esteira, foram trazidas medidas “gerais” originárias do campo da segurança da informação e que, na atualidade, são aplicadas aos dados pessoais de forma ampla. Pontualmente, foram mencionadas algumas medidas específicas aos dados biométricos, como por exemplo, as Técnicas Avançadas e de Aprimoramento de Privacidade (PETs) e Arquitetura de Processamento Local (*On-Device*). As divergências verificadas recaíram sobre a extensão e alcance do nível de transparência, não obstante ser consenso quanto às obrigações trazidas pelo art. 9º, da LGPD. Não houve consenso, ainda, sobre a necessidade de adoção de políticas de governança de dados biométricos específicas, ou, se é suficiente que a temática dos dados biométricos faça parte de políticas organizacionais gerais,

e, por fim, sobre a necessidade de ponderação entre uma abordagem regulatória que incentive a inovação.

Pergunta 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 devidamente informados, tenham controle sobre seus dados e possam exercer seus direitos, mesmo em situações de difícil transparência?

6.62. O avanço tecnológico exige que o direito fundamental à proteção de dados seja analisado de forma contextualizada com a inovação, sob pena de se tornar ineficaz. Diante disso, a pergunta 14 objetiva compreender as opções disponíveis em relação a medidas e ou condutas que possam ser adotadas por controladores para garantir a autodeterminação informativa e, por consequência, a possibilidade do exercício de direitos pelo titular de dados pessoais no contexto de tratamentos contínuos e massivos de dados biométricos.

Pontos convergentes:

6.63. Dentre os elementos comuns identificados nas contribuições, verificam-se entendimentos convergentes quanto a:

- **Eficiência das medidas para fortalecimento da transparência**: Muitas contribuições concordam que uma das maiores dificuldades envolvendo o tratamento de dados biométricos em contextos de monitoramento de grandes multidões é a transparência aos titulares. Alegam que atualmente o cidadão não sabe sequer que seus dados estão sendo tratados. Alegam, assim, que tal conduta não respeita a autodeterminação informativa e, portanto, não está em conformidade com a LGPD. Nesse sentido, a fim de assegurar o direito à informação especificamente para essa modalidade de tratamento, as seguintes medidas são indicadas (OP-966029, OP-977469, OP-1005612):
    - **Sinalização clara e visível nos locais monitorados:** Isso inclui placas com informações básicas e em linguagem simples e QR Codes para acesso rápido a informações adicionais e políticas de privacidade detalhadas;
    - **Canais digitais (websites, portais de privacidade, aplicativos):** Para disponibilizar informações completas, incluindo a finalidade do tratamento e o tempo de retenção. Há sugestões para aplicação de tecnologias complementares de notificação;
    - **Campanhas de conscientização e educação digital:** Para explicar o

funcionamento das tecnologias, seus riscos e potenciais impactos, os direitos dos titulares e os canais de contato dos agentes de tratamento e da ANPD.

- **Promoção de práticas de governança contextualizadas:** Fração significativa das contribuições aponta para o estabelecimento de uma governança de dados com ações específicas para tecnologias de reconhecimento facial. Para isso, afirmam que a participação da ANPD, enquanto entidade fiscalizadora, e a colaboração com os próprios titulares de dados é imprescindível. Adicionalmente, destacam que a conformidade de qualquer operação que envolve dados pessoais pressupõe a adoção dos princípios de *privacy by design/by default* (art. 46, §2º da LGPD) e uma prestação de contas recorrente aos titulares e às autoridades, com ênfase na obrigação de nomear um encarregado de dados (art. 41 da LGPD) (OP-969488, OP-994148, OP-1004895, OP-1005673).
- **Finalidade do tratamento e riscos associados:** Parcela relevante das contribuições ressalta que se a finalidade do monitoramento massivo não for a identificação dos titulares por meio de processos de comparação ou a coleta de dados (por exemplo, apenas para revelar o número de pessoas em uma multidão ou padrões de tráfego), o risco do tratamento é reduzido. Nesses casos, a proteção aos titulares é observada sob outra ótica, pois não há identificação pessoal direta. Assim, concluem que essa diferenciação pode influenciar na aplicação plena das medidas de segurança exigidas pela LGPD (OP-1006098, OP-969154, OP-994148).

Pontos divergentes:

6.64. As divergências indicam dissonância quanto aos seguintes aspectos:

- **Legalidade do tratamento em massa de dados biométricos com a finalidade de vigilância em espaços públicos:** Um grupo de contribuições argumenta que esse tipo de tratamento afronta direitos fundamentais previstos constitucionalmente. Por conseguinte, aduzem que fere fundamentos da LGPD, como a autodeterminação informativa e o livre desenvolvimento da personalidade (art. 2º, II e VII da LGPD), em razão da impossibilidade do exercício de direitos efetivo pelos titulares e afronta a privacidade. Para essa visão, essa modalidade de tratamento deveria ser vedada (OP-1002202, OP-1005260, OP-1004895). Em contraposição, há contribuintes que acreditam que o tratamento em larga escala de dados biométricos não é, por si só, incompatível com a LGPD e que, se houver a implementação de medidas de segurança rigorosas, respeito aos princípios da Lei Geral e emprego de meios para mitigar riscos, não é o caso de restrições ao tratamento. Sendo assim, indicam uma abordagem flexível, ao invés de uma exclusão absoluta dessa espécie de tratamento (OP-1005718, OP-1006132).

- **Aplicabilidade da hipótese legal do consentimento:** Determinadas contribuições asseveram que a hipótese legal do consentimento é inviável ou inadequada como base legal para o tratamento massivo de dados biométricos em espaços públicos, uma vez que há dificuldades práticas em obtê-lo de forma anterior, livre, inequívoca e informada (OP-1004811, OP-1005260). Em sentido contrário, há contribuições que inferem que a escolha da hipótese legal deve ficar a cargo do agente de tratamento, considerando o contexto do tratamento e as tecnologias empregadas. Há, também, quem defenda que impossibilitar a utilização do consentimento para tratamentos dessa natureza afronta a legalidade e o incentivo à inovação (OP-966032, OP-1006220).

6.65. Dos posicionamentos apresentados, notou-se que há convergência sobre a necessidade de implementação de medidas de transparência eficazes no tratamento de dados biométricos no contexto de tratamento contínuo e massivo de dados biométricos. Além disso, mencionou-se sobre a participação indispensável da ANPD e dos titulares no incremento das medidas de governança adotadas pelos agentes de tratamento para essa modalidade de tratamento. Os contribuintes também chamaram atenção quanto ao nível de risco do tratamento cuja finalidade é a de identificação de indivíduos. Por outro lado, houve dissonância quanto ao alinhamento com a LGPD do emprego de tecnologias de monitoramento para fins de vigilância em espaços públicos e sobre a adequação do consentimento como uma base legal apropriada para esses fins.

BLOCO V - DOS DIREITOS DOS TITULARES E GRUPOS VULNERÁVEIS

Pergunta 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?

6.66. Essa questão teve por objetivo identificar as alternativas que são consideradas viáveis para a garantia dos direitos dos titulares de dados pessoais no âmbito do tratamento de dados biométricos, especialmente no que se refere às informações claras, ao direito de acesso, à correção de dados e à revogação do consentimento

Pontos convergentes:

6.67. Dentre os elementos comuns identificados nas contribuições, verificam-se entendimentos convergentes quanto a:

- **Direito à informação clara e transparência abrangente:** Algumas contribuições defendem que a comunicação deve ser detalhada, explicando como os dados são tratados, incluindo a finalidade, a hipótese legal, o tempo de retenção e as medidas de segurança adotadas. Para

facilitar a compreensão, indicou-se o uso de linguagem visual, como infográficos, vídeos e QR Codes, com uma abordagem em "camadas" que ofereça informações resumidas inicialmente e um detalhamento mais aprofundado mediante a iniciativa do titular de dados. Ainda, que a transparência deve ser ativa, contínua e contextualizada, apresentada no momento da coleta e de forma destacada antes da ativação da biometria. É sugerido que a disponibilização das informações deve ser multicanal, cobrindo pontos de coleta, sites, aplicativos, espaços físicos e comunicações eletrônicas (OP-968529, OP-10039891).

- **Direito à revogação do consentimento descomplicado:** A revogação do consentimento, segundo algumas contribuições, deve ser simples, fácil e acessível, preferencialmente com mecanismos diretos como botões, links ou comandos visíveis. As consequências de sua revogação devem ser previamente informadas ao titular, indicando se a ação limitará ou inviabilizará funcionalidades de bens ou serviços, conforme apontam. Por fim, a revogação deve resultar na exclusão dos dados biométricos, a menos que exista previsão em lei que justifique a retenção (OP-1004895, OP-1002202).
- **Direito à revisão de decisões automatizadas e explicabilidade:** Algumas contribuições asseveram que os titulares devem ter o direito à revisão humana de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, nos termos do art. 20, *caput* da LGPD. Adicionalmente, que é imprescindível fornecer explicações claras sobre a lógica envolvida e os critérios adotados na decisão automatizada, em linguagem simples e destacada. Para operações de alto risco, recomenda-se um processo de revisão humana antes que a decisão seja considerada como definitiva (OP-1006132, OP-1006211).
- **Tratamento acessível à grupos vulneráveis:** É necessário garantir um atendimento inclusivo para pessoas com deficiência (PCDs), adaptando os serviços e utilizando técnicas e medidas específicas, como apontam algumas contribuições. Argumenta-se que muitos serviços se baseiam em características físicas que PCDs não dispõem, e, por isso, tais titulares não devem ter o acesso restringido de maneira ilegítima. Para crianças e adolescentes, segundo defendem, o tratamento de dados biométricos deve ser considerado como último recurso e não deve ser utilizado com finalidade comercial em razão do princípio do melhor interesse (art. 14, da LGPD). Recomendam, também, proteger os idosos contra fraudes, especialmente aqueles com baixa escolaridade e analfabetos, garantindo a possibilidade de resposta negativa ao tratamento de forma antecipada, além de modular comunicação com informações claras e inteligível, ou seja, adequada ao público-alvo do tratamento (OP-1006256, OP-1002202, OP-1005106, OP-1006230).
- **Canais acessíveis e eficazes para o exercício de direitos:** Para os contribuintes, os agentes de tratamento devem disponibilizar canais

simples, gratuitos, eficientes e de fácil acesso para que os titulares possam exercer seus direitos, não limitados às informações contidas no art. 18, da LGPD. Nesse sentido, sugerem canais digitais (portais, e-mail, *chat*), físicos (atendimento presencial, *call center*) e que devem ser integrados aos processos de atendimento já existentes das organizações. A presença de seres humanos no atendimento é apontada como importante, especialmente para revisar decisões automatizadas ou oferecer alternativas em caso de falha do processo de coleta dos dados biométricos (OP-966032, OP-945269).

Pontos divergentes:

6.68. As contribuições também apresentaram divergências relevantes:

- **Aplicabilidade da correção aos dados biométricos**: Contribuições sinalizam que o direito de correção não se aplica diretamente ao resultado estatístico da comparação entre o banco de dados e os dados coletados (OP-1005635, OP-1005673 e OP-1005871), e sim, a erros na associação do *template* biométrico com o identificador ou à necessidade de recadastramento por alterações físicas relevantes que degradem a qualidade da autenticação. Para isso, as formas brutas coletadas inicialmente devem estar aptas a serem modificáveis. Outras contribuições afirmam que o titular tem direito à correção dos dados de forma integral, por observância do art. 18, III da LGPD (OP-963578, OP-967368, OP-968529).
- **Retenção do histórico de autenticações pós-revogação:** Uma contribuição argumenta que a revogação do consentimento não implica em uma necessária eliminação do histórico das autenticações já realizadas, se houver finalidades legítimas e independentes do consentimento (ex: obrigações legais, auditorias). Similarmente, menciona-se ainda a necessidade de ponderar a revogação com outras bases legais, devendo o titular ser informado sobre a necessidade de manter ou não os dados para finalidades legítimas. Por outra lado, há contribuições que enfatizam sobre a exclusão ou anonimização dos dados biométricos após a revogação para interromper usos futuros com finalidades inadequadas ou contrárias às apresentadas ao início do tratamento (OP-1005260, OP-1006220).
- **Amplitude da revisão humana em decisões automatizadas no contexto dos dados biométricos:** Algumas contribuições interpretam o art. 20 da LGPD de forma mais restrita, com incidência do direito de revisão humana somente quando a decisão foi tomada unicamente com base em tratamento automatizado e afeta os interesses do titular de forma ilícita ou abusiva (OP-950124, OP-1006132, OP-1006225). Contrariamente, parcela significativa das contribuições recomenda ou exige a revisão humana para todas as decisões automatizadas que tenham quaisquer efeitos relevantes ou em operações de alto risco. Há contribuições (OP-1006230) que sugerem um fluxo de revisão em múltiplos níveis (IA, humano, comitê de ética), mesmo que o art. 20 da LGPD não exija revisão humana obrigatória

(OP-1006230).

- **Minimização de dados e irreversibilidade em IA e representações biométricas revogáveis (RBRs):** Certas contribuições enfatizam a minimização de dados como fator determinante nas hipóteses em que a eliminação completa da influência dos dados no treinamento de modelos de IA seja um desafio técnico (OP-996562 e OP-997897). Nesse caso, o controlador deve provar que o sistema de IA não trata mais o dado pessoal do titular ao invés de simplesmente eliminá-lo. Por isso, destacam a necessidade de informar o titular de forma antecipada sobre a potencial irreversibilidade de seus dados no treinamento de modelos de IA no momento da coleta. Em contraste, outras contribuições focam nas Representações Biométricas Revogáveis (RBRs) (OP-969154). No âmbito das RBRs, a revogabilidade é uma característica-chave que permite a geração de um novo parâmetro de comparação, invalidando a anterior, sem a necessidade de nova coleta. A irreversibilidade (a imagem original não pode ser reconstruída sem os dados pessoais originais) e a não interoperabilidade (os dados não podem ser usados em outros sistemas sem autorização) das RBRs são destacadas como proteções à privacidade.

6.69. Da análise, tem-se que há consenso para fortalecer a transparência e a auditabilidade do tratamento dos dados biométricos, com destaque para a garantia da acessibilidade a grupos vulneráveis, como crianças, adolescentes e idosos. A revogação do consentimento de forma simples e fácil, deve ser primordial. No entanto, questões como o direito de acesso e a aplicabilidade do direito de correção geram discordâncias devido ao processamento de dados biométricos em *templates,* que são incompreensíveis para pessoas naturais. Nesse aspecto, alguns contribuintes mencionaram as RBRs como solução para a divergência. Ressaltou-se também quanto ao alcance da revisão humana em decisões automatizadas, cuja aplicação deve considerar os potenciais efeitos da decisão e os riscos verificados.

Pergunta 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?

6.70. O objetivo foi compreender as maneiras de participação parental e de responsáveis no tratamento de dados biométricos para que esse seja considerado válido e eficaz, tendo como pilar o princípio do melhor interesse, nos termos do art. 14, *caput,* da LGPD. Além disso, buscou-se identificar as condições para garantia desse princípio, considerados todos os fatores que influenciam o tratamento, como a utilização de tecnologias emergentes e

inovadoras.

Pontos convergentes:

- **Informação clara e acessível:** É destacada a necessidade de fornecer informações completas, claras, objetivas, acessíveis e em linguagem simples sobre o tratamento dos dados aos responsáveis legais, especialmente quando a hipótese legal utilizada é o consentimento, nos termos do art. 14, §1º da LGPD. As informações devem incluir detalhes específicos sobre a finalidade, potenciais riscos aos titulares e prazos de término do tratamento. Além de avisos de privacidade, muitos sugerem comunicações específicas e formais aos responsáveis legais (OP-1005871). Outros propõem informar diretamente às crianças e adolescentes em linguagem apropriada à sua maturidade, garantindo a autodeterminação informativa desse grupo de titulares (OP-1004215).
- **Ações pedagógicas e campanhas educativas:** Algumas contribuições expõem a necessidade de a realização de campanhas informativas, palestras, reuniões e até letramento digital para que os responsáveis legais possam compreender melhor os direitos dos titulares, os contextos de tratamento e as limitações previstas em lei. A ANPD ficaria responsável pela promoção das ações envolvendo aspectos gerais de aplicação da LGPD. Os agentes de tratamento estariam incumbidos de fornecer uma visão mais específica sobre o tratamento realizado (OP-1005982, OP-1006220).
- **Princípio do Melhor interesse:** Ao apontar a necessidade de observância ao princípio do melhor interesse, as contribuições destacam certas condições para que o tratamento de dados biométricos ocorra, quais sejam:
    - **Medidas de Segurança:** Deve ser implementado criptografia forte, controle de acesso, segregação de dados, monitoramento, registro de *"logs"*, políticas internas e treinamentos específicos para as equipes que lidam com dados pessoais de crianças e adolescentes;
    - **Políticas de retenção e exclusão de dados**: Há contribuições (OP-966760) que ressaltam que o tratamento iniciado durante a incapacidade civil deve ser interrompido quando o titular de dados se torna civilmente capaz (art. 5º, caput do Código Civil). Isso se justificaria com base na autodeterminação informativa do titular, tendo em vista que o tratamento foi iniciado com base nas declarações dos responsáveis legais. Assim, uma vez civilmente capaz, o titular deve novamente decidir sobre o tratamento.
    - **Avaliação de Impacto à Proteção de Dados (RIPD):**A elaboração de uma Avaliação de Impacto à Proteção de Dados (RIPD), com foco específico em potenciais riscos que foram identificados às crianças e adolescentes, é recomendada por certos contribuintes (OP-1006198,

OP-1002117). O relatório deve ser conduzido anteriormente ao início do tratamento, a fim de não expor crianças e adolescentes a riscos desconhecidos. Ademais, detalham que o RIPD deve avaliar impactos na autonomia, no direito de brincar, aprender, desenvolver-se e na formação da identidade.

- **Dados biométricos como condição de acesso à serviços e funcionalidades:** Parcela significativa das contribuições menciona provável abusividade em condicionar o acesso a serviços, como educação, merenda ou transporte, ao fornecimento de dados biométricos. Nesse contexto, devem ser oferecidas alternativas que não imponham o tratamento de dados biométricos para que os serviços sejam usufruídos, garantindo o direito ao desenvolvimento social e a não discriminação (art. 3º, caput e parágrafo único da Lei nº 8.069/1990 - Estatuto da Criança e do Adolescente - ECA).

Pontos divergentes:

6.71. As contribuições também apresentaram divergências relevantes:

- **Nível de proteção a ser fornecido:** Parcela das contribuições reconhece a necessidade de proteção reforçada aos dados biométricos de crianças e adolescentes, dada a maior vulnerabilidade do grupo e a existência de normas que impõem uma tutela mais especifica a eles (OP-969488, OP-977469, OP-979836). Entretanto, há contribuições (OP-969154) que argumentam sobre a desnecessidade de medidas de segurança adicionais quando há adoção de soluções biométricas baseadas em Referências Biométricas Renováveis (RBRs). Argumenta-se que, nos termos do *AI Act*, os sistemas de verificação biométrica (1:1) são sempre considerados de baixo ou nenhum risco, conforme seu Anexo III, 1 (a) e, por isso, não seria necessário um nível de proteção maior do que o fornecido usualmente.
- **Suficiência do consentimento parental:** Certos contribuintes indicam que o consentimento específico dos pais é uma hipótese legal autossuficiente, fazendo com que a participação da criança e do adolescente seja reduzida nessa fase do tratamento. Baseiam-se nas disposições do Código Civil acerca da representação legal e assistência, com a consequente nulidade de contratos e outros negócios jurídicos (art. 166, I e 171, I) (OP-1006211, OP-1005260, OP-1006155). Outras contribuições vão no sentido de que consentimento dos pais, por si só, não é suficiente (OP-996562, OP-997897). Por isso, propõem que o controlador deve provar que o tratamento gera um benefício direto e plausível para a criança. Diante disso, defendem que os interesses do agente de tratamento não podem ser considerados como uma justificativa válida para a coleta desses dados biométricos.

6.72. Há um consenso no sentido da necessidade de ações educativas aos titulares e aos responsáveis legais para promoção de temas relacionados à

proteção de dados de crianças e adolescente no intuito de fortalecer a transparência e viabilizar o exercício dos direitos do titular de forma mais efetiva. Ademais, práticas como a elaboração de RIPD e políticas de exclusão de dados após o alcance da maioridade civil pelo titular são apontadas como medidas para preservação do princípio de melhor interesse. Todavia, persistem divergências quanto à necessidade de fornecimento de nível de proteção maior para o tratamento de dados biométricos de crianças e adolescentes. Além disso, ao se referirem sobre a hipótese legal do consentimento, há contribuições que indicam que o consentimento parental pode não ser suficiente, exigindo participação ativa dos menores nesse processo e outras seguem em sentido oposto.

Pergunta 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?

6.73. As hipóteses legais aplicáveis ao tratamento de dados biométricos estão alocadas no art. 11 da LGPD. Sendo assim, a questão teve por escopo compreender sobre a necessidade de detalhamentos adicionais quando essa categoria de dado se refere a crianças ou adolescentes. Também se buscaram formas de compatibilizar as medidas de segurança com a hipótese legal utilizada pelo agente de tratamento, considerando o zelo por esse grupo de titulares.

Pontos convergentes:

- **Medidas técnicas e organizacionais eficazes:** Há consenso em relação à necessidade de serem adotas medidas de segurança, técnicas e administrativas conforme dispõe o art. 46, *caput* da LGPD. Porém, as contribuições não revelaram salvaguardas específicas a serem aplicadas quando do tratamento de dados biométricos de crianças e adolescentes. As medidas citadas por vezes têm origem no campo da segurança da informação, como, por exemplo: a criptografia forte, de ponta a ponta, específica para *templates* biométricos (frequentemente citada); o controle de acesso rigoroso, restrito ao perfil profissional ou função exercida, com autenticação multifator tanto em meio físico quanto digital (OP-1000400, OP-1006155, OP-1006052, OP-1002202, OP-1004895, dentre outras). São citadas, ainda, aquelas que decorrem diretamente da LGPD como, por exemplo, a necessidade de RIPD (OP-963578, OP-969154, OP-1006220) ou, por fim, questões de governança que envolvem o desenvolvimento de políticas de armazenamento (art. 16, da LGPD) e descarte seguro, por exemplo (OP-1005625, OP-1006220, OP-967368, dentre outras).

Pontos divergentes:

6.74. As contribuições também apresentaram divergências relevantes:

- **Hipóteses legais admissíveis para o tratamento:** As contribuições evidenciam que o consentimento dos pais ou responsáveis é a única das hipóteses legais empregadas pelos agentes de tratamento para o tratamento de dados biométricos de crianças e adolescentes (OP-1002117, OP-1006211). No entanto, outros contribuintes, em conformidade com o Enunciado CD/ANPD nº 1/2023, reconhecem que outras hipóteses legais trazidas pelo art. 11, da LGPD podem ser utilizadas, desde que o melhor interesse da criança seja o princípio orientador e preponderante (OP-1005725, OP-1005718, OP-1005612). As hipóteses mais citadas, incluem o cumprimento de obrigação legal ou regulatória, a proteção da vida ou incolumidade física do titular e a prevenção à fraude.
- **Necessidade e proporcionalidade:** Parte das contribuições frisa que o tratamento é admissível quando demonstrada sua necessidade real diante de riscos concretos, e não é possível alterar qualquer condição de ordem técnica. Para isso, sugerem que a escolha da tecnologia deve ser precedida por análise de risco, demonstrando que o uso é proporcional, necessário e mais eficaz que alternativas menos intrusivas (OP-1005718).
- **Proibição de usos específicos:** Certas contribuições requerem a proibição do uso de determinadas tecnologias em situações específicas, como por exemplo, a obtenção de informações acerca do estado emocional de alunos por meio de sistemas de reconhecimento facial, sob o risco de vigilância coercitiva, o que impede o livre desenvolvimento da personalidade (art. 2º, VII da LGPD). Contrariamente, outras contribuições afirmam que não há impedimento normativo para o emprego de tecnologias específicas. Logo, qualquer atuação da ANPD no sentido de impedir o uso dessas tecnologias violaria os princípios da legalidade e da livre concorrência (OP-969104, OP-1005024).

6.75. Há consonância quanto em relação à necessidade de serem adotadas medidas de segurança, técnicas e administrativas, contudo, não foram identificadas menções a medidas específicas a serem aplicadas aos grupos vulneráveis. Em contrapartida, há divergência quanto à utilização de outras hipóteses legais que não a do consentimento para o tratamento de dados pessoais de grupos vulneráveis. Por conta dessa limitação, existem contribuições que sugerem a restrição do uso de determinadas tecnologias para o tratamento de dados biométricos de indivíduos vulneráveis, especialmente de crianças e adolescentes, sendo que outras afirmam que tal restrição pode gerar eventuais abusos cometidos pelo Estado e desincentivo ao mercado.

Pergunta 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?

6.76. Considerando a natureza dos dados biométricos e o risco de coleta excessiva, a pergunta teve por objetivo entender a ponderação entre os fatores que influenciam a verificação ou estimação de idade e como compatibilizar tal operação a fim de atender ao princípio do melhor interesse.

Pontos convergentes:

- **Alternativas não biométricas:** Parte das contribuições alega que o uso de dados biométricos para verificação de idade de crianças e adolescentes deve ser considerado uma medida excepcional, utilizada apenas quando indispensável e não existirem alternativas menos invasivas com eficácia similar (OP-963578, OP-1005635). Isso decorre de uma interpretação do princípio da necessidade (art. 6º, III da LGPD) aliada ao princípio do melhor interesse estendido aos meios e instrumentos necessários ao tratamento dos dados pessoais, especialmente, os biométricos. Nesse sentido, algumas contribuições alertam que a biometria não é precisa para verificação de idade, especialmente na infância e adolescência, devido à alteração natural de traços físicos, o que pode gerar riscos de erro, discriminação e restrição indevida de direitos. Como alternativas, citou-se a autodeclaração ou o uso de documentos para comprovação de idade (OP-966032, OP-966760, OP-967368, OP-967752).
- **Transparência aos titulares e seus responsáveis legais:** Com diversas remissões à pergunta 15, os contribuintes reiteraram a importância da transparência em todo o processo de tratamento de dados, inclusive no método empregado para a verificação de idade. Assim, destacam que devem ser fornecidas informações claras, acessíveis e adequadas à idade, sobre a finalidade do tratamento, os riscos, a natureza dos dados tratados, o tempo de retenção e os canais para exercício dos direitos dos titulares (OP-1006217, OP-1002117).
- **Contexto do tratamento e tecnologia empregada:** As contribuições enfatizam que a verificação de idade deve levar em conta o contexto em que o tratamento de dados ocorre (Samsung, OP-1005871). Para isso, argumentam para a necessidade de considerar os riscos envolvidos na utilização de determinada plataforma e as finalidades específicas do tratamento de dados biométricos. Por exemplo, serviços como a oferta de jogos com interação *online*, podem justificar o uso de biometria facial, visto que o serviço pode ser considerado de alto risco, enquanto os de baixo risco, como o acesso a notícias, newsletters, etc., podem ser atendidos por autodeclaração.

Pontos divergentes:

- **Risco de soluções biométricas para estimação de idade**: Há contribuições (OP-969154) que argumentam que a estimação de idade é feita a partir de um sistema de categorização biométrica. Por isso, o risco seria menor, e,

consequentemente, não haveria barreiras ao tratamento de dados biométricos para a verificação de idade. Como a idade, por si só, não é considerada como dado sensível pela legislação de proteção de dados, o nível de risco associado a essa prática seria baixo, uma vez que o sistema não procederia com comparações, reduzindo a chance de erros. Por fim, citou-se que o *AI Act*, nos termos do Anexo III, 1 (a), prevê que verificação biométrica (1:1) não é vista como sistema de alto risco.

- **Autonomia dos agentes de tratamento na escolha de tecnologias**: Há a defesa de que os agentes de tratamento devem ter autonomia para implementar as tecnologias que entenderem válidas e adequadas para verificação de idade, evitando soluções padronizadas para garantir o equilíbrio entre eficácia e privacidade. Isso deve ser feito após uma análise de riscos e potenciais impactos aos titulares (OP-1005627, OP-1005260, OP-1006068). Em contraponto, diversas contribuições enfatizam a necessidade de que as plataformas sejam obrigadas a adotar soluções já consolidadas no mercado, a partir da criação de diretrizes específicas pela ANPD (OP-969154, OP-969488). Contribuintes ressaltam que essa é a prática de autoridades estrangeiras como o ICO, conforme estabelecido no *Children's Code*[1], que criou critérios rigorosos para o emprego de tecnologias baseadas em dados biométricos. Assim, argumenta-se no sentido de limitar a autonomia das empresas e impor a padronização de tecnologias para conformidade com a LGPD.

6.77. As contribuições destacaram a priorização de alternativas menos invasivas à biometria para a verificação de idade, em respeito ao princípio da necessidade, assegurando transparência e informações adequadas aos titulares e responsáveis legais. Em adição, reafirmou-se a necessidade de observar o contexto do tratamento e a precisão da tecnologia utilizada no tratamento como critérios a serem considerados para verificação e estimação de idade. Contudo, persistem divergências quanto à avaliação do risco associado ao uso de soluções biométricas e à autonomia dos agentes de tratamento na escolha das tecnologias, com contribuições defendendo tanto liberdade de escolha quanto a imposição de diretrizes pela ANPD para uniformização e, consequentemente, maior proteção aos titulares dos dados pessoais.

7. DOCUMENTOS RELACIONADOS

- Anexo Contribuição (SEI/ANPD nº 0212868);
- Anexo Contribuição (SEI/ANPD nº 0212869);
- Anexo Contribuição (SEI/ANPD nº 0212878);
- Anexo Contribuição (SEI/ANPD nº 0212880);
- Anexo Contribuição (SEI/ANPD nº 0212887);

- Anexo Contribuição (SEI/ANPD nº 0212888);
- Anexo Contribuição (SEI/ANPD nº 0212889);
- Anexo Contribuição (SEI/ANPD nº 0212890);
- Anexo Contribuição (SEI/ANPD nº 0212892);
- Anexo Contribuição (SEI/ANPD nº 0212894);
- Anexo Contribuição (SEI/ANPD nº 0212895);
- Anexo Contribuição (SEI/ANPD nº 0212897);
- Anexo Contribuição (SEI/ANPD nº 0212899);
- Anexo Contribuição (SEI/ANPD nº 0212901);
- Anexo Contribuição (SEI/ANPD nº 0212903);
- Anexo Contribuição (SEI/ANPD nº 0212904);
- Anexo Contribuição (SEI/ANPD nº 0212905);
- Anexo Contribuição (SEI/ANPD nº 0212906);
- Anexo Contribuição (SEI/ANPD nº 0212907);
- Anexo Contribuição (SEI/ANPD nº 0212908);
- Anexo Contribuição (SEI/ANPD nº 0212909);
- Anexo Contribuição (SEI/ANPD nº 0212910);
- Anexo Contribuição (SEI/ANPD nº 0212911);
- Anexo Contribuição (SEI/ANPD nº 0212912);
- Anexo Contribuição (SEI/ANPD nº 0212913);
- Anexo Contribuição (SEI/ANPD nº 0212914);
- Anexo Contribuição (SEI/ANPD nº 0212915);
- Anexo Contribuição (SEI/ANPD nº 0212917);
- Anexo Contribuição (SEI/ANPD nº 0212918);
- Anexo Contribuição (SEI/ANPD nº 0212919);
- Anexo Contribuição (SEI/ANPD nº 0212920);
- Anexo Contribuição (SEI/ANPD nº 0212921);
- Anexo Contribuição (SEI/ANPD nº 0212922);
- Anexo Contribuição (SEI/ANPD nº 0212923);
- Anexo Contribuição (SEI/ANPD nº 0212924);
- Anexo Contribuições da Plataforma Participa + Brasil (SEI/ANPD nº 0212926).

8. CONCLUSÃO

8.1. Tendo em vista todos os pontos aqui destacados, sugere-se que a presente Nota Técnica conste como insumo para os trabalhos e atividades a

serem realizados no âmbito do Projeto - Item 5 da Agenda Regulatória para o biênio 2025-2026 da ANPD e, também, sirva para a consolidação da instrução processual referente ao citado projeto regulatório.

8.2. Nesses termos, sugere-se, ainda, encaminhar o presente documento, junto com seus anexos, à Secretaria-Geral do Conselho Diretor, para conhecimento dos membros deste Colegiado.

À consideração superior.

Brasília/DF, *na data de sua assinatura.*

JEANE TORELLI CARDOSO
Empregada pública requisitada pela ANPD

BRUNA ARMONAS COLOMBO
Servidora Pública requisitada pela ANPD

GUILHERME FERREIRA MACHADO
Assessor Técnico na Coordenação-Geral de Normatização

CAROLINE CHUCRE KAPPEL
Servidora pública requisitada pela ANPD
Coordenadora de Normatização I

De acordo. Encaminha-se o processo para a Secretaria-Geral.

Brasília/DF, *na data de sua assinatura.*

RODRIGO SANTANA DOS SANTOS
Coordenador-Geral de Normatização

---

[1] 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/

Documento assinado eletronicamente por **Guilherme Ferreira Machado**, **Assessor(a) Técnico(a)**, em 21/11/2025, às 15:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jeane Torelli Cardoso**, **Servidor(a) Requisitado(a)-ANPD**, em 21/11/2025, às 15:53, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Bruna Armonas Colombo**, **Servidor(a) Requisitado(a)-ANPD**, em 21/11/2025, às 17:32, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Caroline Nazaré dos Santos Chucre Kappel**, **Coordenador(a)**, em 25/11/2025, às 11:01, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)-Geral de Normatização**, em 26/11/2025, às 09:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0227479** e o código CRC **23BDE7D3**.

SCN Quadra 06, Ed. Venâncio 3000, Bloco A, 9º andar - Bairro Asa Norte, Brasília/DF, CEP 70716-900
Telefone: (61) 2017-3338 / 3339 - https://www.gov.br/anpd/pt-br