

PERSPECTIVAS DE PROTEÇÃO DE DADOS PARA O FUTURO:

CONVERGÊNCIA REGULATÓRIA E ADAPTAÇÃO

Autores:

Dandara Ramos Silvestre

Thiago Xavier Peregrino

Revisores:

Felipe Gabriades

Fernando Bousso

b/luz

Sumário

Introdução	3
-------------------	----------

1. Convergência regulatória como tendência	4
---	----------

2. A expansão do papel institucional da Agência Nacional de Proteção de Dados	6
--	----------

2.1. A ANPD e o papel indicado no marco regulatório da inteligência artificial	7
--	---

2.2. A atuação da ANPD no ECA Digital e a proteção de crianças e adolescentes no ambiente online	9
--	---

3. Digital Omnibus e os reflexos do debate europeu no Brasil	11
---	-----------

4. Considerações finais: o futuro da proteção de dados no Brasil	13
---	-----------

Introdução

A matéria de privacidade e proteção de dados pessoais atravessa um momento de tensionamento, impulsionado pela expansão do uso de tecnologias baseadas em dados, pela evolução da inteligência artificial e pelo papel central das plataformas digitais na organização da vida social e econômica. Esse contexto tem evidenciado os limites de abordagens regulatórias fragmentadas e reposicionado a proteção de dados como um elemento estratégico da governança do ecossistema digital.

Observa-se, em diferentes jurisdições, uma dupla tendência: de um lado, a consolidação da convergência regulatória, com a articulação entre proteção de dados, segurança da informação, governança algorítmica e responsabilidade das plataformas; e de outro, debates intensos sobre flexibilização, simplificação e proporcionalidade, especialmente em cenários de inovação e competitividade. A proteção de dados passa, assim, a figurar simultaneamente como eixo de integração regulatória e objeto de ajustes voltados à adaptação das normas à complexidade do ambiente digital.

No Brasil, esse movimento se reflete de forma clara na ampliação do papel institucional da Agência Nacional de Proteção de Dados (ANPD), que vem assumindo funções mais amplas de coordenação e orientação normativa, sobretudo diante de agendas emergentes como a regulação da inteligência artificial e a proteção de crianças e adolescentes no ambiente digital. Paralelamente, debates internacionais - como aqueles relacionados ao Digital Omnibus na União Europeia - passam a influenciar expectativas regulatórias e práticas de governança também no contexto brasileiro.

1. Convergência regulatória como tendência

A regulação do ambiente digital tem evoluído a partir do reconhecimento de que seus desafios não se organizam de forma compartimentalizada. Em um cenário de circulação intensiva de dados e crescente complexidade tecnológica, abordagens regulatórias isoladas mostram-se insuficientes, exigindo leituras integradas que considerem a interdependência entre tecnologias, modelos de negócio e riscos jurídicos.

Nesse contexto, reguladores passaram a reconhecer a progressiva diluição das fronteiras entre privacidade, defesa da concorrência, proteção do consumidor e cibersegurança, incentivando a coordenação entre autoridades para lidar com riscos que atravessam múltiplos domínios normativos. A proteção de dados pessoais deixa, assim, de ocupar um espaço normativo restrito e passa a dialogar diretamente com outras áreas centrais do ecossistema digital.

A fragmentação regulatória tende a gerar lacunas de proteção, insegurança jurídica e dificuldades práticas de conformidade, especialmente para empresas que operam em múltiplas jurisdições e precisam lidar com um efetivo mosaico de obrigações setoriais que, quando não harmonizadas, resultam em sobreposições onerosas ou em brechas regulatórias não intencionais.

Esses desafios tornam-se ainda mais evidentes diante de tecnologias transversais e frequentemente transfronteiriças, como inteligência artificial, big data, internet das coisas e plataformas digitais. Sistemas de inteligência artificial, em particular, costumam depender do tratamento massivo e combinado de dados, ampliando riscos relacionados à fundamentação legal da atividade, definição de finalidades, mecanismos de transparência e situações indesejadas de discriminação algorítmica.

A harmonização regulatória apresenta-se, nesse sentido, como instrumento de mitigação de riscos e de promoção da segurança jurídica, ao alinhar princípios mínimos de proteção e reduzir conflitos normativos. Essa convergência também se manifesta na aproximação entre a proteção de dados e outros ramos do direito, como o direito concorrencial, e a segurança da informação, refletindo um entrelaçamento crescente de riscos e impactos já observados em iniciativas regulatórias e casos concretos.

AO REDOR DO MUNDO

No contexto da União Europeia, a atuação regulatória transversal se reflete em iniciativas como o *Digital Markets Act* (DMA)¹, que tem o objetivo de gerar competitividade no mercado digital da região e, para isso, cria regras de compartilhamento de dados entre plataformas e garantia do poder de escolha por parte dos usuários², e o *Digital Services Act* (DSA)³, que visa integrar

¹ UNIÃO EUROPEIA. **Regulation (EU) 2022/1925** of the European Parliament and of the Council, of 14 September 2022, on contestable and fair markets in the digital sector (Digital Markets Act – DMA). Jornal Oficial da União Europeia, Bruxelas, 2022. Disponível em: <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>. Acesso em: 22 de janeiro de 2026.

² COMISSÃO EUROPEIA. **Commission sends preliminary findings to Meta over its “Pay or Consent” advertising model for non-compliance with the DMA**. Web, 2024. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582. Acesso em: 22 de janeiro de 2026.

³ UNIÃO EUROPEIA. **Regulamento (UE) 2022/2065** do Parlamento Europeu e do Conselho, de 19 de outubro de 2022. Relativo a um mercado único para os serviços digitais (Digital Services Act). Jornal Oficial da União Europeia, Bruxelas, 2022. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065>. Acesso em: 22 de janeiro de 2026.

autoridades de proteção de dados e de defesa do consumidor em mecanismos conjuntos de supervisão⁴. Esses instrumentos evidenciam a incorporação de preocupações com privacidade e proteção de dados pessoais em regimes tradicionalmente voltados à concorrência.

Ainda no âmbito europeu, essa lógica também se manifesta na coordenação entre autoridades fiscalizadoras e na articulação com marcos de cibersegurança e resiliência digital, como o NIS2⁵ e o DORA⁶, concebidos para operar de forma a evitar sobreposições sancionatórias⁷.

No Brasil, dinâmica semelhante ocorreu em 2021, quando o Conselho Administrativo de Defesa Econômica (CADE), a Secretaria Nacional do Consumidor (Senacon), o Ministério Público Federal e a ANPD aturam de maneira conjunta na análise de práticas de tratamento dados de entidades privadas⁸. Esse movimento foi institucionalizado por meio de acordos de cooperação entre o CADE e a ANPD⁹, e posteriormente com a Senacon, bem como pela criação do Conselho Nacional de Defesa do Consumidor (CNDC)¹⁰, reforçando a convergência entre concorrência, proteção de dados e proteção dos direitos do consumidor.

A convergência regulatória, portanto, não se limita à harmonização de normas de proteção de dados, mas aponta para a construção de um paradigma regulatório integrado, voltado à governança do ecossistema digital como um todo. É nesse contexto que se fortalece a relevância de autoridades capazes de atuar como pontos de conexão entre regimes jurídicos distintos, algo que foi construído para a ANPD ao longo de 2025, com expectativa de fortalecimento para os próximos anos.

⁴ COMISSÃO EUROPEIA. **The cooperation framework under the Digital Services Act**. Web, 2025. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/dsa-cooperation>. Acesso em: 22 de janeiro de 2026.

⁵ UNIÃO EUROPEIA. **Diretiva (UE) 2022/2555** do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022. Relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União (Diretiva NIS 2). Jornal Oficial da União Europeia, Bruxelas, 2022. Disponível em: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>. Acesso em: 22 de janeiro de 2026.

⁶ UNIÃO EUROPEIA. **Regulamento (UE) 2022/2554** do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022. Relativo à resiliência operacional digital do setor financeiro (Regulamento DORA). Jornal Oficial da União Europeia, Bruxelas, 2022. Disponível em: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>. Acesso em: 22 de janeiro de 2026.

⁷ COMISSÃO EUROPEIA. **Digital Operational Resilience Act (DORA): Factsheet**. Web, s/d. Disponível em: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en. Acesso em: 22 de janeiro de 2026.

⁸ BRASIL. Conselho Administrativo de Defesa Econômica. **Cade, MPF, ANPD e Senacon recomendam que WhatsApp adie entrada em vigor da nova política de privacidade**. Diário Oficial da União, Brasília, DF, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/cade-mpf-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade>. Acesso em: 22 de janeiro de 2026.

⁹ BRASIL. Agência Nacional de Proteção de Dados. **Acordo de Cooperação Técnica nº 5/2021**. Firma cooperação entre a ANPD e o CADE. Diário Oficial da União, Brasília, DF, 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/documentos/act-ca-de_ocultado.pdf. Acesso em: 22 de janeiro de 2026.

¹⁰ BRASIL. Decreto nº 10.417, de 7 de julho de 2020. **Institui o Conselho Nacional de Defesa do Consumidor**. Diário Oficial da União, Brasília, DF, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10417.htm. Acesso em 22 de janeiro de 2026.

2. A expansão do papel institucional da Agência Nacional de Proteção de Dados

A ANPD vem passando por um acelerado processo de amadurecimento institucional desde a sua criação, consolidando-se progressivamente como um dos principais atores do ecossistema regulatório digital brasileiro. Inicialmente concebida para fiscalizar o cumprimento da LGPD, a ANPD, ao longo dos últimos anos, assumiu atribuições que extrapolam a aplicação estrita desse marco, ampliando significativamente o alcance de sua atuação e reforçando sua posição como instância estratégica de coordenação regulatória.

Um primeiro marco desse fortalecimento ocorreu em 2022, quando a ANPD foi transformada de órgão da administração pública federal integrante da Presidência da República em autarquia de natureza especial¹¹, passando a ter maior autonomia administrativa e financeira. Essa mudança preparou o terreno para uma atuação regulatória mais estável, menos dependente de arranjos conjunturais, e mais compatível com a complexidade dos riscos associados ao tratamento de dados no ambiente digital.

Esse processo de fortalecimento institucional atingiu novo patamar em setembro de 2025, quando a ANPD foi elevada ao status de agência reguladora independente por meio da Medida Provisória nº 1.317/2025¹². A transformação formal em agência reguladora, com inserção no regime das agências e reforço de sua autonomia funcional, técnica, decisória, administrativa e financeira, consolida uma ruptura relevante com o desenho institucional anterior e amplia a capacidade da Agência de influenciar, de maneira contínua e estruturante, as políticas públicas no país.

Do ponto de vista material, esse novo patamar altera qualitativamente o modo de atuação da ANPD. A autonomia decisória fortalece a efetividade do poder fiscalizatório e sancionatório, permitindo a instauração de processos administrativos e a aplicação de penalidades com maior independência. Paralelamente, o reforço institucional amplia a capacidade operacional da Agência, inclusive por meio da expansão do quadro técnico especializado, elemento essencial para lidar com demandas complexas de auditoria, inspeção e análise de riscos associados a novas tecnologias. Soma-se a isso o fortalecimento do poder normativo técnico, que consolida a ANPD como instância central de interpretação da LGPD e de emissão de diretrizes aptas a orientar os setores público e privado diante de modelos de negócio inovadores.

Essa evolução institucional ocorre em um contexto no qual os dados pessoais se tornaram infraestrutura essencial para tecnologias emergentes e para dinâmicas econômicas baseadas em plataformas. Como consequência, a ANPD tende a se deslocar de uma

¹¹ BRASIL. Lei nº 14.460, de 25 de outubro de 2022. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados. Diário Oficial da União, Brasília, DF, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2019-2022/2022/lei/l14460.htm. Acesso em 22 de janeiro de 2026.

¹² BRASIL. Medida Provisória Nº 1.317, de 17 de setembro de 2025. Altera a Lei nº 13.709, de 14 de agosto de 2018, para tratar da Agência Nacional de Proteção de Dados, a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, transforma cargos no âmbito do Poder Executivo federal, e dá outras providências. Diário Oficial da União, Brasília, DF, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2023-2026/2025/Mpv/mpv1317.htm. Acesso em 22 de janeiro de 2026.

atuação predominantemente reativa, centrada na fiscalização *ex post*, para funções mais amplas de coordenação, orientação normativa e articulação interinstitucional.

Esse deslocamento é coerente com a tendência de convergência regulatória anteriormente descrita: quanto mais os riscos digitais se sobrepõem, mais relevante se torna uma autoridade capaz de operar como eixo integrador de agendas correlatas.

Nesse sentido, a ampliação do papel da ANPD manifesta-se também na expansão de suas competências materiais. Destacam-se, nesse contexto, dois eixos particularmente relevantes: a proteção de crianças e adolescentes no ambiente digital e a regulação de inteligência artificial. Ambos evidenciam como a proteção de dados pessoais passa a funcionar como fundamento organizador de respostas regulatórias mais amplas, voltadas à tutela de direitos fundamentais em ecossistemas digitais complexos.

No que se refere à proteção de crianças e adolescentes, o Estatuto Digital da Criança e do Adolescente (ECA Digital) atribui à ANPD competências fiscalizatórias relacionadas ao tratamento de dados desse público, projetando a Agência como guardiã administrativa de deveres reforçados de proteção, medidas de segurança e práticas de governança adequadas a menores. Esse movimento amplia o escopo da proteção de dados para além de uma lógica geral de conformidade, aproximando-o da tutela de grupos vulneráveis.

Paralelamente, a crescente centralidade da inteligência artificial na economia digital tem impulsionado a consolidação da ANPD como ator-chave na governança dessas tecnologias.

2.1. A ANPD e o papel indicado no marco regulatório da inteligência artificial

No contexto do texto atualmente em discussão do Projeto de Lei nº 2.338/2023¹³, que institui o marco regulatório da Inteligência Artificial no Brasil, a ANPD assume papel central na arquitetura institucional de governança da IA. O texto aprovado pelo Senado Federal e atualmente em tramitação na Câmara dos Deputados consolida a Agência como uma das principais responsáveis pela regulação, fiscalização e coordenação do uso de sistemas de inteligência artificial.

O projeto atribui à ANPD a função de reguladora residual, conferindo-lhe competência normativa, fiscalizatória e sancionatória para disciplinar sistemas de IA utilizados em setores que não disponham de agência reguladora própria. Nesse modelo, as autoridades setoriais permanecem responsáveis pela regulação das aplicações de IA em seus respectivos domínios, como saúde, finanças ou telecomunicações, enquanto a ANPD atua de forma supletiva nos setores desprovidos de regulação específica. O objetivo é evitar lacunas regulatórias e assegurar um padrão mínimo de proteção jurídica no uso da inteligência artificial, independentemente do setor econômico envolvido.

¹³ BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.338/2023**. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Câmara dos Deputados, Brasília, DF, 2023. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2868197&filename=PL%202338/2023. Acesso em 22 de janeiro de 2026.

Além disso, o PL posiciona a ANPD como autoridade coordenadora do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA). Nessa condição, caberá à Agência articular a atuação das diversas entidades reguladoras que compõem o sistema, promovendo a harmonia normativa, cooperação institucional e coerência das ações de fiscalização relacionadas ao tema. A ANPD também exercerá papel central no Conselho Permanente de Cooperação Regulatória em Inteligência Artificial, instância criada para fomentar o diálogo interinstitucional e a atuação coordenada do Estado na governança desse tipo de tecnologia.

A centralidade da ANPD nesse marco regulatório decorre, em grande medida, de sua vocação institucional para a proteção de dados pessoais e da privacidade — dimensões ligadas ao funcionamento de sistemas de inteligência artificial. O próprio texto do PL reforça que as competências atribuídas à Agência não afastam, mas complementam, aquelas já previstas na LGPD. Nesse sentido, a ANPD passa a desempenhar papel estratégico na garantia de que o desenvolvimento, a implementação e o uso de sistemas de IA observem princípios como finalidade, necessidade, transparência, não discriminação e responsabilização, sobretudo quando envolverem o tratamento automatizado de dados pessoais.

O projeto confere à Agência a incumbência de monitorar e fiscalizar os riscos associados ao uso da inteligência artificial, com especial atenção aos impactos sobre dados pessoais e direitos dos titulares. O modelo proposto prevê a atuação coordenada da ANPD com outros órgãos do SIA em investigações conjuntas, inclusive para a apuração de infrações e aplicação de sanções, especialmente nos casos de sistemas classificados como de alto risco.

Outro eixo relevante diz respeito à competência normativa atribuída à Agência. O PL estabelece que a ANPD será responsável pela edição de normas, orientações e diretrizes técnicas gerais sobre governança de IA, especialmente no que tange ao tratamento automatizado de dados pessoais, à transparência algorítmica, à avaliação de impactos e à comunicação de incidentes relevantes. Essas normas gerais deverão servir de base para regulamentações setoriais específicas, reforçando a função da ANPD como parte estruturante do sistema regulatório.

Do ponto de vista legislativo, embora o PL ainda esteja em fase final de discussão na Câmara dos Deputados, com a possibilidade de ajustes no modelo de governança e na definição das competências da ANPD, o desenho institucional proposto e discutido já aponta para a consolidação da Agência como figura central da regulação da inteligência artificial no Brasil.

REFLEXOS DIRETOS NA ATUAÇÃO DA ANPD

O tema de inteligência artificial passou a integrar de forma consistente a Agenda Regulatória da ANPD, especialmente no biênio 2023–2024, período em que a matéria foi incluída como eixo específico de atuação - o que se mantém na Agenda Regulatória proposta para o biênio 2025–2026¹⁴. Nesse contexto, a Agência conduziu estudos, consultas públicas e tomadas de subsídios voltadas à revisão de decisões automatizadas e ao uso de IA sob a ótica do regimento da LGPD, sinalizando a intenção de regulamentar de forma mais detalhada o artigo 20 da LGPD¹⁵.

¹⁴ BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD nº 31, de 22 de dezembro de 2025**. Altera a Agenda Regulatória para o biênio 2025–2026. Diário Oficial da União, Brasília, DF, 2025. Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-31-de-22-de-dezembro-de-2025-677950080>. Acesso em 22 de janeiro de 2026.

¹⁵ Art. 20: O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

A continuidade desse movimento também é perceptível no Mapa de Temas Prioritários da ANPD, que passou a incluir expressamente a inteligência artificial e tecnologias emergentes como foco prioritário de fiscalização para os anos de 2026 e 2027¹⁶. Esse direcionamento evidencia a preocupação da Agência com riscos como perfilamento excessivo, discriminação algorítmica, opacidade decisória e uso de sistemas automatizados em contextos sensíveis, tanto no setor privado quanto no setor público.

A atuação da ANPD tende a se afirmar como elemento-chave para assegurar que o avanço da inteligência artificial ocorra de forma responsável, ética e juridicamente segura, conciliando desenvolvimento econômico, inovação e proteção de direitos fundamentais. A Agência passa, assim, a ocupar posição estratégica não apenas como reguladora do uso de dados pessoais, mas como um dos principais pilares da governança da inteligência artificial no ordenamento jurídico brasileiro.

2.2. A atuação da ANPD no ECA Digital e a proteção de crianças e adolescentes no ambiente online

Outro vetor central de expansão das competências materiais da ANPD diz respeito à proteção de crianças e adolescentes no ambiente digital. A promulgação do ECA Digital representa um marco relevante nesse processo ao atribuir à ANPD papel institucional explícito na fiscalização do tratamento de dados pessoais desse público em contextos digitais.

A atribuição dessas competências à ANPD não ocorre de forma isolada, mas se insere no mesmo movimento de convergência regulatória observado na governança da inteligência artificial. Na visão da Agência, e em linha com a tradição brasileira de proteção de menores, crianças e adolescentes integram um grupo particularmente vulnerável em ecossistemas digitais marcados por coleta intensiva de dados, técnicas de perfilamento, publicidade comportamental e sistemas algorítmicos de recomendação e fidelização. Nesse cenário, a proteção de dados pessoais passa a funcionar como vetor da tutela de direitos fundamentais, conectando privacidade, segurança, desenvolvimento saudável e proteção contra práticas abusivas.

O ECA Digital consolida a ANPD como autoridade administrativa autônoma responsável pela supervisão do tratamento de dados de crianças e adolescentes, inclusive no que se refere à verificação etária, à obtenção de consentimento parental quando aplicável, à adoção de medidas de segurança adequadas e à implementação de mecanismos de prevenção em plataformas e serviços digitais direcionados ou acessíveis ao público infantojuvenil. Ao assumir esse papel, a ANPD amplia seu mandato original da LGPD, passando a atuar também como guardião de direitos de grupo vulnerável no ambiente online.

Do ponto de vista regulatório, o ECA Digital também potencializa o exercício do poder normativo técnico da ANPD. A Agência passa a deter competência para editar orientações e

¹⁶ BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD nº 30, de 23 de dezembro de 2025**. Aprova o Mapa de Temas Prioritários para o biênio 2026-2027. Diário Oficial da União, Brasília, DF, 2025. Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-30-de-23-de-dezembro-de-2025-677947163>. Acesso em 22 de janeiro de 2026.

diretrizes específicas sobre boas práticas no tratamento de dados de crianças e adolescentes, influenciando diretamente o desenho de produtos digitais, modelos de negócio baseados em dados e estratégias de conformidade de plataformas digitais. Trata-se de um movimento relevante: a proteção de dados deixa de operar apenas como obrigação transversal e passa a condicionar, de forma mais explícita, a própria arquitetura dos serviços digitais destinados a públicos sensíveis, em linha com a metodologia de *Privacy by Design*.

Assim como ocorre no campo da inteligência artificial, a atuação da ANPD no ECA Digital evidencia uma mudança qualitativa em seu papel institucional. A Agência não atua apenas como fiscal de condutas já consolidadas, mas como agente estruturante de uma governança preventiva, orientada à mitigação de riscos desde a concepção de sistemas e serviços digitais. Nesse sentido, ainda que as obrigações do ECA Digital só passem a vigorar em março de 2026, a Agência já iniciou ação de monitoramento prévio em face de diversas empresas impactadas pela entrada em vigor da lei, com a finalidade de avaliar o respectivo nível de maturidade legal e planejamento estratégico para a conformidade contínua em relação à nova regulação¹⁷.

Esse movimento reforça a compreensão de que a proteção de dados pessoais, especialmente quando envolver crianças e adolescentes, constitui elemento central da regulação do ecossistema digital contemporâneo.

AO REDOR DO MUNDO

A opção brasileira de atribuir a uma autoridade responsável por proteção de dados a competência por cuidar da proteção de crianças e adolescentes no mundo digital se destaca do resto do mundo.

Ao compararmos a legislação nacional com o Online Safety Act do Reino Unido¹⁸, marco internacional que influenciou a edição do ECA Digital, percebemos que as responsabilidades da ANPD no Brasil são atribuídas ao Office of Communications (Ofcom) britânico, órgão regulador independente responsável por telecomunicações, rádio, TV e internet. De toda forma, isso não impede que, em contexto específicos, exista a necessidade de cooperação entre o Ofcom e a autoridade britânica de proteção de dados (o Information Commissioner's Office - ICO)¹⁹.

¹⁷ BRASIL. Agência Nacional de Proteção de Dados. **Em ação de monitoramento do ECA Digital, a ANPD estende o prazo para que empresas prestem informações sobre implementação das novas regras**. Web, 2026. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/em-acao-de-monitoramento-do-eca-digital-a-anpd-estende-o-prazo-para-que-empresas-prestem-informacoes-sobre-implementacao-das-novas-regras>. Acesso em: 20 jan. 2026.

¹⁸ REINO UNIDO. **Online Safety Act 2023 Chapter 50**. An Act to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes. The Stationery Office, Londres, 2023. Disponível em: <https://www.legislation.gov.uk/ukpga/2023/50>. Acesso em: 22 de Janeiro de 2026.

¹⁹ OFCOM. **Ofcom and the Information Commissioner's Office (ICO) have published a joint statement on collaboration on the regulation of online services**. Web, 2024. Disponível em: <https://www.ofcom.org.uk/online-safety/safety-technology/online-safety-and-data-protection>. Acesso em: 22 de janeiro de 2026.

3. Digital Omnibus e os reflexos do debate europeu no Brasil

A expansão recente das frentes de atuação da ANPD não se explica apenas por ajustes internos de governança e fortalecimento institucional; ela também se conecta, de maneira crescente, a um ambiente regulatório global em rápida transformação. De um lado, o Brasil assiste ao alargamento do escopo de fiscalização da ANPD no ambiente digital. De outro, observa-se a consolidação de um novo ciclo regulatório europeu, mais amplo, transversal e estrategicamente voltado a unificação do seu ecossistema normativo digital, que tende a irradiar efeitos sobre práticas empresariais e debates legislativos fora da União Europeia. É nesse segundo eixo que se insere o pacote proposto pelo Digital Omnibus, cuja leitura é particularmente relevante para compreender o futuro do debate regulatório brasileiro.

O Digital Omnibus foi apresentado pela Comissão Europeia como um pacote voltado a simplificar e ajustar a implementação de normas digitais estruturantes, buscando reduzir fricções, sobreposições e incertezas práticas. O pacote é composto, em linhas gerais, por duas propostas de regulações distintas: uma com foco digital amplo²⁰, com alterações técnicas e ajustes em múltiplas peças do arcabouço digital europeu; e uma proposta com foco em inteligência artificial²¹, voltada a modificações específicas no regime de implementação e *enforcement* do EU AI Act²². O pacote dialoga com temas adjacentes de privacidade e compliance digital, refletindo a percepção europeia de que a “complexidade acumulada” do arcabouço regulatório, se não for adequadamente tratada, pode comprometer tanto a efetividade quanto a competitividade do bloco.

Para o Brasil, o ponto central não é a importação literal dessas soluções, mas a forma segundo a qual elas se projetam por meio do chamado “Efeito Bruxelas”, isto é, a capacidade da União Europeia de exportar, direta ou indiretamente, seus padrões regulatórios. Essa possível exportação pode ocorrer por dois caminhos.

O primeiro é econômico-operacional: empresas globais tendem a unificar práticas de compliance e governança com base no padrão europeu para evitar fragmentação e custos de segmentação, especialmente quando operam em múltiplas jurisdições. O segundo é normativo-político: legislações e orientações europeias funcionam como referência para reformas locais, influenciando tanto a linguagem jurídica quanto a arquitetura institucional de políticas públicas em países terceiros. Foi assim com o GDPR, cujo impacto transbordou fronteiras, e há sinais consistentes de que a mesma lógica se reforça, agora, com o EU AI Act e com o conjunto de instrumentos que orbitam a regulação digital europeia.

²⁰ UNIÃO EUROPEIA. Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que altera os Regulamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e as Diretivas 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557 no respeitante à simplificação do quadro legislativo digital e que revoga os Regulamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 e a Diretiva (UE) 2019/1024 (Omnibus Digital). Bruxelas, Jornal Oficial da União Europeia, 2025. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52025PC0837>. Acesso em: 22 de janeiro de 2026.

²¹ UNIÃO EUROPEIA. Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que altera os Regulamentos (UE) 2024/1689 e (UE) 2018/1139 no respeitante à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial (pacote Omnibus Digital sobre a IA). Bruxelas, Jornal Oficial da União Europeia, 2025. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52025PC0836>. Acesso em: 22 de janeiro de 2026.

²² UNIÃO EUROPEIA. Regulamento (EU) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). Bruxelas, Jornal Oficial da União Europeia, 2024. Disponível em: <http://data.europa.eu/eli/reg/2024/1689/oj>. Acesso em: 22 de janeiro de 2026.

IMPACTOS NO PLANO REGULATÓRIO

1. Modelagem do *enforcement* e governança institucional

A ênfase europeia em coordenação e supervisão consistente (inclusive com maior centralização de competências em estruturas especializadas) tende a alimentar, no Brasil, debates sobre desenho institucional de fiscalização, integração entre autoridades setoriais e a atuação “residual” de autoridades transversais, especialmente quando o país discute novos marcos legais.

2. Racionalização de compliance como agenda regulatória

O Digital Omnibus parte do diagnóstico de “complexidade acumulada” e tenta, ao menos em tese, reduzir atritos de implementação. Esse tipo de agenda tende a encontrar eco no Brasil, sobretudo em setores regulados e em temas de governança digital, onde a pressão por simplificação convive com a demanda por efetividade.

3. Pressão por convergência e “*benchmark* regulatório”

Mesmo que o Brasil não replique a solução europeia, o debate europeu frequentemente funciona como *benchmark* para legisladores, reguladores e julgadores, influenciando a linguagem do risco, expectativas de *accountability* e definição de deveres mínimos. E aqui há um ponto sensível: se o Digital Omnibus for percebido como flexibilização excessiva por alguns atores, pode gerar reação em sentido oposto (endurecimento local); e se for visto como ajuste pragmático, pode legitimar abordagens mais graduais e orientadas por risco.

Em síntese, o Digital Omnibus deve ser lido como parte do processo de maturação do modelo europeu: não é apenas “menos regulação”, mas uma tentativa de reorganizar o custo de conformidade e o *timing* de implementação, sem abandonar, ao menos formalmente, a estrutura de proteção baseada em risco.

Para o Brasil, o principal efeito é indireto, mas relevante: ele altera o ambiente de referência para políticas públicas e programas corporativos, reposicionando o debate sobre como regular IA e dados sem inviabilizar inovação; e essa tensão pode ser um dos motores centrais da próxima fase da regulação digital.

4. Considerações finais: o futuro da proteção de dados no Brasil

As transformações recentes no campo da privacidade e proteção de dados pessoais indicam que o debate regulatório entrou em uma nova fase, marcada menos pela criação de regimes isolados e mais pela busca de coerência sistêmica, coordenação institucional e adequação das normas à complexidade do ambiente digital. A convergência regulatória emerge, nesse contexto, não como uma opção metodológica, mas como resposta necessária à interdependência entre tecnologias, modelos de negócio e riscos jurídicos que atravessam múltiplos domínios normativos.

No Brasil, esse movimento se materializa de forma particularmente clara na expansão do papel institucional da Agência Nacional de Proteção de Dados. A ANPD deixa de ocupar um espaço restrito à fiscalização da LGPD para se consolidar como autoridade central do ecossistema regulatório digital, com funções que combinam *enforcement*, orientação normativa e articulação interinstitucional.

A incorporação de novas frentes materiais, como a governança da inteligência artificial e a proteção de crianças e adolescentes no ambiente digital, evidencia um deslocamento qualitativo na ANPD: a proteção de dados passa a operar como eixo estruturante de respostas regulatórias mais amplas, voltadas à tutela de direitos fundamentais em contextos tecnológicos complexos.

Paralelamente, o debate europeu em torno do Digital Omnibus revela que o amadurecimento dos regimes também passa por reflexões sobre proporcionalidade, *timing* regulatório e racionalização do custo de conformidade. Longe de representar uma simples retração normativa, essas iniciativas sinalizam uma tentativa de ajustar instrumentos regulatórios para torná-los mais efetivos, sem abandonar uma lógica de proteção baseada em risco.

Nesse cenário, as perspectivas futuras da proteção de dados no país tendem a um modelo menos centrado na conformidade formal e mais orientado à governança, à demonstração de responsabilidade e à integração entre regimes jurídicos. Para empresas, isso implica a necessidade de estruturas de compliance mais sofisticadas, capazes de dialogar simultaneamente com privacidade, segurança da informação, governança algorítmica e proteção de públicos vulneráveis.

Para reguladores, o desafio será equilibrar expansão de competências, coordenação interinstitucional e previsibilidade regulatória, evitando tanto a fragmentação quanto a complexidade normativa.



www.baptistaluz.com.br/

