RESOLUÇÃO CD/ANPD Nº XX, DE XX DE XXXXX DE 202X

Aprova a Agenda Regulatória da Agência Nacional de Proteção de Dados (ANPD) para o biênio 2027-2028.

O CONSELHO DIRETOR DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS - ANPD, no uso de suas atribuições legais, considerando o disposto no art. 21 da Lei nº 13.848, de 25 de junho de 2019, bem como a deliberação tomada no processo nº 00261.002488/2026-86, resolve:

Art. 1º Fica aprovada a Agenda Regulatória para o biênio 2027-2028 da ANPD, na forma do Anexo a esta Resolução.

Art. 2º As ações previstas na Agenda Regulatória para o biênio 2027-2028 observarão as seguintes metas, conforme os prazos indicados no Anexo a esta Resolução:

I - Análise de Impacto Regulatório (AIR): publicação do Relatório de AIR no portal da ANPD na internet após a aprovação pelo Superintendente de Regulação;

II - Consulta à Sociedade (CS): abertura de Tomada de Subsídios ou de Consulta Pública, ou convocação de Audiência Pública; e

III - Aprovação Final (AF): aprovação do instrumento regulatório pelo Conselho Diretor.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

WALDEMAR GONÇALVES ORTUNHO JUNIOR
Diretor-Presidente

ANEXO

AGENDA REGULATÓRIA - 2027-2028

Legenda:

AIR: Análise de Impacto Regulatório
CS: Consulta à Sociedade
AF: Aprovação Final

Eixo Temático 1: Garantia de direitos de crianças e adolescentes e promoção de um ambiente digital seguro						
Item	**Ação**	**Descrição**	**Metas**			
			1º/2027	**2º/2027**	**1º/2028**	**2º/2028**
1	Marco Civil da Internet: escopo e obrigações gerais	O Marco Civil da Internet (Lei nº 12.965/2014), regulamentado pelo Decreto nº 8.771/2016, com a publicação do Decreto nº 12.975 e do Decreto nº 12.976, ambos de 20 de maio de 2026, passou a contemplar um regime de dever de cuidado aplicável aos provedores de aplicações de internet, fundado nos conceitos de dever de cuidado, risco sistêmico, falha sistêmica e dúvida razoável. 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. Principais desafios: (i) escopo do dever de cuidado, definindo quais provedores de aplicações estão a ele sujeitos; e (ii) parâmetros para a caracterização do risco sistêmico e da falha sistêmica que ensejam responsabilização; (iii) relações entre dever de prevenção previsto no Eca Digital e o dever de cuidado; e (iv) tratamento diferenciado e proporcional a serviços de natureza, risco e modelo de negócio distintos, considerando, ainda, o porte econômico do provedor, o nível de interferência na	AIR e CS	AF		

		circulação de conteúdo de terceiros e o estado da técnica.				
2	Transparência, prestação de contas e mecanismos de supervisão e análise periódica	Os arts. 16-A, I, “a” e "b", item 3, 16-B, §§ 1º a 3º, e 16-C do Decreto nº 8.771/2016, o art. 31 do ECA Digital e os arts. 40 e 47 do Decreto nº 12.880/2026 estabelecem obrigações de transparência, prestação de contas e gestão de riscos sistêmicos por provedores de aplicações de internet. Essas obrigações estão associadas aos deveres de cuidado e de prevenção e o seu cumprimento deve ser verificado pela ANPD por mecanismos de supervisão e análise periódica. A ação tem por finalidade principal 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. Principais desafios: (i) conteúdo mínimo, parâmetros uniformes e periodicidade para a prestação de informações a ANPD e para a elaboração e divulgação dos relatórios de transparência, monitoramento e gestão de riscos sistêmicos; e (ii) procedimentos de análise periódica e articulação entre a ANPD e os provedores para o acompanhamento contínuo dos riscos.	AIR	CS e AF		
3	Padrões de *design* seguro	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	AIR	CS	AF	

		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. Principais desafios: (i) definição de critérios para identificação e classificação de práticas manipulativas, enganosas ou coercitivas em produtos ou serviços de tecnologia da informação direcionados a crianças e adolescentes ou de acesso provável por eles; (ii) estabelecimento de requisitos mínimos para avaliação e implementação de padrões de *design* seguro em tais produtos ou serviços; (iii) requisitos de transparência e prestação de contas; (iv) tratamento diferenciado e proporcional a serviços de natureza, risco e modelo de negócio distintos, considerando, ainda, o porte econômico do provedor, o nível de interferência na circulação de conteúdo de terceiros e o estado da técnica.				
4	Uso de IA generativa por crianças e adolescentes	O art. 11 do Decreto nº 12.880/2026 estabelece obrigações específicas para produtos ou serviços capazes de gerar conteúdo e interagir com crianças e adolescentes a partir de instruções em linguagem natural. A rápida difusão de agentes de IA conversacionais e interfaces similares (como *AI companions* e *chatbots*) entre crianças e adolescentes, aliada aos riscos associados ao seu uso em fase de		AIR	CS e AF	

		desenvolvimento, demanda o estabelecimento de parâmetros regulatórios para o efetivo cumprimento do dever de prevenção pelos fornecedores, nos termos dos arts. 5º a 8º do ECA Digital, e para assegurar a proteção integral e o melhor interesse desse público. Entre os principais desafios, destaca-se o estabelecimento de parâmetros para: (i) o adequado gerenciamento de riscos de recursos e funcionalidades; (ii) o desenvolvimento desde a concepção e a adoção por padrão de configurações que evitem o uso compulsivo e previnam a manipulação comportamental; (iii) a implementação de mecanismos de transparência, incluindo a sinalização do caráter sintético e automatizado da interação; e (iv) a avaliação de risco algorítmico e a adoção de salvaguardas mínimas para a proteção desse público.				
5	Canal de denúncia e procedimentos de notificação sobre conteúdos ilícitos ou criminosos	Os arts. 28 a 30 do ECA Digital, o art. 43 do Decreto nº 12.880/2026, os arts. 16-A, II, e 16-D a 16-F do Decreto nº 8.771/2016 e os arts. 5º a 7º do Decreto nº 12.976/2026 estabelecem regras a serem observadas no recebimento de notificações a respeito de conteúdos ilícitos, com o objetivo de garantir o devido processo e o contraditório nesses procedimentos executados por plataformas digitais. A ação regulatória é relevante para estabelecer parâmetros uniformes sobre a disponibilização de canal de denúncias e o processo de recebimento de notificações e retirada de conteúdo. É necessário assegurar que as decisões de moderação sejam tomadas de forma transparente, motivada e passível de contestação, conferindo maior efetividade à garantia de direitos de usuários sem comprometer a celeridade necessária à mitigação de riscos.		AIR	CS	AF

		Principais desafios: (i) parâmetros para a notificação e a motivação das decisões de moderação de conteúdo; (ii) mecanismos efetivos de contestação e de revisão dessas decisões por plataformas e pelos usuários; (iii) prazos e procedimentos uniformes que assegurem a efetividade do devido processo sem prejudicar a celeridade da moderação em situações de maior risco; (iv) requisitos mínimos para a disponibilização de canal de denúncia; e (v) o tratamento diferenciado e proporcional a serviços de natureza, risco e modelo de negócio distintos, considerando, ainda, o porte econômico do provedor, o nível de interferência na circulação de conteúdo de terceiros e o estado da técnica.				
6	Habilitação de entidades representativas de direitos de crianças e adolescentes	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". 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. Principais desafios: (i) requisitos e critérios objetivos de qualificação técnica e institucional das entidades representativas, bem como seus deveres e prerrogativas; (ii) fluxo procedimental de credenciamento, incluindo a área responsável, os prazos e as condições de renovação; (iii) hipóteses de descredenciamento; e (iv)			AIR	CS

		interlocução com demais órgãos públicos, como o Ministério Público.				
7	Uso de IA para geração e modificação de conteúdo íntimo	Os arts. 9º e 10 do Decreto nº 12.976/2026 vedam a geração e a modificação, de conteúdo íntimo de terceiro mediante o uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere a imagem ou som da vítima (*deepfakes*), impondo aos provedores de aplicações de internet o dever de implementar salvaguardas técnicas e procedimentais para prevenir a produção desse conteúdo. A norma legal desloca o modelo tradicional de responsabilização na internet, até então concentrado na remoção de conteúdo já publicado mediante denúncia ou ordem judicial, para a prevenção da própria geração do conteúdo ilícito, mitigando danos que se intensificam com a circulação do material na internet. Principais desafios: (i) alcance conceitual e tecnológico da vedação, de forma capaz de acompanhar a evolução das técnicas de geração e manipulação de conteúdo; (ii) salvaguardas técnicas preventivas exigíveis dos provedores, como filtros de solicitação, classificadores de risco e mecanismos de bloqueio, a serem implementadas de forma escalonada e proporcional ao volume de acessos e ao nível de risco da aplicação; e (iii) parâmetros para a conformidade do cumprimento dos deveres pelos provedores, observadas as hipóteses de responsabilização e as sanções previstas em lei.			AIR	CS
8	Supervisão parental	Os arts. 3º, parágrafo único, 12, § 3º e 16 a 18 do ECA Digital determinam que fornecedores de produtos ou serviços de tecnologia da informação disponibilizem mecanismos eficazes de supervisão parental. O art. 17, § 1º,				AIR

		prevê a edição de regulamento pela ANPD para dispor sobre “diretrizes e padrões mínimos” a serem observados pelos fornecedores. O marco legal não define os critérios técnicos, funcionais e procedimentais para a implementação e avaliação desses mecanismos, o que pode resultar em ferramentas com níveis heterogêneos de proteção e, consequentemente, insuficientes para mitigar riscos relevantes, comprometendo direitos fundamentais como a privacidade e o livre desenvolvimento da personalidade de crianças e adolescentes. Principais desafios: (i) critérios técnicos, funcionais e procedimentais para a implementação e avaliação dos mecanismos de supervisão parental; (ii) parâmetros mínimos de funcionalidades, limites legítimos ao monitoramento parental e salvaguardas de privacidade e proteção de dados; (iii) harmonização entre a proteção integral prevista no ECA Digital e o reconhecimento da autonomia progressiva de crianças e adolescentes, conforme a faixa etária e o estágio de desenvolvimento; e (iv) o tratamento diferenciado e proporcional a serviços de natureza, risco e modelo de negócio distintos, considerando, ainda, o porte econômico do provedor, o nível de interferência na circulação de conteúdo de terceiros e o estado da técnica.				
9	Acesso a dados de provedores de aplicações de internet por instituições acadêmicas, científicas, tecnológicas, de inovação e jornalísticas	O art. 31, parágrafo único, do ECA Digital dispõe sobre mecanismos de acesso a dados de provedores de aplicações de internet por instituições acadêmicas, científicas, tecnológicas, de inovação e jornalísticas. O art. 48 do Decreto nº 12.880/2026 atribui à ANPD competência para habilitar essas instituições por meio de edital público.				AIR

		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. A efetividade desse acesso depende da definição de critérios claros que viabilizem a pesquisa de interesse público sem comprometer a proteção de dados pessoais de usuários ou segredos comerciais e industriais dos agentes regulados. Principais desafios: (i) critérios de elegibilidade e credenciamento de instituições para o acesso a dados; (ii) parâmetros para o acesso à informação para fins de pesquisa de interesse público; (iii) salvaguardas de proteção de dados pessoais, incluindo anonimização ou pseudonimização dos dados disponibilizados; (iv) tratamento diferenciado e proporcional a serviços de natureza, risco e modelo de negócio distintos, considerando, ainda, o porte econômico do provedor, o nível de interferência na circulação de conteúdo de terceiros e o estado da técnica.				
Eixo Temático 2: Privacidade e direito fundamental à proteção de dados pessoais						
10	Direitos dos titulares	A LGPD estabelece os direitos dos titulares, mas diversos pontos demandam regulamentação, em especial os artigos 9º, 18, 19 e 20. O objetivo da ação é conferir maior segurança jurídica aos agentes de tratamento e efetividade ao exercício desses direitos pelos titulares, uniformizando procedimentos e prazos de atendimento.	AF			

		Principais desafios: (i) parâmetros para o exercício dos direitos previstos na LGPD; e (ii) procedimentos, prazos e requisitos para o atendimento das solicitações dos titulares.				
11	Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	De acordo com as competências estabelecidas pelo art. 55-J, inciso XIII, cabe à ANPD editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais. Principais desafios: (i) conteúdo mínimo e a metodologia dos relatórios de impacto à proteção de dados pessoais; e (ii) critérios objetivos a serem observados no processo de elaboração e divulgação do RIPD.	CS	AF		
12	Dados biométricos – reconhecimento facial	O tratamento de dados biométricos se ampliou e se popularizou nos últimos anos, em especial para fins de verificação de identidade, com técnicas de reconhecimento facial em contextos diversos, tais como o ambiente escolar, estádios de futebol e transações financeiras. Se, por um lado, o tratamento desses dados pode ampliar a segurança e auxiliar a prevenção de fraudes; por outro lado, também são ampliados os riscos sobre os titulares, a exemplo de impactos negativos decorrentes de erros dos sistemas utilizados e de efeitos discriminatórios sobre grupos vulneráveis. Principais desafios: (i) parâmetros para o tratamento lícito de dados biométricos por sistemas de reconhecimento facial, em especial para fins de controle de acesso, segurança e prevenção a fraudes; (ii) medidas para garantir o respeito aos direitos fundamentais, aos direitos dos titulares e aos princípios da LGPD, em especial o da não	CS	AF		

		discriminação; e (iii) requisitos de transparência, segurança e governança para o uso desses sistemas pelos agentes de tratamento.				
13	Hipótese Legal - Consentimento	A ação regulatória tem por objetivo estabelecer parâmetros e orientações acerca dos requisitos a serem observados na utilização da hipótese legal do consentimento. A validade do consentimento depende de elementos como a liberdade de escolha, a clareza das informações prestadas, a finalidade específica do tratamento e a possibilidade de revogação a qualquer momento, sem ônus para o titular. Principais desafios: (i) parâmetros para a garantia do consentimento livre, informado e inequívoco; (ii) requisitos quanto à finalidade específica do tratamento fundamentado no consentimento; e (iii) procedimentos para a revogação do consentimento a qualquer momento, sem ônus para o titular.	AIR e CS	AF		
14	Dados de saúde	A LGPD estabelece regras mais rígidas ao tratamento de dados pessoais sensíveis, notadamente dados de saúde. Um dos aspectos considerados pela LGPD é o compartilhamento de dados pessoais referentes à saúde com fins econômicos. Nesse sentido, o art. 11, § 3º, determina que a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da ANPD, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências. Por sua vez, o § 4º do mesmo artigo veda a comunicação ou o uso compartilhado de dados pessoais referentes à saúde entre controladores com objetivo de	AIR	CS	AF	

		obter vantagem econômica, ressalvadas as exceções previstas no mesmo dispositivo e em seus incisos. Principais desafios: (i) conceito de dado pessoal sensível referente à saúde; (ii) hipóteses legais específicas relacionadas à área de saúde, especialmente as previstas no art. 7º, VIII e no art. 11, II, "f", da LGPD; e (iii) critérios para a vedação ou a regulamentação do compartilhamento de dados de saúde entre controladores com finalidade de obtenção de vantagem econômica, nos termos do art. 11, §§ 3º e 4º.				
15	IA generativa e proteção de dados	Diante do uso crescente de dados pessoais no treinamento, desenvolvimento e operação de modelos de inteligência artificial generativa, cria-se um cenário que intensifica 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. Principais desafios: (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.		AIR	CS	AF
16	Hipótese Legal - Proteção ao Crédito	Em um cenário em que as informações financeiras dos indivíduos são cada vez mais utilizadas para análises e decisões de concessão de crédito, a proteção desses dados torna-se crucial para garantir a privacidade e a segurança dos titulares. A ação regulatória sobre a hipótese legal de proteção ao crédito,		AIR	CS	AF

		prevista no art. 7º, X, da LGPD, poderá fornecer orientações aos agentes de tratamento acerca da sua aplicação, permitindo o equilíbrio entre o direito à privacidade dos titulares e a necessidade das instituições financeiras e demais agentes de tratamento de acessar informações relevantes para a análise de risco de crédito. Principais desafios: (i) parâmetros para a aplicação da hipótese legal de proteção ao crédito, prevista no art. 7º, X, da LGPD; (ii) critérios para o equilíbrio entre a proteção de dados dos titulares e a necessidade de acesso a informações pelas instituições financeiras e demais agentes de tratamento, especialmente no contexto da legislação setorial aplicável; e (iii) orientações sobre os limites e os requisitos para o uso de dados pessoais em análises de risco de crédito, notadamente quanto à raspagem e tratamento massivo de dados por agregadores.				
17	Revisão de decisões automatizadas	O art. 20 da LGPD assegura ao titular o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. A ação regulatória torna-se relevante diante da crescente mediação do acesso a serviços e recursos essenciais por sistemas automatizados de decisão e perfilamento, baseados em inteligência artificial, 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			AIR	CS

		superiores, a exemplo de casos envolvendo aplicativos de transporte. Principais desafios: (i) definição de regras procedimentais que assegurem o respeito ao devido processo legal e ao direito de revisão; (ii) estabelecimento de critérios para a eventual exigência de intervenção humana; e (iii) delimitação das obrigações de transparência dos controladores, em atendimento ao dever de fornecer informações claras e adequadas sobre critérios e procedimentos utilizados na decisão.				