Contribuições do CNPD à Agenda Regulatória da ANPD (2027–2028)

Este documento consolida as contribuições encaminhadas pelos membros do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), em sua segunda composição, com o objetivo de subsidiar a elaboração da Agenda Regulatória da Agência Nacional de Proteção de Dados (ANPD) para o biênio 2027–2028, tal como aprovado em Reunião Extraordinária do Conselho, realizada em 25 de junho de 2026.

A Agenda Regulatória da ANPD constitui instrumento de planejamento que orienta sua atuação normativa ao longo do período, definindo temas prioritários, formas de atuação e o cronograma das iniciativas regulatórias, em conformidade com as competências previstas na Lei Geral de Proteção de Dados Pessoais (LGPD).

Considerando a competência consultiva do CNPD, prevista no art. 3º, inciso II, do Decreto nº 12.881/2026, bem como sua participação na elaboração da Agenda Regulatória, nos termos do art. 7º, § 2º, da Portaria nº 16, de 8 de junho de 2021, o Conselho apresenta suas contribuições institucionais ao processo regulatório conduzido pela ANPD.

Os Conselheiros do CNPD encaminharam à ANPD 7 (sete) propostas de temas a serem considerados na Agenda Regulatória, abrangendo, entre outros, os seguintes eixos: relações de trabalho; prevenção a fraudes; certificação e boas práticas; proteção de crianças e adolescentes; uso de biometria; inteligência artificial; governança, segurança e bases legais; além de acesso a dados e responsabilidades de provedores.

As contribuições são apresentadas, na sequência, em ordem alfabética de autoria dos Conselheiros que as submeteram.

A Conselheira Ana Paula Bialer (setor privado) apresenta duas propostas. A primeira trata da regulamentação de selos, certificados e códigos de conduta, com base nos arts. 33, II, "d", 50, §§ 3º e 4º, e 55-J, XIII, da LGPD. Tem duas dimensões. Uma é a operacionalização da hipótese de transferência internacional baseada nesses instrumentos, que permanece sem regulamentação mesmo após a Resolução CD/ANPD nº 19/2024 ter disciplinado as cláusulas contratuais padrão e as normas corporativas globais. A outra é o reconhecimento, pela ANPD, de regras de boas práticas e de governança (art. 50, §§ 3º e 4º), que funcionaria como certificação de conformidade verificável externamente. O prazo sugerido é de Fase 4.

A segunda proposta trata da densificação regulatória dos fundamentos do art. 4º da Lei nº 15.211/2025 (ECA Digital) aplicáveis ao tratamento de dados de crianças e adolescentes, com ênfase na prevalência absoluta de seus interesses (inciso II) e na condição peculiar de pessoa em desenvolvimento biopsicossocial (inciso III). A Conselheira sugere a edição de guia orientativo, com parâmetros para diferenciar obrigações por faixa etária e para equilibrar a proteção reforçada com o acesso a serviços digitais benéficos ao desenvolvimento, em prazo de Fase 1.

A Conselheira Ana Paula Canto de Lima (setor científico) propõe a inclusão de tema voltado ao uso de biometria em estádios de futebol, arenas esportivas, clubes, programas de sócio-torcedor e plataformas de venda de ingressos. O dado biométrico é dado pessoal sensível, e seu tratamento nesses ambientes ocorre em larga escala, com circulação de grande volume de pessoas, atuação de múltiplos agentes públicos e privados e presença frequente de crianças e adolescentes. A Conselheira recomenda que a ANPD edite diretrizes próprias sobre a definição dos agentes de tratamento, a base legal aplicável, o Relatório de Impacto à Proteção de Dados Pessoais, os deveres de transparência, os padrões mínimos de segurança, a indicação de encarregado, os prazos de retenção, a eliminação dos dados e as regras de compartilhamento com terceiros ou autoridades públicas. A proposta inclui tratamento específico da proteção de crianças e adolescentes e busca harmonizar a aplicação da Lei Geral do Esporte com a LGPD.

A Conselheira Débora Sirotheau (setor laboral) apresenta duas propostas, ambas amparadas no art. 55-J da LGPD. A primeira trata da regulamentação do tratamento de dados pessoais nas relações de trabalho. Parte da assimetria estrutural entre empregador e trabalhador, que limita a validade do consentimento, do uso de tecnologias de monitoramento, automação e inteligência artificial, e da insuficiência de mecanismos de transparência e governança no ambiente laboral. O escopo sugerido cobre as bases legais aplicáveis, os limites do monitoramento e do uso de tecnologias, a transparência e o exercício de direitos, e a governança ao longo do ciclo de vida da relação de trabalho, nas fases pré-contratual, contratual e pós-contratual, além de mecanismos de participação coletiva por meio de ACTs e CCTs. A Conselheira sugere uma primeira fase de guia orientativo em até 12 meses e uma segunda fase de eventual norma específica no ciclo 2027–2028. A segunda proposta trata do uso de dados pessoais na prevenção a fraudes e golpes. Reconhece a dupla função do dado pessoal nesse contexto, como vetor de risco e como instrumento de prevenção, e aponta a ausência de diretrizes sobre proporcionalidade, uso de dados sensíveis e inferenciais, compartilhamento e interoperabilidade, segurança da informação e decisões automatizadas. O prazo sugerido segue o mesmo modelo de duas fases.

A Conselheira Isabella Henriques (sociedade civil), com apoio da equipe do Alana, propõe consolidar a proteção de crianças e adolescentes como eixo transversal da atuação regulatória da ANPD, por meio de quatro iniciativas. A primeira é a incorporação expressa das salvaguardas do art. 14 da LGPD na regulamentação dos direitos dos titulares, com transparência adequada à idade, procedimentos para o exercício de direitos por adolescentes segundo a autonomia progressiva e mecanismos de contestação de decisões automatizadas e de perfilização. A segunda é o desenvolvimento de Avaliações de Impacto sobre Direitos de Crianças e Adolescentes (CRIA) e o aprimoramento do Relatório de Impacto previsto no art. 16 do ECA Digital, com revisão do critério cumulativo de alto risco fixado pela Resolução CD/ANPD nº 2/2022. A terceira é a construção de parâmetros para os arts. 22, 25 e 26 do ECA Digital, que vedam a perfilização para exploração comercial e a criação de perfis comportamentais para publicidade direcionada a crianças e adolescentes. A quarta é a elaboração de diretrizes de design ético e preventivo, ancoradas no dever de prevenção do art. 70 do ECA e no art. 8º do ECA Digital, sobre configuração protetiva por padrão e mitigação de funcionalidades que estimulam uso excessivo, problemático ou compulsivo.

O Conselheiro João Brant (governo) apresenta três propostas, todas relacionadas a competências regulatórias atribuídas à ANPD por normas recentes. A primeira trata da caracterização da falha sistêmica quanto ao dever de cuidado dos provedores de aplicações de internet que intermedeiam conteúdo de terceiros (art. 16-B do Decreto nº 12.975, de 20 de maio de 2026), com regulamentação dos aspectos materiais (§§ 1º e 3º) e dos aspectos processuais (§§ 2º e 4º) de sua aferição. A segunda trata do acesso de instituições acadêmicas, científicas, tecnológicas, de inovação e jornalísticas aos dados de provedores de aplicações direcionadas a crianças e adolescentes (art. 31, parágrafo único, da Lei nº 15.211/2025), cuja habilitação cabe à ANPD por força do Decreto nº 12.880/2026. A terceira trata da devida diligência dos provedores que disponibilizam, mediante pagamento, ferramentas de anúncio ou impulsionamento de conteúdo (art. 16-K do Decreto nº 12.975/2026), com definição das medidas adequadas para vedar a contratação de conteúdo que configure crime ou ato ilícito.

O Conselheiro Rodrigo Valadão (sociedade civil), em contribuição da govDADOS, reúne dez proposições selecionadas por três critérios: lacuna regulatória verificável, recorrência do tema no debate técnico e complementaridade com as demais contribuições do Conselho. Duas delas incorporam diagnósticos dos Grupos de Trabalho do CNPD que coordenou, o GT1 (Educação e Capacitação) e o GT3 (Coordenação Interinstitucional). As proposições são: (1) criação da Escola Nacional de Proteção de Dados (ENAD); (2) regulamentação do sistema de acreditação, certificados e selos (arts. 33, II, "d", e 50); (3) tratamento secundário e

interoperabilidade de dados, inclusive nas bases públicas no âmbito do Governo Digital; (4) parâmetros para monetização e patrimonialização de dados pessoais; (5) densificação da hipótese de legítimo interesse (arts. 7º, IX, e 10); (6) anonimização, pseudonimização e padrão jurídico de risco de reidentificação (art. 12); (7) padrões mínimos de segurança (art. 46, § 1º); (8) decisões automatizadas e direito à explicação (art. 20); (9) regime de transição para regularização de bases de dados legadas; e (10) uso de dados pessoais no treinamento de sistemas de IA. Cada proposição traz a respectiva sugestão de priorização por fases.

O Conselheiro Rony Vainzof (setor empresarial) apresenta seis temas em ordem de prioridade, sob a premissa de que segurança jurídica também é proteção de direitos e de que a regulação deve ser preventiva, proporcional e baseada em risco. São eles: (1) tratamento de dados pessoais no ciclo de vida da inteligência artificial, com bases legais para treinamento de modelos, uso de legítimo interesse e de dados sensíveis para mitigação de viés, e web scraping; (2) exercício dos direitos dos titulares, com procedimentos, prazos, autenticação, hipóteses de negativa e atendimento em escala; (3) anonimização e pseudonimização, com critérios de risco de reidentificação e tratamento de dados sintéticos; (4) regras de boas práticas e governança, com autorregulação regulada, certificações e efeitos na dosimetria; (5) medidas de segurança técnicas e administrativas, sob a premissa de que a segurança é obrigação de diligência e não de resultado; e (6) as hipóteses legais de legítimo interesse e consentimento, com teste de balanceamento e critérios de validade da manifestação do titular. O Conselheiro indica ainda sete temas adicionais em ordem de prioridade: tratamento de dados de crianças e adolescentes, Relatório de Impacto à Proteção de Dados Pessoais, proteção ao crédito, agregadores de dados pessoais, tratamento de dados de alto risco, moderação de conteúdo diante da nova competência da ANPD e transferência internacional de dados.

As sete contribuições partem de perspectivas setoriais distintas, mas convergem em alguns eixos. O mais recorrente é a proteção de dados de crianças e adolescentes, presente nas propostas de Ana Paula Bialer, Ana Paula Canto de Lima, Isabella Henriques, João Brant e Rony Vainzof, com pontos comuns na densificação dos fundamentos do ECA Digital, na avaliação de impacto e no design protetivo. Há convergência também na regulamentação de selos, certificados, códigos de conduta e regras de boas práticas (Ana Paula Bialer, Rodrigo Valadão e Rony Vainzof), na densificação do legítimo interesse e das demais hipóteses legais (Débora Sirotheau, Rodrigo Valadão e Rony Vainzof), na anonimização e no risco de reidentificação (Rodrigo Valadão e Rony Vainzof), nos padrões mínimos de segurança (Rodrigo Valadão e Rony Vainzof) e no regime das decisões automatizadas, da perfilização e do direito à explicação (Isabella Henriques, João Brant, Rodrigo Valadão e Rony Vainzof). A inteligência artificial atravessa várias propostas, da definição de bases

legais para treinamento de modelos ao uso de dados sensíveis para mitigação de viés. Em todas elas reaparece a mesma orientação de regulação preventiva, baseada em risco e capaz de oferecer segurança jurídica antes que as lacunas sejam preenchidas por litígios, fiscalizações ou sanções.

Essa convergência entre representantes do setor privado, do setor científico, do setor laboral, da sociedade civil, do governo e do setor empresarial reflete o papel do CNPD na formação de consensos sobre a agenda de proteção de dados. Reunir em um mesmo documento prioridades de origens tão diferentes, e identificar onde elas coincidem, oferece à ANPD um diagnóstico plural para o planejamento de sua atuação normativa. Esse planejamento demonstra a necessidade de que a Agência equilibre, em sua agenda, as frentes da LGPD e do ECA Digital com as novas atribuições trazidas pelos decretos regulamentadores do Marco Civil da Internet (Decretos nº 12.975/2026 e nº 12.976/2026), de modo que a expansão de suas competências não comprometa a continuidade dos temas já em curso.

As contribuições reproduzidas neste documento são de autoria individual de cada Conselheiro e refletem posições pessoais e setoriais de quem as subscreve. Elas não resultam de deliberação ou votação majoritária do Conselho sobre o mérito de cada proposta. A aprovação em Reunião Extraordinária de 25 de junho de 2026 teve por objeto o encaminhamento conjunto das contribuições à ANPD, e não a adesão do colegiado ao conteúdo de cada uma. As convergências indicadas nos resumos descrevem coincidências temáticas entre propostas individuais e não devem ser lidas como posição consensual do Conselho.

O Conselho permanece à disposição da Agência para aprofundar qualquer das propostas, participar de grupos de trabalho, consultas públicas e tomadas de subsídios, e contribuir para a construção de uma agenda regulatória coerente para o biênio 2027–2028.

Victor Oliveira Fernandes

Presidente do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD)

Anexo - Contribuições dos Conselheiros

1. Conselheira Ana Paula Bialer (Setor Privado) ..... fl. 7
2. Conselheira Ana Paula Canto de Lima (Setor científico) ..... fl. 11
3. Conselheira Débora Sirotheau (Setor Laboral)..... fl. 13
4. Conselheira Isabella Henriques (Sociedade civil).....fl. 20
5. Conselheiro João Brant (Governo).....fl. 35
6. Conselheiro Rodrigo Valadão (Sociedade civil).....fl. 40
7. Conselheiro Rony Vainzof (Setor empresarial) ..... fl. 58

Contribuições

Agenda Regulatória da ANPD — Biênio 2027-2028

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Junho de 2026

As contribuições a seguir foram elaboradas nos termos da solicitação da CGAIC/SE/ANPD e observam o formato estruturado indicado para subsidiar a construção da Agenda Regulatória da ANPD para o biênio 2027-2028, compreendendo considerações sobre o processo regulatório e propostas temáticas para o próximo ciclo.

I. Considerações sobre o Processo Regulatório da ANPD

Antes de apresentar as contribuições temáticas para a Agenda Regulatória 2027-2028, entende-se oportuno registrar observações sobre aspectos do processo regulatório da ANPD que, ao longo dos últimos ciclos, têm impactado a qualidade e a efetividade da participação da sociedade.

A participação qualificada da sociedade no processo regulatório pressupõe que os contribuintes possam compreender de que forma suas manifestações influenciaram, ou não, a solução regulatória adotada. Recomenda-se que a ANPD publique, ao final de cada processo de tomada de subsídios ou consulta pública, relatório que identifique as principais contribuições recebidas, indique quais foram acolhidas e em que medida, e apresente justificativa para os pontos em que o posicionamento dos contribuintes não foi incorporado. Essa prática, adotada por autoridades de referência como o ICO (Reino Unido) e a CNIL (França), fortalece a confiança no processo regulatório e estimula a participação qualificada nos ciclos subsequentes.

II. Contribuições Temáticas para a Agenda Regulatória 2027-2028

CONTRIBUIÇÃO 1 — Selos, Certificados e Códigos de Conduta

Tema da iniciativa	Regulamentação de selos, certificados e códigos de conduta como mecanismos de transferência internacional de dados pessoais e como instrumentos autônomos de governança e accountability, nos termos dos arts. 33, II, 'd', 50, §§ 3º e 4º, e 55-J, XIII, da LGPD.
Identificação e descrição do problema	A Resolução CD/ANPD nº 19/2024 consolidou o regime brasileiro de transferência internacional de dados pessoais, regulamentando cláusulas contratuais padrão e normas corporativas globais. Contudo, uma das hipóteses expressamente previstas no art. 33, II, 'd', da LGPD (transferências baseadas em selos, certificados e códigos de conduta) permanece integralmente sem regulamentação, representando lacuna relevante no arcabouço de transferência internacional. Paralelamente, o art. 50, §§ 3º e 4º, da LGPD prevê que a ANPD pode reconhecer e divulgar regras de boas práticas e de governança formuladas por controladores e operadores, individualmente ou por meio de associações. Esse mecanismo, que funciona como certificação de conformidade verificável externamente, tampouco

	foi objeto de regulamentação específica em nenhuma das agendas regulatórias anteriores. A ausência de regulamentação nessas duas dimensões gera consequências práticas relevantes: impede que organizações utilizem selos e certificações internacionalmente reconhecidos como fundamento para transferências internacionais; priva o mercado de um instrumento de diferenciação e incentivo à adoção de boas práticas verificáveis; e deixa sem operacionalidade uma competência expressamente atribuída à ANPD pela LGPD.
Grupos afetados	Organizações brasileiras que transferem dados pessoais para o exterior e que utilizam, ou pretendem utilizar. selos e certificações como fundamento para essas transferências; associações setoriais e entidades de certificação interessadas no desenvolvimento de códigos de conduta reconhecidos pela ANPD; agentes de tratamento que buscam diferenciação competitiva mediante certificação de conformidade verificável; titulares de dados que se beneficiam de maior transparência e accountability no tratamento de seus dados.
Resultados e benefícios esperados	Conclusão do regime de transferência internacional iniciado pela Resolução CD/ANPD nº 19/2024, tornando operacional a hipótese do art. 33, II, 'd', da LGPD. Criação de um sistema de incentivos à adoção de boas práticas de proteção de dados, com reconhecimento formal pela ANPD como mecanismo de diferenciação e accountability. Estímulo ao desenvolvimento de um ecossistema de certificação no Brasil, alinhado a modelos internacionais de referência. Possibilidade de reconhecimento recíproco de certificações estrangeiras, facilitando a integração do Brasil em cadeias globais de valor digital.
Justificativa para intervenção regulatória	A competência para regulamentar selos, certificados e códigos de conduta é atribuída expressamente à ANPD pelos arts. 33, II, 'd', e 55-J, XIII, da LGPD. A ausência de regulamentação configura omissão que deixa sem efetividade instrumentos legalmente previstos e amplamente utilizados em jurisdições de referência. Trata-se, ademais, de tema que foi sinalizado em contribuições apresentadas à ANPD em ciclos regulatórios anteriores, mas que nunca foi formalmente incluído na agenda. O biênio 2027-2028 representa o momento oportuno para seu endereçamento, após a consolidação dos mecanismos contratuais de transferência internacional e da regulamentação de boas práticas e governança prevista na Agenda 2025-2026.
Escopo e prazo	Escopo: (i) regulamentação da hipótese de transferência internacional baseada em selos, certificados e códigos de conduta (art. 33, II, 'd'), incluindo requisitos mínimos, procedimento de aprovação pela ANPD e possibilidade de reconhecimento de instrumentos estrangeiros equivalentes; (ii) regulamentação do procedimento de reconhecimento e divulgação de regras de boas práticas e de governança pela ANPD (art. 50, §§ 3º e 4º), com definição de critérios de avaliação, modelo de autoridade certificadora e periodicidade de atualização. Prazo sugerido: início do processo regulatório em até 2 anos da aprovação da Agenda 2027-2028 (Fase 4).

CONTRIBUIÇÃO 2 — Densificação Regulatória dos Fundamentos do ECA Digital Aplicáveis ao Tratamento de Dados de Crianças e Adolescentes

Tema da iniciativa	Densificação regulatória dos fundamentos estabelecidos no art. 4º da Lei nº 15.211/2025 (ECA Digital) para o tratamento de dados pessoais de crianças e adolescentes, com ênfase na prevalência absoluta de seus interesses (inciso II) e na condição peculiar de pessoa em desenvolvimento biopsicossocial (inciso III), e suas implicações para obrigações de proteção de dados.
Identificação e descrição do problema	A Agenda Regulatória 2025-2026 avança na regulamentação operacional do ECA Digital — escopo de aplicação e obrigações gerais (Item 13), mecanismos de aferição de idade (Item 15) e fiscalização e sanção (Item 14). Contudo, os fundamentos que devem orientar a interpretação e a aplicação de toda essa normativa, previstos no art. 4º do ECA Digital, carecem de densificação regulatória específica. Dois fundamentos apresentam especial relevância para o tratamento de dados pessoais e demandam operacionalização pela ANPD: o inciso II — prevalência absoluta dos interesses de crianças e adolescentes, equivalente ao princípio do melhor interesse consagrado na Convenção sobre os Direitos da Criança — e o inciso III — condição peculiar de pessoa em desenvolvimento biopsicossocial, que impõe diferenciação de tratamento conforme a faixa etária e o grau de maturidade. A ausência de densificação desses fundamentos gera consequências práticas relevantes: agentes de tratamento não dispõem de parâmetros para avaliar se suas práticas são compatíveis com o melhor interesse de crianças e adolescentes; não há critérios que diferenciem obrigações aplicáveis a crianças (até 12 anos) e adolescentes (12 a 18 anos) à luz do desenvolvimento biopsicossocial; e o equilíbrio entre proteção reforçada e acesso a serviços digitais benéficos ao desenvolvimento, educação, cultura, saúde, permanece indefinido, favorecendo interpretações excessivamente restritivas que podem comprometer direitos de acesso à informação e à participação digital. Para alem da densificação dos conceitos, importante que a ANPD possa avançar em orientações mais concretas sobre a mecânica, padrões e interoperabilidade na cadeia de informações sobre aferição etária, um tema desafiador sobre uma perspectiva técnica. Ademais, guias da autoridade que enderecem o entendimento da Agência sobre as práticas abusivas, padrões obscuros e demais aspectos da implementação do safety by design são importantes para harmonizar a implementação da lei.
Grupos afetados	Crianças e adolescentes como titulares de dados e usuários de serviços digitais; pais e responsáveis legais; fornecedores de produtos e serviços de tecnologia da informação sujeitos ao ECA Digital; desenvolvedores de aplicações voltadas ao público infantojuvenil; agentes de tratamento que ofertam serviços educacionais, culturais e de saúde digital; ANPD na qualidade de autoridade administrativa autônoma de proteção dos direitos de crianças e adolescentes no ambiente digital

	(Decreto nº 12.622/2025); demais órgãos do Sistema de Garantia de Direitos de Crianças e Adolescentes.
Resultados e benefícios esperados	Criação de arcabouço interpretativo que oriente a aplicação coerente de toda a regulamentação do ECA Digital, conferindo previsibilidade e segurança jurídica ao ecossistema. Definição de parâmetros para avaliação do melhor interesse de crianças e adolescentes, reduzindo litigiosidade e interpretações divergentes. Orientação sobre diferenciação de obrigações por faixa etária, reconhecendo a condição peculiar de pessoa em desenvolvimento e a autonomia progressiva como critérios relevantes. Delimitação do equilíbrio entre proteção reforçada e acesso a serviços digitais, evitando restrições que prejudiquem o desenvolvimento e a inclusão digital de crianças e adolescentes. Alinhamento com melhores práticas internacionais, em especial o Children's Code do ICO (Reino Unido).
Justificativa para intervenção regulatória	O art. 4º do ECA Digital estabelece os fundamentos que devem orientar toda a utilização de produtos ou serviços de tecnologia da informação por crianças e adolescentes. Sem a densificação desses fundamentos pela ANPD toda a normativa subsequente será interpretada e aplicada sem balizas claras, gerando inconsistências e potencial esvaziamento das proteções legalmente previstas.. A intervenção regulatória neste tema é condição para que o Brasil construa um regime de proteção de crianças e adolescentes no ambiente digital que seja ao mesmo tempo robusto, proporcional e alinhado aos compromissos internacionais assumidos pelo país.
Escopo e prazo	Escopo: guia orientativo abordando: (i) definição operacional da prevalência absoluta dos interesses de crianças e adolescentes (art. 4º, II), com parâmetros para sua aplicação; (ii) implicações da condição peculiar de pessoa em desenvolvimento biopsicossocial (art. 4º, III) para a diferenciação de obrigações por faixa etária; (iii) critérios para o equilíbrio entre proteção reforçada e acesso a serviços digitais benéficos ao desenvolvimento; (iv) articulação dos demais fundamentos do art. 4º. Prazo sugerido: início do processo regulatório em até 12 meses da aprovação da Agenda 2027-2028 (Fase 1), preferencialmente em coordenação com os resultados da regulamentação dos itens 13, 14 e 15 da Agenda 2025-2026.

Outlook

Sugestão de inclusão de tema

De Ana Paula Canto de Lima <anapaula@cantodelima.com.br>
Data Qua, 24/06/2026 12:45
Para CGAIC-ANPD - Coordenação-Geral de Articulação Interna e Apoio aos Colegiados <cgaic.se@anpd.gov.br>

Prezados, boa tarde, desejo que se encontrem bem. Favor acusar o recebimento!

Considerando que estou em viagem de férias, peço licença para contribuir no corpo do e-mail, visto que não tenho condições adequadas para proceder de maneira diversa no momento. Desde já agradeço a compreensão! Contribuo em tempo de aproveitar a extensão de prazo concedida na última reunião do Conselho.

Sugiro a inclusão do tema específico voltado ao tratamento de dados em estádios de futebol, arenas esportivas, clubes, programas de sócio-torcedor e plataformas de venda de ingressos, especialmente no que se refere aos dados biométricos.

A proposta se justifica diante do avanço do uso de reconhecimento facial e de sistemas de cadastramento biométrico para controle de acesso de torcedores, identificação de frequentadores, prevenção de fraudes, segurança nos eventos esportivos e cumprimento de obrigações legais relacionadas à organização de partidas de futebol.

Embora tais tecnologias possam contribuir para a segurança pública, para a gestão de grandes eventos e para a modernização do acesso aos estádios, é preciso reconhecer que a biometria não é um dado comum. Trata-se de dado pessoal sensível, capaz de identificar de forma única uma pessoa natural. Por essa razão, sua coleta, armazenamento, compartilhamento e eventual cruzamento com outras bases de dados devem observar critérios rigorosos de necessidade, proporcionalidade, transparência, segurança e responsabilização.

No contexto dos estádios, a preocupação é ainda maior porque há tratamento em larga escala, circulação de grande volume de pessoas, participação de múltiplos agentes privados e públicos, contratação de empresas terceirizadas de tecnologia, eventual integração com sistemas de segurança e presença frequente de crianças e adolescentes. Esse conjunto de fatores transforma o tema em matéria de alto risco regulatório e exige atuação preventiva da ANPD.

A ausência de parâmetros claros pode gerar insegurança jurídica tanto para os titulares quanto para clubes, federações, administradores de arenas, empresas de bilhetagem e fornecedores de tecnologia. Sem orientação específica, há risco de coleta excessiva de dados, retenção por prazo indeterminado, falta de informação adequada ao torcedor, compartilhamento indevido, dificuldade no exercício dos direitos dos titulares, muitas vezes ausência de encarregado, além do uso da biometria, com possibilidade de uso para finalidades diferentes das originalmente informadas.

Por isso, recomenda-se que a ANPD estabeleça diretrizes próprias para o uso de dados, incluindo a

biometria em ambientes esportivos, especialmente quanto à definição dos agentes de tratamento, à base legal aplicável, à elaboração de Relatório de Impacto à Proteção de Dados Pessoais, aos deveres de transparência, aos padrões mínimos de segurança da informação, indicacao de um encarregado, sendo apontado prazos de retenção, à eliminação dos dados e às regras para eventual compartilhamento com terceiros ou autoridades públicas.

Também é fundamental que a futura orientação trate, de forma específica, da proteção de crianças e adolescentes. A presença de menores em estádios é comum, seja como torcedores, dependentes de sócios, alunos de escolinhas, atletas de base ou participantes de eventos esportivos. Assim, qualquer sistema biométrico que envolva esse público deve observar o princípio do melhor interesse, a proteção integral e a necessidade de informação clara aos pais ou responsáveis.

A inclusão do tema permitiria à ANPD atuar de forma orientativa e preventiva, evitando que a expansão dessas tecnologias ocorra sem salvaguardas adequadas. Além disso, contribuiria para harmonizar a aplicação da Lei Geral do Esporte com a LGPD, deixando claro que eventual obrigação de cadastramento ou identificação não elimina a necessidade de respeito aos princípios da LGPD.

Dessa forma, a regulamentação do uso de biometria em estádios de futebol deve ser compreendida como medida necessária para garantir segurança jurídica, proteção dos direitos fundamentais dos torcedores e desenvolvimento responsável da tecnologia e inovação no ambiente esportivo.

A proposta não busca impedir o uso de soluções biométricas, ou que os dados pessoais sejam tratados, tampouco impedir a inovação ou dificultar a economia, mas assegurar que o tratamento seja realizado de forma transparente, proporcional, segura e compatível com a legislação brasileira de proteção de dados.

Att,

CANTO DE LIMA
ADVOCACIA

ANA PAULA CANTO DE LIMA
Advogada

Tel./WhatsApp: (81) 99750-1315
e-mail: anapaula@cantodelima.com.br

CONTRIBUIÇÃO 1 — Proteção de dados pessoais no contexto laboral

1. **Tema da iniciativa**

Regulamentação do tratamento de dados pessoais no contexto das relações de trabalho, com definição de parâmetros específicos para aplicação da LGPD em relações laborais, considerando suas particularidades estruturais, jurídicas e operacionais.

2. **Identificação e descrição do problema**

O tratamento de dados pessoais no contexto laboral apresenta características próprias que impactam diretamente a aplicação adequada da LGPD.

Destacam-se, entre os principais desafios:

- a **assimetria estrutural** entre empregador e trabalhador, que compromete a liberdade da manifestação de vontade e limita a validade do consentimento como base legal;
- o **uso intensivo de tecnologias de monitoramento, automação e inteligência artificial**, com potencial de afetar a privacidade, a autodeterminação informativa e a dignidade do trabalhador;
- a **insuficiência de mecanismos de transparência, governança e *accountability***, dificultando o exercício efetivo dos direitos dos titulares no ambiente laboral.

A ausência de balizas regulatórias específicas favorece práticas desproporcionais, amplia o risco de tratamentos discriminatórios e dificulta a harmonização entre inovação tecnológica e proteção de direitos fundamentais.

3. **Grupos afetados pela implementação do projeto**

- trabalhadores, em relações formais, informais e novas formas de contratação (incluindo plataformas digitais);
- empregadores dos setores público e privado;
- entidades representativas (sindicatos e associações);
- órgãos de fiscalização e regulação (ANPD, Ministério do Trabalho e Emprego e Ministério Público do Trabalho).

4. **Resultados e benefícios esperados**

- maior **segurança jurídica** na aplicação da LGPD no contexto laboral;
- redução de **litígios e assimetrias interpretativas**;

- fortalecimento da **governança e da *accountability*** nas organizações;
- ampliação da **transparência e do exercício efetivo de direitos** pelos trabalhadores;
- promoção de **equilíbrio entre inovação tecnológica e proteção de direitos fundamentais**.

5. Justificativa para necessidade de intervenção regulatória

Embora a LGPD seja aplicável às relações de trabalho, o contexto laboral exige tratamento regulatório específico, considerando:

- a **limitação estrutural do consentimento** em relações marcadas por subordinação;
- a ausência de parâmetros claros sobre **monitoramento, vigilância e decisões automatizadas**;
- o risco de **tratamentos abusivos, discriminatórios ou desproporcionais**.

Nos termos do art. 55-J da LGPD, compete à ANPD editar normas, diretrizes e boas práticas, especialmente em contextos de maior risco aos titulares.

A atuação regulatória permitirá conferir **previsibilidade, proporcionalidade e efetividade** à aplicação da LGPD nas relações de trabalho.

6. Escopo sugerido

Elaboração de instrumento regulatório e/ou guia orientativo contemplando:

• Bases legais no contexto laboral

- definição de parâmetros para aplicação das bases legais no tratamento de dados pessoais de trabalhadores;
- especial atenção às limitações do consentimento, considerando a assimetria estrutural da relação laboral;
- critérios para utilização de outras bases legais, como obrigação legal, execução de contrato e legítimo interesse, com observância dos princípios da finalidade, necessidade e proporcionalidade.

• Monitoramento e uso de tecnologias

- estabelecimento de limites, condições e salvaguardas para práticas de monitoramento e vigilância no ambiente de trabalho;

- definição de parâmetros para uso de inteligência artificial e decisões automatizadas, incluindo critérios de transparência, revisão e mitigação de vieses;
- delimitação de práticas admissíveis e vedadas, especialmente em contextos de alto risco à dignidade e aos direitos fundamentais dos trabalhadores.

• Transparência e direitos dos titulares

- definição de critérios para prestação de informações claras, acessíveis e contextualizadas no ambiente laboral;
- estabelecimento de meios eficazes para o exercício de direitos pelos trabalhadores, considerando as especificidades da relação de subordinação;
- diretrizes para comunicação contínua e adequada ao contexto organizacional.

• Governança e gestão de riscos

- adoção de abordagem baseada no ciclo de vida da relação laboral, contemplando:

a) Fase pré-contratual

  - critérios para tratamento de dados em processos seletivos e recrutamento;
  - limites para coleta de dados, verificação de antecedentes e uso de dados inferenciais;
  - observância dos princípios da minimização e da transparência.

b) Fase contratual

  - parâmetros para o tratamento de dados necessários à execução do contrato de trabalho;
  - limites e salvaguardas para monitoramento, controle de atividades e uso de tecnologias no ambiente laboral;
  - critérios para utilização de sistemas de avaliação, perfilização e decisões automatizadas;
  - diretrizes para transparência contínua e exercício de direitos pelos trabalhadores durante a relação laboral;

c) Fase pós-contratual

- definição de critérios para retenção, eliminação e anonimização de dados pessoais;
- limites para reutilização de dados após o término do vínculo;
- parâmetros para compartilhamento de informações e manutenção de registros para cumprimento de obrigações legais;

• Participação coletiva

- incentivo à adoção de mecanismos de diálogo social, participação de entidades representativas;
- estímulo à construção de soluções pactuadas e boas práticas setoriais para o tratamento de dados no ambiente laboral através da celebração de instrumentos coletivos como ACTs e CCTs.

7. **Prazo sugerido:**

- **Fase 1 — Guia orientativo (até 12 meses)**
  publicação de guia interpretativo com parâmetros iniciais e boas práticas;
- **Fase 2 — Evolução regulatória (ciclo 2027–2028)**
  eventual elaboração de norma específica, conforme maturidade do tema e evidências regulatórias.

8. **Considerações finais**

A regulamentação do tratamento de dados pessoais no contexto laboral é medida necessária para assegurar a adequada aplicação da LGPD em um ambiente marcado por assimetrias estruturais e crescente uso de tecnologias.

A iniciativa permitirá compatibilizar proteção de dados, relações de trabalho e inovação, promovendo maior segurança jurídica e um ambiente laboral mais transparente e equilibrado.

CONTRIBUIÇÃO 2 — Prevenção de fraudes e golpes com uso de dados pessoais

1. Tema da iniciativa

Regulamentação do tratamento de dados pessoais em contextos de prevenção a fraudes digitais, com definição de parâmetros para uso proporcional, eficaz e responsável de dados pessoais em atividades antifraude.

2. Identificação e descrição do problema

A crescente digitalização das relações sociais e econômicas tem sido acompanhada pela sofisticação das fraudes digitais, com uso intensivo de:

- engenharia social e exploração do fator humano;
- manipulação de identidades digitais;
- tecnologias emergentes, como inteligência artificial e deepfakes.

Nesse contexto, os dados pessoais assumem dupla função:

- como **vetor de risco**, quando utilizados para a prática de fraudes;
- como **instrumento essencial de prevenção**, ao permitir identificação, autenticação e mitigação de riscos.

Apesar dessa centralidade, persistem limitações relevantes:

- **fragmentação informacional e baixa interoperabilidade** entre setores público e privado;
- ausência de **diretrizes regulatórias específicas** para uso de dados em atividades antifraude;
- **incerteza quanto à aplicação das bases legais**;
- riscos associados ao uso de **dados sensíveis, inferenciais e decisões automatizadas**.

Esse cenário reduz a efetividade das iniciativas de prevenção e gera insegurança jurídica para agentes de tratamento.

3. Grupos afetados pela implementação do projeto

- titulares de dados pessoais, como beneficiários diretos da redução de fraudes;
- agentes de tratamento públicos e privados (instituições financeiras, empresas de tecnologia, órgãos públicos);

- autoridades reguladoras e de segurança;
- ecossistema digital como um todo.

4. Resultados e benefícios esperados

- maior **segurança jurídica** para uso de dados em atividades antifraude;
- utilização mais **eficiente, proporcional e responsável** dos dados pessoais;
- aumento da efetividade na **prevenção, detecção e resposta a fraudes**;
- fortalecimento da **cooperação interinstitucional**;
- aumento da **confiança no ambiente digital**.

5. Justificativa para necessidade de intervenção regulatória

Embora a LGPD preveja bases legais aplicáveis — como legítimo interesse e prevenção à fraude —, não há parâmetros claros quanto a:

- proporcionalidade, necessidade e minimização no uso de dados;
- utilização de **dados biométricos e inferenciais**;
- **compartilhamento e interoperabilidade segura**;
- governança e responsabilização;
- uso de **inteligência artificial e decisões automatizadas**.

Nos termos do art. 55-J da LGPD, cabe à ANPD estabelecer diretrizes em contextos de maior risco.

A regulamentação permitirá harmonizar proteção de dados, segurança da informação e interesse público, promovendo maior efetividade na prevenção de fraudes.

6. Escopo e prazo para implementação

Escopo sugerido:

Elaboração de diretrizes regulatórias e/ou guia orientativo contemplando:

- **Uso de dados em atividades antifraude**
    - parâmetros para aplicação das bases legais e uso de dados biométricos e inferenciais;
- **Compartilhamento e cooperação institucional**

- diretrizes para intercâmbio seguro e interoperável de dados;

- **Segurança da informação**
  - requisitos mínimos de medidas técnicas e administrativas;
- **Governança e gestão de riscos**
  - incentivos a programas estruturados e RIPD;
- **Inteligência artificial e decisões automatizadas**
  - parâmetros de transparência, explicabilidade e mitigação de vieses;
- **Educação e cultura de prevenção**
  - ações de conscientização e capacitação.

7. Prazo sugerido:

- **Fase 1 — Guia orientativo (até 12 meses)**
  publicação de orientações técnicas e parâmetros iniciais;
- **Fase 2 — Evolução regulatória (ciclo 2027–2028)**
  eventual regulamentação estruturada, com atualização contínua conforme evolução tecnológica.

8. Considerações finais

A regulamentação do uso de dados pessoais em atividades antifraude é estratégica para enfrentar a crescente complexidade dos ilícitos digitais.

A definição de parâmetros claros permitirá equilibrar proteção de dados e segurança, promovendo um ambiente digital mais seguro, confiável e resiliente.

CONTRIBUIÇÃO CONSELHEIRA ISABELA HENRIQUES

TOMADA DE SUBSÍDIOS SOBRE REVISÃO DA AGENDA REGULATÓRIA 2027-2028

JUNHO DE 2026

Apoio pela Equipe Alana:

Júlia Mendonça

SUMÁRIO

CONSOLIDAÇÃO DA PROTEÇÃO DE CRIANÇAS E ADOLESCENTES COMO EIXO TRANSVERSAL DA ATUAÇÃO REGULATÓRIA DA ANPD..... 2

1. Proteção de dados de crianças e adolescentes como dimensão transversal da regulamentação dos direitos dos titulares da LGPD..... 2

1.2 Tabela com respostas aos tópicos propostos por email..... 3

2. Avaliações de Impacto sobre Direitos de Crianças e Adolescentes (CRIA) e aprimoramento do Relatório de Impacto à Proteção de Dados previsto no ECA Digital... 4

2.1 Tabela com respostas aos tópicos propostos por email..... 6

3. Proteção de crianças e adolescentes contra exploração comercial a partir da perfilização e sistemas algorítmicos.....8

3.1 Tabela com respostas aos tópicos propostos por email..... 9

4. Diretrizes de Design Ético e Preventivo para a Proteção de Crianças e Adolescentes no Ambiente Digital..... 11

4.1 Tabela com respostas aos tópicos propostos por email..... 12

CONSOLIDAÇÃO DA PROTEÇÃO DE CRIANÇAS E ADOLESCENTES COMO EIXO TRANSVERSAL DA ATUAÇÃO REGULATÓRIA DA ANPD

1. Proteção de dados de crianças e adolescentes como dimensão transversal da regulamentação dos direitos dos titulares da LGPD

A proteção de dados pessoais de crianças e adolescentes não se limita às disposições específicas da Lei nº 15.211/2025 (ECA Digital), devendo constituir eixo transversal de toda a atuação regulatória da ANPD..

Embora a LGPD assegure a todos os titulares um conjunto de direitos relacionados à transparência, acesso, correção, eliminação, portabilidade e revisão de decisões automatizadas (previstos nos artigos 9º, 18, 19, 20 e 23 da LGPD), o artigo 14 estabelece salvaguardas específicas para o tratamento de dados de crianças e adolescentes, reconhecendo sua condição de titulares em situação de desenvolvimento e hipervulnerabilidade. O dispositivo introduz obrigações qualificadas, como o princípio da necessidade (§4º) e o dever de transparência (§2º e §6º), que demandam parâmetros próprios de aplicação.

Desse modo, a regulamentação dos direitos dos titulares deve incluir expressamente o artigo 14, garantindo que as diretrizes da ANPD contemplem as especificidades da proteção de dados de crianças e adolescentes.

A experiência regulatória nacional e internacional demonstra que o simples reconhecimento formal de direitos não é suficiente para assegurar sua efetiva fruição. Em muitos casos, mecanismos de exercício de direitos são desenvolvidos para adultos e pressupõem

capacidades cognitivas, informacionais e técnicas incompatíveis com diferentes estágios do desenvolvimento infantojuvenil.

Nesse sentido, a Agenda Regulatória 2027-2028 representa oportunidade para que a ANPD aprofunde a regulamentação dos direitos dos titulares à luz das disposições do artigo 14 da LGPD, promovendo maior concretude ao princípio do melhor interesse e à prioridade absoluta assegurada pelo artigo 227 da Constituição Federal.

Recomenda-se, nesse contexto, que a Agência desenvolva orientações específicas relacionadas a:

- transparência adequada à idade, considerando diferentes níveis de desenvolvimento e capacidade de compreensão;
- utilização de linguagem acessível, recursos visuais e mecanismos pedagógicos destinados à comunicação com crianças e adolescentes;
- parâmetros para prestação de informações em ambientes digitais utilizados predominantemente ou provavelmente por crianças e adolescentes;
- procedimentos para exercício de direitos por adolescentes, observando sua autonomia progressiva e capacidade crescente de participação nas decisões relacionadas ao tratamento de seus dados pessoais;
- critérios para harmonização entre o exercício de direitos por crianças e adolescentes e a atuação de pais, mães ou responsáveis legais;
- mecanismos específicos para contestação de decisões automatizadas, sistemas de recomendação e processos de perfilização que afetem crianças e adolescentes;
- boas práticas voltadas à promoção da participação significativa de crianças e adolescentes em processos relacionados à governança de seus dados pessoais.

1.2 Tabela com respostas aos tópicos propostos por email

RESPOSTAS AOS TÓPICOS PROPOSTOS

Proteção de dados de crianças e adolescentes como dimensão transversal da regulamentação dos direitos dos titulares

- **Tema da iniciativa**

Regulamentação dos direitos dos titulares de dados pessoais com incorporação expressa das salvaguardas previstas no art. 14 da LGPD para crianças e adolescentes.

- **Identificação e descrição do problema**

Embora a LGPD assegure direitos a todos os titulares de dados pessoais, a regulamentação vigente ainda não contempla de forma suficiente as especificidades do

tratamento de dados de crianças e adolescentes. Os mecanismos de transparência, acesso, correção, eliminação, portabilidade e revisão de decisões automatizadas foram concebidos predominantemente para usuários adultos, desconsiderando diferentes níveis de desenvolvimento cognitivo, autonomia progressiva e necessidades de comunicação adequadas à idade.

- **Grupos afetados pela implementação do projeto**
  - Crianças e adolescentes;
  - Pais, mães e responsáveis legais;
  - Plataformas digitais, aplicações de internet e provedores de serviços digitais;
  - Controladores e operadores que tratam dados de crianças e adolescentes;
  - Órgãos de proteção e defesa de direitos.

- **Resultados e benefícios esperados**
  - Maior efetividade dos direitos previstos na LGPD;
  - Ampliação da transparência adequada à idade;
  - Redução de barreiras ao exercício de direitos por crianças e adolescentes;
  - Harmonização entre autonomia progressiva e supervisão parental;
  - Maior segurança jurídica para agentes de tratamento.
  - Justificativa para necessidade de intervenção por meio de regulamentação

- **Escopo e prazo para implementação**

Elaboração de guia orientativo e/ou regulamento específico no ciclo 2027-2028, contemplando transparência adequada à idade, exercício de direitos por adolescentes, participação infantil e contestação de decisões automatizadas.

2. Avaliações de Impacto sobre Direitos de Crianças e Adolescentes (CRIA) e aprimoramento do Relatório de Impacto à Proteção de Dados previsto no ECA Digital

A Lei nº 15.211/2025 (ECA Digital) estabelece, em seu artigo 16, a obrigatoriedade de elaboração de relatórios de impacto, monitoramento e avaliação da proteção de dados pessoais em hipóteses específicas envolvendo crianças e adolescentes. Trata-se de importante ponto de destaque legislativo que reforça a centralidade da prevenção de riscos e da responsabilização dos agentes de tratamento na proteção desse público.

Atualmente, os instrumentos de avaliação de impacto previstos no âmbito da proteção de dados concentram-se predominantemente na análise de riscos à privacidade e à proteção de dados pessoais. Embora tais dimensões sejam essenciais, elas não esgotam os potenciais impactos produzidos por sistemas digitais sobre crianças e adolescentes.

Produtos e serviços digitais podem gerar efeitos significativos sobre o desenvolvimento cognitivo, emocional e social, influenciar processos decisórios, ampliar vulnerabilidades

decorrentes da idade, estimular padrões de uso compulsivo, afetar a autonomia progressiva, interferir na liberdade de expressão e participação, bem como impactar direitos relacionados à saúde, educação, convivência familiar e proteção contra exploração econômica.

Por essa razão, recomenda-se que a ANPD priorize a construção de diretrizes específicas para avaliações de impacto voltadas à proteção dos direitos de crianças e adolescentes, inspiradas em modelos internacionais de Avaliações de Impacto sobre Direitos de Crianças e Adolescentes (CRIA), amplamente utilizados por organismos internacionais e autoridades reguladoras que atuam na promoção dos direitos da infância em ambientes digitais.

A incorporação de elementos próprios de avaliações de impacto sobre direitos da criança permitirá que os agentes de tratamento realizem análises mais abrangentes, capazes de identificar não apenas riscos à privacidade, mas também potenciais impactos sobre o conjunto de direitos assegurados pelo artigo 227 da Constituição Federal, pelo Estatuto da Criança e do Adolescente, pela Convenção sobre os Direitos da Criança e pela Lei Geral de Proteção de Dados Pessoais.

Nesse mesmo sentido, a Resolução CD/ANPD nº 2/2022 atualmente condiciona a obrigatoriedade do RIPD à presença cumulativa de dois critérios de alto risco, sendo o tratamento de dados de crianças e adolescentes apenas um deles. A incorporação do modelo CRIA no âmbito do ECA Digital pode, portanto, aperfeiçoar o regime regulatório vigente, garantindo uma avaliação de riscos mais protetiva e condizente com o dever de prevenção e o princípio da prioridade absoluta estabelecidos pela Constituição Federal, pela LGPD e pelo ECA Digital.

A construção de diretrizes específicas para avaliações de impacto também contribuirá para conferir maior segurança jurídica aos agentes regulados, promovendo maior previsibilidade quanto às expectativas regulatórias da ANPD e reduzindo assimetrias na implementação das obrigações previstas pelo ECA Digital.

Nesse sentido, sugere-se a inclusão, na Agenda Regulatória 2027-2028, de iniciativa voltada à elaboração de parâmetros normativos, guias orientativos ou modelos referenciais para avaliações de impacto sobre direitos de crianças e adolescentes, contemplando, entre outros aspectos:

- identificação dos riscos específicos decorrentes do tratamento de dados pessoais de crianças e adolescentes;
- avaliação dos impactos potenciais sobre direitos fundamentais além da proteção de dados pessoais, incluindo desenvolvimento, saúde, educação, proteção contra exploração econômica, participação e autonomia progressiva;
- critérios para aferição de necessidade, adequação e proporcionalidade do tratamento;
- parâmetros para avaliação de sistemas algorítmicos e mecanismos automatizados de recomendação e personalização;

- análise de riscos decorrentes da utilização de dados biométricos, mecanismos de aferição etária e tecnologias emergentes;
- mecanismos de mitigação, monitoramento contínuo e revisão periódica dos riscos identificados;
- procedimentos para documentação e demonstração de conformidade com os princípios do melhor interesse, da proteção integral e da prioridade absoluta.

2.1 Tabela com respostas aos tópicos propostos por email

RESPOSTAS AOS TÓPICOS PROPOSTOS

Avaliações de Impacto sobre Direitos de Crianças e Adolescentes (CRIA) e aprimoramento do Relatório de Impacto à Proteção de Dados (RIPD)

- **Tema da iniciativa**

Desenvolvimento de parâmetros regulatórios para avaliações de impacto sobre direitos de crianças e adolescentes (CRIA) e integração com o Relatório de Impacto à Proteção de Dados (RIPD) previsto na LGPD e no ECA Digital.

- **Identificação e descrição do problema**

O artigo 16 da Lei nº 15.211/2025 (ECA Digital) introduziu a obrigatoriedade de elaboração de relatórios de impacto, monitoramento e avaliação da proteção de dados pessoais em hipóteses específicas envolvendo crianças e adolescentes. Contudo, os instrumentos atualmente existentes concentram-se predominantemente na análise de riscos à privacidade e à proteção de dados pessoais, sem contemplar de forma adequada os impactos mais amplos que produtos e serviços digitais podem produzir sobre os direitos de crianças e adolescentes.

Além dos riscos relacionados à proteção de dados, tecnologias digitais podem afetar o desenvolvimento cognitivo, emocional e social, a autonomia progressiva, a participação, a saúde, a educação, a convivência familiar e a proteção contra exploração econômica. Apesar da relevância desses impactos, ainda não existem parâmetros regulatórios específicos capazes de orientar a elaboração de avaliações de impacto sob uma perspectiva abrangente de direitos da criança e do adolescente.

- **Grupos afetados pela implementação do projeto**
  - Crianças e adolescentes;
  - Pais, mães e responsáveis legais;
  - Desenvolvedores de tecnologias e plataformas digitais;
  - Controladores e operadores que tratam dados pessoais de crianças e adolescentes;

- Instituições educacionais;
- Órgãos reguladores, fiscalizatórios e integrantes do Sistema de Garantia de Direitos.
- Resultados e benefícios esperados
- Aprimoramento da prevenção e mitigação de riscos envolvendo crianças e adolescentes;
- Fortalecimento da accountability e da governança dos agentes de tratamento;
- Maior proteção dos direitos fundamentais de crianças e adolescentes no ambiente digital;
- Harmonização entre LGPD, ECA Digital e referenciais internacionais de proteção da infância;
- Incorporação do princípio da proteção integral e do melhor interesse da criança nos processos de avaliação de riscos.

- **Justificativa para necessidade de intervenção por meio de regulamentação**

Embora o artigo 16 do ECA Digital tenha estabelecido obrigação específica de elaboração de relatórios de impacto, ainda não existem parâmetros normativos ou orientações capazes de operacionalizar esse dever sob uma perspectiva abrangente de direitos da criança e do adolescente. Além disso, a Resolução CD/ANPD nº 2/2022 atualmente condiciona a obrigatoriedade do RIPD à presença cumulativa de critérios de alto risco, o que evidencia a necessidade de aperfeiçoamento do modelo regulatório para contemplar adequadamente as especificidades do tratamento de dados de crianças e adolescentes.

A regulamentação do tema permitirá conferir efetividade às obrigações já previstas no ECA Digital, promovendo avaliações mais completas e compatíveis com os princípios da proteção integral, da prioridade absoluta, do melhor interesse da criança e do dever de prevenção.

- **Escopo e prazo para implementação**

Elaboração de guia orientativo, template de referência e/ou regulamento específico no ciclo 2027-2028, contemplando critérios para avaliações de impacto sobre direitos de crianças e adolescentes (CRIA), integração com o RIPD previsto na LGPD e no ECA Digital, parâmetros para avaliação de riscos decorrentes de sistemas algorítmicos, mecanismos de recomendação, tecnologias biométricas, mecanismos de aferição etária e outras tecnologias emergentes, bem como procedimentos para mitigação, monitoramento contínuo e demonstração de conformidade.

3. Proteção de crianças e adolescentes contra exploração comercial a partir da perfilização e sistemas algorítmicos

A proteção de crianças e adolescentes no ambiente digital exige atenção crescente aos impactos produzidos por sistemas algorítmicos, mecanismos de recomendação, personalização de conteúdo e práticas de perfilização baseadas no tratamento massivo de dados pessoais, influenciando o acesso à informação, a exposição a conteúdos, as interações sociais, os padrões de consumo e os processos de tomada de decisão de crianças e adolescentes.

Visando endereçar tal problemática, o ECA digital estabeleceu limites expressos à exploração comercial de crianças e adolescentes por meio de seus dados pessoais. O artigo 22 veda expressamente a perfilização para fins de exploração comercial, enquanto o artigo 25 determina que provedores de redes sociais adotem regras específicas para o tratamento de dados de crianças e adolescentes, definidas de forma concreta, documentada e fundamentadas em seu melhor interesse. Complementarmente, o artigo 26 proíbe a criação de perfis comportamentais para fins de direcionamento de publicidade comercial, inclusive quando baseados em dados obtidos por mecanismos de verificação de idade ou em dados grupais e coletivos.

Nesse contexto, a Agenda Regulatória 2027-2028 constitui oportunidade para que a ANPD desenvolva orientações e parâmetros regulatórios destinados a conferir efetividade às obrigações já estabelecidas pelo ECA Digital, especialmente aquelas relacionadas à vedação da exploração comercial de crianças e adolescentes por meio de seus dados pessoais, à proibição da criação de perfis comportamentais para fins publicitários e ao dever de adoção de regras específicas para o tratamento de dados desse público. **Trata-se de comandos legais cogentes que demandam maior densificação regulatória para assegurar interpretação uniforme, aplicação consistente e fiscalização efetiva pelos agentes regulados e pela própria Autoridade.**

Recomenda-se, nesse sentido, a priorização de iniciativas destinadas à construção de parâmetros regulatórios relacionados a:

- a caracterização de práticas de perfilização e exploração comercial baseadas em dados pessoais de crianças e adolescentes;
- a utilização de sistemas de recomendação, personalização e segmentação baseados em dados comportamentais
- a realização de inferências algorítmicas relacionadas a interesses, preferências ou padrões de comportamento
- o emprego de métricas de engajamento como elemento de organização de experiências digitais acessadas por crianças e adolescentes;
- mecanismos de transparência e prestação de contas aplicáveis a sistemas automatizados; e

- critérios para avaliação e mitigação de riscos decorrentes da utilização de inteligência artificial e outros sistemas algorítmicos em produtos ou serviços de provável acesso por crianças e adolescentes.

3.1 Tabela com respostas aos tópicos propostos por email

RESPOSTAS AOS TÓPICOS PROPOSTOS

Proteção de crianças e adolescentes contra exploração comercial a partir da perfilização e sistemas algorítmicos

- **Tema da iniciativa**

Desenvolvimento de parâmetros regulatórios para implementação, interpretação e fiscalização das disposições do ECA Digital relacionadas à exploração comercial de crianças e adolescentes por meio de dados pessoais, perfilização, publicidade comportamental e sistemas algorítmicos.

- **Identificação e descrição do problema**

A proteção de crianças e adolescentes no ambiente digital exige atenção crescente aos impactos produzidos por sistemas algorítmicos, mecanismos de recomendação, personalização de conteúdo e práticas de perfilização baseadas no tratamento massivo de dados pessoais. Essas tecnologias influenciam diretamente o acesso à informação, a exposição a conteúdos, as interações sociais, os padrões de consumo e os processos de tomada de decisão de crianças e adolescentes.

Com o objetivo de enfrentar esses riscos, a Lei nº 15.211/2025 (ECA Digital) estabeleceu limites expressos à exploração comercial de crianças e adolescentes por meio de seus dados pessoais. O artigo 22 veda a perfilização para fins de exploração comercial, o artigo 25 determina que provedores de redes sociais adotem regras específicas para o tratamento de dados de crianças e adolescentes fundamentadas em seu melhor interesse, e o artigo 26 proíbe a criação de perfis comportamentais para fins de direcionamento de publicidade comercial, inclusive com base em dados obtidos por mecanismos de verificação de idade ou em dados grupais e coletivos.

Apesar da existência dessas disposições legais, permanecem desafios interpretativos e operacionais relacionados à caracterização de práticas de perfilização, à utilização de sistemas de recomendação e personalização, às inferências algorítmicas e aos mecanismos de exploração comercial baseados em dados pessoais, o que demanda maior densificação regulatória para garantir a efetividade das normas já vigentes.

- **Grupos afetados pela implementação do projeto**
  - Crianças e adolescentes;

- Pais, mães e responsáveis legais;
- Plataformas digitais e aplicações de internet;
- Provedores de redes sociais;
- Empresas de publicidade digital e tecnologia publicitária (adtech);
- Desenvolvedores de sistemas algorítmicos e de inteligência artificial;
- Controladores e operadores que tratam dados pessoais de crianças e adolescentes;
- Órgãos reguladores e fiscalizatórios.
- Resultados e benefícios esperados
- Maior efetividade das disposições previstas nos artigos 22, 25 e 26 do ECA Digital;
- Redução de práticas de exploração comercial baseadas no tratamento de dados pessoais de crianças e adolescentes;
- Maior transparência e prestação de contas na utilização de sistemas automatizados e algorítmicos;
- Fortalecimento da proteção da autonomia, do desenvolvimento e do melhor interesse de crianças e adolescentes;
- Maior segurança jurídica para agentes regulados quanto aos limites legais aplicáveis à perfilização e à publicidade comportamental;
- Harmonização entre a proteção de dados pessoais, a proteção integral e a regulação de sistemas algorítmicos.

- **Justificativa para necessidade de intervenção por meio de regulamentação**

Os artigos 22, 25 e 26 do ECA Digital estabelecem comandos legais cogentes destinados a restringir práticas de exploração comercial e perfilização de crianças e adolescentes. Contudo, a efetividade dessas disposições depende da construção de parâmetros regulatórios capazes de orientar sua interpretação, implementação e fiscalização.

A crescente utilização de sistemas de recomendação, personalização, segmentação comportamental e inteligência artificial em produtos e serviços digitais amplia a necessidade de orientações específicas sobre os limites do tratamento de dados pessoais de crianças e adolescentes. A regulamentação permitirá conferir maior segurança jurídica aos agentes regulados, reduzir assimetrias interpretativas e fortalecer a capacidade fiscalizatória da ANPD em matéria de proteção integral da infância e da adolescência no ambiente digital.

- **Escopo e prazo para implementação**

Elaboração de guia orientativo e/ou regulamento específico no ciclo 2027-2028, contemplando critérios para caracterização de práticas de perfilização e exploração comercial de crianças e adolescentes, parâmetros aplicáveis a sistemas de recomendação, personalização e segmentação comportamental, mecanismos de transparência e prestação de contas para sistemas automatizados, critérios para

avaliação e mitigação de riscos algorítmicos e orientações para implementação das obrigações previstas nos artigos 22, 25 e 26 do ECA Digital.

4. Diretrizes de Design Ético e Preventivo para a Proteção de Crianças e Adolescentes no Ambiente Digital

A Lei nº 15.211/2025 (ECA Digital) consolidou, no ambiente digital, uma lógica regulatória fortemente orientada pelo dever de prevenção, princípio historicamente consagrado por todo arcabouço de proteção jurídica da infância e adolescência e pelo artigo 70 do Estatuto da Criança e do Adolescente, segundo o qual é dever de todos prevenir a ocorrência de ameaça ou violação dos direitos da criança e do adolescente. Mais do que reagir a danos já consumados, o ordenamento jurídico brasileiro impõe a adoção de medidas capazes de identificar, reduzir e mitigar riscos antes que estes se concretizem, especialmente quando envolvem pessoas em condição peculiar de desenvolvimento.

Essa diretriz foi expressamente incorporada pelo ECA Digital ao estabelecer obrigações de governança preventiva aplicáveis aos fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes ou de acesso provável por eles. Em especial, o artigo 8º determina que tais agentes realizem o gerenciamento de riscos de recursos, funcionalidades e sistemas e de seus impactos sobre a segurança e a saúde de crianças e adolescentes, bem como desenvolvam, desde a concepção e adotem por padrão, configurações destinadas a evitar o uso compulsivo de produtos e serviços por esse público. Em conjunto, esses dispositivos evidenciam que a proteção integral deve ser incorporada desde as etapas de concepção, desenvolvimento, implementação e monitoramento de produtos e serviços digitais.

O Decreto regulamentador do ECA Digital avançou significativamente na concretização desses deveres ao estabelecer parâmetros relacionados à prevenção do uso excessivo, problemático ou compulsivo de produtos e serviços digitais, identificando mecanismos de incentivo ao engajamento excessivo, como a ocultação de pontos naturais de parada, a reprodução automática de conteúdos, recompensas associadas ao tempo de uso e notificações excessivas. O Decreto também reconheceu a necessidade de coibir práticas manipulativas, enganosas ou coercitivas que interfiram na autonomia decisória de crianças e adolescentes ou explorem suas vulnerabilidades cognitivas e etárias, além de prever obrigações específicas relacionadas à avaliação de riscos algorítmicos e à proteção do desenvolvimento físico, mental e psicossocial em sistemas capazes de interagir com usuários por meio de linguagem natural.

De igual modo, **merece destaque a interpretação construída pela própria ANPD no Guia de Fornecedores, que compreende o dever de prevenção como obrigação de atuação proativa e diligente ao longo de todo o ciclo de vida dos produtos e serviços, abrangendo dimensões complementares de prevenção, proteção, informação e segurança**. Trata-se de importante avanço regulatório que contribui para consolidar uma abordagem baseada em gestão contínua de riscos e proteção integral.

Não obstante os avanços já promovidos pela legislação, pelo Decreto e pelas iniciativas regulatórias em curso, permanece a oportunidade **de consolidar parâmetros mais estruturados de design ético voltados à proteção de crianças e adolescentes no ambiente digital.**

Nesse contexto, recomenda-se a inclusão, na Agenda Regulatória 2027-2028, de iniciativa destinada à elaboração de Diretrizes de Design Ético e Avaliação de Riscos para a Proteção Integral de Crianças e Adolescentes, acompanhadas de orientações e modelos referenciais capazes de apoiar a implementação das obrigações previstas no ECA Digital. A iniciativa não teria por objetivo substituir ou revisar os parâmetros já estabelecidos pela legislação e pelo Decreto, mas complementá-los mediante a sistematização de boas práticas, critérios de avaliação e instrumentos de demonstração de conformidade.

A iniciativa poderia contemplar, entre outros aspectos:

- parâmetros para configuração protetiva por padrão em produtos e serviços digitais acessados por crianças e adolescentes;
- diretrizes para identificação, avaliação e mitigação de funcionalidades suscetíveis de estimular uso excessivo, problemático ou compulsivo;
- orientações para prevenção de práticas manipulativas, enganosas ou coercitivas que interfiram na autonomia decisória de crianças e adolescentes;
- critérios para avaliação de riscos à saúde, à segurança, ao desenvolvimento e à privacidade decorrentes de recursos, funcionalidades e sistemas digitais;
- parâmetros para avaliação dos impactos produzidos por sistemas algorítmicos, mecanismos de recomendação, personalização e inteligência artificial;
- orientações relacionadas à transparência adequada à idade e à comunicação compatível com diferentes estágios de desenvolvimento;

4.1 Tabela com respostas aos tópicos propostos por email

RESPOSTAS AOS TÓPICOS PROPOSTOS

Diretrizes de Design Ético e Preventivo para a Proteção de Crianças e Adolescentes no Ambiente Digital

- **Tema da iniciativa**

Desenvolvimento de Diretrizes de Design Ético e Avaliação de Riscos para a Proteção Integral de Crianças e Adolescentes no Ambiente Digital, voltadas à implementação dos deveres de prevenção, proteção, informação e segurança previstos no Estatuto da Criança e do Adolescente, na LGPD e no ECA Digital.

Identificação e descrição do problema

A Lei nº 15.211/2025 (ECA Digital) consolidou uma abordagem regulatória baseada na prevenção de riscos e na incorporação da proteção integral desde a concepção de produtos e serviços digitais direcionados a crianças e adolescentes ou de provável acesso por eles. Em especial, o artigo 8º estabelece obrigações relacionadas ao gerenciamento de riscos de recursos, funcionalidades e sistemas, bem como à adoção, desde a concepção e por padrão, de medidas destinadas a evitar o uso compulsivo de produtos e serviços digitais.

O Decreto regulamentador do ECA Digital avançou significativamente na concretização desses deveres ao estabelecer parâmetros relacionados à prevenção do uso excessivo, problemático ou compulsivo, à mitigação de mecanismos de engajamento excessivo, à proibição de práticas manipulativas, enganosas ou coercitivas e à avaliação de riscos associados a sistemas algorítmicos e tecnologias de inteligência artificial. De igual modo, a própria ANPD vem desenvolvendo interpretação relevante sobre o dever de prevenção por meio do Guia de Fornecedores, compreendendo-o como obrigação contínua de gestão de riscos ao longo de todo o ciclo de vida dos produtos e serviços.

Apesar desses avanços, ainda inexistem referenciais regulatórios integrados capazes de orientar fornecedores quanto à implementação prática dessas obrigações, especialmente no que se refere à incorporação da proteção integral, da segurança, da saúde, da privacidade e do melhor interesse de crianças e adolescentes desde as etapas de concepção, desenvolvimento, implementação e monitoramento de tecnologias digitais.

- **Grupos afetados pela implementação do projeto**
    - Crianças e adolescentes;
    - Pais, mães e responsáveis legais;
    - Desenvolvedores de aplicativos, plataformas e serviços digitais;
    - Empresas de tecnologia e provedores de aplicações de internet;
    - Desenvolvedores e fornecedores de sistemas de inteligência artificial;
    - Controladores e operadores que tratam dados pessoais de crianças e adolescentes;
    - Órgãos reguladores, fiscalizatórios e integrantes do Sistema de Garantia de Direitos.
    - Resultados e benefícios esperados
    - Fortalecimento da cultura de prevenção de riscos e proteção integral no ambiente digital;
    - Maior efetividade das obrigações previstas no ECA Digital e em sua regulamentação;
    - Redução da exposição de crianças e adolescentes a mecanismos de uso excessivo, problemático ou compulsivo;
    - Mitigação de práticas manipulativas, enganosas ou coercitivas em ambientes digitais;
    - Promoção de produtos e serviços concebidos de forma compatível com o melhor interesse da criança e do adolescente;

- Maior previsibilidade regulatória e segurança jurídica para os agentes regulados;
- Fortalecimento da governança de riscos e da demonstração de conformidade por parte dos fornecedores.
- Justificativa para necessidade de intervenção por meio de regulamentação

O dever de prevenção constitui princípio estruturante do sistema brasileiro de proteção da infância e da adolescência, encontrando fundamento no artigo 70 do Estatuto da Criança e do Adolescente e sendo expressamente incorporado pelo ECA Digital. Embora a legislação, o Decreto regulamentador e os instrumentos orientativos já tenham estabelecido obrigações relevantes relacionadas à prevenção de riscos, proteção por padrão, segurança e mitigação de práticas nocivas, permanece a necessidade de consolidar parâmetros regulatórios que permitam sua implementação uniforme e efetiva.

A elaboração de diretrizes de design ético não visa substituir ou revisar as obrigações já previstas no ECA Digital, mas complementá-las por meio da sistematização de boas práticas, critérios de avaliação de riscos e instrumentos de demonstração de conformidade. A iniciativa permitirá conferir maior efetividade aos deveres legais já existentes, promovendo maior segurança jurídica para os agentes regulados e fortalecendo a capacidade de monitoramento e fiscalização da ANPD.

- **Escopo e prazo para implementação**

Elaboração de guia orientativo, parâmetros regulatórios ou instrumento normativo complementar no ciclo 2027-2028, contemplando diretrizes de design ético e proteção por padrão, critérios para identificação e mitigação de funcionalidades que estimulem uso excessivo, problemático ou compulsivo, parâmetros para prevenção de práticas manipulativas, enganosas ou coercitivas, critérios para avaliação de riscos à saúde, segurança, desenvolvimento e privacidade, orientações para avaliação de impactos de sistemas algorítmicos e inteligência artificial, bem como mecanismos de demonstração de conformidade compatíveis com as obrigações previstas no ECA Digital e em sua regulamentação.

Falha sistêmica (Decreto MCI, art. 16-B)

• Tema da iniciativa proposta:

Definição da caracterização de falha sistêmica quanto ao dever de cuidado dos provedores de aplicações de internet que realizem a intermediação de conteúdo gerado por terceiro (decreto nº 12.975, de 20 de maio de 2026)

• Identificação e descrição do problema a ser enfrentado:

O decreto nº 12.975 apresenta, no art. 16-B, elementos para a incorrência em falha sistêmica e para avaliar a sua ocorrência.

O dispositivo prevê, em seu § 1º, que incorre em falha sistêmica o provedor que não comprovar a adoção de medidas adequadas de prevenção ou remoção de um rol taxativo de conteúdos ilícitos, que forneçam os níveis mais elevados de segurança para o tipo de serviço que oferecem e que inibam a circulação massiva desses conteúdos ilícitos. Já o § 3º prevê que a existência de conteúdos de forma isolada não caracteriza falha sistêmica. Esses dois parágrafos fornecem, portanto, elementos materiais para a avaliação de ocorrência de falha sistêmica passíveis de regulamentação pela ANPD.

O § 2º prevê que a autoridade competente deve avaliar a ocorrência de falha sistêmica por meio de mecanismos de supervisão e análise periódica e o § 4º que os provedores de aplicações de internet deverão disponibilizar às autoridades competentes as informações e os dados que permitam verificar a incorrência de falha sistêmica. Esses dois parágrafos contêm elementos processuais para a avaliação de ocorrência de falha sistêmica, sujeitos a regulamentação pela ANPD.

• Grupos potencialmente afetados pela implementação da iniciativa:

Provedores de aplicações de internet que realizem intermediação de conteúdo gerado por terceiros.

Usuários desses provedores de aplicações de internet.

• Resultados e benefícios esperados:

A regulamentação da matéria pode assegurar maior efetividade à indisponibilização dos conteúdos ilícitos previstos no art. 16-B do decreto nº 12.975.

• Justificativa para a necessidade de intervenção regulatória pela ANPD:

O detalhamento dos parâmetros previstos no decreto pode dar maior efetividade à proteção de direitos fundamentais em ambientes digitais.

• Escopo da proposta e prazo estimado para sua implementação:

Regulamentação dos aspectos materiais de incorrência de falha sistêmica (art. 16-B, § 1º e § 3º): (i) “medidas adequadas de prevenção e remoção”, (ii) níveis mais elevados de segurança, apresentando tipologia de serviço oferecido, (iii) o que configura circulação massiva e sua inibição.

Regulamentação dos aspectos processuais de incorrência em falha sistêmica (art. 16-B, § 2º e § 4º): (i) definição dos mecanismos de supervisão e análise periódica e (ii) especificação das informações e dados a serem fornecidos pelos provedores, e da forma e periodicidade de seu fornecimento.

Acesso a dados para pesquisa (ECA Digital, art. 31)

• Tema da iniciativa proposta:

Acesso de instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas a dados de provedores de aplicações de internet direcionadas a crianças e adolescentes (art. 31, parágrafo único, da lei nº 15.211, de 17 de setembro de 2025).

• Identificação e descrição do problema a ser enfrentado:

O art. 31, parágrafo único, do ECA Digital, prevê que instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas possam acessar os dados de provedores de aplicações de internet que sejam necessários para pesquisar os impactos dos produtos e serviços nos direitos e crianças e adolescentes. O dispositivo determina, ainda, que regulamento definirá os critérios e requisitos para o fornecimento desses dados por parte dos provedores.

Já decreto 12.880, de 18 de março de 2026, que regulamenta o ECA Digital, prevê que a ANPD habilitará as instituições para acesso aos dados previstos na lei e apresenta critérios para tal habilitação.

• Grupos potencialmente afetados pela implementação da iniciativa:

Provedores de aplicações de internet direcionadas a crianças e adolescentes

Crianças e adolescentes

Pais, mães e responsáveis legais

Pesquisadores

• Resultados e benefícios esperados:

A regulamentação do acesso a dados dos provedores de aplicações de internet é fundamental para compreender como seus produtos e serviços afetam os direitos de crianças e adolescentes, para garantir o exercício desses direitos e para a fiscalização do cumprimento da lei nº 15.211 (ECA Digital).

• Justificativa para a necessidade de intervenção regulatória pela ANPD:

A lei (art. 31, parágrafo único) prevê expressamente a necessidade de regulamentação do tema.

• Escopo da proposta e prazo estimado para sua implementação:

Regulamentação de quais dados deverão ser acessados e a forma como deverá se dar esse acesso.

Publicidade programática e devida diligência

• Tema da iniciativa proposta:

Devida diligência dos provedores que disponibilizem ferramentas para anúncio ou impulsionamento de conteúdo (art. 16-K do decreto nº 12.975, de 20 de maio de 2026).

• Identificação e descrição do problema a ser enfrentado:

O art. 16-K do decreto nº 12.975, de 20 de maio de 2026 prevê que "os provedores de aplicações de internet que, mediante pagamento, disponibilizem ferramentas para anúncio ou impulsionamento de conteúdo adotarão medidas adequadas para vedar a contratação de conteúdo que configure crime ou ato ilícito". A regulamentação pela ANPD pode detalhar quais medidas são consideradas adequadas na vedação de tal contratação.

• Grupos potencialmente afetados pela implementação da iniciativa:

Provedores de aplicações de internet que realizem intermediação de conteúdo gerado por terceiros.

Usuários desses provedores de aplicações de internet.

• Resultados e benefícios esperados:

Redução da disseminação e do conteúdo de conteúdos que configurem crimes ou atos ilícitos em ambientes digitais.

• Justificativa para a necessidade de intervenção regulatória pela ANPD

Ferramentas de anúncio e de impulsionamento permitam que conteúdos criminosos e ilícitos sejam distribuídos pelos provedores de aplicações de internet a um número maior de pessoas, que podem ser potenciais vítimas. Portanto, a adoção de medidas

pelos provedores que disponibilizam tais ferramentas é importante para a proteção de direitos e o enfrentamento a crimes e ilícitos na internet.

- Escopo da proposta e prazo estimado para sua implementação.

Definição de quais medidas os provedores de aplicações de internet devem adotar ao fornecerem ferramentas de anúncio e impulsionamento pago e qual nível aceitável de ocorrência de publicidade de fraudes, golpes, de produtos e serviços ilícitos ou de publicidade abusiva.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

Contribuições para a Agenda Regulatória da ANPD (Biênio 2027–2028)

Rodrigo Borges Valadão
Representante da Sociedade Civil
Associado Fundador da govDADOS
Conselheiro do CNPD | Membro do CCGD

Brasília, 24 de junho de 2026

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Sumário

1. Introdução **3**

2. Contribuições **3**

2.1. Escola Nacional de Proteção de Dados (ENAD) 4

2.2. Sistema de Acreditação, Certificados e Selos 5

2.3. Tratamento Secundário e Interoperabilidade 6

2.4. Monetização e Patrimonialização de Dados Pessoais 8

2.5. Hipótese Legal do Legítimo Interesse 9

2.6. Anonimização, Pseudonimização e Padrão Jurídico de Risco de Reidentificação 10

2.7. Padrões Mínimos de Segurança 11

2.8. Decisões Automatizadas, Perfilização e Direito à Explicação (artigo 20 da LGPD) 12

2.9. Regime de Transição e Regularização de Bases de Dados Legadas 13

2.10. Bases Legais para Treinamento de Modelos e interface com IA 15

3. Agenda Regulatória Proposta **16**

4. Considerações Finais **17**

gov DADOS

1. Introdução

Em resposta à tomada de subsídios da CGAIC/SE/ANPD, a Associação Brasileira de Governança de Dados (govDADOS) apresenta dez proposições temáticas para a Agenda Regulatória (biênio 2027-28) da Agência Nacional de Proteção de Dados (ANPD), de acordo com o modelo estruturado indicado.[1]

A seleção observou três critérios cumulativos: (i) lacuna regulatória verificável (ou seja, uma competência atribuída à ANPD pela LGPD ou por norma superveniente ainda não exercida); (ii) recorrência do tema no debate técnico-acadêmico e nos balanços institucionais da ANPD; e (iii) complementaridade com as contribuições dos demais conselheiros, indicando uma efetiva *zona de convergência* com as propostas aqui sustentadas. Duas proposições incorporam, ainda, os diagnósticos dos Grupos de Trabalho do CNPD coordenados pelo proponente: o GT1 (Educação e Capacitação)[2] e o GT3 (Coordenação Interinstitucional e Eficiência Administrativa).[3]

2. Contribuições

As proposições estão dispostas em sequência temática, sem hierarquia de prioridade entre si, de modo a permitir leitura e avaliação autônomas. Elas formam um conjunto articulado em três eixos: (i) institucional e de governança (itens 1 e 2), com foco na educação, capacitação e no sistema de certificação; (ii) circuitos e hipóteses específicos de tratamento (itens 3, 4 e 5), endereçando o tratamento secundário, a monetização de dados e a densificação do legítimo interesse; e (iii) desafios regulatórios emergentes (itens 6 a 10), como (a) padrões técnicos e de

[1] Nota metodológica: O presente relatório foi elaborado com o auxílio de ferramentas de inteligência artificial generativa, utilizadas como suporte à pesquisa, à organização das informações e à redação inicial dos textos. Ademais, todas as proposições foram elaboradas em observância à diretriz da regulação preventiva, baseada em risco e orientada por evidências, em consonância com os princípios da boa regulação inscritos na Lei n.º 13.848/2019, cujo alcance foi reforçado pela conversão da ANPD em agência reguladora (Lei n.º 15.352/2026). A perspectiva comparada com o GDPR foi adotada, quando necessário, não como modelo a ser transplantado acriticamente, mas como parâmetro metodológico para identificar lacunas, avaliar alternativas regulatórias e antecipar desafios que o sistema brasileiro terá de enfrentar em horizonte próximo.

[2] GT1 – Educação e Capacitação em Proteção de Dados. Relatório Final (v.1.2). CNPD, 20.02.2025. Coordenação: Rodrigo Borges Valadão.

[3] GT3 – Coordenação Interinstitucional e Eficiência Administrativa da ANPD. Relatório Final. CNPD, 02.06.2026. Coordenação: Rodrigo Borges Valadão; instituído pela Portaria CNPD n.º 03/2025. A dimensão da coordenação interinstitucional (autoridade condutora e prevenção do bis in idem) foi incorporada transversalmente aos itens 2.3 e 2.7.

segurança (anonimização, riscos de reidentificação e padrões mínimos de segurança, (b) decisões automatizadas e direito à explicação, (c) regularização de bases legadas e (d) regulamentação das bases legais para treinamento de IA.

2.1. Escola Nacional de Proteção de Dados (ENAD)

A primeira contribuição propõe a criação da Escola Nacional de Proteção de Dados (ENAD), instituição dedicada a ser o ponto focal da ANPD em relação à educação e capacitação em proteção de dados pessoais para cidadãos, profissionais e servidores públicos (fase 2).

Tema: Eixo estruturante de educação e capacitação na Política Nacional de Proteção de Dados (Item 10 da Agenda vigente), materializado na criação da Escola Nacional de Proteção de Dados (ENAD).

Problema: Baixa maturidade e assimetria de letramento em proteção de dados; a efetividade da LGPD depende de um aculturamento que hoje carece de coordenação, de institucionalidade e de política estruturada, dispersando-se em iniciativas pontuais e não cumulativas.

Grupos afetados: Cidadãos, em especial vulneráveis (crianças e adolescentes, idosos, populações de baixa renda); escolas e universidades; servidores públicos; profissionais do setor.

Resultados esperados: Cidadania digital; redução da assimetria informacional; fortalecimento da autodeterminação informativa; padronização e certificação de competências em proteção de dados.

Justificativa: Diagnóstico do GT1/CNPD, que recomendou a ENAD como ponto focal de todas as ações da ANPD que envolvam temas relacionados às ações educativas.[4]

Escopo: Criação da ENAD, com catálogo de cursos, produção de materiais, parcerias com instituições de ensino (ENAP, OAB, universidades) e sistema de certificação de profissionais e organizações.

Estado atual: Inexistente como instituição. A ANPD desenvolve ações educativas pontuais e mantém o Plano Institucional de Ações Educativas; o tema tangencia o Item 10 da Agenda 2025–2026 (Diretrizes para a Política Nacional, Fase 2). Não há escola estruturada nem sistema de certificação.

2.2. Sistema de Acreditação, Certificados e Selos

A segunda contribuição trata da regulamentação do sistema de acreditação e certificação, instrumentos expressamente previstos na LGPD e ainda sem regulamentação específica (fase 4).

Tema. Criação de um sistema de acreditação e certificação que (i) estimule e reconheça boas práticas e governança como instrumento autônomo de *accountability* (artigo 50, §§ 3.º e 4.º) e (ii) amplie o número de atores capazes de difundir profissionalmente a proteção de dados.

Problema. A emissão de certificados e selos (expressamente prevista no artigo 33, II) permanece integralmente sem regulamentação. Paralelamente, a faculdade de a ANPD reconhecer e divulgar regras de boas práticas (artigo 50, §§ 3.º e

[4] GT1/CNPD, Relatório Final (2025). Modelo de referência: o ICO (Reino Unido) e a CNIL (França) mantêm áreas educativas estruturadas. A ANPD já possui Plano Institucional de Ações Educativas, ainda não consolidado em instituição de ensino própria.

4.º) jamais foi operacionalizada, privando o mercado de instrumento de diferenciação e de incentivo verificável à conformidade.

Grupos afetados. Profissionais de proteção de dados; associações setoriais e entidades certificadoras; agentes que buscam diferenciação competitiva por conformidade verificável; titulares beneficiados por maior transparência.

Resultados esperados. Criação de um ecossistema de certificação alinhado a padrões internacionais; possibilidade de reconhecimento recíproco de certificações estrangeiras; e sistema de incentivos à adoção de boas práticas, com efeitos concretos na dosimetria (demonstração de boa-fé e diligência).

Justificativa. Convergência parcial com a Contribuição 1 da Conselheira Ana Bialer, acrescida da dimensão de acreditação de entidades certificadoras e da articulação com a dosimetria. A competência é expressa (artigos 33, II, "d", 50 e 55-J, XIII); sua inércia configura omissão que esvazia instrumentos legalmente previstos.[5]

Escopo. Procedimento de acreditação de entidades certificadoras de capacitação e processos (artigo 50, §§ 3.º e 4.º).

Estado atual. Sem regulamentação. A Resolução CD/ANPD n.º 19/2024 disciplinou a transferência internacional por cláusulas-padrão e normas corporativas globais, mas não os selos, certificados e códigos de conduta. As "Regras de boas práticas e de governança" constam da Agenda 2025–2026 (Item 17, Fase 4), sem disciplina específica de acreditação ou certificação.

2.3. Tratamento Secundário e Interoperabilidade

A terceira contribuição aborda a lacuna regulatória relativa ao tratamento secundário de dados e à interoperabilidade de bases públicas no contexto do Governo Digital (fases 1-2).

[5] Referência comparada: GDPR, artigos 40–43 (códigos de conduta e certificação) e artigos 42–43 (organismos de certificação e acreditação), e artigos 45–47 (transferências). A arquitetura europeia distingue acreditação (do certificador) de certificação (do agente), modelo útil ao desenho brasileiro.

Tema. Regulamentação do tratamento secundário, do compartilhamento público-privado e da interoperabilidade de bases públicas no âmbito do Governo Digital (Lei n.º 14.129/2021), incluída a coordenação com reguladores setoriais.

Problema. O Item 3 da Agenda 2025–2026 cobre o compartilhamento (artigos 26, 27 e 30 da LGPD), mas não o reuso para finalidade distinta da coleta original nem a interoperabilidade entre bases; faltam critérios de compatibilidade de finalidades e definição da base legal aplicável (artigo 7.º, III, e artigo 11, II, "b"). A interoperabilidade, ademais, materializa a sobreposição de competências entre a ANPD e os reguladores setoriais detentores das bases, demandando protocolos de cooperação.

Grupos afetados. Órgãos e entidades públicas; titulares-administrados; empresas e organizações da sociedade civil que recebem dados do Poder Público; órgãos de controle.

Resultados esperados. Segurança jurídica para o Governo Digital; salvaguardas de finalidade na interoperabilidade; redução de litígios; e prevenção de diretrizes contraditórias entre a ANPD e os reguladores setoriais.

Justificativa. Competência do artigo 30 e do Capítulo IV da LGPD; o tema conecta-se à atuação das procuradorias e órgãos de controle e ao diagnóstico do GT3/CNPD sobre coordenação interinstitucional[6].

Escopo. Guia orientativo e/ou regulamentação fixando critérios de compatibilidade de finalidades, requisitos do compartilhamento público-privado e salvaguardas de interoperabilidade, em coordenação com o Item 3 da Agenda.

Estado atual. O Item 3 da Agenda 2025–2026 (Fase 1) regulamenta o compartilhamento de dados pelo Poder Público; a ANPD publicou o Guia Orientativo de

[6] Cf. VALADÃO, R. B. Regime Jurídico do Tratamento Secundário de Dados Pessoais pelo Poder Público. In: Comentários aos Regulamentos e Orientações da ANPD. São Paulo: RT, 2022. Referência comparada: teste de compatibilidade do artigo 6(4) do GDPR e princípio da vinculação à finalidade (Zweckbindung). Coordenação: GT3/CNPD (Acordos de Cooperação Técnica — Decreto n.º 11.531/2023).

Tratamento de Dados Pessoais pelo Poder Público (2022). O uso secundário e a interoperabilidade (Lei n.º 14.129/2021) não foram objeto de disciplina específica.

2.4. Monetização e Patrimonialização de Dados Pessoais

A quarta contribuição propõe a definição de parâmetros jurídicos para a monetização primária de dados pessoais, tema inédito nas agendas regulatórias anteriores da ANPD (fase 2).

Tema. Orientação sobre requisitos para a monetização primária de dados pessoais: modelos de "consentir ou pagar" (*pay-or-consent*), oferta de dados como contraprestação e limites jurídicos da patrimonialização.

Problema. A LGPD não disciplina a exploração econômica direta do dado pessoal; subsiste tensão dogmática entre sua circulação patrimonial e sua natureza de direito fundamental, sem parâmetros sobre a validade do consentimento nesses modelos. Lacuna presente em todas as agendas anteriores.

Grupos afetados. Titulares; plataformas digitais e aplicações; anunciantes e *adtech*; agentes de tratamento orientados por dados; órgãos de defesa da concorrência e do consumidor.

Resultados esperados. Segurança jurídica sobre os limites da monetização; proteção do titular contra a coisificação do dado; previsibilidade para modelos de negócio.

Justificativa. A ausência de balizas transfere a definição do tema ao litígio; a competência orientadora da ANPD (artigo 55-J) recomenda posição própria, sensível

ao contexto brasileiro, ante o contraste entre a Opinião 08/2024 do EDPB e a Diretiva (UE) 2019/770[7].

Escopo. Estudo técnico (Radar Tecnológico), seguido de guia orientativo ou resolução, com articulação à tutela concorrencial e do consumidor.

Estado atual. Inédito. Nenhuma das agendas (2021–2022, 2023–2024, 2025–2026) contemplou a monetização primária; o Item 11 (agregadores de dados, Fase 2) tangencia apenas o mercado secundário e a raspagem de dados.

2.5. Hipótese Legal do Legítimo Interesse

A quinta contribuição propõe a densificação dos critérios do legítimo interesse, hipótese legal subutilizada em razão da ausência de parâmetros regulatórios claros (fase 2).

Tema. Densificação dos critérios do legítimo interesse (artigo 7.º, IX, e artigo 10), com teste de proporcionalidade e tratamento do legítimo interesse.

Problema. Subutilização por receio regulatório e uso do consentimento como solução-padrão, mesmo quando sua validade é questionável; controvérsia sobre o legítimo interesse do Poder Público (artigos 7.º, III, vs. IX).

Grupos afetados. Controladores; titulares; setor público; áreas de marketing, antifraude, crédito e segurança.

Resultados esperados. Uso adequado das bases legais; redução de consentimentos desnecessários; documentação do teste de balanceamento; segurança para tratamentos legítimos.

[7]EDPB. Opinion 08/2024 (consent or pay), 17.04.2024 — "dados não são mercadoria"; impugnada pela Meta (TJUE T-319/24). Diretiva (UE) 2019/770 (dado como contraprestação). Cf. TJUE C-252/21 (Meta v. Bundeskartellamt). Conexão com o Item 11 da Agenda (agregadores de dados). Tema da pesquisa de pós-doutorado do proponente.

Justificativa. Convergência com a contribuição do Conselheiro Rony Vainzof, adensada pela dimensão pública e pelo rigor metodológico do teste.[8]

Escopo. Regulamentação, com parâmetros de documentação do LIA, legítima expectativa, transparência e oposição.

Estado atual. Sem regulamentação específica. O Guia Orientativo sobre Hipóteses Legais de Tratamento (fev/2024) aborda as bases de forma geral; o consentimento (Item 18) e a proteção ao crédito (Item 19) constam da Agenda (Fase 4); o legítimo interesse carece de item próprio.

2.6. Anonimização, Pseudonimização e Padrão Jurídico de Risco de Reidentificação

A sexta contribuição aprofunda o tratamento da anonimização e pseudonimização, com foco na definição do padrão jurídico de risco de reidentificação e no estatuto dos dados pseudonimizados (fase 1; aprofundamento).

Tema. Aprofundamento do Item 9 da Agenda, com o padrão dos "meios razoavelmente disponíveis" (artigo 12 da LGPD; Considerando 26 do GDPR) e a definição do estatuto dos dados pseudonimizados, que permanecem dados pessoais.

Problema. Insegurança sobre técnicas aceitáveis, critérios de risco e a distinção entre anonimização, pseudonimização, agregação e dados sintéticos, com revisão periódica do risco de reidentificação.

Grupos afetados. Empresas orientadas por dados; áreas de analytics, IA e pesquisa; titulares.

[8] Referências comparadas: artigo 6(1)(f) do GDPR; EDPB, Guidelines 1/2024 sobre legítimo interesse; TJUE C-621/22 (KNLTB), que admite o interesse comercial como legítimo, desde que necessário e ponderado.

Resultados esperados. Abordagem baseada em risco e relativa ao contexto; incentivo a tecnologias de reforço da privacidade (*privacy-enhancing technologies*); redução de litígios sobre reidentificação.

Justificativa. Convergência com a contribuição do Conselheiro Rony Vainzof; conexão com os itens 2.4 e 2.10 (monetização e IA)[9].

Escopo. Aprofundamento do Item 9, via guia orientativo, com critérios de avaliação de risco, reidentificação e governança de ambientes analíticos.

Estado atual. Consta da Agenda 2025–2026 (Item 9, Fase 1), com Tomada de Subsídios realizada e processo regulatório em curso; falta densificação do padrão de reidentificação e do estatuto dos pseudonimizados.

2.7. Padrões Mínimos de Segurança

A sétima contribuição propõe a regulamentação dos padrões mínimos de segurança da informação e os critérios de responsabilização por incidentes, ajudando a diferenciar o agente diligente do negligente (fase 1).

Tema. Padrões mínimos de segurança (artigo 46, §1.º) e regime de responsabilidade por incidentes (obrigação de diligência, não de resultado)

Problema. Faltam *baseline* de controles e critérios que diferenciem o agente negligente da vítima de ataque sofisticado, bem como da diferença dos padrões mínimos a serem adotados em conformidade com o porte da organização, bem como com a quantidade e a criticalidade dos dados tratados.

Grupos afetados. Controladores e operadores; titulares; áreas de segurança da informação e jurídico.

[9] Referência comparada: Tribunal Geral da UE, T-557/20 (SRB v. EDPS), sobre o caráter relativo e contextual da identificabilidade. A fixação do limiar de risco é decisão valorativa que demanda parâmetros objetivos da Autoridade.

Resultados esperados. Elevação da maturidade de segurança; previsibilidade na dosimetria.

Justificativa. Convergência com a contribuição do Conselheiro Rony Vainzof (Item 5) e com a recomendação do GT3/CNPD de notificação compartilhada de incidentes e de protocolo de autoridade condutora[10].

Escopo. Guia orientativo e/ou regulamentação de padrões mínimos, articulada ao RDAS (Resolução n.º 4/2023).

Estado atual. A comunicação de incidentes é regulada pela Resolução CD/ANPD n.º 15/2024; os padrões mínimos de segurança constam do Item 5 da Agenda (Fase 1), em elaboração

2.8. Decisões Automatizadas, Perfilização e Direito à Explicação (artigo 20 da LGPD)

A oitava contribuição propõe a densificação do regime de decisões automatizadas e perfilização, com a definição do conteúdo mínimo do direito à explicação previsto no artigo 20 da LGPD (fases 1-2).

Tema. Densificação do regime de decisões automatizadas e perfilização e definição do conteúdo mínimo do direito à explicação.

Problema. O artigo 20 assegura a revisão, mas o direito à explicação e os limites da perfilização carecem de densidade; o Item 6 (IA) tangencia o tema sem enfrentar a perfilização como prática autônoma nem o conteúdo do dever de explicar.

[10] Referências: Resolução CD/ANPD n.º 15/2024 (Comunicação de Incidente de Segurança) e n.º 4/2023 (RDAS — dosimetria). Comparada: artigo 32 do GDPR; Diretiva NIS2; balcão único do artigo 56 do GDPR; Ato Normativo Conjunto BCB-CADE n.º 1/2018. Casos: vazamentos do PIX (2021 ss.), WhatsApp (2021) e Grok/X (2026).

Grupos afetados. Titulares; controladores; setores de crédito, seguros, publicidade e plataformas; crianças e adolescentes.

Resultados esperados. Critérios sobre decisão "unicamente automatizada"; conteúdo mínimo da explicação; limites da perfilização.

Justificativa. Convergência com as contribuições dos Conselheiros Rony Vainzof (IA), Isabela Henriques (perfilização de crianças, artigos 22, 25 e 26 do ECA Digital) e João Brant (moderação)[11].

Escopo. Guia orientativo e/ou regulamentação, articulado ao Item 6 da Agenda.

Estado atual. O artigo 20 é tratado parcialmente no Item 6 da Agenda (IA, Fase 1), com Tomada de Subsídios sobre IA (nov/2024). O direito à explicação e a perfilização como prática autônoma carecem de disciplina.

2.9. Regime de Transição e Regularização de Bases de Dados Legadas

A nona contribuição endereça uma lacuna estrutural de alto impacto prático: o estabelecimento de um regime de transição para a regularização de bases de dados constituídas antes da vigência da LGPD ou sem documentação adequada da base legal (fases 2-3).

Tema. Regime de transição e de regularização do tratamento de bases de dados legadas – dados coletados antes da vigência da LGPD ou sem registro documentado de base legal e finalidade – e do passivo informacional de organizações públicas e privadas.

Problema. Parcela expressiva do acervo de dados foi constituída antes de setembro de 2020 ou sem documentação da base legal e da finalidade. A LGPD não prevê regime de transição expresso, gerando insegurança sobre (i) a licitude do tratamento continuado; (ii) a possibilidade de realocação superveniente de base

[11] Referências comparadas: TJUE C-634/21 (SCHUFA), que reconhece o scoring de crédito como decisão automatizada, e C-203/22 (Dun & Bradstreet), sobre a extensão do direito à explicação; artigo 22 do GDPR.

legal (legítimo interesse, obrigação legal); (iii) o dever de eliminação *versus* conservação; e (iv) o ônus de obter novo consentimento para acervos massivos. A indefinição estimula tanto a inércia (manutenção de bases ilícitas) quanto a destruição excessiva de acervos úteis.

Grupos afetados. Controladores públicos e privados com acervos históricos (instituições financeiras, saúde, varejo, administração pública, arquivos); titulares; arquivos públicos e órgãos de controle.

Resultados esperados. Segurança jurídica para a regularização de passivos; critérios de convalidação/realocação de base legal; parâmetros de eliminação, anonimização ou conservação; redução de litígios e da destruição desnecessária de acervos de valor histórico, científico ou probatório.

Justificativa. Lacuna estrutural não enfrentada por nenhuma agenda, com elevado impacto prático; conecta-se ao princípio da finalidade, às bases legais (item 2.5), à anonimização (item 2.6) e ao tratamento pelo Poder Público (item 2.3). O direito comparado oferece parâmetro metodológico[12].

Escopo. Guia orientativo e/ou regulamentação fixando o regime de transição, critérios de realocação de base legal, parâmetros de eliminação/anonimização e o tratamento de acervos de interesse público, histórico, científico ou probatório.

Estado atual. Inédito. Não há regime de transição ou de regularização para bases legadas; a matéria é hoje resolvida casuisticamente, por fiscalização e jurisprudência, com soluções divergentes.

[12] GDPR, artigo 94 e Considerando 171, que admitiram a continuidade de tratamentos baseados em consentimento pré-existente desde que compatível com o Regulamento, fixando regime de transição. No Brasil, cf. artigos 7.º, §3.º, 15 e 16 da LGPD (término do tratamento e conservação).

2.10. Bases Legais para Treinamento de Modelos e interface com IA

A décima contribuição trata da coordenação normativa entre a LGPD e o futuro Marco Legal da IA, definindo parâmetros para as bases legais aplicáveis ao ciclo de vida dos modelos de inteligência artificial (fase 2).

Tema. Coordenação normativa entre a LGPD e o futuro Marco Legal da IA e parâmetros para o tratamento de dados no ciclo de vida dos modelos (web scraping, bases públicas, dados sensíveis para mitigação de viés).

Problema. O PL n.º 2.338/2023 tramita na Câmara (aprovado no Senado em dezembro de 2024) e prevê o Sistema Nacional de Regulação e Governança da IA (SIA); sem definição prévia, há risco de sobreposição ou vácuo entre a LGPD e o novo marco.

Grupos afetados. Desenvolvedores e aplicadores de IA; titulares; setores regulados; a ANPD e a futura governança do SIA.

Resultados esperados. Posição coordenada (não fragmentária); segurança jurídica para a inovação responsável; clareza sobre bases legais de treinamento e sobre o uso de dados sensíveis para mitigação de viés.

Justificativa. Convergência com a contribuição do Conselheiro Rony Vainzof (IA), com foco próprio na interface normativa e na coordenação institucional.[13]

Escopo. Estudo e nota técnica de coordenação; guia orientativo, articulado ao Item 6 da Agenda.

Estado atual. O Item 6 da Agenda (IA, Fase 1) trata da aplicação da LGPD ao treinamento e uso de IA de forma geral; a interface com o futuro Marco Legal da IA e os parâmetros de *web scraping* e de dados sensíveis para mitigação de viés permanecem pendentes.

[13] Status (junho/2026): PL n.º 2.338/2023, em tramitação. Referência comparada: articulação entre o AI Act (Regulamento (UE) 2024/1689) e o GDPR; pronunciamentos de autoridades europeias sobre modelos de linguagem.

3. Agenda Regulatória Proposta

As dez proposições são sintetizadas a seguir no modelo das agendas regulatórias da ANPD (colunas Item, Iniciativa, Descrição e Priorização), para facilitar a eventual incorporação à minuta da Agenda 2027–2028. A coluna "priorização" adota a sistemática de fases das Resoluções CD/ANPD n.º 23/2024 e n.º 31/2025.[14]

Item	Iniciativa	Descrição	Priorização
1	**Escola Nacional de Proteção de Dados (ENAD)**	Estruturação de eixo de educação e capacitação na Política Nacional, com criação da ENAD (artigo 55-J).	**Fase 2**
2	**Acreditação, certificados e selos (artigo 33, II, "d"; artigo 50)**	Regulamentação do processo de acreditação de entes públicos e privados como agentes certificadores	**Fase 4**
3	**Tratamento secundário e interoperabilidade**	Disciplina do tratamento secundário e da interoperabilidade, com critérios de compatibilidade de finalidades.	**Fase 1-2**
4	**Monetização e patrimonialização de dados**	Fixação de parâmetros para a monetização primária de dados pessoais: modelos de "consentir ou pagar", dado como contraprestação e limites da patrimonialização.	**Fase 2**
5	**Legítimo interesse: densificação e teste (LIA)**	Densificação dos critérios do legítimo interesse (artigo 7.º, IX, e artigo 10), com teste de proporcionalidade e tratamento do legítimo interesse no setor público.	**Fase 1**
6	**Anonimização, pseudonimização e reidentificação**	Aprofundamento dos padrões de anonimização e pseudonimização (artigo 12), com o critério dos "meios razoavelmente disponíveis" e o estatuto dos dados pseudonimizados.	**Fase 1**

[14] Legenda de priorização (Resoluções CD/ANPD n.º 23/2024 e 31/2025): a) Fase 1: início do processo regulatório provém de agenda anterior ou em até 1 ano; b) Fase 2: até 1 ano; c) Fase 3: até 1 ano e 6 meses; d) Fase 4: até 2 anos.

Item	Iniciativa	Descrição	Priorização
7	**Segurança e notificação coordenada de incidentes**	Guia orientativo ou regulamentação dos padrões mínimos de segurança (artigo 46, §1.º)	**Fase 1**
8	**Decisões automatizadas e direito à explicação**	Densificação do regime de decisões automatizadas e perfilização e definição do conteúdo mínimo do direito à explicação (artigo 20).	**Fase 1-2**
9	**Regime de transição de bases legadas**	Instituição de regime de transição e regularização do tratamento de bases de dados legadas, ou seja, dos dados coletados antes da LGPD ou sem base legal documentada.	**Fase 2-3**
10	**Interface LGPD × Marco Legal da IA**	Parâmetros para bases legais de treinamento de modelos de IA (web scraping; dados sensíveis para mitigação de viés).	**Fase 2**

4. Considerações Finais

As proposições foram concebidas para complementar – não duplicar – as contribuições dos demais conselheiros, e dialogam com os diagnósticos dos GTs do CNPD. As *lacunas próprias*, nas áreas de especialização do proponente, são os itens 3 (uso secundário e interoperabilidade), 4 (monetização) e 9 (bases legadas). O item 1 incorpora o Relatório Final do GT1 (educação); o diagnóstico do GT3 (coordenação interinstitucional) foi incorporado transversalmente aos itens 3 e 7, em vez de constituir item autônomo. As *convergências* com o Conselho são: itens 5, 6, 7 e 10 com o Conselheiro Rony Vainzof; item 2 com a Conselheira Ana Bialer; e item 8 com os Conselheiros Rony Vainzof, Isabela Henriques e João Brant.

1. Escola Nacional de Proteção de Dados (ENAD) — *GT1 · transversal - Fase 2*

2. Acreditação, certificados e selos (artigo 33, II; artigo 50) — *conv. Ana Bialer · Fase 4*

3. Tratamento secundário e interoperabilidade — *lacuna própria + GT3 · Fase 1/2*

4. Monetização e patrimonialização de dados — *lacuna própria · Fase 2*

5. Legítimo interesse — *conv. Rony Vainzof · Fase 1*

6. Anonimização e risco de reidentificação — *conv. Rony Vainzof · Fase 1*

7. Padrões mínimos de segurança — *conv. Rony + GT3 · Fase 1*

8. Decisões automatizadas e direito à explicação — *conv. Rony/Isabela/Brant · Fase 1/2*

9. Regime de transição de bases legadas — *lacuna própria · Fase 2/3*

10. Interface LGPD × Marco Legal da IA — *conv. Rony Vainzof · Fase 2*

Por fim, a govDADOS informa que permanece à disposição da ANPD para aprofundar quaisquer das proposições apresentadas, participar de grupos de trabalho, consultas públicas ou tomadas de subsídios sobre os temas, e contribuir com a elaboração dos instrumentos regulatórios correspondentes. A consolidação de uma agenda regulatória robusta e coerente para o biênio 2027–2028 é condição necessária para que o Brasil afirme sua posição como jurisdição de proteção de dados madura, interoperável com os principais sistemas internacionais e efetivamente capaz de assegurar a autodeterminação informativa dos titulares.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Confidencial
De São Paulo para Brasília, 17 de junho de 2026.

Ref.: Contribuições para a Agenda Regulatória da ANPD (2027-2028)
Autoria: Rony Vainzof - Conselheiro Titular pelo Setor Empresarial

Prezados(as),

Conforme solicitado, considerando a Resolução CD/ANPD Nº 31/25, seguem contribuições do Conselheiro Rony Vainzof (Titular – Setor Empresarial), para a Agenda Regulatória da Agência Nacional de Proteção de Dados 2027-2028, seguindo o modelo proposto:

Sumário

CONSIDERAÇÕES INICIAIS RELEVANTES..... 1
1. INTELIGÊNCIA ARTIFICIAL..... 2
2. DIREITOS DOS TITULARES..... 3
3. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO..... 5
4. REGRAS DE BOAS PRÁTICAS E DE GOVERNANÇA..... 6
5. MEDIDAS DE SEGURANÇA, TÉCNICAS E ADMINISTRATIVAS, INCLUINDO PADRÕES TÉCNICOS..... 7
6. HIPÓTESE LEGAL: LEGÍTIMO INTERESSE E CONSENTIMENTO..... 9
7. OUTROS ITENS, EM ORDEM DE PRIORIDADE:..... 11

CONSIDERAÇÕES INICIAIS RELEVANTES

Segurança jurídica também é proteção de direitos. Empresas que sabem claramente quais padrões seguir conseguem proteger melhor titulares, reduzir riscos, inovar com responsabilidade e investir melhor.

Assim, recomendo que a Agenda Regulatória da ANPD 2027-2028 priorize temas capazes de transformar a LGPD em regulação **a ser seguida para o uso ético, lícito e responsável de dados pessoais ainda mais clara, previsível e compatível com a economia digital.**

Diversos temas relevantes vêm sendo postergados ou tratados apenas parcialmente, em razão da amplitude e complexidade da agenda regulatória **frente à estrutura ainda em consolidação da ANPD**.

Com o fortalecimento institucional da Agência, torna-se essencial que esses temas avancem de forma consistente, coordenada e transparente, **sob a perspectiva da regulamentação preventiva, da segurança jurídica e da redução de assimetrias interpretativas.**

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

A proteção de dados pessoais deve caminhar junto com inovação, competitividade e desenvolvimento econômico. Para isso, sugere-se que **a ANPD privilegie a regulação proporcional, baseada em risco e orientada por evidências, evitando que lacunas normativas sejam preenchidas predominantemente por litígios, fiscalizações ou sanções.**

Assim, seguem sugestões dos temas da Agenda em ordem de prioridade para regulamentação:

1. INTELIGÊNCIA ARTIFICIAL

Regulamentação do tratamento de dados pessoais no ciclo de vida de aplicações de inteligência artificial e decisões automatizadas, incluindo coleta, curadoria, treinamento, validação, fine-tuning, implantação, inferência, monitoramento, retreinamento e uso de IA generativa.

Identificação e descrição do problema
A IA é estratégica para inovação, produtividade, competitividade, segurança, prevenção a fraudes, crédito, saúde, educação, atendimento, marketing, indústria e serviços. No entanto, a ausência de parâmetros regulatórios específicos gera insegurança jurídica para empresas que precisam desenvolver, aplicar, contratar ou utilizar sistemas de IA em conformidade com a LGPD.

As principais questões que exigem orientação da ANPD incluem:

- aplicação dos princípios da finalidade, necessidade e adequação, diante da importância do tratamento massivo de dados para maior precisão da IA;
- definição da base legal adequada para treinamento de modelos, especialmente diante da complexidade, viabilidade ou proporcionalidade de se obter consentimento individual;
- uso do legítimo interesse para IA, com critérios para teste de balanceamento, legítima expectativa, transparência e oposição, quando aplicável;
- avaliação das diferentes fases do ciclo de IA, pois o dado pode ter natureza e risco distintos na coleta, no treinamento, na validação, na inferência e no retreinamento;
- distinção entre dados pessoais, dados anonimizados, dados pseudonimizados, dados sintéticos e modelos que possam memorizar ou permitir extração de informações pessoais;
- tratamento de dados sensíveis para mitigação de vieses, discriminação e sub-representação, inclusive em hipóteses nas quais o consentimento seja inviável;
- dificuldade prática de individualizar cada variável de dado pessoal utilizada pelo modelo, já que a relevância de cada atributo pode ser definida dinamicamente pelo próprio sistema;

- uso de bases públicas, bases de terceiros e web scraping;
- transparência compatível com a complexidade técnica dos modelos;
- direitos dos titulares em decisões automatizadas;
- governança de fornecedores, modelos fundacionais, IA generativa e agentes autônomos;
- documentação, logs, segurança, auditoria e monitoramento de riscos.

Grupos afetados pela implementação do projeto
Titulares de dados; grandes e médias empresas; desenvolvedores, aplicadores e usuários de IA; startups; fornecedores de modelos fundacionais; plataformas digitais; instituições financeiras; seguradoras; varejo; saúde; educação; telecomunicações; indústria; áreas de inovação, tecnologia, dados, jurídico, compliance, segurança, produto, RH, marketing e atendimento.

Resultados e benefícios esperados
A regulamentação deve gerar segurança jurídica para inovação responsável, reduzir assimetrias interpretativas, prevenir litígios, orientar fiscalizações, proteger titulares e permitir que empresas adotem IA com governança proporcional ao risco.

Também se espera maior clareza sobre bases legais, aplicação dos princípios da LGPD, uso de dados sensíveis para mitigação de vieses, critérios de anonimização, documentação mínima, transparência, revisão de decisões automatizadas, governança de fornecedores e controles aplicáveis ao ciclo de vida da IA.

Justificativa para necessidade de intervenção por meio de regulamentação
A LGPD já se aplica à IA quando há tratamento de dados pessoais, mas não resolve de forma suficiente os desafios operacionais, técnicos e jurídicos dos modelos atuais e futuros. A falta de parâmetros prévios pode transformar fiscalização, judicialização e sanção em mecanismos indiretos de regulação.

A ANPD deve atuar de forma preventiva, estabelecendo balizas claras, proporcionais e tecnologicamente neutras, que permitam diferenciar tratamentos legítimos e governados de práticas abusivas ou de alto risco.

Escopo e prazo para implementação
Fase 1, por meio de regulamentação.

2. DIREITOS DOS TITULARES

Regulamentação sobre o exercício dos direitos dos titulares, com definição de procedimentos, prazos, autenticação, limites, hipóteses de negativa, abuso de direito, atendimento em escala, portabilidade, oposição, eliminação, confirmação de tratamento, acesso e revisão de decisões automatizadas.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Identificação e descrição do problema

Principalmente empresas de médio e grande porte recebem volumes crescentes de solicitações de titulares, muitas vezes genéricas, repetitivas, automatizadas, formuladas por terceiros ou desconectadas do contexto específico do tratamento.

Persistem dúvidas relevantes sobre autenticação do titular, representação por terceiros, extensão do direito de acesso, formato da resposta, prazos, hipóteses de negativa, pedidos abusivos, tratamento de dados em backup, eliminação quando há obrigação legal de retenção e complexidade tecnológica, portabilidade e interação entre controlador, operador e parceiros comerciais.

Também é necessário esclarecer o alcance do direito de oposição. A LGPD prevê a oposição quando o tratamento for realizado com fundamento em uma das hipóteses de dispensa de consentimento e houver descumprimento da lei, justamente para não inviabilizar importantes tratamentos de dados pessoais, como para prevenção à fraude.

Sem critérios claros, empresas ficam expostas a reclamações, litígios e procedimentos administrativos mesmo quando adotam esforços razoáveis para atender titulares.

Grupos afetados pela implementação do projeto

Titulares; controladores; encarregados; áreas de atendimento, jurídico e tecnologia.

Resultados e benefícios esperados

- melhor experiência para titulares;
- redução de disputas administrativas e judiciais;
- padronização de procedimentos;
- diminuição de custos operacionais;
- segurança para respostas negativas fundamentadas;
- esclarecer quando o direito de oposição é aplicável, quais fundamentos devem ser apresentados pelo titular, como o controlador deve avaliar o pedido e em quais situações a continuidade do tratamento é legítima, especialmente diante de obrigação legal, exercício regular de direitos, proteção ao crédito, prevenção a fraudes, segurança, execução de contrato ou legítimo interesse devidamente documentado;
- clareza sobre autenticação e representação;
- maior eficiência no atendimento em escala;
- fortalecimento da governança e da accountability.

Justificativa para necessidade de intervenção por meio de regulamentação

A LGPD prevê direitos, mas não detalha suficientemente sua operacionalização. Essa lacuna cria insegurança para titulares e agentes de tratamento.

A regulamentação é necessária para evitar que a definição dos contornos dos direitos ocorra predominantemente por meio de reclamações, judicializações, procedimentos

de fiscalização ou sanções. Direitos devem ser exercidos com efetividade, mas também com proporcionalidade, segurança e previsibilidade.

Escopo e prazo para implementação
Fase 1, por meio de regulamentação.

3. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Regulamentação técnica e jurídica sobre anonimização, pseudonimização, dados agregados, dados sintéticos, risco de reidentificação e governança.

Identificação e descrição do problema
Empresas utilizam dados para analytics, inteligência artificial, estatística, segurança, pesquisa, desenvolvimento de produtos, prevenção a fraudes e melhoria de serviços. Contudo, ainda há insegurança sobre:

- técnicas aceitáveis de anonimização e pseudonimização;
- critérios de avaliação de risco;
- distinção entre anonimização, pseudonimização, agregação e dados sintéticos;
- possibilidade de reidentificação;
- atualização periódica do risco;
- compartilhamento de bases anonimizadas;
- uso de dados anonimizados para IA e pesquisa;
- medidas organizacionais e contratuais complementares.

Grupos afetados pela implementação do projeto
Empresas orientadas por dados; áreas de analytics, IA, segurança, produto, marketing, pesquisa, ciência de dados, saúde, educação, financeiro, indústria, varejo, universidades e centros de pesquisa.

Resultados e benefícios esperados
- segurança jurídica para inovação baseada em dados;
- redução de exposição de titulares;
- incentivo ao uso de privacy-enhancing technologies;
- maior qualidade técnica em processos de anonimização e pseudonimização;
- segurança para projetos de IA, estatística e pesquisa;
- redução de litígios sobre reidentificação;
- melhor governança de ambientes analíticos.

O escopo deve incluir técnicas, avaliação de risco, reidentificação, pseudonimização, dados sintéticos, dados agregados, ambientes controlados, testes periódicos, governança, documentação, contratos e uso em IA.

Justificativa para necessidade de intervenção por meio de regulamentação
A anonimização e pseudonimização são pontes estratégicas entre proteção de dados e inovação. A ausência de parâmetros objetivos faz com que algumas empresas deixem de usar dados de forma segura, enquanto outras assumem riscos excessivos por falta de maturidade técnica.

A ANPD deve estabelecer abordagem baseada em risco, reconhecendo que a suficiência das técnicas depende do contexto, dos meios razoavelmente disponíveis e das salvaguardas implementadas.

Escopo e prazo para implementação
Fase 1, por meio de guia orientativo.

4. REGRAS DE BOAS PRÁTICAS E DE GOVERNANÇA

Regulamentação de programas de governança em privacidade, regras de boas práticas, códigos de conduta, mecanismos de autorregulação regulada, certificações, selos e critérios de reconhecimento regulatório pela ANPD.

Identificação e descrição do problema
Empresas têm investido em programas de privacidade, segurança da informação e governança de dados, mas ainda não há clareza suficiente sobre como essas iniciativas serão reconhecidas pela ANPD em fiscalizações, incidentes, dosimetria de sanções e demonstração de boa-fé.

Também falta maior desenvolvimento regulatório sobre códigos de conduta e mecanismos de autorregulação do setor privado. Setores econômicos possuem diferentes níveis de risco, maturidade, modelos de negócio e estruturas operacionais, o que torna recomendável a construção de parâmetros setoriais reconhecidos pela ANPD, em lógica de corregulação ou autorregulação regulada.

Outro ponto relevante é a possibilidade de a ANPD atuar como acreditadora, ou definir critérios para acreditação, de entidades certificadoras, de modo a viabilizar selos, certificações e mecanismos independentes de verificação de conformidade.

Grupos afetados pela implementação do projeto
Empresas de todos os portes; associações setoriais; entidades de autorregulação; certificadoras; auditorias independentes; encarregados; titulares; setores regulados; áreas de compliance, jurídico, riscos, tecnologia, segurança da informação e governança corporativa.

Resultados e benefícios esperados
- incentivo à maturidade em privacidade;

- reconhecimento de boas práticas;
- redução de assimetrias entre agentes regulados;
- previsibilidade em fiscalizações;
- critérios objetivos para dosimetria;
- estímulo a códigos setoriais;
- mecanismos de autorregulação reconhecidos pela ANPD;
- certificações confiáveis, selos de conformidade e critérios objetivos para que boas práticas produzam efeitos regulatórios concretos;
- fortalecimento da confiança no mercado;
- valorização de investimentos preventivos.

Justificativa para necessidade de intervenção por meio de regulamentação
A LGPD prevê regras de boas práticas e governança, mas o mercado ainda carece de critérios claros para sua implementação, validação e reconhecimento.

A regulamentação é necessária para que a governança deixe de ser apenas uma obrigação abstrata e passe a operar como instrumento efetivo de accountability, previsibilidade e incentivo à conformidade.

Além disso, a ANPD pode ampliar sua capacidade regulatória ao reconhecer códigos de conduta e mecanismos privados de autorregulação, sem renunciar à supervisão pública.

Esse modelo permite combinar conhecimento técnico-setorial, agilidade do setor privado e controle regulatório, reduzindo a necessidade de intervenção exclusivamente sancionatória.

Escopo e prazo para implementação
Fase 1, por meio de regulamentação.

5. MEDIDAS DE SEGURANÇA, TÉCNICAS E ADMINISTRATIVAS, INCLUINDO PADRÕES TÉCNICOS

Regulamentação de padrões mínimos de segurança da informação e medidas técnicas e administrativas aplicáveis ao tratamento de dados pessoais, com abordagem proporcional ao risco, porte, setor, criticidade da operação e evolução das ameaças cibernéticas.

Identificação e descrição do problema

Empresas investem tempo, recursos financeiros, tecnologia, pessoas e processos para proteger dados pessoais. Ainda assim, nenhuma organização está imune a incidentes de segurança, especialmente diante do aumento da sofisticação dos ataques, do uso de

alta tecnologia por agentes maliciosos, da exploração em tempo real de vulnerabilidades e da complexidade das cadeias digitais.

Nesse contexto, é essencial que a regulamentação reconheça que segurança da informação é obrigação de diligência, governança e mitigação de riscos, mas não de resultado absoluto.

Empresas também podem ser vítimas de ataques cibernéticos e não devem ser punidas automaticamente pela ocorrência de incidentes, especialmente quando demonstrarem adoção de medidas técnicas e administrativas adequadas, resposta tempestiva, transparência e boa-fé.

Persistem dúvidas sobre quais controles mínimos serão considerados adequados pela ANPD em fiscalizações, comunicações de incidentes e avaliações de conformidade, incluindo criptografia, gestão de acessos, logs, backup, segregação de ambientes, gestão de vulnerabilidades, resposta a incidentes, gestão de fornecedores, cloud, descarte seguro, testes de segurança e continuidade de negócios.

Grupos afetados pela implementação do projeto
Controladores; operadores; titulares; CISOs; encarregados; áreas de tecnologia, segurança da informação, jurídico, riscos, compras, auditoria, fornecedores de cloud, SaaS, BPO, infraestrutura crítica, serviços essenciais, instituições financeiras, saúde, educação, varejo, telecomunicações e demais setores intensivos em dados.

Resultados e benefícios esperados

- estabelecer parâmetros para diferenciar empresas negligentes de empresas diligentes que, apesar de controles razoáveis e proporcionais, venham a sofrer ataques sofisticados previsibilidade regulatória;
- reconhecer evidências de governança, medidas preventivas, resposta adequada, comunicação tempestiva, contenção, remediação e cooperação como elementos relevantes na avaliação de responsabilidade e eventual dosimetria de sanções;
- redução de incidentes;
- melhoria da resiliência operacional;
- critérios claros para fiscalização;
- maior alinhamento entre privacidade, cibersegurança e gestão de riscos;
- maturidade contratual na cadeia de fornecedores;
- redução de litigiosidade após incidentes;
- melhoria da proteção efetiva dos titulares.

Justificativa para necessidade de intervenção por meio de regulamentação
A LGPD exige medidas técnicas e administrativas aptas a proteger dados pessoais, mas não define um baseline regulatório nem critérios para avaliação de diligência.

A ausência desses parâmetros aumenta o risco de análise retrospectiva e sancionatória após incidentes, sem clareza prévia suficiente sobre o padrão esperado. Isso pode gerar insegurança jurídica, judicialização e desincentivo à transparência.

A regulamentação deve orientar o mercado sobre controles mínimos e evidências de conformidade, reconhecendo que o objetivo regulatório deve ser elevar a maturidade de segurança, e não presumir culpa pela mera ocorrência de um ataque.

Escopo e prazo para implementação
Fase 1, por meio de guia orientativo.

6. HIPÓTESE LEGAL: LEGÍTIMO INTERESSE E CONSENTIMENTO

Regulamentação sobre legítimo interesse e consentimento, com critérios para aplicação, documentação, transparência, oposição, granularidade, teste de balanceamento e validade da manifestação do titular.

Identificação e descrição do problema
Embora o consentimento seja base legal relevante, sua validade exige que a manifestação seja livre, informada e inequívoca. Na prática, titulares muitas vezes não se recordam dos consentimentos concedidos, não compreendem integralmente seus efeitos ou interagem com jornadas digitais em que pode ser complexo demonstrar ausência de vício, adequada granularidade e real capacidade de escolha.

Esse cenário gera:

- fadiga de consentimento;
- baixa qualidade da manifestação de vontade;
- excesso de banners e checkboxes;
- insegurança em marketing, treinamento de IA, antifraude, segurança, analytics e relacionamento com clientes;
- dificuldade de documentação;
- aumento de reclamações e litígios;
- risco de avaliação posterior divergente por autoridades ou pelo Judiciário.

Nesse contexto, o legítimo interesse aparece como importante inovação da LGPD para viabilizar o uso responsável de dados pessoais sem dependência excessiva do consentimento. Trata-se de base legal especialmente relevante para usos legítimos, proporcionais, sociais e economicamente úteis, como prevenção a fraudes, segurança da informação, melhoria de produtos e serviços, analytics, personalização razoável da experiência, publicidade, prevenção de abuso em plataformas, proteção da integridade de redes, relacionamento com clientes, comunicação institucional, inteligência de mercado, modelos de risco, eficiência operacional e determinadas atividades de inovação.

Ao mesmo tempo, o legítimo interesse não é autorização ampla ou automática. Ao contrário, exige que o controlador se debruce de forma mais profunda sobre a legalidade e a proporcionalidade do tratamento, mediante avaliação concreta de finalidade, necessidade, legítima expectativa do titular, impactos, salvaguardas, transparência e possibilidade de oposição, quando houver violação à LGPD. O teste de balanceamento é justamente o mecanismo que diferencia o uso responsável dessa base legal de práticas excessivas ou incompatíveis com a LGPD.

Sem parâmetros claros, empresas ficam expostas a interpretações divergentes sobre quando o consentimento é válido, quando o legítimo interesse é adequado e quais salvaguardas devem ser adotadas.

Grupos afetados pela implementação do projeto
Controladores; titulares; áreas de marketing, publicidade, crédito, antifraude, segurança, analytics, produto, CRM, jurídico, compliance, encarregados, plataformas digitais e empresas com operações B2C e B2B2C.

Resultados e benefícios esperados

- uso mais adequado das bases legais;
- redução de consentimentos desnecessários;
- esclarecer os requisitos para consentimento válido, evitando sua banalização como solução universal e reforçando sua aplicação em situações nas quais a escolha do titular seja efetivamente livre, informada e inequívoca;
- maior qualidade da transparência;
- segurança para tratamentos legítimos;
- documentação do teste de balanceamento;
- esclarecer quando é aplicável o direito de oposição;
- redução de litígios e procedimentos de fiscalização sobre bases legais;
- maior previsibilidade para operações empresariais.

Justificativa para necessidade de intervenção por meio de regulamentação
A intervenção regulatória é necessária diante de duas questões relevantes: o uso do consentimento como solução padrão, mesmo quando sua validade pode ser questionável, e a subutilização do legítimo interesse por receio regulatório.

A ANPD deve estabelecer critérios práticos, exemplos e parâmetros de documentação para que o legítimo interesse seja utilizado de forma responsável, transparente e proporcional. Essa regulamentação permitirá destravar usos legítimos de dados relevantes para inovação, segurança, prevenção a fraudes, melhoria de serviços e eficiência econômica, sem reduzir a proteção dos titulares.

Isso evita que a análise sobre a adequação das bases legais ocorra apenas posteriormente, por meio de reclamações, litígios, fiscalizações ou sanções.

Escopo e prazo para implementação
Fase 1, por meio de regulamentação.

7. OUTROS ITENS, EM ORDEM DE PRIORIDADE:

a. Tratamento de dados pessoais de crianças e adolescentes

b. Relatório de Impacto à Proteção de Dados Pessoais — RIPD

c. Hipótese legal: proteção ao crédito

d. Agregadores de dados pessoais

e. Tratamento de dados pessoais de alto risco

f. Moderação de conteúdo diante da nova competência da ANPD

g. Transferência internacional de dados: selos, certificações e mecanismos internacionais de confiança

Atenciosamente,

Rony Vainzof – Conselheiro Titular do CNPD (Setor Empresarial)