Agência Nacional de Proteção de Dados
Superintendência de Regulação
Coordenação-Geral de Planejamento e Análise Regulatória
Coordenação de Planejamento Regulatório

Nota Técnica nº 20/2026/COPR/CGPAR/SRE/ANPD

1. INTERESSADO

1.1. Conselho Diretor

2. ASSUNTO

2.1. Proposta de Agenda Regulatória da Agência Nacional de Proteção de Dados (ANPD) para o biênio 2027–2028.

3. REFERÊNCIAS

3.1. Processo SEI/ANPD nº 00261.002488/2026-86.

4. RELATÓRIO

4.1. Trata-se de proposta de Agenda Regulatória da ANPD para o biênio 2027–2028.

4.2. Em 04/05/2026, a Superintendência de Regulação (SRE) encaminhou à Superintendência Executiva despacho com o objetivo de propor ao Conselho Diretor da ANPD a realização de tomada de subsídios, do tipo aberta, a ser efetivada por meio de encaminhamento de contribuições escritas pela "Plataforma Brasil Participativo". Ainda, noticiou a previsão normativa quanto à possibilidade de participação do Conselho Nacional de Proteção de Dados e da Privacidade (CNPD) na elaboração da Agenda por meio do envio de sugestões de temas prioritários, nos termos do art. 7º, §2º, da Portaria ANPD nº 16/2021.

4.3. Também em 04/05/2026, esta SRE emitiu Ofício Circular nº 1/2026/CGPAR/SRE (SEI nº 0271135) aos Gabinetes dos Diretores(as), à Superintendência Executiva, à Superintendência de Inovação e Tecnologia, à Superintendência de Fiscalização, à Superintendência de Relações Institucionais e Internacionais e à Ouvidoria, a fim de realizar consulta interna para indicação dos temas prioritários e recorrentes recebidos por meio de consultas, denúncias ou, ainda, mediante pedidos de acesso à informação.

4.4. Em 07/05/2026, por meio do Ofício nº 12/2026/SE/ANPD (SEI nº 0277446), encaminhou-se convite ao CNPD, para que sugerisse suas contribuições à formação da AR para o biênio 2025-2026, preferencialmente até a data de 22/05/2026.

4.5. Em 30/06/2026, por meio do Ofício nº 25/2026/DPDD-SEDIGI/SEDIGI/MJ, foram recebidas as contribuições do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD).

4.6. Deste modo, encaminham-se as conclusões referentes às análises efetuadas, estruturadas a partir dos seguintes tópicos, os quais refletem os procedimentos descritos na Portaria ANPD nº 16/2021.

4.7. É o relatório.

5. ANÁLISE

5.1. Contextualização

5.1.1. A ANPD foi transformada em Agência Reguladora por meio da Medida Provisória nº 1.317/2025, posteriormente convertida na Lei nº 15.352, de 25 de fevereiro de 2026. Com a nova legislação, a Autoridade Nacional de Proteção de Dados passou a denominar-se Agência Nacional de Proteção de Dados, mantida a sigla ANPD, consolidando-se como autarquia de natureza especial, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, vinculada ao Ministério da Justiça e Segurança Pública. A nova lei submete expressamente esta Agência ao regime disciplinado pela Lei nº 13.848/2019 (Lei Geral das Agências Reguladoras), incorporando-a, assim, ao conjunto das agências reguladoras federais.

5.1.2. Cumpre destacar que essa reconfiguração institucional não constitui mero ato de reorganização administrativa: acarreta a incidência, sobre esta Agência, de todo o arcabouço normativo aplicável às agências reguladoras, notadamente no que concerne à Agenda Regulatória como conjunto de temas prioritários a serem regulamentados durante sua vigência.

5.1.3. Não obstante, tal exigência já vinha sendo observada pela ANPD, nos termos da Portaria nº 16/2021, que disciplina os procedimentos para elaboração, revisão e monitoramento da Agenda Regulatória. Com a formal integração ao regime das agências reguladoras, esse dever de planejamento deixa de decorrer apenas de normativo interno e passa a encontrar fundamento direto na legislação das agências reguladoras federais.

5.1.4. A consolidação institucional da ANPD como agência reguladora coincide com a ampliação de suas atribuições regulatórias, especialmente diante da necessidade de regulamentar e fiscalizar o cumprimento da Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente – ECA Digital) e do Decreto nº 12.975/2026, que alterou o Decreto nº 8.771/2016, que regulamenta a Lei nº 12.965/2014 (Marco Civil da Internet) e

do Decreto nº 12.976/2026, que estabelece diretrizes para a proteção de mulheres na internet e para o enfrentamento da violência contra mulheres em ambiente digital.

5.1.5. Diante desse contexto, identificou-se a conveniência de aprofundar, no âmbito da Agenda Regulatória da ANPD, a análise de temas relacionados aos normativos legais e infralegais, com vistas a avaliar a necessidade de eventual complementação normativa e a promover maior previsibilidade regulatória para os agentes de tratamento, observadas as competências legais da Agência.

5.2. **Insumos**

5.2.1. **Agenda Regulatória 2025-2026**

5.2.1.1. A Agenda Regulatória constitui instrumento fundamental para o planejamento, a gestão e a transparência da atividade regulatória. Sua elaboração permite conferir maior previsibilidade à atuação normativa da Agência, ao estabelecer, de forma pública e estruturada, os temas que serão objeto de priorização durante determinado ciclo regulatório.

5.2.1.2. Nesse contexto, a Agenda Regulatória para o biênio 2025–2026 foi inicialmente aprovada pelo Conselho Diretor da ANPD por meio da Resolução nº 23/2024. Em sua versão original, a Agenda contemplava 16 iniciativas regulatórias, das quais 10 eram remanescentes do biênio anterior e 6 constituíam novos temas prioritários. A definição dessas iniciativas buscou conferir continuidade ao processo de regulamentação da LGPD, ao mesmo tempo em que incorporou temas decorrentes da evolução tecnológica e dos novos desafios relacionados à proteção de dados pessoais.

5.2.1.3. A dinâmica regulatória, contudo, exigiu que a Agenda fosse capaz de responder a alterações relevantes no ordenamento jurídico e às novas competências atribuídas à Agência. Foi nesse cenário que a Agenda Regulatória foi alterada por meio da Resolução CD/ANPD nº 31/2025. A revisão decorreu, especialmente, da promulgação do ECA Digital e a designação da ANPD como autoridade administrativa autônoma responsável pela proteção dos direitos de crianças e adolescentes no ambiente digital, nos termos do Decreto nº 12.622/2025.

5.2.1.4. Na revisão foram incorporadas à Agenda três iniciativas relacionadas à implementação do ECA Digital, passando a contemplar 19 iniciativas, que conciliou a continuidade das ações originalmente planejadas com as novas demandas regulatórias decorrentes da legislação superveniente.

5.2.1.5. Quanto à execução da Agenda, o balanço demonstra que a maior parte das iniciativas encontra-se em desenvolvimento. Das 19 ações atualmente integrantes da Agenda, uma foi concluída, 17 encontram-se em andamento e uma ainda não foi iniciada. A iniciativa concluída foi a relativa às Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, e o respectivo documento encontra-se disponível no portal da Agência. Por sua vez, a iniciativa referente à hipótese legal de proteção ao crédito, até o presente momento, consta como não iniciada. As demais 17 iniciativas encontram-se em andamento, em diferentes estágios de desenvolvimento, como pode ser observado no Acompanhamento da Agenda Regulatória, disponível na página da ANPD na internet [1].

5.2.2. **Contribuições do Conselho Nacional de Proteção de Dados**

5.2.2.1. Tendo em vista a natureza da atuação do CNPD, nos termos do art. 3º, I do Decreto nº 10.474, de 26 de agosto de 2020, expediu-se Ofício nº 12/2026/SE/ANPD (SEI nº 0277446), para que este colegiado consultivo encaminhasse as sugestões de temas prioritários.

5.2.2.2. As contribuições apresentadas contemplaram um conjunto diversificado de temas relacionados ao aprimoramento da regulamentação de proteção de dados pessoais e à atuação da ANPD diante de novos contextos de tratamento. Entre as propostas, destacam-se a regulamentação de selos, certificados, códigos de conduta e mecanismos de governança e *accountability*, inclusive no contexto das transferências internacionais de dados; o estabelecimento de parâmetros para o tratamento de dados pessoais de crianças e adolescentes, especialmente à luz da Lei nº 15.211/2025, abrangendo direitos dos titulares, avaliações de impacto, exploração comercial, perfilização, publicidade comportamental, sistemas algorítmicos e design ético; e a definição de critérios para o uso de dados biométricos em diferentes contextos, com atenção aos requisitos de necessidade, proporcionalidade, transparência, segurança e responsabilização.

5.2.2.3. Também foram apresentadas propostas relativas à proteção de dados no contexto laboral, à prevenção de fraudes e golpes, ao tratamento de dados em ambientes esportivos, à educação e capacitação em proteção de dados e à criação de mecanismos de acreditação e certificação. No âmbito do ambiente digital, as contribuições abordaram ainda os deveres de cuidado e devida diligência de provedores de aplicações de internet, a caracterização de falha sistêmica, a moderação de conteúdo e o acesso de instituições acadêmicas, científicas, tecnológicas, de inovação e jornalísticas a dados de plataformas, nos termos do ECA Digital.

5.2.2.4. Outro conjunto relevante de propostas concentrou-se nos fundamentos jurídicos e nas técnicas aplicáveis ao tratamento de dados pessoais, incluindo o legítimo interesse e o consentimento, a anonimização e a pseudonimização, os dados agregados e sintéticos e os riscos de reidentificação. Foram igualmente sugeridos parâmetros para segurança da informação e responsabilidade por incidentes, tratamento de bases de dados legadas, compartilhamento e interoperabilidade de bases

públicas, monetização de dados pessoais e exercício dos direitos dos titulares.

5.2.2.5. As contribuições também conferiram especial atenção às decisões automatizadas, à perfilização e à inteligência artificial, propondo regras para o tratamento de dados ao longo do ciclo de vida de sistemas de IA, incluindo coleta, treinamento, validação, implantação, inferência e monitoramento, bem como parâmetros para decisões automatizadas, direito à explicação e utilização de IA generativa. Nesse eixo, foi ainda sugerida a coordenação entre a LGPD e o futuro marco legal da inteligência artificial, incluindo questões relacionadas ao uso de bases públicas, *web scraping* e tratamento de dados para mitigação de vieses.

5.2.2.6. De forma geral, portanto, as contribuições do colegiado refletiram preocupações tanto com lacunas regulatórias já identificadas na aplicação da LGPD quanto com novos desafios decorrentes da transformação digital, especialmente aqueles relacionados à proteção de crianças e adolescentes, ao funcionamento das plataformas digitais, à inteligência artificial e ao uso de técnicas e tecnologias capazes de produzir impactos relevantes sobre os titulares.

5.2.2.7. Verifica-se que parte relevante dessas preocupações encontra correspondência nos temas que vieram a ser selecionados para a agenda regulatória, ainda que, em diversos casos, os temas selecionados apresentem recorte, abrangência ou formulação distintos daqueles originalmente propostos.

5.2.2.8. Nesse sentido, a incorporação de diversos temas à agenda não implica necessariamente o tratamento integral de cada uma das propostas apresentadas, mas evidencia a convergência entre as contribuições recebidas e as prioridades regulatórias posteriormente definidas, especialmente nos temas relacionados ao ECA Digital, ao uso de dados biométricos, à atuação e às responsabilidades das plataformas digitais, ao acesso a dados para pesquisa, à anonimização e pseudonimização, às decisões automatizadas, ao consentimento e à inteligência artificial.

5.2.2.9. Ademais, ressalta-se que as sugestões não endereçadas nesta Agenda Regulatória foram mapeadas e serão avaliadas nas próximas agendas.

5.2.3. **Contribuições das áreas finalísticas**

5.2.3.1. Também com o intuito de obter sugestões, as demais áreas finalísticas desta Agência foram questionadas pelo Ofício Circular nº1/2026/CGPAR/SRE (SEI nº 0271135) para que fossem sugeridos temas prioritários antes da submissão da proposta à participação social.

5.2.3.2. A Superintendência de Fiscalização encaminhou quinze sugestões de temas para a Agenda Regulatória. As propostas concentram-se, em sua maioria, na regulamentação de aspectos relacionados à proteção de dados pessoais e à privacidade, com fundamento na LGPD, abrangendo temas como o tratamento de dados biométricos, critérios para anonimização e pseudoanonimização, inferência comportamental, emocional e de dados sensíveis, inclusive por sistemas de IA, além do tratamento de dados em contextos específicos, como poder público e dispositivos vestíveis. Também foram apresentadas iniciativas voltadas à segurança da informação, incluindo parâmetros para classificação e comunicação de incidentes de segurança, atualização de orientações para agentes de tratamento e instrumentos de conformidade e fiscalização. Destacam-se, ainda, propostas direcionadas à proteção de crianças e adolescentes em ambientes digitais, contemplando a regulamentação de mecanismos de supervisão parental e medidas para prevenção do uso excessivo de produtos e serviços de tecnologia da informação.

5.2.3.3. A Superintendência de Inovação Tecnológica encaminhou quatro sugestões de temas para a Agenda Regulatória. As propostas concentram-se, principalmente, na proteção de crianças e adolescentes no ambiente digital, abrangendo a definição de parâmetros para aferição e sinalização de idade, o perfilamento para fins de direcionamento publicitário e o estabelecimento de requisitos mínimos para mecanismos de supervisão parental. Também foi apresentada proposta relacionada à portabilidade de dados pessoais.

5.2.3.4. No âmbito da Superintendência de Regulação, foram identificadas iniciativas que se concentram na regulamentação de dispositivos do ECA Digital e do Decreto nº 12.976/2026, com foco na proteção de crianças e adolescentes e de mulheres e meninas no ambiente digital. As propostas abrangem o estabelecimento de medidas para prevenir a criação de *deepfakes* de nudez e conteúdo sexual; a articulação entre o ECA Digital, a LGPD e outros normativos correlatos; a definição de requisitos mínimos para a restrição do alcance de conteúdos de violência contra a mulher; e diretrizes relativas à marcação digital de conteúdos e aos respectivos prazos de implementação.

5.2.3.5. Foram recebidas, ainda, propostas das áreas da Superintendência de Relações Institucionais e Internacionais e da Superintendência Executiva. Após avaliação, verificou-se que as matérias não justificam, neste momento, sua inclusão na Agenda Regulatória, seja por não demandarem atuação regulatória prioritária, seja por poderem ser tratadas por outros instrumentos institucionais.

5.2.3.6. Também foram consideradas propostas oriundas da análise de temas relacionados à aplicação da LGPD e da Tomada de Subsídios sobre Inteligência Artificial e Revisão de Decisões Automatizadas, realizada em 2024. As iniciativas abrangem, respectivamente, a regulamentação de medidas voltadas à prevenção e mitigação de vieses em sistemas de tratamento

automatizado de dados pessoais, com vistas à redução de riscos discriminatórios e à promoção da observância dos princípios da LGPD, bem como a definição de diretrizes para o exercício do direito à revisão de decisões automatizadas, contemplando aspectos relacionados à transparência, explicabilidade, revisão humana e mecanismos de garantia dos direitos dos titulares. Considerando a relevância dos temas para a promoção da proteção de dados pessoais e o amadurecimento da atuação regulatória da Agência, ambas as propostas foram incorporadas à Agenda Regulatória do biênio.

5.2.3.7. Além disso, no âmbito da regulamentação do Marco Civil da Internet (Lei nº 12.965/2014) pelos Decretos nº 12.975/2026 e nº 12.976/2026, a ANPD iniciou, em 30 de junho de 2026, Tomada de Subsídios destinada a colher contribuições da sociedade sobre a implementação das novas obrigações atribuídas aos provedores de aplicações de internet, com contribuições recebidas pela plataforma Brasil Participativo até 17 de agosto de 2026.

5.2.3.8. No âmbito do estudo preliminar para a realização da tomada de subsídios, conforme pode ser observado na Nota Técnica nº 5/2026/CGTAD/SRE/ANPD (SEI nº 0299747), a Agência definiu temas prioritários para eventual inclusão na Agenda Regulatória 2027-2028, como conceitos gerais, dever de elaboração de relatórios de transparência, dever de cuidado, medidas de gestão para riscos sistêmicos, geração e modificação de conteúdo íntimo gerado artificialmente e canal de denúncias de procedimentos de notificação sobre conteúdos ilícitos ou criminosos.

5.2.3.9. Nesse sentido, os resultados dessa tomada de subsídios foram preliminarmente considerados na composição da minuta da Agenda Regulatória 27/28, tanto para subsidiar o desenho de novas ações regulatórias quanto para assegurar coerência com iniciativas já em curso, como a atualização dos Regulamentos de Fiscalização e de Dosimetria. Ressalte-se que as contribuições recebidas na Tomada de Subsídios referente ao Marco Civil da Internet ainda serão analisadas de forma conclusiva pela SRE, de modo que, posteriormente, também serão consideradas no processo de elaboração da Agenda Regulatória para o biênio 2027-2028.

5.2.4. **Relatório de inteligência regulatória**

5.2.4.1. **Abordagem de inteligência regulatória**

5.2.4.2. A definição dos temas propostos para a Agenda Regulatória foi subsidiada por uma abordagem de inteligência regulatória, entendida como um conjunto de práticas destinadas à coleta, sistematização, análise e interpretação de informações relevantes para apoiar processos decisórios e aprimorar a atuação institucional. Essa abordagem permite identificar tendências, acompanhar transformações tecnológicas e sociais, compreender riscos regulatórios e avaliar a pertinência de possíveis intervenções normativas. Como resultado desse trabalho, foi elaborado o relatório técnico, que consolida os achados do estudo e integra o Relatório (SEI nº 0329031), sendo anexado à presente Nota Técnica como documento de referência.

5.2.4.3. Nesse contexto, foi realizado levantamento exploratório baseado em técnicas de mapeamento de tendências (*horizon scanning*) como instrumento complementar de análise. A metodologia teve como objetivo verificar a recorrência, a visibilidade e a relevância dos temas previamente identificados no debate público, técnico e regulatório nacional e internacional, contribuindo para a validação das prioridades regulatórias propostas.

5.2.4.4. O procedimento consistiu na coleta automatizada de informações disponíveis em fontes públicas selecionadas, por meio de raspagem de dados, utilizando palavras-chave relacionadas aos eixos temáticos analisados. Os dados obtidos foram submetidos a tratamento e organização com a finalidade de identificar padrões de ocorrência, concentração temática e presença dos assuntos em discussões institucionais, acadêmicas e regulatórias.

5.2.4.5. Ressalta-se que o levantamento não teve como finalidade substituir a análise qualitativa ou determinar, de forma isolada, a necessidade de regulação. Seus resultados foram utilizados como evidência complementar, em conjunto com a análise jurídica, o diagnóstico dos problemas regulatórios, o acompanhamento de iniciativas internacionais e a avaliação das competências institucionais aplicáveis.

5.2.4.6. Dessa forma, a aplicação de técnicas de coleta e análise automatizada de informações contribuiu para uma abordagem baseada em evidências, fortalecendo a identificação de tendências e temas propostos para a Agenda Regulatória.

5.2.4.7. **Aplicação dos resultados na priorização regulatória**

5.2.4.8. Foram analisados 2.030 artigos e notícias, coletados em 1º de junho de 2026, provenientes de 31 fontes nacionais e internacionais especializadas em tecnologia, proteção de dados, inteligência artificial e direitos digitais.

5.2.4.9. A coleta dos dados foi realizada por meio de procedimentos automatizados de raspagem, em observância às políticas de acesso e utilização definidas por cada fonte. O processo foi configurado para respeitar limites de requisições, intervalos de acesso e demais boas práticas de coleta automatizada, de modo a evitar a sobrecarga dos servidores e garantir a obtenção dos dados de forma ética e responsável.

5.2.4.10. A análise de frequência indicou **forte centralidade da inteligência artificial** no conjunto de documentos monitorados, estando presente em 67% dos conteúdos

analisados. Esse resultado sugere que a IA atua como eixo transversal dos debates sobre governança digital, proteção de dados e direitos de crianças e adolescentes, configurando-se como o principal elemento organizador do ecossistema informacional observado.

5.2.4.11. Entre os temas relacionados à proteção de dados e à privacidade, destacaram-se proteção de dados, dados pessoais e cibersegurança, indicando que as preocupações com o tratamento, a segurança e o uso de informações pessoais permanecem centrais nas discussões contemporâneas. A presença expressiva de conceitos como discriminação algorítmica e IA generativa sugere, ainda, um **deslocamento gradual do debate para os impactos sociais e éticos dos sistemas de inteligência artificial**, especialmente em contextos de tomada de decisão automatizada.

5.2.4.12. Também foi realizada uma análise de redes semânticas, que permitiu identificar automaticamente a estrutura de agrupamento dos conceitos com base em suas relações de coocorrência. Observou-se que a estrutura resultante não corresponde a uma segmentação temática estritamente delimitada entre os grupos. Ao contrário, verifica-se a existência de um grande núcleo central interligado, indicando que os diferentes conceitos mantêm numerosas relações entre si, conforme pode ser observado na figura 1 a seguir.

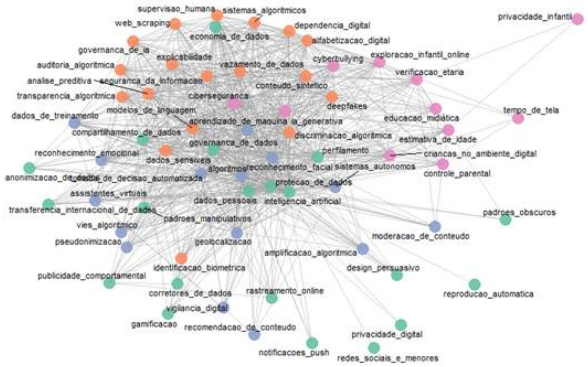

Figura 1 - Mapeamento da rede semântica

5.2.4.13. O principal núcleo articulador da rede é o conceito de inteligência artificial. Ao seu redor, organizam-se comunidades temáticas relativamente bem definidas — governança algorítmica, proteção de dados, economia digital e proteção de crianças no ambiente digital — conectadas por conceitos-chave como proteção de dados, governança de dados, perfilamento e IA generativa. Essa configuração evidencia que **a inteligência artificial não constitui apenas um fenômeno tecnológico, mas um tema transversal que envolve desafios regulatórios, éticos, econômicos e relacionados aos direitos fundamentais, especialmente no contexto da proteção de crianças e adolescentes**. A elevada densidade de conexões sugere, ainda, que esses temas são tratados de forma interdependente, reforçando a complexidade e a multidimensionalidade do debate.

5.2.4.14. As análises convergem para um mesmo diagnóstico: observa-se **uma crescente integração entre as agendas de proteção de dados e de inteligência artificial**. Temas como dados pessoais, governança de dados, tomada de decisão automatizada, discriminação algorítmica, IA generativa e cibersegurança aparecem de forma recorrente e fortemente associados entre si, sugerindo que futuras iniciativas regulatórias tendem a demandar abordagens transversais, capazes de lidar simultaneamente com aspectos tecnológicos, jurídicos e sociais. Os resultados também evidenciam que questões relacionadas a crianças e adolescentes permanecem relevantes, especialmente quando associadas aos impactos de sistemas algorítmicos, mecanismos de recomendação de conteúdo, verificação etária e riscos decorrentes da crescente digitalização das interações sociais.

5.2.4.15. Portanto, os resultados obtidos subsidiaram a seleção dos temas propostos para a Agenda Regulatória, funcionando como evidência complementar para corroborar sua relevância e contribuindo para a definição dos eixos prioritários de atuação.

5.3. **Marcos normativos legais e infralegais**

5.3.1. A LGPD, o ECA Digital e o Marco Civil da Internet operam de forma complementar e não isolada, formando um arcabouço regulatório coeso para o ambiente digital brasileiro. Enquanto a LGPD estabelece os princípios e fundamentos gerais de proteção de dados pessoais, aplicáveis a qualquer titular, o ECA Digital e seu Decreto nº 12.880/2026 particularizam essa proteção para crianças e adolescentes, impondo obrigações específicas de segurança, design seguro à idade e aferição etária. Já o Marco Civil da Internet, regulamentado pelos Decretos nº 12.975/2026 e nº 12.976/2026, disciplina o funcionamento da internet de forma mais ampla, estabelecendo deveres dos provedores de aplicações de internet, incluindo regras relativas ao devido processo de recebimento e tratamento de denúncias de conteúdo ilícito.

5.3.2. Esse arcabouço legal e regulatório em camadas permite que a ANPD, atuando como autoridade competente em múltiplos instrumentos legais, exerça suas competências de forma articulada e integrada, buscando estabelecer sinergias regulatórias e evitar sobreposições normativas. Como resultado, pode-se assegurar maior efetividade à proteção de dados pessoais e à segurança no ambiente digital de públicos vulneráveis.

5.3.3. **ECA Digital e Marco Civil da Internet – Decreto nº 12.975/2026 e Decreto nº 12.976/2026**

5.3.3.1. O avanço acelerado da presença de crianças e adolescentes em ambientes digitais evidenciou lacunas regulatórias que a legislação geral de proteção de dados, por si só, não conseguia endereçar de forma satisfatória. Nesse contexto, o ECA Digital surge como resposta normativa específica à necessidade de estabelecer parâmetros claros de responsabilização para fornecedores de produtos e serviços de tecnologia da informação, reconhecendo que crianças e adolescentes constituem público vulnerável que demanda proteções diferenciadas frente a riscos como exposição a conteúdo inadequado, manipulação comportamental por meio de padrões manipulativos (*dark patterns*) e ausência de mecanismos efetivos de aferição etária. A regulamentação por meio do Decreto nº 12.880/2026 complementa esse arcabouço ao detalhar obrigações operacionais, classificar categorias de plataformas conforme a atividade efetivamente exercida e delinear a cadeia de responsabilidades entre desenvolvedores de sistemas operacionais, lojas de aplicativos e provedores de aplicação.

5.3.3.2. Paralelamente, o Marco Civil da Internet (Lei nº 12.965/2014) foi objeto de nova regulamentação em maio de 2026, por meio dos Decretos nº 12.975/2026 e nº 12.976/2026, ambos publicados em 21 de maio de 2026. O primeiro promoveu atualização da regulamentação do Marco Civil da Internet ao alterar o Decreto nº 8.771, de 2016, estabelecendo novos deveres para provedores de conexão e de aplicações de internet, reforçando mecanismos de transparência, monitoramento e gestão dos riscos sistêmicos, definindo parâmetros para o cumprimento do dever de cuidado e disciplinando aspectos relacionados à fiscalização e à apuração de infrações, em articulação com as competências da ANPD. O decreto representa um marco geral de fortalecimento da governança dos serviços digitais e da proteção dos direitos dos usuários da internet, seguindo os parâmetros fixados em decisão recente do Supremo Tribunal Federal sobre o assunto (RE nº1037396 e nº 1057258).

5.3.3.3. Na sequência, o Decreto nº 12.976 de 2026, conferiu especial atenção à prevenção da violência digital contra mulheres e meninas. Em especial, os arts. 7º a 12 estabelecem deveres voltados à adoção de medidas destinadas a impedir ou reduzir a geração de conteúdos sintéticos que promovam exploração sexual, exposição íntima não consentida, falsificação da identidade e outras formas de violência facilitadas por sistemas de inteligência artificial e tecnologias de geração automatizada de conteúdo. O enfoque do decreto desloca a atuação regulatória para a origem do problema, buscando reduzir a produção desses conteúdos antes mesmo de sua circulação nas plataformas digitais.

5.3.3.4. Ademais, a implementação desse novo marco regulatório apresenta estreita relação com a proteção de dados pessoais, uma vez que a geração desses conteúdos normalmente depende do tratamento de dados capazes de identificar pessoas naturais, tais como fotografias, vídeos, registros biométricos, voz e outros atributos pessoais. A utilização dessas informações para criação de conteúdos sintéticos lesivos envolve operações de tratamento sujeitas às disposições da LGPD, especialmente no que se refere aos princípios da finalidade, necessidade, prevenção, segurança, não discriminação e responsabilização, bem como à proteção conferida aos direitos fundamentais dos titulares.

5.3.3.5. Sob a perspectiva regulatória, a aplicação articulada dos novos comandos normativos demanda reflexão acerca das medidas técnicas e organizacionais que podem ser adotadas pelos agentes de tratamento e pelos provedores de aplicações de internet para reduzir os riscos associados ao desenvolvimento e à utilização de sistemas capazes de gerar conteúdos ilícitos.

5.3.3.6. A convergência entre o ECA Digital, seu decreto regulamentador e esse novo arcabouço do Marco Civil, sob a coordenação técnica da ANPD à luz da LGPD, busca construir um ambiente digital mais seguro por meio de exigências proporcionais e tecnicamente fundamentadas, como aferição de idade adequada ao risco do conteúdo, design seguro por padrão, responsabilização em caso de falha sistêmica, de modo a equilibrar a proteção efetiva de públicos vulneráveis com a preservação de direitos fundamentais no meio digital.

5.3.3.7. Diante desse cenário, a inclusão de temas relacionados ao Marco Civil da Internet na próxima Agenda Regulatória permitirá à ANPD aprofundar medidas que instrumentalizem as obrigações e garantias previstas na legislação e nos Decretos nº 12.975 e nº 12.976 de 2026, contribuindo para a definição de parâmetros regulatórios voltados à prevenção de um ambiente digital mais protegido, incluindo a proteção dos direitos de mulheres e meninas.

5.3.4. **Proteção de dados pessoais**

5.3.4.1. A crescente digitalização das relações sociais, econômicas e institucionais, aliada ao desenvolvimento acelerado de sistemas de inteligência artificial, tem ampliado significativamente a utilização de dados pessoais como insumo para a prestação de serviços, a formulação de políticas públicas,

a oferta de produtos e a tomada de decisões automatizadas. Nesse contexto, a proteção de dados pessoais e da privacidade assume papel central na promoção da confiança no ambiente digital e na garantia dos direitos fundamentais dos titulares de dados.

5.3.4.2. A LGPD estabelece o marco normativo brasileiro para a disciplina do tratamento de dados pessoais, fundamentando-se em princípios como a finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização. Esses princípios adquirem especial relevância diante da crescente adoção de tecnologias baseadas em inteligência artificial, cujos modelos dependem, em larga medida, da coleta, utilização e análise de volumes massivos de dados para treinamento, desenvolvimento e operação.

5.3.4.3. A evolução dessas tecnologias tem intensificado debates acerca dos impactos do tratamento automatizado de dados pessoais sobre direitos e liberdades fundamentais. Entre os principais desafios regulatórios destacam-se a ocorrência de vieses algorítmicos capazes de produzir resultados discriminatórios ou injustos, a realização de inferências comportamentais e preditivas a partir de dados pessoais, o perfilamento de indivíduos para fins comerciais, administrativos ou decisórios, bem como a crescente utilização de sistemas de decisão automatizada com potencial de produzir efeitos relevantes sobre os titulares.

5.3.4.4. A utilização de modelos de inteligência artificial também amplia a complexidade dos processos de tratamento de dados pessoais, tornando mais desafiadora a observância de princípios como a transparência e a explicabilidade das decisões automatizadas. Em muitos casos, a elevada complexidade técnica dos sistemas dificulta a compreensão dos critérios empregados na tomada de decisões, o exercício efetivo dos direitos dos titulares e a demonstração da conformidade pelos agentes de tratamento, reforçando a necessidade de parâmetros regulatórios que promovam maior segurança jurídica e reduzam riscos aos direitos fundamentais.

5.3.4.5. A própria LGPD contempla mecanismos destinados a enfrentar parte desses desafios, ao prever direitos relacionados às decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, bem como ao estabelecer a adoção de medidas de segurança, prevenção e governança capazes de mitigar riscos decorrentes das atividades de tratamento. Entretanto, a rápida evolução tecnológica e a crescente diversidade de aplicações de inteligência artificial evidenciam a necessidade de aprofundamento regulatório sobre aspectos relacionados à utilização responsável dessas tecnologias, especialmente em situações que envolvam elevado potencial de impacto sobre direitos individuais e coletivos.

5.3.4.6. Ademais, como notado no cenário internacional, observa-se um movimento de fortalecimento das estruturas regulatórias voltadas à governança da inteligência artificial, com crescente preocupação em assegurar que o desenvolvimento e a utilização dessas tecnologias ocorram de forma ética, transparente, segura e compatível com os direitos fundamentais. Esse contexto reforça a importância de uma atuação regulatória coordenada em matéria de proteção de dados pessoais, capaz de harmonizar inovação tecnológica, desenvolvimento econômico e salvaguardas adequadas à privacidade e à autodeterminação informativa.

5.4. **Cenário internacional**

5.4.1. **Garantia de direitos de crianças e adolescentes e promoção de um ambiente digital seguro**

5.4.1.1. O benchmarking internacional evidencia que a proteção de crianças e adolescentes constitui prioridade consolidada entre as principais autoridades de proteção de dados,
como *European Data Protection Board* (EDPB), *Commission Nationale de l'Informatique et des Libertés* (CNIL), *Information Commissioner's Office* (ICO), *Federal Trade Commission* (FTC)
e *Office of the Australian Information Commissioner* (OAIC).

5.4.1.2. A relevância da proteção de crianças e adolescentes na agenda institucional do EDPB foi reafirmada no Dia Europeu da Proteção de Dados de 2026, ocasião em que o órgão destacou sua trajetória de atuação voltada à manutenção da segurança dos dados pessoais de crianças no ambiente digital.Entre as iniciativas mencionadas, destaca-se a adoção, em fevereiro de 2024, de uma declaração sobre os desenvolvimentos legislativos relacionados à Proposta de Regulamento destinado àprevenção e ao combate do abuso sexual infantil online [2].Em fevereiro de 2025, o EDPB adotou ainda uma declaração sobremecanismos deverificação etária(*ageassurance* [3]), com o objetivo de orientar organizações na implementação de métodos para verificação etária compatíveis com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR). No mesmo documento, o EDPB estabeleceu dez princípios para o tratamento lícito de dados pessoais em processos de determinação da idade ou da faixa etária de indivíduos. Além dessas iniciativas, a proteção de crianças permanece inserida na agenda estratégica do Conselho para o período 2024-2027. Entre as ações em desenvolvimento destaca-se a elaboração dediretrizes específicas sobre o tratamento de dados pessoais de crianças, destinadas a promover maior uniformidade interpretativa e orientar controladores e operadores quanto às obrigações decorrentes do GDPR nesse contexto.

5.4.1.3. A CNIL, em janeiro de 2025, publicou seuPlano Estratégico 2025-2028, [4] estruturado em quatro grandes eixos: inteligência artificial, proteção de crianças e adolescentes, cibersegurança e usos cotidianos do ambiente digital. A proteção de crianças e adolescentes ocupa o segundo eixo estratégico,

sendo declarada "prioridade absoluta" pela presidenta do CNIL.

5.4.1.4. A prioridade absoluta conferida à proteção de crianças e adolescentes revela-se pela criação de um eixo estratégico específico denominado “Proteger os menores e seus dados no universo digital”. Esse eixo estrutura-se em quatro objetivos complementares. O primeiro consiste em ampliar a presença da CNIL junto a crianças, pais e agentes educacionais, por meio de ações de sensibilização, parcerias com a comunidade educativa e fortalecimento da atuação territorial da autoridade. O segundo busca assegurar a crianças e adolescentes o exercício efetivo de seus direitos, incluindo iniciativas para ampliar a compreensão sobre proteção de dados, adaptar interfaces digitais às necessidades desse público e facilitar o acesso a mecanismos de reclamação e exercício de direitos. O terceiro objetivo é promover o uso responsável do ambiente digital em âmbito nacional e internacional, mediante ações educativas voltadas à compreensão dos riscos associados aos serviços digitais, ao desenvolvimento de materiais pedagógicos elaborados com a participação dos próprios jovens e à articulação com redes institucionais nacionais e internacionais. Por fim, o quarto objetivo prevê o controle e a fiscalização dos operadores que oferecem serviços online ao público infantojuvenil, com foco especial em redes sociais, plataformas educacionais, jogos eletrônicos e demais serviços digitais utilizados por menores, especialmente quanto às práticas de coleta de consentimento, publicidade e tratamento de dados pessoais.

5.4.1.5. Os quatro objetivos revelam uma concepção abrangente de proteção infantojuvenil, baseada na combinação entre educação, garantia de direitos, participação social e fiscalização regulatória. A estratégia aproxima-se das tendências internacionais mais recentes de governança digital voltadas à infância, nas quais a proteção de dados deixa de ser uma questão meramente técnica para assumir uma dimensão de desenvolvimento integral, segurança digital e promoção dos direitos fundamentais de crianças e adolescentes. Essa abordagem sugere que, para a CNIL, a proteção da privacidade de crianças e adolescentes constitui não apenas um tema setorial, mas uma condição necessária para o exercício seguro da cidadania na sociedade digital.

5.4.1.6. Já a abordagem adotada pelo ICO parte do entendimento de que determinadas populações enfrentam assimetrias de poder mais intensas nas relações de tratamento de dados, exigindo atenção regulatória reforçada. Nesse contexto, crianças figuram entre os públicos prioritários da estratégia institucional de proteção e empoderamento de pessoas, especialmente no âmbito do objetivo estratégico de “salvaguardar e empoderar o público, particularmente os grupos vulneráveis”.

5.4.1.7. A principal manifestação dessa prioridade ocorre por meio da implementação e fiscalização do *Children’s Code* (*Age Appropriate Design Code*), instrumento regulatório que estabelece padrões para serviços digitais acessados por crianças. O plano prevê a continuidade das ações de fiscalização e de influência regulatória sobre plataformas digitais, incluindo redes sociais, serviços de streaming e plataformas de jogos, com foco na verificação da idade dos usuários, na limitação de práticas deperfilização, na proteção contra o compartilhamento excessivo de dados e na adoção de avisos de privacidade compreensíveis para o público infantil. A estratégia demonstra preocupação não apenas com a conformidade formal das organizações, mas também com a efetividade da experiência digital das crianças, aproximando-se da lógica de *privacy by design* e de proteção adequada ao estágio de desenvolvimento do usuário.

5.4.1.8. O tema também aparece associado aos impactos de tecnologias emergentes sobre grupos vulneráveis. O ICO reconhece que sistemas algorítmicos, inteligência artificial, tecnologias biométricas e mecanismos de rastreamento online podem produzir efeitos discriminatórios ou ampliar vulnerabilidades preexistentes. Embora as crianças não sejam o único grupo contemplado por essas preocupações, elas integram o conjunto de indivíduos potencialmente expostos a riscos decorrentes da coleta massiva de dados, daperfilizaçãocomportamental e da tomada automatizada de decisões. A estratégia, portanto, articula a proteção da infância com debates mais amplos sobre governança algorítmica, transparência e uso ético de tecnologias digitais.

5.4.1.9. Os Estados Unidos da América não adotam um modelo de proteção de dados baseado em uma legislação geral e abrangente equivalente ao GDPR europeu ou à LGPD brasileira. Em vez disso, o país possui uma estrutura regulatória fragmentada, composta por normas setoriais e estaduais aplicáveis a contextos específicos.

5.4.1.10. Nesse cenário, a *Federal Trade Commission* desempenha papel central na supervisão de práticas relacionadas à privacidade e ao uso de dados pessoais. Contudo, sua atuação está fundamentada predominantemente na proteção do consumidor e na repressão a práticas comerciais desleais ou enganosas, e não em uma concepção da proteção de dados como direito fundamental autônomo.

5.4.1.11. A análise do Plano Estratégico 2026–2030 do FTC [5] revela que a proteção de crianças e adolescentes ocupa posição de destaque na agenda, sendo apresentada como “uma das mais importantes questões contemporâneas de proteção do consumidor do nosso tempo”. Crianças e adolescentes são tratados como consumidores particularmente vulneráveis a fraudes, golpes, práticas abusivas e riscos do ambiente digital.

5.4.1.12. No “Objetivo Estratégico 1: Proteger os americanos de atos ou práticas injustas ou enganosas no mercado”, é

estabelecido que

> Proteger as crianças online também é uma preocupação central, e um ponto onde a FTC está concentrando suas ferramentas e recursos de proteção ao consumidor. O Congresso autorizou o papel da FTC na aplicação da lei nessa área, principalmente por meio da Lei de Proteção à Privacidade Online das Crianças (COPPA), que proíbe operadores de sites de coletar, usar ou divulgar dados pessoais de usuários menores de treze anos sem consentimento dos pais. Um dos trabalhos mais valiosos da FTC são seus esforços contínuos para aplicar a COPPA contra empresas que não cumprem seus requisitos. A FTC também está dedicada a explorar outras formas de proteger as crianças e apoiar suas famílias, inclusive por meio de sua nova competência sob a Lei *Take It Down* (FTC, 2026, p.7).

5.4.1.13. A centralidade atribuída à COPPA demonstra que a estratégia da agência está fortemente ancorada no controle da coleta e do uso de informações pessoais de menores de 13 anos por empresas e plataformas digitais. Nesse sentido, a prioridade institucional não é apenas educativa ou preventiva, mas sobretudo de *enforcement*, com destaque para a responsabilização de organizações que descumprem as regras de consentimento parental e tratamento de dados de crianças. O trecho também evidencia uma ampliação gradual do escopo de atuação da FTC. Embora a COPPA continue sendo o principal instrumento jurídico para a proteção da privacidade infantil, a referência à Lei *Take It Down Act*, norma recentemente aprovada e que considera ilegal a publicação de imagens íntimas reais ou geradas ou modificadas por IA sem consentimento, sugere uma preocupação crescente com novos riscos digitais que afetam crianças e adolescentes, especialmente aqueles relacionados à disseminação de conteúdos íntimos, exploração online e outras formas de danos decorrentes do ambiente digital. Observa-se, portanto, um movimento de expansão da proteção infantil para além da privacidade, incorporando preocupações mais amplas com segurança, bem-estar e proteção contra abusos digitais.

5.4.1.14. O OAIC, agência federal australiana, recebeu a responsabilidade de desenvolver o *Children's Online Privacy Code* (COPC) até dezembro de 2026 após a aprovação da *Privacy and Other Legislation Amendment Act* 2024 (POLA *Act*), a maior reforma da legislação de privacidade do país em mais de 30 anos.

5.4.1.15. O código aplica-se a mídiassociais, serviços eletrônicos eoutrosserviços deinternet.A minutado COPC propõe obrigações que incluem: configurações de privacidade por padrão para crianças; restrições à publicidade direcionada; direito à eliminaçãode dados; limitações ao uso de dados para perfilação; e requisitos reforçados de transparência. O OAIC destacou que algumas dessas proteções serão inéditas, buscando garantir que as crianças australianas se beneficiem de abordagens do estado da arte em proteção da privacidade.

5.4.1.16. Em complemento ao COPC, a Austrália é o primeiro país do mundo a proibir, por lei, o acesso de menores de 16 anos a redes sociais. O *Online Safety Amendment (Social Media Minimum Age) Act*, aprovado em novembro de 2024, entrou em vigor em dezembro de 2025. O OAIC sinalizou que oCOPC cobrirá uma gama muito mais ampla de serviços online do que apenas as plataformas de redes sociais, protegendo a privacidade infantil também em jogos, plataformas de streaming e ferramentas educacionais.

5.4.1.17. O fortalecimento de mecanismos destinados a prevenir a utilização abusiva de dados pessoais na geração de conteúdos sintéticos lesivos configura uma tendência regulatória internacional em consolidação. Em 23 de fevereiro de 2026, a Global Privacy Assembly (GPA) coordenou a *Joint Statement on AI-Generated Imagery and the Protection of Privacy* [6], com apoio do EDPB, por meio da qual se recomenda que desenvolvedores e fornecedores de sistemas de inteligência artificial adotem medidas técnicas e organizacionais para prevenir a geração de conteúdos sintéticos que possam violar direitos fundamentais, com especial atenção aos riscos de exploração sexual, falsificação de identidade, exposição íntima não consentida e outras formas de violência digital que afetam de maneira desproporcional mulheres e crianças e adolescentes.

5.4.1.18. Essa orientação é consistente com a abordagem adotada pela União Europeia no *AI Act*, que introduz obrigações de transparência para conteúdos sintéticos e reforça a necessidade de gestão de riscos, governança e implementação de salvaguardas ao longo do ciclo de vida dos sistemas de inteligência artificial. Em conjunto, esses instrumentos evidenciam uma mudança de enfoque regulatório, que passa a atribuir maior responsabilidade aos desenvolvedores e fornecedores de sistemas de IA na gestão de riscos e na prevenção de danos antes da disponibilização e utilização das tecnologias.

5.4.1.19. No mesmo sentido, o ICO, signatário da declaração da GPA, tem recomendado, por meio de seus guias sobre inteligência artificial e proteção de dados, a adoção de mecanismos de *privacy by design*, avaliações prévias de risco e controles técnicos destinados a reduzir a geração de conteúdos sintéticos abusivos. A CNIL, em seu *AI Action Plan* e nas orientações sobre desenvolvimento de sistemas de IA em conformidade com o GDPR, também enfatiza a incorporação de salvaguardas para proteção da identidade, da imagem e dos direitos da personalidade, especialmente em aplicações baseadas em modelos generativos. Na Austrália, o OAIC recomenda que desenvolvedores realizem avaliações de impacto e implementem mecanismos de governança capazes de mitigar riscos associados ao uso de dados pessoais e biométricos em

sistemas generativos. Nos Estados Unidos, a FTC, embora sob a ótica da proteção do consumidor, tem intensificado ações de *enforcement* contra usos enganosos da inteligência artificial, incluindo práticas relacionadas à falsificação de identidade, à manipulação digital e ao uso indevido da imagem de pessoas naturais.

5.4.2. **Privacidade e direito fundamental à proteção de dados pessoais**

5.4.2.1. O benchmarking internacional contemplou a atuação das principais autoridades de proteção de dados com produção normativa e regulatória relevante sobre o tratamento de dados pessoais no contexto da inteligência artificial e com foco na garantia de direitos de usuários e na proteção de crianças e adolescentes no ambiente digital: o EDPB, o ICO, a CNIL, a FTC e o OAIC.

5.4.2.2. De modo geral, verifica-se convergência entre essas autoridades quanto à necessidade de que o desenvolvimento e a utilização de sistemas de inteligência artificial observem princípios de proteção de dados pessoais, tais como finalidade, necessidade, minimização, transparência, segurança, não discriminação, responsabilização (*accountability*) e proteção de dados desde a concepção (*privacy by design*) e por padrão (*privacy by default*).

5.4.2.3. No âmbito europeu, o EDPB tem consolidado a interpretação do GDPR por meio de diretrizes sobre decisões automatizadas, perfilamento, interesse legítimo, avaliações de impacto sobre a proteção de dados (*Data Protection Impact Assessment* – DPIA) e, mais recentemente, pareceres relacionados ao desenvolvimento e à utilização de modelos de inteligência artificial. Essas orientações dialogam diretamente com o novo marco europeu estabelecido pelo *AI Act*, que adota abordagem baseada em risco e prevê obrigações específicas para provedores e usuários de sistemas de IA de alto risco.

5.4.2.4. No Reino Unido, o ICO desenvolveu um conjunto abrangente de instrumentos voltados à governança da inteligência artificial, destacando-se o *AI Auditing Framework*, o *AI and Data Protection Risk Toolkit* e as orientações sobre decisões automatizadas e explicabilidade (*Explaining Decisions Made with AI*). Esses documentos enfatizam a realização de avaliações de risco, a supervisão humana, a mitigação de vieses algorítmicos e a adoção de mecanismos de prestação de contas.

5.4.2.5. Na França, a CNIL publicou uma estratégia específica para inteligência artificial (*AI Action Plan*), acompanhada de uma série de guias sobre inteligência artificial generativa, treinamento de modelos, reutilização de bases de dados, anonimização e utilização de dados públicos. A autoridade francesa também tem enfatizado a compatibilização entre inovação tecnológica e proteção dos direitos fundamentais, especialmente quanto à transparência, à governança dos dados e à qualidade dos conjuntos utilizados para treinamento.

5.4.2.6. Nos Estados Unidos, embora inexista uma legislação federal abrangente de proteção de dados pessoais, a FTC vem desempenhando papel central na disciplina do uso de dados em sistemas de IA por meio de sua atuação fiscalizatória e da publicação de documentos como *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI* e *Keep Your AI Claims in Check*. A atuação da agência concentra-se na prevenção de práticas enganosas, na mitigação de discriminação algorítmica e na responsabilização de empresas que utilizem dados pessoais de forma incompatível com as expectativas dos consumidores ou realizem alegações infundadas sobre sistemas de IA.

5.4.2.7. Na Austrália, o OAIC tem estruturado sua atuação por meio de orientações sobre privacidade e inteligência artificial, em especial o documento *Guidance on Privacy and Developing and Training Generative AI Models*, além de recomendações para realização de avaliações de impacto, adoção de medidas de *privacy by design* e fortalecimento da governança de dados ao longo do ciclo de vida dos sistemas de IA.

5.4.2.8. Em conjunto, esses referenciais demonstram tendência regulatória convergente no sentido de fortalecer mecanismos de governança, gestão de riscos e prestação de contas, avaliações prévias de impacto, transparência, supervisão humana, prevenção de discriminação algorítmica e responsabilização dos agentes de tratamento, buscando assegurar que o desenvolvimento e a utilização de sistemas de inteligência artificial sejam compatíveis com a proteção dos direitos fundamentais e da privacidade dos titulares de dados.

5.5. **Ações Regulatórias**

5.5.1. Com vistas a conferir maior organização, clareza e comunicabilidade às ações que compõem a Agenda Regulatória 2027/2028, optou-se pela estruturação das ações regulatórias em dois eixos temáticos distintos: (i) **Garantia de Direitos de Crianças e Adolescentes e Promoção de um Ambiente Digital Seguro**, que reúne as ações voltadas à proteção de usuários no ambiente digital, com destaque para a regulamentação do ECA Digital e para os desdobramentos regulatórios relacionados à proteção de públicos vulneráveis nas plataformas digitais; e (ii) **Privacidade e Direito Fundamental à Proteção de Dados Pessoais**, que congrega as ações relacionadas à aplicação e ao aprimoramento regulatório da LGPD.

5.5.2. **Ações regulatórias propostas**

Eixo Temático 1: Garantia de direitos de crianças e adolescentes e promoção de um ambiente digital seguro

Padrões de *design* seguro

5.5.2.1. Os dark pa*tterns* consistem em elementos de design de interfaces digitais concebidos para influenciar, direcionar ou manipular o comportamento dos usuários de maneira contrária ou potencialmente contrária aos seus interesses, comprometendo sua capacidade de realizar escolhas livres, conscientes e informadas. Essas práticas podem se manifestar por meio da arquitetura das interfaces, da organização das informações, da utilização de mecanismos de pressão psicológica, da exploração de vieses cognitivos ou da criação de obstáculos artificiais ao exercício de direitos, influenciando decisões relacionadas ao compartilhamento de dados pessoais, à contratação de serviços, à realização de compras, ao fornecimento de consentimento e à permanência em ambientes digitais.

5.5.2.2. A crescente sofisticação das interfaces digitais, aliada ao uso intensivo de dados pessoais, técnicas de personalização e sistemas algorítmicos, ampliou a capacidade dos fornecedores de produtos e serviços digitais de moldar o comportamento dos usuários por meio do design das plataformas. Em muitos casos, essas estratégias não se limitam a melhorar a experiência do usuário, mas são utilizadas para induzir decisões que favorecem interesses comerciais dos fornecedores, reduzindo a autonomia dos titulares e dificultando o exercício de seus direitos.

5.5.2.3. Os riscos decorrentes dessas práticas tornam-se ainda mais relevantes quando envolvem crianças e adolescentes, em razão de sua menor capacidade de identificar mecanismos de manipulação comportamental e de sua maior suscetibilidade à influência exercida pela arquitetura das interfaces digitais. Nessas situações, escolhas relacionadas ao compartilhamento de dados pessoais, ao consumo de conteúdos, à realização de compras ou ao exercício de direitos podem ser significativamente condicionadas por elementos de design concebidos para direcionar comportamentos.

5.5.2.4. Os arts. 8º, IV, 17, § 4º, II e 18, § 2º do ECA Digital e o art. 9º do Decreto nº 12.880/2026 exigem que fornecedores de produtos e serviços de tecnologia da informação adotem padrões de design seguros e implementem mecanismos contra o uso excessivo, problemático ou compulsivo por crianças e adolescentes. O art. 10 do Decreto nº 12.880/2026 atribui à ANPD competência para estabelecer requisitos mínimos de segurança por padrão e coibir a adoção de práticas manipulativas, enganosas ou coercitivas. A criação de um marco conceitual uniforme para identificar tais práticas no arcabouço regulatório visa a aprimorar a atuação da Agência e proteger o melhor interesse desse público.

5.5.2.5. Nesse contexto, o escopo preliminar da ação regulatória consiste em estabelecer requisitos mínimos para avaliação e implementação de padrões de *design* seguro em produtos ou serviços de tecnologia da informação, incluindo requisitos de transparência e prestação de contas. É relevante, ainda, conferir tratamento diferenciado e proporcional a serviços de natureza, risco e modelo de negócio distintos, considerando, ademais, o porte econômico do provedor, o nível de interferência na circulação de conteúdo de terceiros e o estado da técnica.

Uso de IA generativa por crianças e adolescentes

5.5.2.6. O art. 11 do Decreto nº 12.880/2026 estabelece obrigações para fornecedores de produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes ou de acesso provável por eles capazes de gerar conteúdo e interagir com usuários em linguagem natural. A rápida difusão de sistemas de inteligência artificial generativa, especialmente agentes conversacionais e interfaces similares (como *AI companions* e *chatbots*) entre crianças e adolescentes, traz desafios específicos para a proteção desse público, em razão da possibilidade de antropomorfismo, criação de vínculos afetivos, dependência emocional, manipulação comportamental e estímulo a condutas de risco. Nesse contexto, a necessidade de regulamentação decorre da necessidade de conferir efetividade às obrigações previstas no decreto e assegurar sua aplicação de forma compatível com a proteção integral e o melhor interesse de crianças e adolescentes.

5.5.2.7. A ação regulatória tem como objetivo estabelecer parâmetros claros e proporcionais para a implementação das obrigações previstas no art. 11, considerando os diferentes riscos associados ao uso de sistemas de inteligência artificial generativa por crianças e adolescentes. Entre os principais aspectos a serem disciplinados estão a transparência e a sinalização do caráter sintético e automatizado das interações; a prevenção de práticas de manipulação comportamental, inclusive aquelas relacionadas ao antropomorfismo e à formação de vínculos afetivos; os critérios para identificação, avaliação e mitigação de riscos algorítmicos à segurança, à saúde e ao desenvolvimento físico, mental e psicossocial; e a definição de salvaguardas mínimas e proporcionais aos riscos identificados.

5.5.2.8. A intervenção regulatória busca, assim, reduzir a incerteza quanto à aplicação das obrigações impostas aos fornecedores, promover maior uniformidade na adoção de medidas de proteção e fornecer parâmetros que possibilitem a fiscalização de sua implementação. Espera-se, com isso, fortalecer a segurança e a transparência no uso de inteligência artificial generativa por crianças e adolescentes, prevenir a exploração de suas vulnerabilidades e assegurar que o desenvolvimento e a disponibilização desses sistemas sejam compatíveis com a proteção integral, o melhor interesse e a autonomia progressiva desse público.

Supervisão parental

5.5.2.9. Os arts. 16 a 18 do ECA Digital estabelecem que fornecedores de plataformas e serviços digitais que apresentem risco significativo para crianças e adolescentes devem disponibilizar mecanismos eficazes de supervisão parental, bem como submetê-los à apreciação da autoridade administrativa autônoma, nos termos previstos na própria lei.

5.5.2.10. Entretanto, o marco legal não define os critérios técnicos, funcionais e procedimentais para a implementação, avaliação e aprovação desses mecanismos. Também não estabelece parâmetros mínimos quanto às funcionalidades obrigatórias, aos limites legítimos do monitoramento parental, às salvaguardas de privacidade e proteção de dados, aos requisitos de transparência, à usabilidade ou ao tratamento diferenciado conforme a faixa etária e o desenvolvimento progressivo da criança e do adolescente.

5.5.2.11. A ausência de regulamentação pode resultar na oferta de ferramentas com níveis heterogêneos de proteção, insuficientes para mitigar riscos relevantes ou, em sentido oposto, excessivamente invasivas, comprometendo direitos fundamentais como a privacidade, a autodeterminação informacional e o livre desenvolvimento da personalidade, especialmente no caso dos adolescentes.

5.5.2.12. Nesse contexto, o escopo preliminar da ação regulatória consiste em estabelecer critérios e procedimentos para a apreciação, implementação e funcionamento dos mecanismos de supervisão parental previstos no ECA Digital, disciplinando requisitos mínimos de eficácia, transparência, segurança, proteção de dados pessoais, acessibilidade, interoperabilidade e proporcionalidade, bem como parâmetros para sua avaliação pela autoridade administrativa competente.

5.5.2.13. Embora diversos fornecedores disponibilizem ferramentas de controle parental, inexiste padronização quanto às funcionalidades essenciais, aos níveis de proteção esperados, às salvaguardas de privacidade e aos critérios para sua utilização de forma proporcional às diferentes faixas etárias. Essa heterogeneidade gera insegurança jurídica para os agentes regulados, dificulta a fiscalização pela ANPD e pode comprometer tanto a proteção integral de crianças e adolescentes quanto o respeito aos seus direitos fundamentais.

5.5.2.14. Além disso, a própria lei atribui à ANPD a competência para poder apreciar os mecanismos de supervisão parental, tornando indispensável a definição de critérios técnicos, procedimentais e de governança que assegurem previsibilidade, isonomia e transparência na análise dos mecanismos submetidos à sua apreciação.

5.5.2.15. Assim, a intervenção regulatória mostra-se necessária para conferir efetividade aos arts. 16 a 18 do ECA Digital, mediante a definição de critérios objetivos para a implementação e avaliação dos mecanismos de supervisão parental.

Habilitação de entidades representativas de direitos de crianças e adolescentes

5.5.2.16. O art. 29 do Eca Digital estabelece o dever de fornecedores de remover conteúdos que violem direitos de crianças e adolescentes após notificação efetuada, entre outros, por “entidades representativas de defesa de direitos de crianças e de adolescentes”.

5.5.2.17. O art. 44 do Decreto nº 12.880/2026 atribui a ANPD competência para dispor sobre requisitos, procedimentos e prazos relativos ao credenciamento, supervisão e o descredenciamento dessas entidades. Não obstante a regra provisória prevista no art. 52 do Decreto nº 12.880/2026, é necessário disciplinar a matéria para assegurar previsibilidade, isonomia e efetividade ao processo de credenciamento.

5.5.2.18. A ausência de disciplina específica pode resultar em interpretações divergentes quanto aos requisitos necessários ao reconhecimento das entidades, dificultar a uniformidade das decisões administrativas e comprometer a transparência, a previsibilidade e a segurança jurídica do processo de credenciamento.

5.5.2.19. Nesse contexto, o escopo preliminar da ação regulatória consiste em estabelecer os requisitos de qualificação das entidades representativas dos direitos de crianças e adolescentes e disciplinar o procedimento de credenciamento, abrangendo, entre outros aspectos, o fluxo processual, a unidade administrativa responsável pela análise dos pedidos, os prazos aplicáveis, os critérios para renovação da habilitação, as hipóteses e o procedimento de descredenciamento, bem como os direitos e as prerrogativas decorrentes da habilitação.

5.5.2.20. A regulamentação busca, portanto, estabelecer parâmetros uniformes e procedimentos padronizados que assegurem tratamento isonômico às entidades interessadas, transparência, segurança jurídica e eficiência administrativa, promovendo um processo de credenciamento objetivo, previsível e compatível com as finalidades do Decreto nº 12.880/2026 e do ECA Digital.

Canal de denúncia e procedimentos de notificação sobre conteúdos ilícitos ou criminosos

5.5.2.21. Os arts. 28 a 30 do ECA Digital estabelecem obrigações aos fornecedores de produtos e serviços de tecnologia da informação quanto à disponibilização de mecanismos de notificação de violações aos direitos de crianças e adolescentes, à retirada prioritária e imediata de conteúdos ofensivos e à garantia do direito de contestação das decisões de moderação. O art. 43 do Decreto nº 12.880/2026 complementa esse regime ao disciplinar as hipóteses de retirada imediata de conteúdo, enquanto os arts. 16-D, parágrafo único, e 16-F do Decreto nº

12.975/2026 estabelecem regras gerais sobre notificações extrajudiciais e medidas para prevenir o uso abusivo dos sistemas de denúncia, em especial com vistas a assegurar o respeito à liberdade de expressão.

5.5.2.22. Embora o marco normativo discipline as obrigações essenciais, permanecem indefinidos os parâmetros para sua operacionalização, especialmente quanto aos requisitos das notificações, aos fluxos procedimentais, aos prazos, às formas de comunicação das decisões, aos procedimentos de contestação e revisão e às salvaguardas contra denúncias abusivas. A ausência de regulamentação específica pode resultar em procedimentos distintos entre os fornecedores, insegurança jurídica e dificuldades na fiscalização do cumprimento das obrigações legais.

5.5.2.23. Nesse contexto, o escopo preliminar da ação regulatória consiste em estabelecer diretrizes e requisitos mínimos para os procedimentos de notificação, retirada, contestação e revisão de conteúdos ilícitos ou criminosos, incluindo aqueles que violem direitos de crianças e adolescentes, disciplinando os requisitos das notificações, os fluxos procedimentais, os prazos, os requisitos mínimos para a disponibilização de canal de denúncia, os deveres de comunicação e transparência, as salvaguardas contra notificações abusivas e a harmonização entre o regime especial do ECA Digital e as regras gerais do Decreto nº 12.975/2026.

5.5.2.24. A regulamentação busca conferir efetividade ao marco normativo, promovendo maior uniformidade, previsibilidade, transparência e segurança jurídica na implementação dos procedimentos de notificação e moderação, de forma a fortalecer a proteção integral de crianças e adolescentes e assegurar o equilíbrio entre a celeridade na remoção de conteúdos ilícitos, o devido processo e os direitos dos usuários.

Acesso a dados de provedores de aplicações de internet por instituições acadêmicas, científicas, tecnológicas, de inovação e jornalísticas

5.5.2.25. O parágrafo único do art. 31 da Lei nº 15.211/2025 dispõe que os provedores de aplicações de internet deverão viabilizar, de forma gratuita, o acesso a dados necessários à realização de pesquisas sobre os impactos de seus produtos e serviços nos direitos de crianças e adolescentes, por instituições acadêmicas, científicas, tecnológicas, de inovação ou jornalísticas, observados os critérios definidos em regulamento e os princípios da finalidade, necessidade, segurança e confidencialidade. O art. 48 do Decreto nº 12.880/2026 atribui à ANPD a competência para habilitar essas instituições, mediante edital público, com base em requisitos mínimos relacionados à finalidade institucional, qualificação técnica, plano de pesquisa, inexistência de finalidade comercial e governança e segurança da informação.

5.5.2.26. A disponibilização de dados a essas instituições integra e fortalece a transparência, a prestação de contas e o processo de supervisão e análise periódica de provedores de aplicações de internet, notadamente quanto a aspectos como o monitoramento de riscos sistêmicos relacionados às suas atividades, na forma prevista no Marco Civil da Internet e decretos regulamentadores.

5.5.2.27. Embora o marco normativo estabeleça critérios gerais para a habilitação, permanecem indefinidos os procedimentos para seleção, certificação e supervisão das instituições, bem como as condições de acesso, utilização, compartilhamento, retenção e eliminação dos dados, as responsabilidades dos agentes envolvidos e as salvaguardas necessárias à proteção de dados pessoais, de informações sensíveis e de segredos comerciais. A ausência de regulamentação específica pode gerar insegurança jurídica, dificultar o acesso a dados para pesquisas de interesse público e comprometer a uniformidade, a transparência e a segurança no tratamento dessas informações.

5.5.2.28. Nesse contexto, o escopo preliminar da ação regulatória consiste em estabelecer diretrizes e requisitos mínimos para a habilitação das instituições previstas no art. 48 do Decreto nº 12.880/2026 e disciplinar as condições de acesso, tratamento, utilização, compartilhamento, retenção e eliminação dos dados disponibilizados pelos provedores de aplicações de internet, bem como os procedimentos de supervisão, prestação de contas e responsabilização das instituições habilitadas.

5.5.2.29. A regulamentação busca conferir efetividade ao marco normativo, promovendo maior previsibilidade, uniformidade, transparência e segurança jurídica no acesso e tratamento dos dados, assegurando a proteção dos direitos dos titulares, a preservação de informações protegidas por sigilo e o fortalecimento da produção de conhecimento científico e técnico voltado à proteção de crianças e adolescentes no ambiente digital.

Marco Civil da Internet: escopo e obrigações gerais

5.5.2.30. O Marco Civil da Internet, conforme regulamentado pelo Decreto nº 8.771/2016, com redação dada pelo Decreto nº 12.975/2026, dispõe sobre obrigações gerais aplicáveis aos provedores de aplicações de internet voltadas à prevenção e mitigação de riscos decorrentes da prestação de seus serviços, incorporando conceitos como dever de cuidado, risco sistêmico, falha sistêmica e dúvida razoável. Embora o decreto institua essas obrigações e conceitos, sua aplicação prática demanda regulamentação complementar que confira maior objetividade, previsibilidade e uniformidade à sua interpretação e implementação.

5.5.2.31. A ação regulatória tem objetivo de delimitar o

alcance dessas obrigações gerais, conferindo segurança jurídica aos agentes regulados e efetividade à atuação fiscalizatória da ANPD.

5.5.2.32. Nesse contexto, o escopo preliminar da ação regulatória consiste em estabelecer diretrizes e critérios para a interpretação e aplicação dos conceitos de dever de cuidado, risco sistêmico, falha sistêmica e dúvida razoável, bem como definir parâmetros mínimos para o cumprimento das obrigações gerais previstas no Decreto nº 12.975/2026, observados os princípios da proporcionalidade, da transparência, da proteção dos direitos fundamentais, da segurança jurídica e da adequada gestão de riscos no ambiente digital.

5.5.2.33. A regulamentação busca conferir efetividade ao marco regulatório, promovendo maior segurança jurídica, uniformidade conceitual e transparência na implementação das obrigações gerais, de modo a favorecer práticas consistentes de gestão de riscos, prevenção de danos e proteção dos direitos fundamentais, preservando a inovação tecnológica e a livre iniciativa.

Transparência, prestação de contas e mecanismos de supervisão e análise periódica

5.5.2.34. O art. 31 do ECA Digital dispõe que os provedores de aplicações de internet direcionadas ou de acesso provável por crianças e adolescentes com mais de 1.000.000 de usuários registrados nessa faixa etária deverão elaborar e publicar, semestralmente, relatórios sobre canais de denúncia, moderação de conteúdo, identificação de contas infantis e atos ilícitos, proteção de dados pessoais, consentimento parental e avaliação e gestão de riscos. Os arts. 16-A a 16-C do Decreto nº 8.771/2016, com redação dada pelo Decreto nº 12.975/2026, complementam esse regime ao disciplinar obrigações de transparência, monitoramento e gestão contínua de riscos sistêmicos, enquanto o art. 47 do Decreto nº 12.880/2026 trata do acompanhamento dessas obrigações pela autoridade competente.

5.5.2.35. Embora o marco normativo estabeleça deveres de transparência, prestação de contas e gestão de riscos, permanecem indefinidos os parâmetros mínimos relativos ao conteúdo, ao grau de detalhamento, às metodologias, ao formato e à padronização dos relatórios, bem como aos mecanismos de supervisão e análise periódica. A ausência de regulamentação específica pode comprometer a uniformidade das informações, dificultar a fiscalização, a comparação entre provedores e a avaliação da efetividade das medidas de proteção previstas na legislação.

5.5.2.36. Nesse contexto, o escopo preliminar da ação regulatória consiste em estabelecer procedimentos e prazos para a prestação de informações à ANPD e para a elaboração e a divulgação de relatórios de transparência, monitoramento e gestão dos riscos sistêmicos. A regulamentação dessas obrigações e de outras correlatas, como a constituição e a manutenção de sede e representante legal no país, deve conferir tratamento diferenciado e proporcional a serviços de natureza, risco e modelo de negócio distintos, considerando especialmente o porte econômico do provedor e o nível de interferência na circulação de conteúdo de terceiros.

5.5.2.37. A regulamentação busca conferir efetividade ao marco normativo, promovendo maior uniformidade, transparência, comparabilidade, previsibilidade e segurança jurídica na elaboração dos relatórios e na implementação dos mecanismos de monitoramento e gestão de riscos, fortalecendo a capacidade de fiscalização da ANPD e a proteção de crianças e adolescentes no ambiente digital.

Uso de IA para geração e modificação de conteúdo íntimo

5.5.2.38. A geração e a modificação de conteúdo íntimo criado artificialmente — comumente denominadas *deepfakes* de nudez ou de atos sexuais — consistem na criação ou alteração de imagens, vídeos ou áudios que retratam uma pessoa, real ou aparentemente identificável, em contexto de sexo, nudez, seminudez ou ato libidinoso sem seu consentimento inequívoco. Em regra, o processo envolve a obtenção de dados biométricos reais (imagem, vídeo ou voz); a manipulação por sistema de inteligência artificial ou recurso tecnológico equivalente; a produção de contextos de sexo, nudez, seminudez ou ato libidinoso, gerando um conteúdo sintético com aparência de autenticidade e falta de consentimento inequívoco. Embora o dano possa ocorrer já na criação do arquivo, ele normalmente se intensifica com sua circulação em plataformas digitais.

5.5.2.39. A produção desse conteúdo, portanto, normalmente compreende cinco etapas. A primeira é a coleta de dados pessoais que pode ocorrer de maneira inicialmente lícita, consentida, e há um desvio de finalidade ou coleta de maneira totalmente ilícita. A segunda etapa é a solicitação (*prompt*), quando o usuário instrui a ferramenta a produzir ou modificar conteúdo íntimo, por exemplo: “remova a roupa desta pessoa”, “crie uma foto nua usando esta imagem” ou “utilize esta voz em um vídeo de conteúdo sexual”. A terceira etapa corresponde à geração ou modificação do conteúdo, momento em que a ferramenta produz a representação sintética. A quarta é o armazenamento do arquivo, em dispositivo, servidor ou nuvem. Por fim, na quinta etapa, pode ocorrer a publicação, quando o material é disponibilizado em redes sociais, aplicativos de mensagens, fóruns, sítios pornográficos ou serviços de armazenamento com links, dando início à exposição pública da vítima.

5.5.2.40. Do ponto de vista regulatório, os arts. 9º e 10 do Decreto nº 12.976/2026 inauguram um modelo regulatório que desloca o foco da remoção do conteúdo já publicado para a

prevenção da geração do conteúdo ilícito. Em vez de atuar apenas após a ocorrência do dano, o Decreto nº 12.976/2026 impõe obrigações *ex ante* aos provedores de aplicações de internet baseadas em inteligência artificial ou equivalentes, exigindo que adotem medidas capazes de impedir que o conteúdo íntimo sintético seja produzido.

5.5.2.41. O art. 9º estabelece que:

> Aos provedores de aplicações de internet são vedadas a geração e a modificação de conteúdo íntimo de terceiro mediante uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima.

5.5.2.42. Esse dispositivo apresenta características jurídicas relevantes. Primeiro, ele endereça a intervenção da contenção do dano para a origem do risco. O pressuposto é que impedir a geração do *deepfake* produz maior proteção do que depender exclusivamente de mecanismos posteriores de remoção. Segundo, a vedação possui redação tecnologicamente neutra. O Decreto nº 12.976/2026 não se limita à inteligência artificial generativa, abrangendo "qualquer outro recurso tecnológico" capaz de alterar imagem ou som. Essa opção evita obsolescência regulatória diante da rápida evolução tecnológica. Ademais, o objeto da proteção é o conteúdo íntimo de terceiro. O núcleo da ilicitude não está na pornografia sintética em si, mas na utilização da identidade, imagem ou voz de outra pessoa sem consentimento para criar representações íntimas falsas. Observa-se que a norma alcança tanto a geração quanto a modificação. Assim, abrange desde imagens inteiramente produzidas por inteligência artificial até técnicas de edição, *face swap*, *voice cloning*, "nudificação" (*nudification*) e outras formas de manipulação audiovisual. Por fim, trata-se de uma obrigação dirigida aos provedores de aplicações de internet e não aos usuários individualmente considerados. Assim, a ação regulatória busca induzir comportamentos seguros por parte dos agentes que controlam a arquitetura tecnológica.

5.5.2.43. O art. 10 complementa a vedação do art. 9º ao impor uma obrigação positiva: "*Os provedores (...) deverão implementar salvaguardas técnicas e procedimentais para identificar e bloquear solicitações de geração de conteúdos vedados (...)*." Enquanto o art. 9º define o que não pode ser produzido, o art. 10 estabelece como o provedor deve prevenir essa produção. O dispositivo dispõe de um mecanismo restritivo em observância ao dever de cuidado tecnológico, exigindo mecanismos preventivos incorporados ao funcionamento das aplicações.

5.5.2.44. Os arts. 9º e 10, em linha com as recentes decisões do STF por meio dos Temas nº 987 e 533/RG, representam uma mudança importante em relação ao modelo tradicional de responsabilização na internet. Desde a entrada em vigor do Marco Civil da Internet, a disciplina jurídica concentrou-se na remoção de conteúdo já publicado, mediante denúncia da vítima ou ordem judicial. Nesse modelo, o dano normalmente já ocorreu e a resposta é predominantemente reativa. O Decreto nº 12.976/2026 introduz uma abordagem preventiva. A obrigação regulatória deixa de incidir apenas sobre a moderação de conteúdo e passa a alcançar o próprio desenho tecnológico da aplicação, exigindo que riscos previsíveis sejam mitigados antes da disponibilização da funcionalidade aos usuários.

5.5.2.45. Nesse sentido, a obrigação prevista no Decreto nº 12.976/2026 recai sobre quem controla a ferramenta, porque é ele quem tem capacidade de inserir salvaguardas técnicas. O usuário individual não constitui o destinatário direto das obrigações regulatórias específicas previstas nos arts. 9º e 10 do Decreto nº 12.976/2026, sem prejuízo da incidência de outras normas sobre sua conduta.

Eixo temático 2: Privacidade e direito fundamental à proteção de dados pessoais

Revisão de decisões automatizadas

5.5.2.46. Atualmente, o acesso a serviços e a recursos essenciais é mediado por sistemas de tomada de decisão automatizada e perfilamento baseados em inteligência artificial e análise de dados. Nesse sentido, as decisões automatizadas interferem diretamente nos direitos dos cidadãos, por exemplo na avaliação de risco de crédito, na avaliação de trabalhadores por algoritmos de RH, no setor de seguros, na concessão de benefícios assistenciais e na priorização no atendimento de saúde [7,9].

5.5.2.47. Esse cenário é marcado por uma assimetria informacional e técnica entre os agentes de tratamento e os titulares de dados, pois a economia de dados confere aos controladores uma vantagem desproporcional, na qual os titulares encontram-se em posição de vulnerabilidade, visto que raras vezes possuem o letramento digital e o conhecimento técnico necessários para compreender ou contestar a lógica de tratamento das informações que lhes digam respeito [7, 9].

5.5.2.48. O rápido avanço de sistemas baseados em aprendizado de máquina e redes neurais profundas acentua as preocupações no âmbito das tomadas de decisões automatizadas [9, 10]. Enquanto nos sistemas clássicos de computação as instruções são codificadas [8], em alguns sistemas de aprendizado de máquina os modelos escrevem seus próprios programas, combinam instruções anteriores de modo iterativo e ajustam parâmetros probabilísticos com base na interação dinâmica com volumes de dados massivos. Nesses modelos, a lógica computacional entre os dados de entrada e o resultado obtido é pouco transparente e, em determinadas situações, ininteligível para seres humanos, caracterizando o fenômeno das chamadas *caixas-pretas*, sistemas opacos e que não possuem

uma maneira simples de serem auditados, pois as razões específicas pelas quais uma máquina gerou um determinado resultado podem ser desconhecidas até mesmo para os desenvolvedores, além dos entraves relacionados à propriedade intelectual e ao segredo industrial [9, 10].

5.5.2.49. Em suma, a ação regulatória torna-se relevante diante da crescente mediação do acesso a serviços e recursos essenciais por sistemas automatizados de decisão e perfilamento, os quais operam sob acentuada assimetria informacional entre titulares e agentes de tratamento e, em muitos casos, mediante modelos opacos (caixas-pretas) cuja lógica é de difícil auditoria e explicabilidade. Destaca-se, ainda, a existência de decisões judiciais que fixaram entendimentos relevantes sobre o assunto, incluindo de tribunais superiores, a exemplo de casos envolvendo aplicativos de transporte.

5.5.3. **Ações regulatórias mantidas**

5.5.3.1. As ações regulatórias a seguir decorrem da Agenda Regulatória 2025–2026 e permanecem relevantes para o ciclo subsequente. Sua manutenção não representa reinício dos respectivos projetos, mas preservação da continuidade regulatória até a conclusão dos produtos planejados. Na versão final, cada ação deverá indicar o estágio alcançado, os insumos já produzidos, as etapas remanescentes e o produto esperado para o biênio 2027–2028.

Direitos dos titulares

5.5.3.2. A manutenção decorre da necessidade de dar continuidade à análise e ao processo de deliberação da proposta de regulamentação, considerando a necessidade de consolidar parâmetros, procedimentos, prazos e requisitos para o exercício dos direitos dos titulares de dados pessoais. A continuidade da iniciativa permitirá o aperfeiçoamento da solução regulatória e o avanço das etapas necessárias à sua conclusão.

IA generativa e proteção de dados pessoais

5.5.3.3. A manutenção, com adaptações, justifica-se pela expansão do uso de modelos generativos e pela necessidade de consolidar parâmetros sobre bases de treinamento, desenvolvimento e operação de modelos de inteligência artificial generativa. Nesse cenário, intensificam-se os desafios relacionados à transparência, à proteção de dados pessoais e à privacidade, exigindo parâmetros regulatórios que promovam segurança jurídica e reduzam riscos aos direitos fundamentais dos titulares.

5.5.3.4. Cumpre destacar que o escopo da ação regulatória prevista na Agenda Regulatória 2025/2026 foi reduzido. Estudos preliminares evidenciaram a necessidade de tal redução, de modo a possibilitar maior aprofundamento do tema, tendo em vista a complexidade e o impacto da IA generativa na proteção de dados pessoais.

5.5.3.5. Entre os principais aspectos a serem abordados, destacam-se os seguintes: (i) parâmetros para a utilização da hipótese legal do legítimo interesse como fundamento para o uso de dados pessoais para treinamento, desenvolvimento e operação de sistemas de IA generativa; (ii) salvaguardas para o uso de dados sensíveis para o treinamento de sistemas de IA generativa; (iii) transparência, governança e direitos dos titulares aplicáveis ao contexto de uso de sistemas de IA generativa.

Relatório de Impacto à Proteção de Dados Pessoais

5.5.3.6. A manutenção decorre da necessidade de aprofundar a análise dos impactos regulatórios e consolidar a proposta de regulamentação, de modo a assegurar que o RIPD seja estabelecido como instrumento efetivo de prevenção, governança e prestação de contas no tratamento de dados pessoais.

5.5.3.7. Ademais, a ação regulatória “tratamento de alto risco” prevista na atual Agenda Regulatória foi incorporada nesta ação, considerando a sinergia entre as duas ações e o potencial de sobreposição dos temas.

Dados pessoais sensíveis: dados de saúde

5.5.3.8. A manutenção permite aprofundar parâmetros aplicáveis ao tratamento, compartilhamento e governança de dados de saúde, considerando a sensibilidade das informações, a diversidade de agentes envolvidos, a interoperabilidade dos sistemas e as salvaguardas necessárias para pesquisa, assistência e gestão em saúde.

Dados biométricos - reconhecimento facial

5.5.3.9. A manutenção decorre da necessidade de aprofundar a análise dos impactos regulatórios e consolidar a proposta de regulamentação. A ação regulatória deverá aproveitar os insumos já produzidos no projeto sobre tratamento de dados biométricos e definir parâmetros proporcionais aos diferentes contextos de uso.

5.5.3.10. A regulamentação busca reduzir a fragmentação de práticas, estabelecer expectativas mínimas de conformidade e orientar tanto o setor privado quanto o Poder Público. Espera-se promover a utilização responsável de tecnologias biométricas, preservar aplicações legítimas e inovadoras e, simultaneamente, prevenir tratamentos excessivos, discriminatórios ou incompatíveis com os direitos e as liberdades fundamentais dos titulares.

Hipótese Legal – Consentimento

5.5.3.11. A manutenção visa consolidar entendimentos sobre os requisitos de validade do consentimento, sua demonstração, granularidade, revogação, renovação, destaque, relação com outras hipóteses legais e condições específicas aplicáveis a

ambientes digitais e a titulares em situação de vulnerabilidade.

Hipótese Legal – Proteção ao crédito

5.5.3.12. A manutenção busca delimitar o alcance e os requisitos da hipótese legal de proteção ao crédito, esclarecer sua articulação com outras bases legais e com a legislação setorial e estabelecer salvaguardas quanto à transparência, qualidade dos dados, compartilhamento, perfilamento e exercício de direitos.

5.5.3.13. A ação regulatória "agregadores de dados pessoais", prevista na atual Agenda Regulatória, foi incorporada a esta ação, tendo em vista a proximidade temática entre as duas ações regulatórias.

5.5.4. **Ações regulatórias removidas**

Medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança)

5.5.4.1. Estudos preliminares indicaram que os problemas regulatórios, suscitados quando da elaboração da Agenda Regulatória 2025/2026, foram endereçados pela publicação do Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte.

5.5.4.2. Ademais, verificou-se que a publicação de norma nesse momento correria o risco de sobrepor-se, ou mesmo conflitar, com as orientações já disseminadas e assimiladas pelo mercado regulado, exigindo readequação de agentes que recentemente ajustaram suas práticas ao Guia.

5.5.4.3. Além disso, considerando as novas prioridades com as novas competências do ECA Digital e Marco Civil da Internet, entende-se oportuno remover essa ação da agenda para promover maior capacidade operacional da ANPD concluir as ações prioritárias.

5.5.4.4. Diante disso, sugere-se a remoção deste item da Agenda Regulatória 2027/2028.

Agregadores de dados pessoais

5.5.4.5. Estudos preliminares apontaram sinergia com a ação regulatória de hipótese legal de proteção ao crédito. Identificou-se substancial coincidência do universo de agentes regulados, como bancos de dados de proteção ao crédito (a exemplo de birôs de crédito e cadastros positivos e negativos) que operam, na prática, como agregadores de dados pessoais provenientes de múltiplas fontes.

5.5.4.6. Também a ação regulatória "IA generativa e proteção de dados pessoais" contempla aspectos aplicáveis aos "agregadores de dados pessoais", em especial no que concerne à utilização do legítimo interesse para fins do uso de dados pessoais para treinamento de sistemas de IA, bem como à definição de parâmetros de transparência e para o exercício dos direitos dos titulares nesse contexto.

5.5.4.7. Nesse sentido, sugere-se que essa iniciativa seja incorporada à ação regulatória de hipótese legal de proteção ao crédito, considerando-se, ainda, que parte dos problemas regulatórios serão endereçados na ação regulatória de IA generativa e proteção de dados pessoais.

Regras de boas práticas e de governança

5.5.4.8. A sugestão de remoção da ação regulatória relativa às Regras de Boas Práticas e de Governança (art. 50 da LGPD) da Agenda Regulatória para o biênio 2027/2028 justifica-se por razões técnico-regulatórias.

5.5.4.9. Os programas de governança em privacidade, para que sejam efetivos, pressupõem parâmetros normativos já consolidados quanto aos processos que constituem seu próprio objeto de disciplina, como os mecanismos de exercício de direitos dos titulares e a metodologia de Relatório de Impacto à Proteção de Dados Pessoais. Regulamentar boas práticas e governança antes da conclusão dessas ações regulatórias essenciais implicaria disciplinar a estrutura (o programa de governança) sem que os elementos que a compõem (fluxos de atendimento a titulares, critérios e modelo de RIPD, por exemplo) estivessem normativamente definidos, elevam o risco de o instrumento regulatório ser ineficaz e inefetivo.

5.5.4.10. Assim, sugere-se a remoção deste item da agenda regulatória. Não obstante a retirada, o tema pode ser retornado em momento oportuno.

Tratamento de dados pessoais de alto risco

5.5.4.11. A incorporação da ação regulatória relativa à definição de hipóteses de tratamento de alto risco à ação regulatória do Relatório de Impacto à Proteção de Dados Pessoais justifica-se por relação lógica e normativa entre as duas matérias, conferindo-se maior eficiência à atuação da ANPD.

5.5.4.12. A própria definição legal de RIPD condiciona sua elaboração às operações de tratamento "que possam gerar riscos às liberdades civis e aos direitos fundamentais" (art. 5º, XVII, LGPD), de modo que a caracterização do que constitui tratamento de alto risco não é uma matéria autônoma, mas antes um elemento constitutivo do próprio critério de acionamento da obrigação de elaborar o RIPD. Nessa linha, o art. 55-J, XIII, da LGPD, se refere à necessidade de definição de procedimentos sobre RIPD "para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais".

5.5.4.13. Nesse sentido, sugere-se a incorporação desta iniciativa à ação regulatória do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) na Agenda Regulatória 2027/2028.

5.5.5. **Ações regulatórias concluídas ou em fase**

avançada

5.5.5.1. Algumas ações regulatórias da agenda regulatória 2025-26 não foram mantidas para o próximo biênio porque já foram concluídas ou estão em fase avançada, com previsão de aprovação até o fim do ano de 2026.

5.5.5.2. A ação regulatória "Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade" foi concluída, após a sua aprovação pelo Conselho Diretor e disponibilização na página da ANPD na internet [11].

5.5.5.3. Já as ações regulatórias relacionadas ao ECA Digital estão previstas para serem concluídas até o final de 2026, conforme o cronograma disponibilizado na página da ANPD na internet [12]. São elas: "Fornecedores de produtos ou serviços de tecnologia da informação: escopo e obrigações gerais do ECA Digital"; "Fiscalização e Sanção do ECA Digital - Revisão das Resoluções CD/ANPD nº 1, de 28 de outubro de 2021, e nº 4, de 24 de fevereiro de 2023"; e "Mecanismos de aferição de idade".

5.5.5.4. Também está prevista para ser concluída até o final de 2026 a ação regulatória "Processo normativo no âmbito da Agência Nacional de Proteção de Dados: revisão da Portaria 16, de 08 de julho de 2021", conforme estabelecido no Despacho Decisório CD/ANPD nº 43/2026 [13].

5.5.5.5. Por sua vez, as seguintes ações se encontram em fase final de aprovação e por isso não devem constar da agenda regulatória para o próximo biênio: "compartilhamento de dados pelo Poder Público", "organizações religiosas" e "anonimização e pseudonimização".

5.5.6. **Das metas das ações regulatórias**

5.5.6.1. A Agenda Regulatória para o biênio 2025/2026 estabelecia as metas de cada ação regulatória a partir de fases relacionadas à abertura dos projetos regulatórios, sem vinculação direta a entregas formais no âmbito do processo regulatório. Essa sistemática, embora adequada para uma visão panorâmica do andamento das ações, dificultava a aferição objetiva do cumprimento das metas pactuadas e a comparação das etapas de execução entre as ações regulatórias.

5.5.6.2. Esse aprimoramento metodológico ganha especial relevância à luz da transformação institucional da ANPD em agência reguladora, promovida pela Lei nº 15.352, de 25 de fevereiro de 2026 (fruto da conversão da Medida Provisória nº 1.317/2025), que inseriu a Agência no rol do art. 2º da Lei nº 13.848, de 25 de junho de 2019 (Lei das Agências Reguladoras), processo esse concluído com a publicação do Decreto nº 12.881/2026. Ao assumir o status de agência reguladora federal, a ANPD passou a se submeter aos mesmos parâmetros de processo decisório, governança e transparência regulatória aplicáveis às demais agências setoriais (a exemplo de Aneel, Anatel, Anvisa, ANS e ANP), o que reforça a necessidade de que sua Agenda Regulatória adote um padrão de acompanhamento compatível com essas exigências.

5.5.6.3. Com vistas a conferir maior objetividade, verificabilidade e transparência ao acompanhamento da Agenda Regulatória, optou-se pela adoção de um modelo de metas fundamentado nas entregas previstas no processo regulatório, tendo como base o Decreto nº 10.411/2020, a Portaria ANPD nº 16/2021 e detalhadas nos termos do art. 2º da Resolução que aprova a Agenda: (i) a publicação do Relatório de Análise de Impacto Regulatório (AIR) no portal da ANPD, após aprovação pelo Superintendente de Regulação; (ii) a abertura de Consulta à Sociedade (CS), compreendendo Tomada de Subsídios, Consulta Pública ou Audiência Pública; e (iii) a Aprovação Final (AF) do instrumento regulatório pelo Conselho Diretor.

6. CONCLUSÃO

6.1. Diante do exposto, sugere-se realização de tomada de subsídios da proposta de Agenda Regulatória da ANPD para o biênio 2027-2028, por meio da plataforma Brasil Participativo pelo prazo de 45 (quarenta e cinco) dias, nos termos do anexo (SEI 0329032) a esta nota técnica.

À consideração superior.

CAROLINE RODRIGUES LOPES
Servidora na Coordenação-Geral de Planejamento e Análise Regulatória

LAURA CONDE TRESCA
Servidora na Coordenação-Geral de Planejamento e Análise Regulatória

HUGO LINS DE ALBUQUERQUE VIEIRA
Servidor na Coordenação-Geral de Planejamento e Análise Regulatória

DENIS MARCELO DE OLIVEIRA
Coordenador de Planejamento Regulatório

RODRIGO SANTANA DOS SANTOS
Coordenador-Geral de Planejamento e Análise Regulatória

De acordo. Encaminhe-se o presente processo para que sejam tomadas as providências necessárias para publicação da Tomada de Subsídios.

Brasília, *na data da assinatura.*

LUCAS BORGES DE CARVALHO

Superintendente de Regulação

7. REFERÊNCIAS

[1] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/regulacao/agenda-regulatoria-1?activeAccordion=ae7cc106-7a8d-4fd0-8bda-fabb5d8b2996.

[2] EUROPEAN DATA PROTECTION BOARD (EDPB). Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse. Brussels: EDPB, 14 Feb. 2024. Disponível em: https://www.edpb.europa.eu/documents/reports-statements-and-letters/statement-12024-on-legislative-developments-regarding-the_en.

[3] EUROPEAN DATA PROTECTION BOARD (EDPB). Statement 1/2025 on Age Assurance. Brussels: EDPB, 12 Feb. 2025. Disponível em: https://www.edpb.europa.eu/documents/statement/statement-12025-on-age-assurance_en.

[4] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). Plan stratégique 2025-2028 : protéger les données de chacun pour sécuriser l'avenir numérique de tous. Paris: CNIL, 2025. Disponível em: https://www.cnil.fr/sites/cnil/files/2025-01/plan_strategique_cnil_2025-2028.pdf.

[5] FEDERAL TRADE COMMISSION (FTC). FTC Strategic Plan for Fiscal Years 2026 to 2030. Washington, D.C.: FTC, 2026. Disponível em: https://www.ftc.gov/system/files/ftc_gov/pdf/fy-2026-2030-ftc-strategic-plan.pdf.

[6] GLOBAL PRIVACY ASSEMBLY (GPA). Joint Statement on AI-Generated Imagery and the Protection of Privacy. [S. l.]: GPA, 23 Feb. 2026. Disponível em: https://www.edpb.europa.eu/system/files/2026-02/2026.02.23-joint-statement-ai-generated-imagery-61-signatories-distributed-21.02.2026.pdf.

[7] AMORIM, Gutemberg. LGPD + IA: decisões automatizadas e discriminação algorítmica: o direito de revisão no art. 20 da LGPD. 2026. Disponível em: https://gutembergamorim.com.br/lgpd-ia-decisoes-automatizadas-e-discriminacao-algoritmica-o-direito-de-revisao-no-art-20-da-lgpd/.

[8] ROCHA, Heloísa Rodrigues da. O direito à revisão de decisões automatizadas baseadas em inteligência artificial aplicado à proteção do direito à saúde de vieses discriminatórios. São Paulo: Quipá Editora, 2023.

[9] WIMMER, Miriam. Responsabilidade de agentes empresariais por ilícitos administrativos praticados por sistemas de inteligência artificial. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). Inteligência artificial e Direito: ética, regulação e responsabilidade. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

[10] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Nota Técnica nº 12/2025/CON1/CGN/ANPD: consolidação das contribuições recebidas na Tomada de Subsídios. Processo nº 00261.006920/2024-46. Brasília, DF: ANPD, 3 abr. 2025. Disponível em: documento oficial.

[11] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade. Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/diretrizes-para-a-politica-nacional-de-protecao-de-dados-pessoais-e-da-privacidade-pnpd.pdf/@@display-file/file.

[12] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ECA Digital. Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital.

[13] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Despacho Decisório CD/ANPD nº 43/2026: planejamento de adequação da regulamentação da ANPD aos preceitos da Lei nº 15.352/2026. Processo nº 00261.002006/2026-98. Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/eca-digital/plano-de-adequacao-lei-15352.pdf/@@display-file/file.

Documento assinado eletronicamente por **Lucas Borges de Carvalho**, **Superintendente**, em 31/08/2026, às 15:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)-Geral**, em 31/08/2026, às 15:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Denis Marcelo de**

Oliveira, **Coordenador(a)**, em 31/08/2026, às 15:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Hugo Lins de Albuquerque Vieira**, **Servidor(a) Temporário(a)**, em 31/08/2026, às 15:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Caroline Rodrigues Lopes**, **Servidor(a) Temporário(a)**, em 31/08/2026, às 15:49, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Laura Conde Tresca**, **Servidor(a) Temporário(a)**, em 31/08/2026, às 15:54, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.anpd.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0329033** e o código CRC **90A61E19**.

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