VLK Direito, Inovação & Tecnologia

Onde o **Direito** impulsiona a **Inovação**

DIREITO DIGITAL, REGULAÇÃO E GOVERNANÇA

RETROSPECTIVA 2025

Quais os 10 principais temas de destaque de 2025?

TENDÊNCIAS 2026

Quais os 10 principais temas que pautarão 2026?

www.vlklaw.com.br

Direito,
Inovação
& Tecnologia

RETROSPECTIVA 2025

TENDÊNCIAS 2026

Este sumário é interativo. Clique nos títulos para acessar diretamente o conteúdo desejado.

Sobre nós

Autores

1. STF e novo regime de responsabilidade civil na moderação (Art. 19 MCI)

Em junho de 2025, o Supremo Tribunal Federal (STF) redefiniu o regime de responsabilidade civil na moderação de conteúdo online. A Corte reconheceu a inconstitucionalidade parcial e progressiva do art. 19 Marco Civil da Internet (MCI) e instituiu modelo plural de responsabilização, no qual a exigência de ordem judicial prévia para responsabilização dos provedores deixa de ser a regra geral, e passa a depender de deveres de diligência e governança na resposta a conteúdo potencialmente ilícitos, no seguinte sentido:

» **Nova regra predominante:** responsabilidade civil vinculada ao não atendimento de notificações extrajudiciais em casos de crimes ou ilícitos em geral e de contas denunciadas como inautênticas;

» **Regra preservada (art. 19):** (i) responsabilidade civil somente no caso de descumprimento de ordem judicial para crimes contra a honra; e (ii) contextos com tratamento próprio: a) provedores de e-mail; b) aplicações de reuniões fechadas (voz/vídeo); e c) serviços de mensageria privada;

» **Para anúncios e impulsionamentos pagos:** ou rede artificial de distribuição, há presunção de responsabilidade, independentemente de notificação extrajudicial, exceto se os provedores comprovarem que atuaram diligentemente e em tempo razoável para tornar indisponível o conteúdo ilícito;

» **Dever de cuidado:** associado a falhas sistêmicas de governança, fixando rol taxativo de crimes graves, que impõe às plataformas a indisponibilização

imediata de conteúdos, sob pena de responsabilização civil, como terrorismo, instigação ao suicídio, racismo e pornografia infantil;

» **Marketplaces:** respondem civilmente de acordo com o Código de Defesa do Consumidor; e

» **Representação no Brasil:** os provedores com atuação no Brasil devem constituir e manter sede e representante no país, com plenos poderes para conseguirem cumprir o previsto na decisão.

O acórdão do julgamento foi publicado em 7 de novembro de 2025 e as novas regras estão valendo, mas com efeitos modulados: aplicam-se apenas a casos futuros a partir da decisão, preservando processos que já transitaram em julgado. Alguns grandes provedores de aplicação opuseram Embargos de Declaração solicitando a correção de pontos da decisão e pleiteando 6 meses de prazo para adaptação às novas regras, sob pena de insegurança jurídica. Enquanto o STF não se manifesta sobre o pedido, a decisão de mérito continua válida. No entanto, na prática, a aplicação de multas ou punições imediatas pelo descumprimento de novas obrigações deve ser tratada com cautela pelo Judiciário, enquanto houver recursos pendentes sobre a implementação.

IMPACTOS - A decisão amplia a responsabilidade das plataformas como intermediárias no Brasil, exigindo atuação ainda mais diligente diante de notificações extrajudiciais acerca de conteúdos potencialmente ilícitos. Também impõe novas obrigações de compliance, como criar sistemas internos de moderação, mecanismos eficazes de notificação extrajudicial, relatórios de transparência, representação local e medidas proativas contra crimes graves. Há acertos importantes na decisão do STF, no entanto, ela pode estimular a remoção indiscriminada de conteúdos, fomentar a indústria de indenizações, desestimular o empreendedorismo digital e restringir a oferta de serviços globais no Brasil.

2. ECA Digital: lei sancionada e início da regulamentação e do monitoramento

O Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025 –ECA Digital) foi sancionado em setembro de 2025 e marcou histórico avanço na proteção de crianças e adolescentes no ambiente digital, com destaque para as obrigações de produtos e serviços de tecnologia da informação direcionados ou de acesso provável por eles:

» Mecanismos de aferição etária;

» Ferramentas de controle parental;

» Medidas para prevenir e mitigar riscos de acesso, exposição, recomendação ou facilitação de contato a conteúdo sensível;

» Vedação a utilização de técnicas de perfilamento para direcionamento de publicidade comercial;

» Vedação as caixas de recompensa (loot boxes) direcionadas ou de acesso provável, conforme classificação indicativa; e

» Vedação de monetização e impulsionamento de conteúdo de erotização.

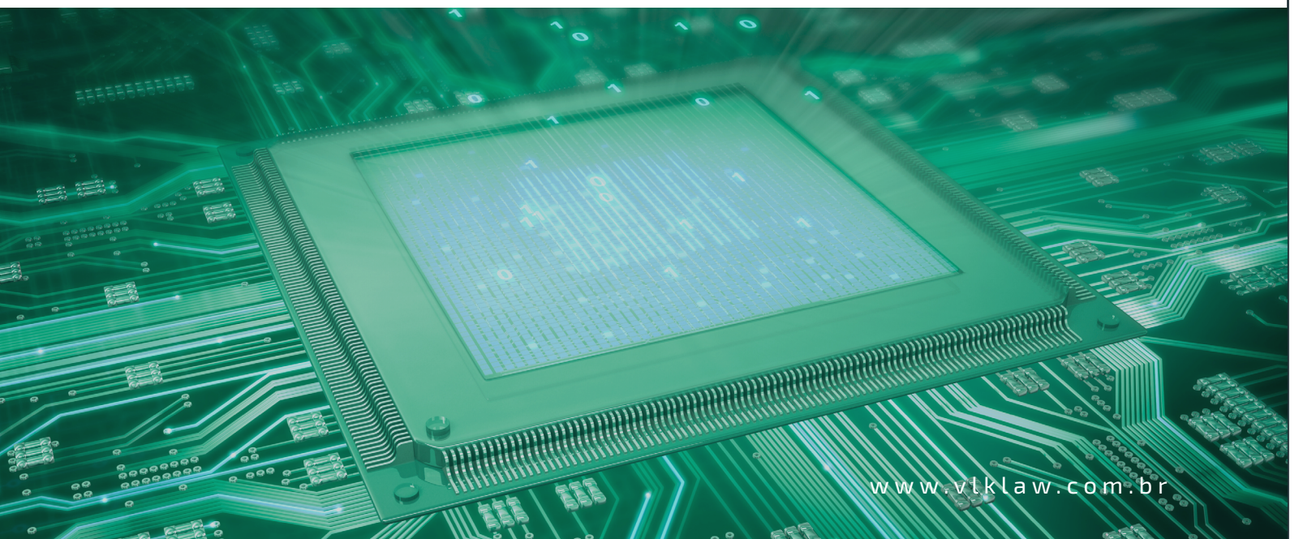
O Decreto nº 12.622/2025 atribuiu à Agência Nacional de Proteção de Dados (ANPD) papel de autoridade central para a regulamentação, fiscalização e aplicação das sanções do ECA Digital.

» Diante curto prazo para adequação (6 meses), ainda em 2025:

» A ANPD e o Ministério da Justiça e da Segurança Pública abriram consultas públicas sobre conceitos e obrigações do ECA Digital, como mecanismos de aferição de idade, antecipando debates sobre padrões técnicos, proporcionalidade regulatória e responsabilidades dos agentes econômicos;

» A ANPD oficiou 37 empresas requerendo informações iniciais relacionadas a adequação normativa, com o objetivo de compreender os desafios enfrentados na implementação da nova Lei e subsidiar ações futuras de orientação e fiscalização.

IMPACTOS – O ECA Digital inaugura novo nível de accountability no desenvolvimento e na operação de produtos e serviços digitais voltados ou acessíveis a crianças e adolescentes, o que exige dever de cuidado ativo, incluindo configurações de privacidade e segurança por padrão, mecanismos robustos de verificação de idade, ferramentas de supervisão parental, avaliações de impacto (segurança, saúde e proteção de dados pessoais) e diligência algorítmica. Na prática, serão necessários ajustes de arquitetura e governança em toda a cadeia (interna e junto a fornecedores), cabendo a todos os envolvidos garantir a proteção integral de crianças e de adolescentes. Isso tende a resultar em produtos e serviços mais seguros e confiáveis, além de reduzir exposição a riscos regulatórios, mitigando fiscalizações e potenciais sanções pela ANPD.



3. ANPD: Agência Reguladora, empoderada e com novas atribuições

A Medida Provisória (MP) 1.317/2025 alterou a natureza jurídica da ANPD de autarquia de natureza especial para Agência Reguladora. Com esse novo status, a ANPD passou a dispor de autonomia funcional, técnica, decisória, administrativa e financeira, reforçando sua capacidade de fiscalização, normatização e aplicação de sanções no âmbito da LGPD e, de maneira inédita, do ECA Digital.

A mudança reposiciona a ANPD como ator central do ecossistema regulatório digital brasileiro, com maior estabilidade institucional e poder de enforcement. Ainda, a ANPD está prevista como autoridade competente do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA) no texto atual do PL 2338/2023.

A ANPD planeja dobrar o quadro atual (cerca de 218 servidores) já a partir de 2026, com foco imediato em adequar estrutura física e operacional para receber o aumento. A estratégia é sustentar um ciclo de expansão que pode levar a ANPD a triplicar de tamanho até 2027 (no que teria cerca de 600 servidores), fortalecendo sua maturidade institucional e avançando para autonomia administrativa, típica de agências reguladoras.

IMPACTOS - A ANPD avança na consolidação como reguladora central da proteção de dados e do ambiente digital, ocupando papel estratégico na convergência entre Direito e inovação - duas agendas que se potencializam. A LGPD, o ECA Digital e o futuro Marco Legal da IA precisam ser interpretados não apenas como mecanismos de proteção, mas como instrumentos de modernização, confiança e competitividade. O trabalho da ANPD já fez com que a LGPD, por exemplo, fosse elevada à agenda executiva das organizações, conectando proteção de dados a vantagem competitiva, credibilidade institucional e sustentabilidade do negócio. Nesse novo cenário e com novas atribuições, a ANPD terá papel decisivo na construção de ecossistema digital seguro, estável e propício ao desenvolvimento econômico e tecnológico.

4. IA no Brasil: Marco Regulatório e Governança

Em 2025, a Inteligência Artificial ("IA") passou de tema emergente a prioridade estruturante das agendas de competitividade, governança e regulatória brasileira, com avanços relevantes nas discussões do marco legal e medidas empresariais para mitigação de riscos. Destacamos quatro eixos:

a. PL 2.338/23 – tramitação e principais discussões

Desde a sua concepção em 2023, o Projeto de Lei 2.338 apresentou avanços, como desidratação de medidas de governança excessivas e amadurecimento do modelo de regulação baseada em risco. O texto aprovado em dezembro de 2024 no Senado, foi discutido durante todo o ano de 2025 na Comissão Especial da Câmara dos Deputados, mas o seu Relatório final e votação ficaram para 2026.

A agenda regulatória nacional para IA exige cautela em três pontos principais: i) análise robusta do impacto regulatório do futuro Marco de IA para evitar desalinhamentos com o Plano Brasileiro de IA; ii) preservação do treinamento de modelos (input) diante de debates sobre direitos autorais, convergindo para práticas como fair use (EUA) e exceções de text and data mining (UE); e iii) tratamento autônomo do Redata, dada a centralidade dos data centers para outras tecnologias, além da IA.

Ainda que não concluído, o avanço do PL em 2025 passou a orientar, de forma indireta, em conjunto com outros frameworks internacionais (NIST, ISO e EU AI Act) e das leis já existentes (como LGPD, Marco Civil da Internet, Código de Defesa do Consumidor) programas de governança empresarial para o uso seguro e responsável da IA

b. PL 6.237/25 – SIA e Atuação do Poder Executivo Federal

De iniciativa do poder Executivo Federal, o PL 6.237/25 institui o SIA (Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial), principalmente como forma de evitar "vício de iniciativa" do SIA previsto no PL

2.338/23: projetos de lei que estabeleçam estruturas governamentais precisam ser enviados pelo Executivo ao Congresso. Resultado da sinergia entre os poderes Executivo e Legislativo, sinaliza que a aprovação dos dois projetos pode estar próxima, o que pode ocorrer no primeiro semestre de 2026.

c. Treinamento de IA: Direitos Autorais e Proteção de Dados Pessoais

O treinamento de modelos de IA tornou-se tema crítico para os negócios, pois concentra incertezas jurídicas relevantes especialmente em direitos autorais e proteção de dados pessoais. Em geral, conteúdos potencialmente protegidos, obras autorais e dados pessoais devidamente anonimizados são tratados como insumos técnicos para o aprendizado estatístico do modelo. Ou seja, para ensinar relações probabilísticas entre padrões e elementos, e não para reproduzir conteúdo individualizado.

» **Proteção de dados pessoais:** no treinamento de grandes modelos, os dados pessoais usualmente podem ser considerados anonimizados e, portanto, fora do escopo de proteção da LGPD. Ademais, o consentimento exclusivo para o treinamento enfrenta limites técnicos e operacionais. Nesse cenário, quando envolver dados pessoais, o legítimo interesse, desde que sustentado por salvaguardas robustas (como *minimização*, segurança, transparência e opt-out efetivo), tem sido defendido como base legal capaz de equilibrar inovação e proteção de direitos. Em termos de dados pessoais sensíveis, restringir o treinamento somente aos titulares que consentem, pode gerar viés amostral, reduzindo a qualidade, representatividade e segurança dos modelos.

Na União Europeia (UE), iniciativas regulatórias vêm buscando ampliar a aplicabilidade do legítimo interesse para treinamento de IA, como ocorre no debate em torno do chamado Digital Omnibus. No Brasil, o precedente recente envolvendo a atuação da ANPD, que inicialmente suspendeu preventivamente prática de treinamento por uma rede social e posteriormente autorizou o uso mediante maior transparência e mecanismos efetivos de oposição, indica, ainda que de forma preliminar, que o legítimo interesse pode ser viável para esse tipo de atividade quando combinado a medidas adequadas de governança.

» **Direitos autorais:** no debate sobre fair training, os argumentos mais recorrentes são:

i) os dados são utilizados apenas como insumos técnicos, para ensinar padrões estatísticos, e não para copiar as obras originais;

ii) o aprendizado de máquina é comparável ao processo humano de indução e generalização; e

iii) a responsabilização continua em relação aos outputs que violem direitos autorais.

Entre os principais casos em andamento, destacam-se: nos EUA, o litígio entre The New York Times e OpenAI/Microsoft; e no Brasil, a ação movida pela Folha de São Paulo contra a OpenAI.

A falta de solução legislativa definitiva mantém o debate focado em bases legais, exceções aos direitos autorais, anonimização e transparência, com impactos diretos sobre contratos, políticas de dados e gestão de risco regulatório. Ao mesmo tempo, o setor produtivo passou a demandar maior equilíbrio regulatório, defendendo segurança jurídica e proporcionalidade para não comprometer inovação e competitividade, especialmente no contexto do PL nº 2.338/23,

consolidando o tema como estratégico para compliance e desenvolvimento tecnológico. O Brasil não pode se precipitar com texto restritivo. Sobre proteção de dados pessoais, espera-se equilíbrio da ANPD em eventuais regulamentações e fiscalizações.

d. Segurança da Informação e IA

A IA está acelerando o risco cibernético: 40% dos ataques de phishing direcionados a empresas já são gerados por IA (Vipre) e a automação pode reduzir em até 95% os custos das campanhas fraudulentas (HBR). Ao mesmo tempo, Shadow AI (uso de IA sem aprovação corporativa) já aparece em 20% das violações e adiciona, em média, US$ 670 mil por incidente (IBM, 2025). Além disso, 97% dos incidentes com IA ocorreram em sistemas sem controles adequados (IBM, 2025). Outros riscos como model poisoning, data leakage, uso indevido de modelos e falhas de explicabilidade passaram a ser analisados sob a ótica de responsabilidade civil, dever de segurança e governança corporativa. Empresas que utilizam IA e automação extensivamente conseguiram reduzir em US$ 1,9 milhão os custos médios de violações e encurtar em 80 dias o ciclo de resposta a incidentes (IBM, 2025). Ou seja, a conexão entre Segurança da IA, proteção de dados, cibersegurança e dever de diligência reforçou a necessidade de controles internos, auditorias e documentação técnica como instrumentos jurídicos de mitigação de risco.

e. Plano Brasileiro de IA (PBIA)

O PBIA avançou em 2025, com a publicação da sua versão final e instrumento de coordenação de políticas públicas, com o lema "IA para o bem de todos" e organizado em cinco eixos principais: Infraestrutura e desenvolvimento de IA; Difusão, formação e capacitação em IA; IA para melhoria do serviço público; IA para inovação empresarial; e Apoio ao processo regulatório e de governança da IA.

IMPACTOS - O avanço do Marco Regulatório e das práticas de governança em IA em 2025 transforma a adoção dessas tecnologias em decisão estratégica de risco e compliance, e não apenas de inovação. O uso, desenvolvimento ou a contratação de sistemas de IA passa a exigir avaliação prévia de riscos, revisão de contratos, políticas de dados e direitos autorais, além da implementação de controles de segurança, documentação técnica e mecanismos de accountability. Empresas que anteciparem esses padrões, alinhando governança, segurança e transparência às diretrizes do PL 2.338/23 e do PBIA, reduzem exposição regulatória, preservam competitividade e ampliam sua capacidade de escalar soluções de IA de forma sustentável e responsável.

5. AI Act (UE): início de implementação e cronograma faseado

O EU AI Act (Regulation (EU) 2024/1689), publicado em 12/07/2024, não entrou em vigor integralmente de uma vez. Ele foi desenhado para aplicar-se em ondas, permitindo adaptação do mercado e a construção de instrumentos complementares (guidelines, standards e codes of practice).

O EU AI Act (Regulation (EU) 2024/1689), publicado em 12/07/2024, não entrou em vigor integralmente de uma vez. Ele foi desenhado para aplicar-se em ondas, permitindo adaptação do mercado e a construção de instrumentos complementares (guidelines, standards e codes of practice).

Em fevereiro de 2025, passaram a aplicar-se as obrigações de literacia de IA (medidas para garantir capacitação adequada de pessoas que operam/uso de IA em nome da organização) e as IAs proibidas (ex.: social scoring; uso de IA para "emotion recognition" de trabalhadores; e restrições severas, com exceções estritas, para identificação biométrica remota em tempo real em espaços acessíveis ao público). A Comissão Europeia publicou Guidelines sobre práticas proibidas em 29/07/2025, para apoiar interpretação uniforme dessas proibições

Em agosto de 2025, passaram a aplicar-se obrigações para modelos de IA de uso geral (GPAI), incluindo transparência e governança (p.ex., documentação e medidas relacionadas a copyright e segurança). Em 10/07/2025, a Comissão Europeia disponibilizou o General-Purpose AI Code of Practice, coordenado pelo European AI Office, com três blocos (Transparência, Copyright e Safety & Security). O Code é voluntário, mas serve como referência prática para demonstrar aderência às obrigações aplicáveis do AI Act para GPAI.

Assim, 2025 funcionou como ano de preparação regulatória intensiva, especialmente para organizações com operações globais ou impacto extraterritorial do AI Act. O modelo europeu é uma das principais referências normativas a serem acompanhadas nos próximos anos: a maior parte do AI Act

passa a ser aplicável de maneira ampla em agosto de 2026, incluindo quase todas as obrigações para sistemas de IA, e a sua implementação integral se dará em agosto de 2027. Trata-se de processo contínuo de governança e accountability.

Ao mesmo tempo, discute-se se a carga regulatória pode ser excessiva, levando a rediscussão de diversas leis de direito digital na Europa, incluindo o AI Act, conforme será abordado no tópico 6 ("Digital Omnibus"), a seguir.

IMPACTOS – O chamado efeito Bruxelas, ou seja, a inspiração do padrão regulatório europeu para além de suas fronteiras, manifesta-se de forma clara no EU AI Act, que já influencia iniciativas legislativas em outros mercados, como o PL nº 2.338/23 no Brasil. Mesmo sem presença física na UE, empresas que desenvolvem, utilizam ou contratam IA passam a enfrentar exigências indiretas de governança, transparência e gestão de riscos para manter acesso a mercados, cadeias globais e parceiros internacionais. Nesse contexto, adotar o AI Act como um dos frameworks de referência, de maneira proporcional e filtrada à realidade do negócio, permite antecipar convergências regulatórias, reduzir riscos jurídicos e comerciais futuros e evitar barreiras regulatórias. Mais do que conformidade, trata-se de posicionamento estratégico, capaz de diferenciar o negócio em um ambiente de crescente padronização regulatória internacional.

6. Digital Omnibus: simplificação e recalibração regulatória na UE

Em novembro de 2025, a Comissão Europeia apresentou o Digital Omnibus, pacote legislativo destinado a reduzir a burocracia e simplificar o arcabouço regulatório da União Europeia para a economia digital, incluindo o GDPR, o AI Act, o NIS2 e o Data Act. A proposta sinaliza esforço institucional para tornar a aplicação da regulação digital da UE mais coerente, previsível e operacional, após anos de aplicação e construção normativa. Isso tende a reduzir a complexidade, tanto para as empresas, quanto para as autoridades competentes, estimulando a segurança jurídica.

Do ponto de vista jurídico e estratégico, a proposta introduz ajustes relevantes: a consolidação e simplificação de regras sobre livre fluxo de dados, governança e open data no âmbito do Data Act, com reforço à proteção de segredos comerciais.

No eixo de privacidade e IA, a proposta busca clarificar pontos operacionais do GDPR (sem alterar sua lógica central), incluindo parâmetros sobre uso de dados no desenvolvimento e operação de sistemas/modelos de IA, com referência ao legítimo interesse sob salvaguardas e reforço de direitos (como oposição), e ajustes procedimentais para reduzir fricção e aumentar previsibilidade regulatória.

Destacam-se ainda a tentativa de reduzir a fadiga de consentimento ao permitir maior alinhamento entre GDPR e ePrivacy no uso de cookies, a simplificação do reporte de incidentes de segurança por meio de ponto único de notificação para múltiplos regimes (GDPR, NIS2, DORA) e a revogação da Regulação de Plataformas e Empresas (P2B Regulation), diante da sobreposição com o DSA e o DMA.

IMPACTOS - O Digital Omnibus indica inflexão relevante da União Europeia em direção à simplificação e maior coerência da regulação digital, com efeitos diretos sobre estratégias de compliance e operações globais. A redução de sobreposições entre GDPR, AI Act e regimes de cibersegurança aumenta a previsibilidade jurídica e diminui custos de conformidade. Há tendência de que tais ajustes influenciem padrões regulatórios e interpretativos no Brasil, especialmente em proteção de dados, uso de IA e governança digital.

7. Cibersegurança: nova estratégia nacional e desenho de marco regulatório

A cibersegurança ganhou protagonismo no Brasil em 2025, como tema jurídico, técnico e de política pública estratégica, com a publicação da nova Estratégia Nacional de Cibersegurança (E-Ciber) pelo Decreto nº 12.573/2025, que substituiu a versão anterior e elevou a maturidade institucional da resposta nacional à ameaça digital. A E-Ciber, formulada pelo Comitê Nacional de Cibersegurança (CNCiber) com participação de governo, setor privado, sociedade civil e academia, estruturou-se em quatro eixos temáticos que integram proteção e conscientização da sociedade, segurança e resiliência de serviços essenciais e infraestruturas críticas, cooperação multissetorial e soberania digital, promovendo governança centralizada e coordenação de políticas públicas para prevenção, mitigação e resposta a incidentes cibernéticos.

Além disso, em dezembro de 2025 houve avanço legislativo do PL 4.752/2025 (Marco Legal da Cibersegurança), com a aprovação do texto pela Comissão de Constituição e Justiça (CCJ) do Senado. O PL é focado primariamente na cibersegurança do setor público. A proposta seguirá para análise da Comissão de Ciência, Tecnologia, Inovação e Informática.

Em paralelo, o CNCiber aprovou sua proposta de Lei Geral da Cibersegurança e o encaminhamento para avaliação do Governo Federal de 4 opções de órgãos de governança autoridade (Agência Reguladora específica; Autarquia não especial; Secretaria da administração direta; ou Anatel). Essa proposta é vista como complementar ao PL 4.752. O conjunto do trabalho (Marco Legal da Cibersegurança + Propostas de Modelo de Governança Central - ANCiber) será encaminhado à CREDEN.

A partir daí, caberá ao Governo avaliar a oportunidade e o formato de apresentação da proposta ao Congresso, alinhando política pública, visão de Estado e ambição regulatória com as necessidades crescentes do país em cibersegurança.

IMPACTOS - A nova Estratégia Nacional de Cibersegurança e o avanço do Marco Legal consolidam a cibersegurança como elemento central de responsabilidade jurídica e governança empresarial. A ausência de um órgão regulador nacional e intersetorial compromete a implementação de normas transversais, recomendadas pelas boas práticas internacionais. Essa lacuna pode ajudar a explicar por que o Brasil figura entre os países mais atacados do mundo. Sem regras claras, a cibersegurança é frequentemente negligenciada e os prejuízos só se evidenciam quando já é tarde demais. Em outras palavras, cibersegurança deixou de ser uma questão meramente técnica. É uma escolha estratégica e essencial - de autoridade públicas, empresas, líderes e, acima de tudo, das nações.

8. Consentimento, escolha do usuário e concorrência nos mercados digitais: o

Em geral, os modelos *"consent or pay"* oferecem às pessoas as seguintes alternativas:

(i) consentir para a utilização de dados pessoais para publicidade personalizada ou outras finalidades, a fim de acessar um produto ou serviço;

(ii) pagar um valor para acessar o produto ou serviço, sem que se utilize seus dados pessoais para publicidade personalizada ou outra finalidade; ou

(iii) não usar o produto ou serviço.

A discussão jurídica desse modelo envolve o equilíbrio entre a proteção de dados dos usuários, a liberdade de escolha no exercício de direitos fundamentais e a manutenção de mercados digitais competitivos. Em regra, a possibilidade binária entre consentir ou pagar, por si só, pode não garantir consentimento válido e, em alguns casos, ser questionada sob a perspectiva concorrencial.

Em 2025, além do "como coletar consentimento", o foco regulatório envolveu o "quão livre, informada e economicamente viável é a escolha do usuário", com destaque para:

(i) No Brasil, a ANPD manteve o entendimento de que o modelo "consent or pay" é especialmente problemático quando envolve dados biométricos, como a íris do olho, mantendo a suspensão do oferecimento de compensação financeira por meio de criptomoedas (Worldcoin). O entendimento da Agência é que a troca do escaneamento da íris compromete a liberdade de escolha do titular, pois o incentivo financeiro funciona como pressão econômica, sobretudo em contextos de assimetria de informação. A ANPD também rejeitou o argumento de que a conversão da íris em códigos matemáticos configuraria anonimização suficiente, destacando risco de reidentificação e caráter irreversível. Vale destacar esse trecho da ANPD: "a existência de contrapartida financeira constitui uma intervenção do controlador, que, na prática, implica uma interferência indevida sobre a manifestação de vontade autônoma do titular, razão pela qual o consentimento obtido não pode ser qualificado como livre".

(ii) Na União Europeia, multa aplicada a uma rede social com base no Digital Market Act (DMA) levou o modelo "consent or pay" ao centro da agenda de concorrência nos mercados digitais, mesmo sendo um debate que historicamente surgiu no âmbito do GDPR. A Comissão Europeia deixou claro que, para plataformas classificadas como gatekeepers, oferecer apenas a alternativa entre consentir com o uso extensivo de dados pessoais ou pagar para evitá-lo pode não representar uma escolha real para o usuário. Ao deslocar a análise do plano estrito da validade do consentimento para o impacto econômico do design de escolha, a decisão conectou proteção de dados e concorrência. Ou seja, mesmo que um modelo seja defendido sob a lógica do GDPR, ele precisa também ser avaliado sob o DMA quando a monetização de dados pessoais se torna condição estrutural de acesso e mecanismo de manutenção de eventual dominância. Há recurso da decisão em trâmite.

(iii) Já no Reino Unido, a ICO publicou orientações específicas sobre o modelo "consent or pay", com abordagem um pouco mais aberta. As empresas podem adotá-lo, mas se conseguirem provar que a pessoa realmente tem liberdade de escolha. Ou seja, que não é pressionada a aceitar o uso dos seus dados pessoais. Para isso, o valor cobrado para recusar o rastreamento, por

exemplo, deve ser justo, as opções

oferecidas devem ser equivalentes e o serviço não pode ser pior para quem não consente. Além disso, a empresa precisa demonstrar que pensou na proteção da privacidade desde o início do produto e documentou essa análise. O próprio ICO esclarece que essas orientações estão sendo revistas após a entrada em vigor de uma nova lei de dados no Reino Unido, em junho de 2025;

(iv) Voltando para a UE, há intensificação do enforcement do GDPR por autoridades europeias sobre mecanismos de consentimento, incluindo banners de cookies e outros fluxos de escolha, com foco na efetividade do consentimento, repressão a dark patterns e vedação de práticas que esvaziem a liberdade decisória do titular. Também um movimento de revisão e simplificação do regimento europeu de cookies e tecnologias semelhantes, refletindo preocupação mais ampla com a qualidade do consentimento e com a sustentabilidade de modelos baseados em escolhas binárias rígidas.

IMPACTO - Esses elementos combinados marcaram mudança qualitativa na venda de serviços e na regulação da publicidade digital na União Europeia, com efeitos estruturais sobre modelos de negócio e governança de dados. O futuro da economia digital na Europa tende a privilegiar soluções menos intrusivas, maior atenção ao privacy by design, estruturas de escolha mais equilibradas e alinhamento cada vez mais estreito entre enforcement de proteção de dados e concorrência. Ou seja, há crescente convergência entre proteção de dados e direito concorrencial, incorporando fatores como assimetria de poder, dependência econômica do usuário, ausência de alternativas equivalentes e impactos econômicos da escolha como elementos juridicamente relevantes para análise da liberdade do consentimento. Esse movimento antecipa ambiente regulatório mais exigente e integrado, com potenciais reflexos também no Brasil, especialmente no contexto da interpretação da LGPD e da incorporação de análises econômicas e concorrenciais pelo CADE.

9. Transferência Internacional de Dados: vigência e dúvidas operacionais

A transferência internacional de dados pessoais já está em implementação prática no Brasil, com a consolidação dos efeitos da Resolução CD/ANPD nº 19/2024. O principal marco do ano foi o encerramento, em agosto de 2025, do prazo para adequação às Cláusulas-Padrão Contratuais (SCCs, na sigla em inglês) da ANPD, tornando obrigatória a revisão e atualização de contratos que envolvem fluxos internacionais de dados. Esse movimento deslocou o tema do plano normativo para o núcleo do compliance regulatório, impactando grupos econômicos, cadeias globais de fornecedores e operações transnacionais que dependem de transferência contínua de dados pessoais.

2025 também revelou desafios operacionais relevantes na implementação do novo regime, especialmente quanto à integração das SCCs da ANPD com cláusulas contratuais globais, à necessidade de avaliações complementares de risco e equivalência de proteção, e à capacidade de demonstrar accountability perante a Autoridade.

IMPACTOS - A conformidade em transferência internacional não se esgota documental, exigindo governança contínua, mapeamento de fluxos, controles de segurança e preparo para fiscalização. Além disso, a ANPD já está recebendo pedidos de equiparação de Normas Corporativas Globais oriundas da Europa e vem questionando as organizações sobre pontos relacionados a essas solicitações.

10. Política Nacional de Data Centers e incentivos (Redata)

Em setembro de 2025, a Medida Provisória nº 1.318/2025 instituiu o Redata (Regime Especial de Tributação para Serviços de Data Center), criando marco legal voltado à atração de investimentos privados em data centers, por meio de incentivos tributários (isenção de IPI, PIS/Cofins em equipamentos de Tecnologia da Informação) em troca de investimentos em P&D e metas de produção nacional, com foco em soberania digital e desenvolvimento regional.

Embora a MP ainda não tenha sido convertida em lei, há expectativa para que a votação ocorra no mês de fevereiro de 2026. Desse modo, o tema foi importante em 2025 para promover articulação entre política industrial, transformação digital e regulação do ambiente de dados, com o Redata funcionando como instrumento capaz de promover investimentos e maior autonomia tecnológica. A adoção de incentivos tributários alinhados a metas de P&D e produção nacional coloca desafios e oportunidades para o direito regulatório, tributário e de compliance: por um lado, exige segurança jurídica e coordenação normativa entre diferentes áreas (dados, energia, meio ambiente, proteção de dados e cibersegurança); por outro, cria ambiente propício para negociação de contratos de longo prazo, investimento estrangeiro e desenvolvimento de cadeias locais de valor em TIC.

IMPACTOS - O REDATA tem potencial para atrair investimentos significativos para o Brasil no setor digital, fortalecendo o ecossistema tecnológico local. Isso pode ampliar a oferta e qualidade dos serviços digitais disponíveis, beneficiando empresas com maior soberania e segurança no tratamento de dados. Ademais, data centers contemplam infraestruturas complexas e fundamentais para diversas tecnologias, incluindo, mas não se limitando à IA. Dessa forma, é importante ponderar se essa política de incentivos deve ser tratada separadamente do Marco Legal de IA, diante das suas particularidades técnicas, econômicas e estratégicas, minimizando conflitos normativos e promovendo a eficiência regulatória para ambos os setores.

1. Governança Digital Empresarial Integrada (Privacidade, Cibersegurança e IA)

A convergência regulatória, impulsionada pela atuação mais madura da ANPD, entrada em vigor do ECA Digital, pelo avanço da regulação de IA e crescente exigência de segurança cibernética, reposiciona a governança digital no centro da estratégia corporativa.

Nesse cenário, dados, segurança e IA deixam de ser domínios isolados e passam a operar de forma interdependente, exigindo modelo integrado de governança digital, capaz de alinhar tecnologia, risco, estratégia e accountability. A coordenação clara e funcional entre CPO (Chief Privacy Officer), CSO (Chief Security Officer) e do CAIO (Chief AI Officer) torna-se fator-chave para conformidade regulatória, eficiência operacional e velocidade de resposta.

Organizações que estruturam essa governança integrada elevam sua capacidade de: antecipar riscos regulatórios e tecnológicos; responder de forma coordenada a fiscalizações e incidentes; sustentar deveres crescentes de transparência, explicabilidade algorítmica e segurança; e demonstrar maturidade institucional ao mercado e ao poder público.

Além de mitigar riscos regulatórios e reputacionais, essa abordagem tende a gerar vantagem competitiva em contratos, processos de M&A, parcerias e relações com o poder público, reforçando confiança institucional. Em 2026, a governança integrada tende a se consolidar como infraestrutura jurídica essencial para sustentabilidade, inovação e resiliência no ambiente digital.

Relatório de Riscos Globais do World Economic Forum e Riscos Digitais (Cibersegurança, Desinformação e IA):

1. Cibersegurança

» Curto prazo (2 anos): Cyber insecurity aparece no top 6.

» Longo prazo (10 anos): segue relevante, no top 8.

Associado ao aumento da frequência e sofisticação de ataques cibernéticos e exposição de infraestruturas críticas e serviços essenciais.

O relatório conecta a ciberinsegurança a tensões geopolíticas, interrupções em cadeias de valor e vulnerabilidades em sistemas interconectados.

2. Desinformação

» Curto prazo: Misinformation and disinformation é risco nº 2.

» Longo prazo: permanece no top 4, mostrando efeito estrutural e persistente.

Identificado como um dos principais riscos globais no curto prazo, pois amplifica polarização social, causa erosão na confiança em instituições públicas e privadas, destacando-se o papel de plataformas digitais, conteúdo sintético, bem como tecnologias emergentes, incluindo IA, na escala e velocidade da desinformação.

3. Riscos de IA

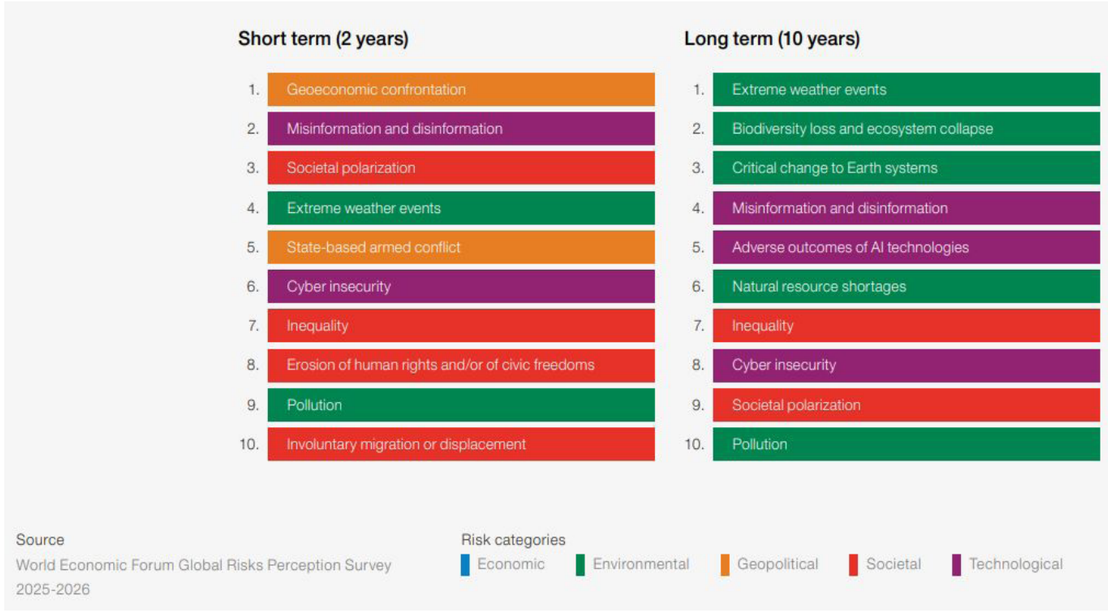
» Longo prazo: Adverse outcomes of AI technologies aparece explicitamente no top 5.

Efeitos adversos associados a: uso de sistemas de IA em larga escala; automação de decisões com baixa transparência; e reprodução de vieses existentes nos dados.

Impactos potenciais em: emprego e reorganização do mercado de trabalho;

desigualdade social; e segurança e competição geopolítica.

O documento também menciona que muitos desses efeitos são ainda insuficientemente compreendidos, sobretudo em termos sistêmicos.



IMPACTOS - A convergência regulatória eleva o padrão de cobrança sobre governança demonstrável: não basta ter políticas isoladas; será necessário comprovar, de forma integrada, como a organização identifica riscos, decide e opera controles em dados, IA e segurança. Isso implica alinhar responsabilidades claras e fluxos decisórios, manter trilhas de auditoria e documentação coerente (avaliações de impacto, registros de incidentes, critérios de transparência/explicabilidade e controles de terceiros). As organizações que não priorizarem a governança digital estruturada enfrentarão desafios crescentes em termos de conformidade, gerenciamento de riscos, reputação e competitividade.

2. Soberania Digital: dados, IA, ciber, data centers e dependência tecnológica

A soberania digital pode ser analisada a partir de diferentes perspectivas, incluindo a jurídica (capacidade de um Estado de criar, implementar e fazer cumprir leis e regulamentos), tecnológica (domínio de um país sobre sua infraestrutura digital e tecnologias emergentes), cibersegurança e econômica (proteger suas indústrias e promover inovação local).

Essa agenda se materializa, de forma concreta, em exigências relacionadas à localização e ao controle de dados, no desenvolvimento de estratégias de soberania e continuidade operacional e na consolidação do cloud exit plan como elemento central de governança corporativa. Trata-se de movimento que impacta diretamente a arquitetura de sistemas, estrutura contratual, gestão de riscos e o compliance regulatório, especialmente em ambientes marcados por tensões geopolíticas, dependência de fornecedores globais e intensificação do enforcement digital.

a. Localização de dados/data residency

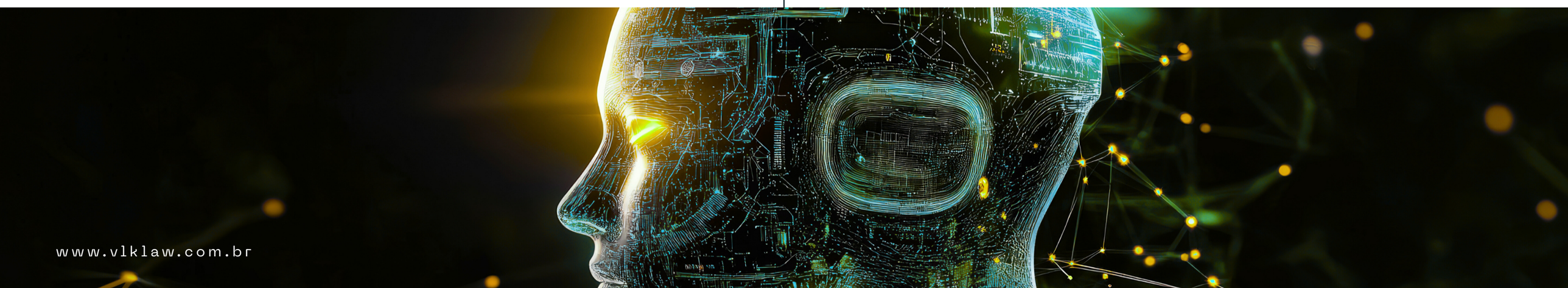
A localização de dados tende a assumir caráter progressivamente normativo, ainda que nem sempre por meio de obrigações expressas. A combinação entre regras de transferência internacional, políticas de cibersegurança e incentivos a data centers nacionais indica que o data residency será tratado como instrumento de soberania, mitigação de risco geopolítico e garantia de enforcement regulatório, impactando arquitetura de sistemas e estratégias contratuais globais. Esse movimento impacta afeta decisões de arquitetura de sistemas, escolha de provedores, estratégias de contratação global e desenho de fluxos de dados, exigindo das organizações maior racionalidade jurídica e técnica na definição de onde, como e sob qual jurisdição os dados são armazenados e processados.

b. Estratégias de soberania e continuidade operacional

As estratégias de soberania e continuidade operacional visam assegurar que organizações e nações sejam capazes de operar de forma segura, contínua e autônoma, reduzindo a dependência de infraestruturas externas e recuperando-se rapidamente de interrupções relevantes. Na perspectiva da soberania digital, há associação direta entre autonomia tecnológica e a capacidade de continuidade operacional em cenários de crise regulatória, cibernética ou geopolítica.
Espera-se maior exigência de planos estruturados de resiliência, integrando governança de dados, segurança cibernética, redundância de infraestrutura e autonomia decisória local. Do ponto de vista jurídico, essas estratégias passam a ser avaliadas como dever de diligência, influenciando responsabilidade civil, fiscalização regulatória e critérios de contratação pública e privada.

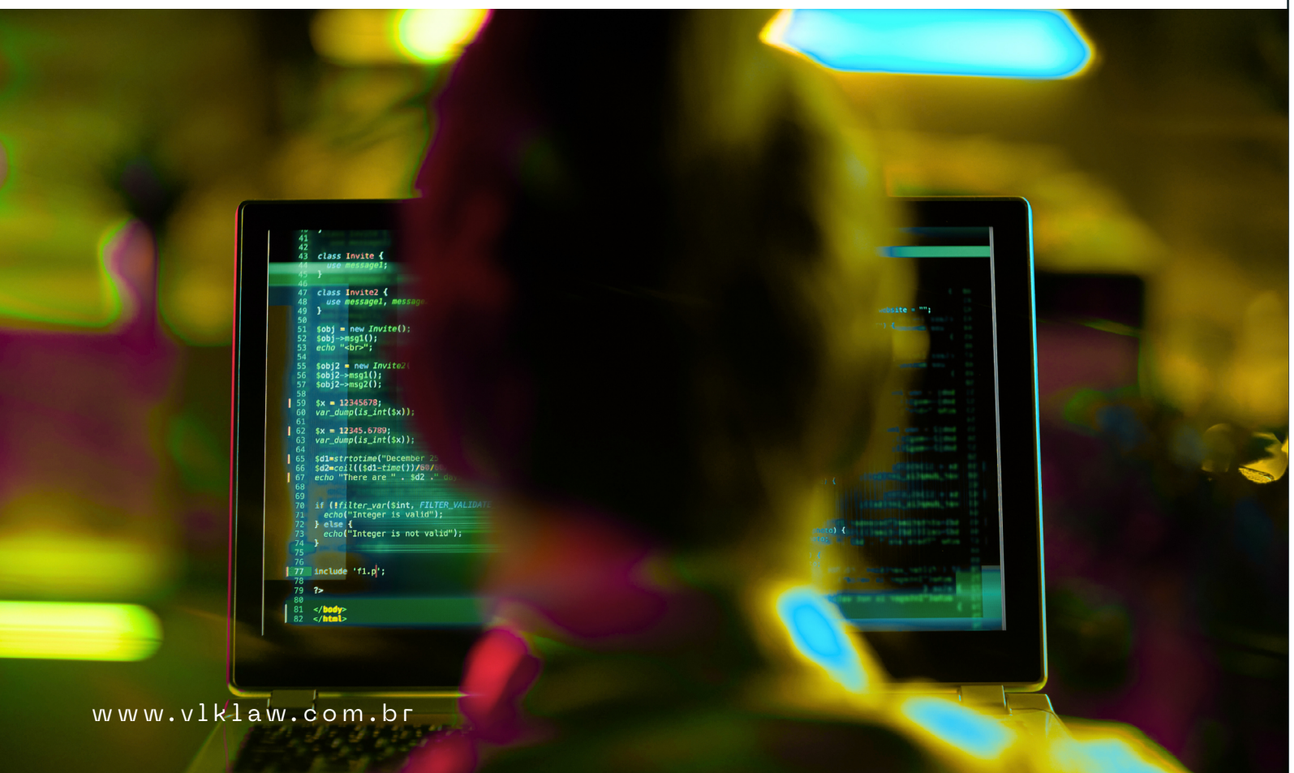
c. *Cloud exit plan* como requisito corporativo

Diversas regulamentações e boas práticas de governança exigem que as organizações demonstrem a capacidade de manter a continuidade dos negócios e proteger dados, independentemente do provedor de serviços de nuvem. A



prevenção de vendor lock-in, a capacidade de migração de dados e serviços e a manutenção da operação diante de falhas, sanções ou restrições contratuais passam a integrar expectativas de governança responsável e compliance tecnológico. Empresas que estruturarem planos documentados de saída, com cláusulas contratuais adequadas, interoperabilidade e testes periódicos, estarão melhor posicionadas para demonstrar accountability, resiliência e aderência às novas demandas de soberania digital.

IMPACTOS - A agenda da soberania digital transforma decisões técnicas sobre dados, nuvem e IA em temas centrais de risco jurídico, governança e estratégia empresarial. A crescente valorização de data residency, resiliência operacional e autonomia tecnológica impacta diretamente contratos com provedores globais, arquitetura de sistemas, planos de continuidade e governança corporativa. Empresas que não endereçarem dependência tecnológica, localização de dados e ausência de cloud exit plan tendem a enfrentar maior exposição regulatória, operacional e reputacional. Sob a perspectiva de políticas públicas, a soberania digital deve ser competitiva, sem cair em ufanismo digital que priorize isolamento ou protecionismo extremo. Essa abordagem pragmática permite que países e organizações alcancem autonomia tecnológica e segurança, mas sem comprometer os benefícios da colaboração global, da inovação e do comércio internacional



3. 3. Convergência Global em Cibersegurança:

Incidentes cibernéticos despontam como preocupação crítica de curto e longo prazo. A pauta vai além de fraudes e vazamentos de dados: ataques cibernéticos têm potencial para paralisar empresas, instituições e até países inteiros.

No cenário internacional, a movimentação regulatória para fazer frente aos riscos já começou há décadas. A partir da segunda década dos anos 2000, a União Europeia aprovou a diretiva NIS (Network and Information Systems Directive), obrigando os 27 países do bloco a criarem legislações e estruturas nacionais de cibersegurança. Países como China, Rússia, Japão e Coreia do Sul também desenvolveram leis e órgãos específicos. Mais recentemente, a UE aprovou a NIS2, elevando o nível de exigência.

No Brasil, os avanços têm sido tímidos. Apenas em 2023 o país promulgou sua adesão à Convenção de Budapeste. As exigências existentes são, em geral, setoriais e não harmonizadas. Leis como o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Propriedade Industrial e a LGPD, por exemplo, contêm dispositivos relacionados ao tema, assim como regulações específicas para setores como o financeiro, telecomunicações, seguros e saúde. No entanto, falta corpo normativo comum, além de outros setores sequer contarem com exigências mínimas em cibersegurança.

Em 2026, a convergência global em cibersegurança consolida-se como um dos vetores mais críticos na agenda regulatória e jurídica internacional e nacional. Este movimento é impulsionado pela elevação dos padrões internacionais de resiliência, responsabilização e gestão de riscos, com destaque para a influência extraterritorial de regulamentos europeus como a NIS2 e a DORA; o avanço robusto do marco legal brasileiro e o fortalecimento do papel de autoridades de fiscalização, como a ANPD e os reguladores setoriais; e a crescente sofisticação e

o volume das ameaças cibernéticas que atingem ecossistemas globais.

Essa conjunção de fatores sinaliza a transição definitiva para novo modelo: a cibersegurança, deixando de ser questão meramente técnica, assume o status de agenda estratégica e prioritária, tanto para o nível corporativo, quanto para a segurança e soberania nacional.

a. NIS2 + DORA puxando o padrão de mercado

As diretivas europeias NIS2 e DORA (Digital Operational Resilience Act) estão impulsionando a padronização global dos padrões de cibersegurança e resiliência operacional, estabelecendo referências rigorosas que transcendem as fronteiras da União Europeia.

A NIS2 amplia significativamente o escopo subjetivo e material da regulação. A norma expande a categoria de Essential and Important Entities (EIEs), incorporando novos setores críticos e impondo obrigações reforçadas de gestão de risco, segurança da informação e notificação de incidentes. Seu principal vetor extraterritorial exige que as entidades reguladas avaliem e mitiguem riscos cibernéticos associados à sua cadeia de suprimentos direta e indireta, incluindo fornecedores não europeus.

Na prática, empresas de terceiros países que fornecem serviços ou tecnologias essenciais a EIEs europeias devem comprovar conformidade com os padrões técnicos de segurança e resiliência da NIS2, sob pena de exclusão comercial ou impacto regulatório indireto sobre seus clientes na UE.

O DORA, por sua vez, adota abordagem focada em resiliência operacional digital, indo além da prevenção e abrangendo resposta, continuidade e recuperação de serviços críticos. O regulamento impõe às instituições financeiras europeias requisitos rigorosos de governança de risco de TICs, testes de resiliência, gestão de incidentes e controle de dependência de terceiros. Seu efeito extraterritorial se materializa especialmente no regime aplicável aos ICT Third-Party Providers, permitindo que as Autoridades Europeias de Supervisão designem fornecedores

não europeus como terceiros críticos. Uma vez designados, esses fornecedores passam a se submeter a framework de supervisão direta, incluindo exigências de estrutura jurídica na UE, auditorias, inspeções e revisões técnicas, com impacto direto sobre contratos globais de cloud, outsourcing e serviços digitais.

Em conjunto, NIS2 e DORA operam como mecanismos regulatórios de regulação do risco na origem, elevando o padrão técnico de due diligence, contratação e governança de terceiros. Para empresas brasileiras, a aderência a esses requisitos pode deixar de ser boa prática e passar a funcionar como condição técnica de acesso ao mercado europeu, configurando requisito regulatório baseado em interoperabilidade normativa e maturidade em governança de risco cibernético e digital.

b. Marco Legal e Órgão Central para Cibersegurança no Brasil

Neste ano, a tendência é que o Brasil avance na institucionalização de marco legal robusto de cibersegurança, acompanhado da definição formal de órgão central de coordenação e autoridade nacional nessa matéria. Discussões recentes no CNCiber indicaram a ANATEL como possível autoridade central de cibersegurança, refletindo a necessidade de estrutura capaz de articular respostas a incidentes, supervisionar setores críticos e coordenar políticas públicas.

c. O papel da ANPD e da LGPD na Cibersegurança

A LGPD, coordenada pela atuação da ANPD, tende a ser cada vez mais integrada às políticas de cibersegurança em 2026, reforçando a noção de que a proteção de dados e a segurança da informação são dimensões indissociáveis da governança digital. A ANPD deverá intensificar orientações técnicas, padrões mínimos de segurança e expectativas de compliance, especialmente em contextos de incidentes que envolvam dados pessoais, na linha de iniciativas internacionais que vinculam proteção de dados a requisitos operacionais de segurança cibernética. Inclusive, medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança), está como item prioritário da Agenda Regulatória da ANPD.

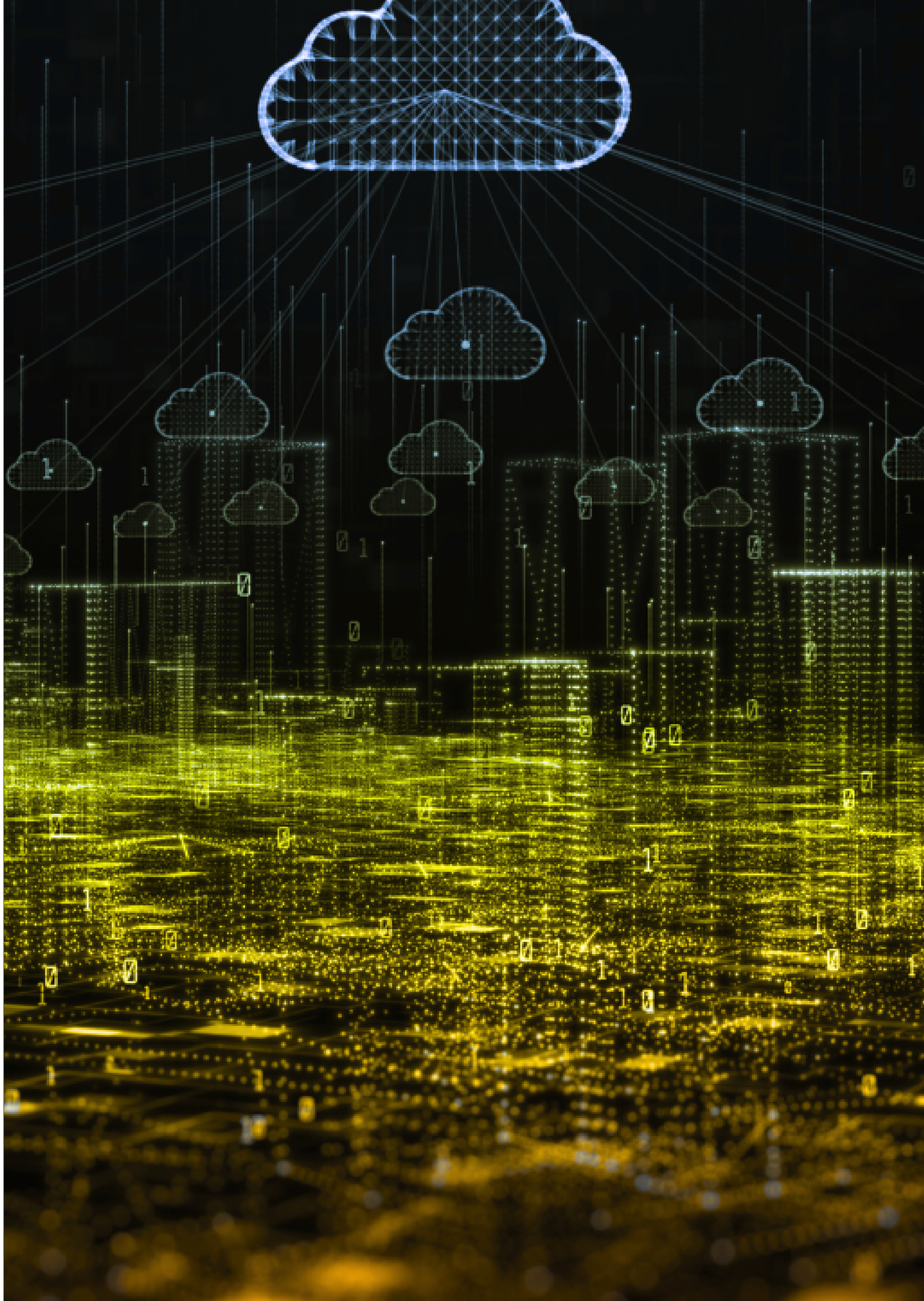
d. Cibersegurança setorial (financeiro, saúde, energia e telecom)

Além do marco regulatório geral, há tendência do fortalecimento de regimes setoriais de cibersegurança, com exigências específicas para setores de maior criticidade.

No setor financeiro tende a haver maior rigidez sobre resiliência operacional, continuidade de serviços e mitigação de fraudes. A agenda regulatória do Banco Central desenvolvida em 2025 sinalizou que resiliência cibernética e operacional serão pilares estratégicos de confiança institucional, com exigência de revisões de processos, investimentos em infraestrutura e maior transparência regulatória para integrar segurança e continuidade de serviços financeiros ao core do compliance corporativo.

A Resolução BCB Nº 538/2025 aumentou a fiscalização sobre sistemas críticos como o PIX e a Rede do Sistema Financeiro Nacional (RSFN), impondo a obrigatoriedade de testes de intrusão anuais e independentes como requisitos de resiliência cibernética.

A Resolução CMN nº 5.274/2025 elevou o padrão de governança ao detalhar o conteúdo mínimo obrigatório das políticas de segurança cibernética, exigindo mecanismos específicos de autenticação, criptografia, prevenção de vazamento de informações e gestão de cópias de segurança, atualizando em parte a Res. 4.893/21. Paralelamente, a responsabilidade e o controle sobre terceiros foram



reforçados pela Resolução BCB Nº 498/2025, que incluiu a contratação de seguros cibernéticos como requisito de credenciamento para os Provedores de Serviços de Tecnologia da Informação (PSTIs) que atuam no Sistema Financeiro Nacional.

No setor de saúde persistem exigências relacionadas a proteção de dados sensíveis e à segurança das redes clínicas. A adesão do Brasil à Health AI, com participação da Agência Nacional de Saúde Suplementar (ANS), indica alinhamento a padrões internacionais de uso responsável de IA na saúde e reforça o papel dos reguladores setoriais. Com a expectativa de norma do Conselho Federal de Medicina (CFM) e o avanço do PL nº 6.237/2025, o setor se prepara para exigências mais claras de governança de IA clínica já em 2026, envolvendo explicabilidade, gestão de riscos e segurança da informação para prestadores, operadoras e empresas de tecnologia em saúde. O Decreto nº 12.560/2025, estabeleceu as regras de Governança e Proteção da Rede Nacional de Dados em Saúde, tornando obrigatório o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) prévio para o compartilhamento de dados e a necessidade de parâmetros mínimos de segurança da informação para o tratamento de dados. Complementarmente, a Portaria GM/MS Nº 7.678/2025 instituiu a Estratégia de uso de Cloud Computing no Ministério da Saúde, estabelecendo regras claras de segurança e privacidade para o uso da nuvem, garantindo a proteção e o sigilo dos dados pessoais em ambientes digitais e alinhando-se aos

requisitos de cibersegurança mais amplos.

Para o setor de telecomunicações, o rigor foi intensificado pela entrada em vigor da Resolução nº 767/2024, que fortaleceu o poder de fiscalização ao consolidar e detalhar os deveres e obrigações das prestadoras de serviços, em reforço à Resolução nº 740/2020. Além disso, a definição de infraestrutura crítica foi expandida pela Resolução Anatel Nº 780/2025, que passou a reconhecer formalmente os data centers como parte essencial da infraestrutura de telecomunicações. Assim, espera-se maior consolidação das exigências de cibersegurança, impulsionada pela própria agenda regulatória da Anatel para o biênio 2025/2026.

Essa evolução setorial reforça que a cibersegurança deixa de ser um requisito técnico isolado e se integra a obrigatoriedades jurídicas vinculadas à continuidade de operações essenciais, à proteção de direitos fundamentais e promoção de novos negócios.

IMPACTOS - A elevação do padrão regulatório nacional e internacional, combinada ao fortalecimento da LGPD, da atuação da ANPD e dos regimes setoriais no Brasil, exige das empresas uma governança contínua e estruturada de riscos cibernéticos. Isso envolve a revisão integrada de políticas internas, contratos, arquitetura tecnológica e cadeias de fornecedores, bem como a capacidade efetiva de detecção, resposta e reporte de incidentes. Organizações que não internalizarem esses requisitos tendem a enfrentar maior exposição regulatória, fragilidade operacional e riscos reputacionais, enquanto aquelas que anteciparem esse alinhamento estarão melhor posicionadas para sustentar operações digitais resilientes em um ambiente regulatório cada vez mais exigente.

4. ECA Digital em vigor: regulamentação e fiscalização

A aprovação do Estatuto Digital da Criança e do Adolescente representa marco relevante para fortalecer a proteção de crianças e adolescentes no ambiente digital. O ponto crítico é a redução da vacatio legis para 6 meses, que cria cenário de implementação complexo, porque exige mudanças simultâneas em múltiplas camadas - regulatórias, institucionais, operacionais e tecnológicas.

A própria lei já deixa evidente essa complexidade ao prever obrigações que envolvem, por exemplo, sistemas de aferição etária e controle de acesso a conteúdo e serviços, mecanismos de supervisão parental, adoção de medidas de governança e design voltadas à proteção integral, procedimentos céleres para remoção de conteúdos de exploração ou outras violações graves, além da realização de avaliações de risco e relatórios de impacto. Tudo isso depende de regulamentação, critérios técnicos, processos claros e capacidade de fiscalização.

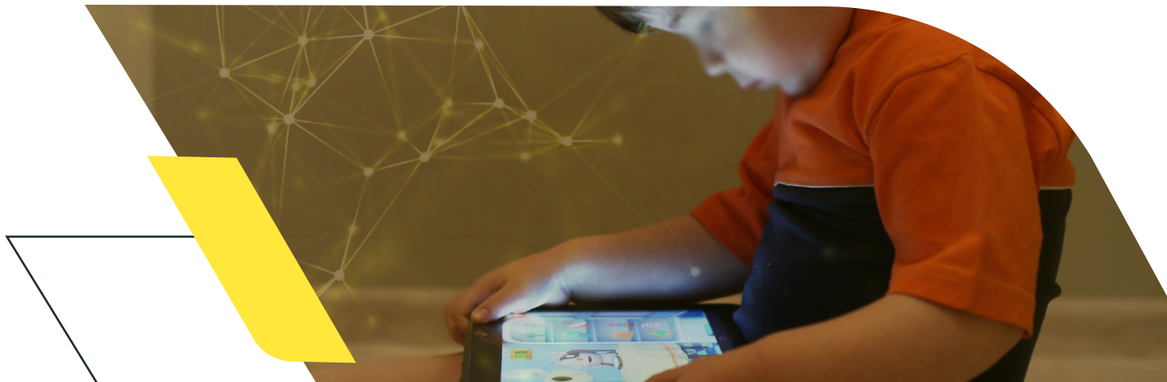
Com entrada em vigor prevista para março de 2026, o cenário pós-vigência do ECA Digital tende a intensificar a necessidade de avaliações de risco, auditorias regulatórias e litigância estratégica, tornando a governança digital voltada ao público infantojuvenil um dos eixos centrais para compliance e enforcement no direito digital brasileiro.

A regulamentação infralegal (especialmente no que se refere a mecanismos de aferição etária, controle parental, design adequado à idade e mitigação de riscos) deve ganhar densidade, ao mesmo tempo em que a ANPD e o Ministério da Justiça e Segurança Pública (MJSP) passam a exercer atuação mais coordenada, sendo esperado para: i) fevereiro a publicação de Decreto do Poder Executivo; ii) até abril a realização de consulta pública pela ANPD acerca de Guia sobre o ECA Digital (que terá os objetivos de esclarecer conceitos gerais e orientar a aplicação prática, com foco em pontos como: a quem se aplica; “acesso provável”; interpretação de “a cada acesso”; responsabilidade dos agentes, entre outros temas); e iii) até agosto a realização de consulta pública para regulamentação dos temas de aferição de idade e controle parental.

A ANPD prevê realizar atividades de monitoramento no primeiro semestre de 2026, que já se iniciaram em relação a 37 empresas; 15 atividades de fiscalização sobre configuração por design e por padrão de modelo mais protetivo disponível, no primeiro semestre de 2027; e 15 atividades de fiscalização para verificar a adoção para impedir que crianças e adolescentes acessem conteúdos impróprios, incluindo mecanismos de aferição de idade, no primeiro semestre de 2027.

O desafio central para 2026 será equilibrar proteção infantojuvenil, proporcionalidade regulatória e viabilidade técnica, em um contexto de pressão por soluções rápidas e escaláveis para verificação de idade. Além de vetor de enforcement, o ECA Digital também é oportunidade de negócios e inovação regulada, estimulando o desenvolvimento de soluções tecnológicas para verificação etária, design seguro, governança de conteúdo e serviços digitais.

IMPACTOS - Para empresas, o cenário exige governança contínua e revisões concretas de produtos, arquitetura tecnológica, contratos e fluxos de dados, sob pena de sanções administrativas, restrições operacionais e impactos reputacionais, consolidando o ECA Digital como um dos eixos centrais do compliance digital em 2026. Ao mesmo tempo, o novo regime abre espaço para diferenciação competitiva e inovação aplicada, por meio do desenvolvimento de soluções de design adequado à idade, verificação etária, controle parental e serviços digitais orientados à segurança e à confiança, com potencial de atrair investimentos e viabilizar a expansão de modelos de negócio alinhados aos novos padrões regulatórios, como mecanismos de aferição de idade e controle parental.



5. Decisão de Adequação Brasil–UE: Transferência Internacional de Dados

Em 2026, a decisão de adequação entre Brasil e União Europeia tende a representar um dos marcos mais relevantes para a transferência internacional de dados. A publicação, em setembro de 2025, de versão preliminar da decisão de adequação pela Comissão Europeia, reconhecendo o nível de proteção de dados brasileiro como substancialmente equivalente ao do GDPR, sinalizou a possibilidade concreta de eliminação da necessidade de salvaguardas adicionais, como SCCs e avaliações complementares de risco, para fluxos de dados entre as duas regiões. Paralelamente, a atuação da ANPD na construção de regime de reciprocidade reforça a convergência regulatória e amplia a previsibilidade jurídica para empresas que operam em cadeias globais de dados.

A expectativa para 2026 é de concretização do reconhecimento mútuo, com efeitos diretos sobre custos de compliance, estruturação contratual e competitividade internacional das empresas brasileiras e europeias. A adequação Brasil-UE tende a funcionar como selo regulatório internacional, facilitando não apenas os fluxos bilaterais de dados, mas também novas decisões de adequação entre o Brasil e outros países, especialmente aqueles já reconhecidos pela UE. Esse movimento consolida um ecossistema de proteção de dados mais harmonizado, fortalece a posição institucional da ANPD e reposiciona o Brasil como hub regulatório confiável para a economia digital, com impactos positivos sobre investimentos, inovação e integração global em 2026 e nos anos seguintes.

IMPACTOS – A adequação Brasil-UE tende a funcionar como "selo" regulatório internacional, reposicionando o Brasil como jurisdição confiável na economia digital, ampliando a atratividade para investimentos, parcerias tecnológicas e expansão internacional a partir de 2026. Para as empresas, o desafio passa a ser capturar os benefícios da adequação por meio da revisão de contratos, políticas internas e governança de dados, mantendo aderência à LGPD e às expectativas europeias.

6. Agenda concorrencial digital: CADE e plataformas

A agenda concorrencial digital tende a ganhar centralidade na atuação do CADE neste ano, com foco crescente sobre plataformas digitais, mercados de dados e ecossistemas baseados em IA. A experiência acumulada em investigações recentes e a interação cada vez mais intensa com reguladores setoriais indicam atuação mais proativa e estrutural, voltada a práticas como auto preferência (favoritismo a serviços próprios), fechamento de mercado e aprisionamento tecnológico (lock-in), exploração de dados como vantagem competitiva e integração vertical em ambientes digitais.

O acesso e o uso de dados são os novos diferenciais competitivos e o CADE está se preparando para fiscalizar a fronteira da IA e a adoção de regras específicas de caráter preventivo (ex-ante) para plataformas digitais consideradas sistemicamente relevantes (gatekeepers), de forma similar ao Digital Markets Act (DMA) da União Europeia, como:

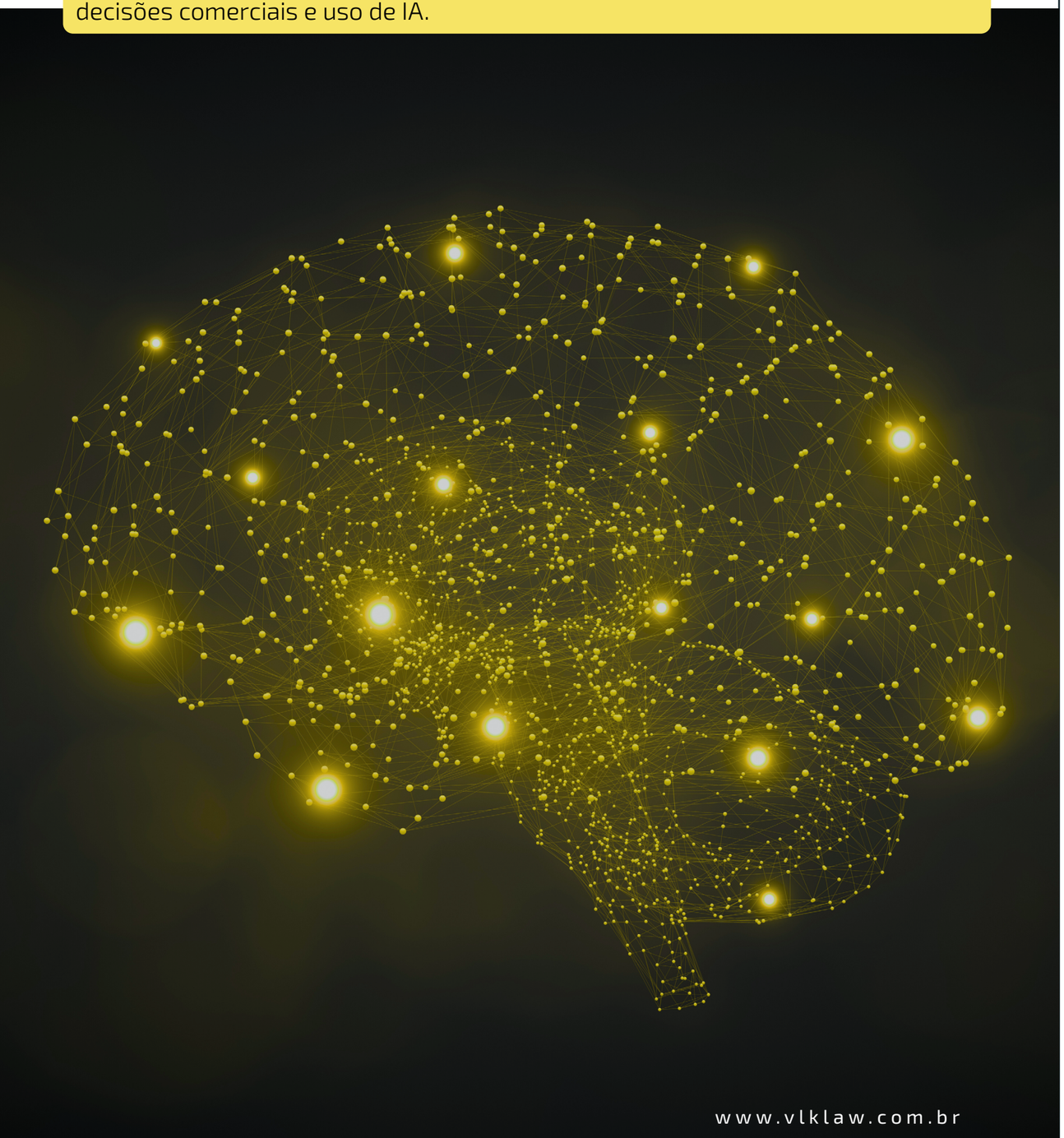
» **Exploração de Dados como Vantagem:** análise de como o acúmulo massivo de dados cria barreiras de entrada intransponíveis (data-moat);

» **Algoritmos de Precificação:** vigilância sobre o uso de Inteligência Artificial para coordenar preços, sob a perspectiva de colusão (acordos anticompetitivos), mesmo que de forma não intencional ou implícita; e

» **Ecossistemas Baseados em IA:** como os modelos de IA Generativa impactam a concorrência e como garantir a liberdade de escolha e autonomia do consumidor nesse novo ambiente.

Assim, 2026 tende a consolidar cenário concorrencial mais sofisticado e coordenado, especialmente na interseção entre concorrência, proteção de dados, IA e regulação digital. Espera-se maior escrutínio sobre modelos de negócio baseados em dados, publicidade digital, IA generativa e condições de acesso a infraestruturas essenciais, bem como o uso de remédios comportamentais e estruturais em operações envolvendo plataformas.

IMPACTOS - Em ambiente de enforcement mais coordenado com reguladores digitais, a capacidade de antecipar impactos concorrenciais, documentar decisões econômicas e ajustar modelos de negócio de forma preventiva será determinante para evitar remédios restritivos e danos reputacionais. Para mitigar esses riscos sem comprometer a inovação, as organizações devem estruturar programas de governança de dados, incorporar análises concorrenciais ex ante no desenho de produtos, algoritmos e estratégias de monetização de dados, revisar práticas de acesso a dados, publicidade e parcerias, e fortalecer a governança interna sobre decisões comerciais e uso de IA.



7. Definição dos PLs 2.338/23 e 6.237/25, SIA e Execução do Plano Brasileiro de IA e IA Agêntica

A definição do marco regulatório brasileiro de IA, por meio da votação e eventual aprovação do PL nº 2.338/23, em conjunto com o PL 6.237/25, representam tendência significativa para o direito digital, pois consolidam a transição de ambiente predominantemente principiológico para regime jurídico mais denso de IA, orientado à regulação baseada em risco, à responsabilização diferenciada e à imposição de deveres formais de governança sobre aplicações de IA.

» **PL 2.338/2023:** normas gerais: de iniciativa do poder Legislativo Federal, dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da IA. Aprovado no Senado em 10.12.2024, tramita na Câmara dos Deputados e deve ser votado no início de 2026, após apresentação do Relatório da Comissão Especial, presidida pela Deputada Luisa Canziani e de Relatoria do Deputado Aguinaldo Ribeiro;

» **PL 6.237/2025:** arquitetura institucional e Atuação do Executivo: de iniciativa do poder Executivo Federal, institui o SIA (Sistema Nacional para Desenvolvimento, Regulação e Governança de Inteligência Artificial).

A aprovação desses Projetos tende a ativar a execução coordenada do Plano Brasileiro de Inteligência Artificial, aproximando regulação, fomento e políticas públicas. A consolidação de um ecossistema nacional de Inteligência Artificial exige a convergência entre o futuro Marco Legal de IA e o atual PBIA. A desconexão entre ambos comprometerá a efetividade de políticas públicas e fragmentará a segurança jurídica em diversos setores. Por isso, é fundamental a análise do impacto regulatório do Marco de IA, de forma a convergir com os anseios do PBIA.

Para mitigar os impactos dessa tendência, é recomendado que as empresas se antecipem e fiquem atentas às exigências legais, criando governança robusta

para sistemas de IA, alinhada com guias e melhores práticas internacionais. As organizações devem ponderar o melhor framework para governança de IA e consolidá-los mediante medidas, como:

» **Prioridade Estratégica:** alinhar IA aos objetivos corporativos, valores éticos e frameworks regulatórios;

» **Literacia em IA:** capacitar e aprimorar a cultura organizacional, do conselho, executivos, e colaboradores em aspectos éticos, regulatórios e estratégicos da IA;

» **Mapeamento:** mapear aplicações de IA desenvolvidas, implementadas ou utilizadas;

» **Cadeia de Valor:** identificar os papéis desempenhados como "agentes de IA" em cada aplicação e enquadrar a organização para cada aplicação como desenvolvedor ou aplicador, por exemplo;

» **Grau de Risco:** classificar o grau de risco das aplicações de IA conforme o seu uso e finalidades;

» **Gestão de IAs de terceiros:** avaliar riscos no uso de sistemas de IA de terceiros, especialmente os de propósito geral;

» **Governança:** definir medidas de governança adequadas, com base nos riscos, nas finalidades e papéis desempenhados;

» **Estruturar programa de governança** com comitês de ética, políticas e cláusulas contratuais claras;

» **Realizar Avaliações de Impacto Algorítmico** para aplicações de IA de alto risco; e

» **Monitorar continuamente o programa**, estabelecendo métricas e responsáveis.

Por fim, a IA Agêntica está emergindo como o próximo grande avanço. São sistemas que não apenas geram conteúdo, mas podem planejar, decidir e agir em ambientes digitais em nome dos usuários. Na prática, a tecnologia viabiliza agentes que pesquisam informações, planejam atividades, executam transações, interagem com sistemas internos e externos e tomam decisões com mínima intervenção humana, como agentes que organizam agendas, automatizam processos internos, realizam compras, apoiam decisões de negócio, detectam ameaças de cibersegurança ou executam tarefas administrativas.

Agentes com finalidades claramente definidas, acesso limitado apenas aos dados e sistemas necessários, com monitoramento contínuo, registros das ações e possibilidade de intervenção humana são recomendações de governança preciosas. Exemplos positivos incluem agentes que automatizam tarefas administrativas com escopo controlado; de cibersegurança que identificam vulnerabilidades e alertam humanos; ou agentes internos que apoiam decisões sem executá-las de forma irreversível. Também são considerados desejáveis sistemas desenhados com privacy by design, controles de acesso granulares e mecanismos claros para explicar decisões e permitir contestação .Por outro lado, exemplos problemáticos incluem agentes com finalidades excessivamente genéricas, acesso irrestrito a múltiplas bases de dados, tomada de decisões

automatizadas com efeitos legais ou significativos sem supervisão humana, ou agentes que inferem dados sensíveis de forma não intencional. Ainda, propagação de informações incorretas (“alucinações em cascata”), perda de transparência em ambientes multiagentes, falhas de segurança e dificuldade de atribuir responsabilidades.

Ou seja, mesmo com autonomia, a responsabilidade legal e regulatória permanece integralmente com a organização que desenvolve ou utiliza esses agentes.

IMPACTOS – A interação entre o novo regime jurídico de IA, as diretrizes do PBIA e a orquestração da fiscalização do SIA tende a acelerar a imposição de exigências concretas de governança, documentação técnica, transparência e gestão de riscos. Esses requisitos impactam diretamente contratos, cadeias de fornecimento tecnológico, desenvolvimento e aquisição de sistemas, bem como modelos de negócio baseados em IA e agentes de IA. Organizações que não se prepararem para esse novo ambiente tendem a enfrentar custos de adaptação tardia, insegurança jurídica, restrições operacionais e maior exposição a fiscalizações e sanções. Já aquelas que anteciparem o mapeamento de sistemas e a classificação de riscos, integrarem requisitos regulatórios às decisões de negócios e estruturarem modelos de governança alinhados à estratégia corporativa estarão melhor posicionadas para enfrentar o ciclo inicial de fiscalização e, ao mesmo tempo, capturar oportunidades em um mercado de IA progressivamente regulado, institucionalizado e orientado à confiança.

8. 8. Agenda regulatória e fiscalizatória da ANPD

A consolidação da ANPD como regulador central do ecossistema digital deverá se refletir em atuação mais coordenada entre normatização, guias orientativos e fiscalização, com especial ênfase na implementação do ECA Digital e IA.
A atualização da Agenda Regulatória 2025–2026, com metas quantitativas de ações de fiscalização e a elaboração antecipada do Mapa de Temas Prioritários de Fiscalização 2026–2027 indicam que o próximo ciclo será marcado por modelo de regulação progressiva seguido de enforcement seletivo, técnico e estruturado:

Nova Agenda Regulatória do biênio 2025–2026 (fase 1):

1. **Direitos dos titulares:** regulamentação, contemplando em especial os artigos 9º, 18, 19 e 20 da LGPD;

2. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD): editar regulamento e procedimentos sobre RIPDs** para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais;

3. **Compartilhamento de dados pelo Poder Público:** estabelecer os requisitos a serem observados nas hipóteses de compartilhamento de dados pessoais pelo Poder Público. Além disso, é necessária a regulamentação dos arts. 26 e 27 da LGPD, que tratam do compartilhamento de dados do Poder Público com pessoa de direito privado;

4. **Dados pessoais sensíveis/dados biométricos:** o tratamento de dados biométricos 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, controle de fronteiras, estádios de futebol e transações financeiras. A ANPD entendeu necessária a sua intervenção, seja mediante regulamentação ou documentos de caráter orientativo, com vistas ao estabelecimento de parâmetros que assegurem a realização do tratamento de dados biométricos de forma equilibrada e compatível com a legislação;

5. **Medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança):** nos termos do art. 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. O § 1º do referido artigo estabelece que a ANPD poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no citado dispositivo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos na lei;

6. **Inteligência Artificial:** especialmente, o estabelecimento de parâmetros interpretativos para a aplicação do art. 20 da LGPD, que dispõe sobre o direito de revisão de decisões automatizadas. Além disso, tendo em vista a aplicação da LGPD nos contextos de treinamento e uso de sistemas de IA, também serão considerados no projeto os seguintes aspectos: i) direitos dos titulares; ii) princípios da LGPD; iii) hipóteses legais; e iv) boas práticas e governança;

7. **Tratamento de dados pessoais de alto risco:** o objetivo principal é disponibilizar aos agentes de tratamento, em especial os de pequeno porte, orientações e parâmetros para a definição e a identificação de hipóteses de tratamento de dados pessoais de alto risco;

8. **Organizações religiosas:** estabelecer orientações para as organizações religiosas quanto às medidas necessárias para a sua adequação à LGPD, considerando as suas especificidades; e

9. **Anonimização e pseudonimização:** em atendimento ao art. 12, §3º, da LGPD, a ação regulatória tem por objetivo dispor sobre padrões e técnicas utilizados em processos de anonimização e de pseudonimização, de forma a apresentar orientações e esclarecimentos sobre o tema.

ECA Digital:

1. **Mecanismos de aferição de idade – fase 2:** a ação busca propor solução regulatória com base em requisitos para o uso de mecanismos de aferição de idade, considerando modelos de negócio, riscos às crianças e adolescentes e salvaguardas para o tratamento de dados pessoais. Para isso, devem ser consideradas as premissas teóricas e de proporcionalidade regulatória diante dos métodos relacionados à verificação, estimativa, inferência e outras soluções técnicas disponíveis. A ação levará em consideração o ato do Poder Executivo a ser expedido nos termos do art. 12, § 3º, do ECA Digital.

2. **Fornecedores de produtos ou serviços de tecnologia da informação:** escopo e obrigações gerais do ECA Digital – fase 2: elaboração de guia orientativo com o objetivo de esclarecer o alcance dos principais conceitos relacionados ao escopo de aplicação do ECA Digital. e

3. **Fiscalização e sanção do ECA Digital, com revisão das Resoluções nº 1/2021 e nº 4/2023 – fase 2:** parâmetros específicos que devem ser considerados na aplicação das sanções de advertência e multa, conforme o ECA Digital, além de abarcar esclarecimentos sobre, por exemplo, a participação de amicus curiae e terceiros interessados, fases e prazos processuais, prazos para decisão em recursos administrativos, prescrição administrativa, termos de ajustamento de conduta, entre outros temas.

4. A Resolução CD/ANPD nº 30/2025 (**aqui**) aprovou o Mapa de Temas Prioritários para a atividade de fiscalização da ANPD no biênio 2026-2027, priorizando:

1. Direitos dos titulares de dados pessoais

Direitos dos titulares de dados pessoais, especialmente quanto ao tratamento de dados biométricos (a ANPD ressaltou medidas técnicas de segurança e hipótese legal fundamentadora), de saúde, financeiros e para fins publicitários. A Agência indica também que deve realizar:

Tipo de atividade	Quantidade
Atividades de fiscalização relacionadas a direitos dos titulares em temas diversos	25
Atividades de fiscalização relacionadas a tratamentos de dados biométricos, de saúde ou financeiro	10
Atividades de fiscalização relacionadas ao uso secundário de dados pessoais para entrega de publicidade comercial direcionada, especialmente mediante técnicas de perfilamento	5

2. Proteção de crianças e adolescentes no ambiente digital para verificar:

i) os planos de adequação de controladores às exigências do ECA Digital;

ii) as atividades de fiscalização voltadas a verificar a legalidade do tratamento de dados pessoais desses titulares; e,

iii) ainda, de proposição de salvaguardas a controladores, no âmbito das atividades de fiscalização, para a proteção de crianças e adolescentes no ambiente digital (como, por exemplo, mecanismos de garantia de idade).

Para tanto, a ANPD deve realizar:

1. Atividades de monitoramento sobre a adequação às exigências legais do ECA Digital, de fornecedores de produtos ou serviços;

2. 15 atividades de fiscalização a fim de verificar, em fornecedores de produtos ou serviços, a configuração, por design e por padrão, de modelo mais

protetivo disponível em relação à privacidade e à proteção de dados pessoais, considerando, inclusive, ferramentas de supervisão parental; e

3. 15 atividades de fiscalização a fim de verificar, em fornecedores de produtos ou serviços, a adoção de medidas para impedir que crianças e adolescentes acessem conteúdos impróprios, inadequados ou proibidos por lei, incluindo mecanismos de aferição de idade.

3. Tratamento de dados pessoais pelo Poder Público

Tratamento de dados pessoais pelo Poder Público, preferencialmente voltados a casos de compartilhamento de dados pessoais; de salvaguardas técnicas na gestão e governança dos dados pessoais, especialmente em face do número de incidentes de segurança que afetam órgãos públicos; e de uso de dados biométricos.

Como ação subsidiária, a edição de orientações, em casos de fiscalização, voltadas ao tratamento de dados pessoais para fins de segurança pública, nos termos do que prevê o art. 4º, §3º, da LGPD.

Além disso, cada ente deve realizar:

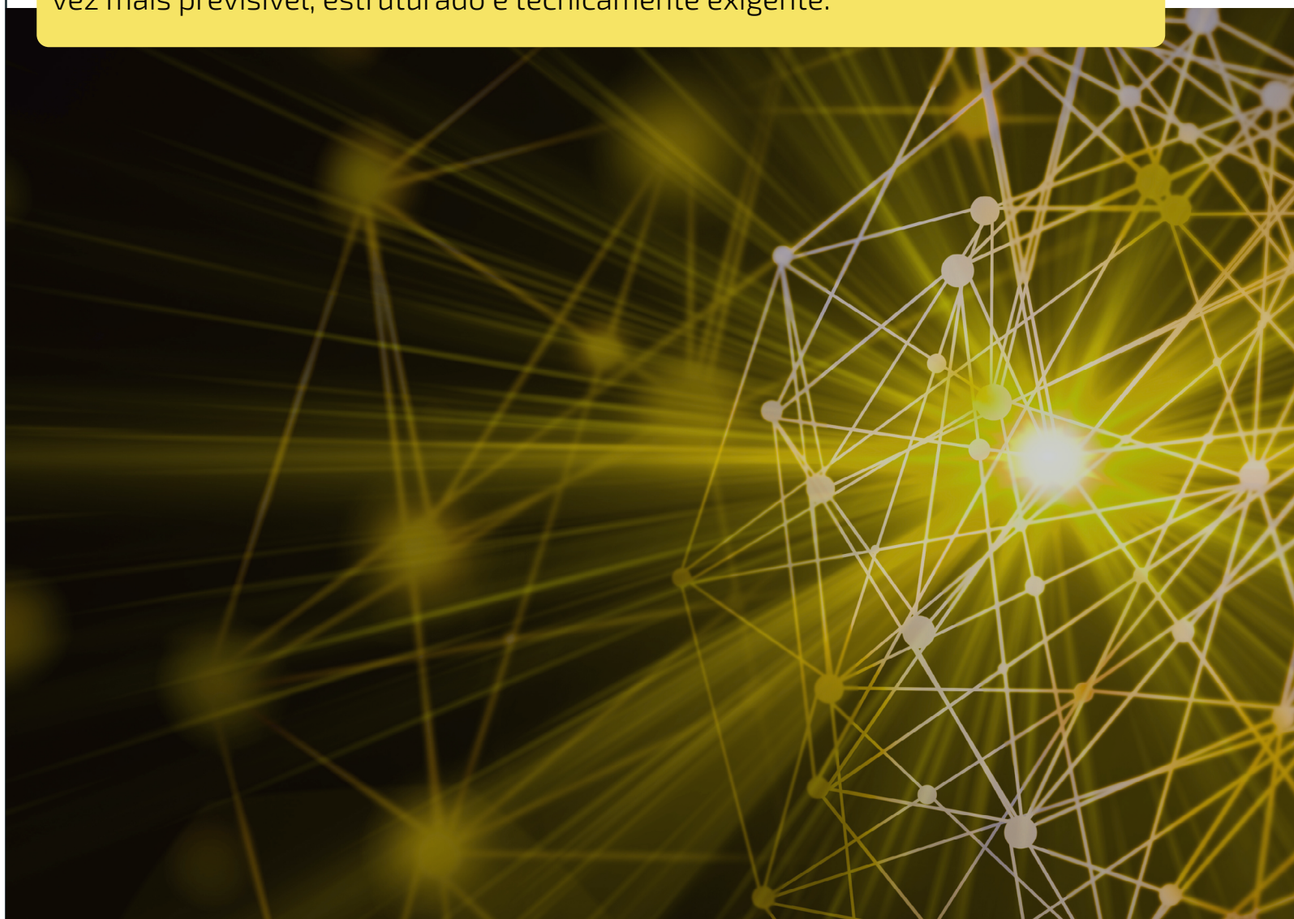
Fiscalização	Monitoramento
20 atividades de fiscalização que contemplem tratamento de dados pessoais pelo Poder Público;	Atividades de monitoramento sobre a adequação ao Regulamento de Uso Compartilhado de Dados Pessoais pelo Poder Público.

4. Inteligência artificial e tecnologias emergentes

Inteligência artificial e tecnologias emergentes no contexto do tratamento de dados pessoais. A ANPD deve realizar:

20 atividades de fiscalização relacionadas ao tratamento de dados pessoais, inclusive de crianças e adolescentes, no contexto de sistemas de inteligência artificial e tecnologias emergentes.

IMPACTOS – Empresas que não consigam demonstrar, de forma estruturada, consistente e documentada, como coletam, utilizam, compartilham e protegem dados (em especial de crianças e adolescentes, dados biométricos e tratamentos baseados em IA) estarão mais expostas a fiscalizações, sanções administrativas e repercussões públicas negativas. Em contrapartida, organizações que internalizarem governança integrada de dados e de IA, apoiada em avaliações de impacto robustas, controles técnicos efetivos e prontidão documental, estarão melhor posicionadas para interagir proativamente com a ANPD, reduzir assimetrias informacionais e mitigar riscos em um ambiente de supervisão cada vez mais previsível, estruturado e tecnicamente exigente.



9. Legal Marketing e Comunicação

a) Marketing de Emboscada - Copa do Mundo: a Copa do Mundo de 2026 intensifica os riscos jurídicos para o legal marketing, exigindo atenção redobrada às estratégias publicitárias associadas ao universo esportivo. À luz da Lei Geral do Esporte (Lei nº 14.597/2023), tais estratégias devem ser cuidadosamente avaliadas para evitar o enquadramento em práticas de marketing de emboscada, especialmente quando as ações publicitárias sugerem associação ao evento sem deter o patrocínio oficial.

IMPACTOS - Ainda que o anunciante não faça uso de logotipos ou ativos oficialmente protegidos, o emprego de identidades visuais, cores, expressões, narrativas ou ambientações que remetam direta ou indiretamente ao evento pode caracterizar a conduta ilícita. Nesse contexto, recomenda-se atenção às ações publicitárias, para que: i) sejam previamente avaliadas e aprovadas; ii) não sejam veiculadas em contextos físicos ou digitais que possam induzir à percepção de vínculo com o evento; iii) respeitem os perímetros oficiais do evento, incluindo arenas, zonas de exclusividade e fan zones; e iv) envolvendo o patrocínio de atletas ou seleções, construam narrativas que evitem a associação ilícita da marca ao evento.

b) Influenciadores Mirins: em 2026, a entrada em vigor do ECA Digital reposiciona o debate sobre influenciadores mirins ao ampliar o foco regulatório para além da mensagem veiculada pelo influenciador e à necessidade de obtenção das devidas autorizações para que possa promover a comunicação – como alvarás judiciais, passando a alcançar os mecanismos de distribuição da publicidade. Isso porque, será vedado o perfilamento e a publicidade direcionada ao público infantil, o que poderá impactar diretamente a estratégia de contratação desses influenciadores.

IMPACTOS - Ainda que os conteúdos de influenciadores mirins sigam as diretrizes previstas pelo CONAR, estes deixarão de ser admissíveis se impulsionados por ferramentas algorítmicas que utilizem dados de navegação, interesses ou comportamento de menores de idade para entrega de publicidade direcionada, exigindo das empresas uma estratégia de blindagem algorítmica e controle rigoroso dos meios de impulsionamento, impactando diretamente a lógica de uso de influenciadores mirins e trazendo à discussão a necessidade de revisão dos contratos que viabilizarão essas parcerias, com a incorporação de cláusulas que delimitem responsabilidades claras em relação à distribuição do conteúdo.

c) Participação ativa das plataformas digitais na autorregulamentação publicitária - CONAR: com a associação de big techs ao CONAR, como Meta, Google e TikTok, espera-se que 2026 seja marcado por governança publicitária mais integrada, que consolide a compreensão de que a conformidade publicitária não se restringe mais a anunciantes, agências e influenciadores, mas passa a abranger também os agentes tecnológicos responsáveis pela distribuição e amplificação das mensagens publicitárias, reconhecendo a relevância do marketing digital no contexto publicitário.

IMPACTOS - A participação ativa dessas plataformas no CONAR tende a qualificar o diálogo da autorregulamentação publicitária, na medida em que permite a incorporação de insights técnicos e operacionais sobre dinâmicas específicas no cenário digital. Com isso, o mercado publicitário passa a dispor de oportunidades para antecipar riscos, identificar potenciais irregularidades e ajustar práticas publicitárias com maior agilidade, assegurando que a evolução das estratégias de comunicação acompanhe a velocidade das inovações tecnológicas e fortaleça a proteção do consumidor de forma mais ampla e eficaz.

d) Política Nacional de Linguagem Simples (Lei 15.263/2025 - PNLS) e outras regulações exigindo comunicação mais acessível: a promulgação de leis como a PNLS marca uma mudança estrutural na forma como o direito se comunica com o cidadão, ao transformar clareza, objetividade e acessibilidade em requisitos centrais de conformidade regulatória. Tais requisitos influenciam não apenas a atuação do setor público, mas passarão a impactar diretamente na expectativa da sociedade como um todo por conteúdos jurídicos claros e compreensíveis, inclusive na esfera privada. Na prática, isso significa que as empresas serão cada vez mais pressionadas para estruturar de forma acessível e inteligível seus contratos, termos de uso, políticas de privacidade e comunicações institucionais, sob pena de questionamentos, sanções administrativas e desgaste reputacional.

IMPACTOS - O mercado intensificará demandas de revisão estratégica da comunicação jurídica, abrindo espaço para a adoção de metodologias como Legal Design e Visual Law. Ao traduzir comunicações complexas em formatos claros, intuitivos e acessíveis, essas ferramentas deixam de ser um diferencial estético e se consolidam como instrumentos de mitigação de riscos, eficiência operacional e fortalecimento da confiança, posicionando o jurídico como um verdadeiro viabilizador de negócios às empresas.

10. Direito Eleitoral – Uso de IA e Dados Pessoais

Ano de eleições gerais no Brasil, o direito eleitoral digital será testado de forma concreta, especialmente no que se refere ao uso de IA (em particular IA generativa) e de dados pessoais na propaganda eleitoral, além da moderação de conteúdo.

A Resolução do Tribunal Superior Eleitora (TSE) nº 23.732/2024 tende a ser novamente o eixo normativo desse processo, ao estabelecer limites para a propaganda eleitoral digital, impor deveres de transparência e rastreabilidade e introduzir regime de corresponsabilidade que alcança partidos políticos, campanhas, empresas de comunicação e propaganda, bem como plataformas e redes sociais, exigindo governança preventiva, controles técnicos e diligência contínua ao longo de toda a cadeia de produção e difusão de conteúdo político-eleitoral. Vejamos:

Proibição de Deepfakes: é vedado o uso de conteúdo sintético em formato de áudio, vídeo ou combinação de ambos, para criar, substituir ou alterar imagem ou voz de pessoa viva, falecida ou fictícia para prejudicar ou favorecer candidatura.

Rotulagem Obrigatória: o uso de qualquer conteúdo gerado por IA deve vir acompanhado de informação explícita, destacada e em formato acessível (rótulo informativo).

Vedação de Chatbots: proíbe-se o uso de IA para simular interlocução (diálogo) com o eleitor, como robôs ou avatares que fingem ser o candidato ou pessoa real.

Dever de Cuidado dos provedores de aplicação: i) dever de adotar e a publicizar medidas para impedir ou diminuir a circulação de fatos notoriamente inverídicos ou gravemente descontextualizados que possam atingir a integridade do processo eleitoral; e ii) são responsáveis se não removerem imediatamente conteúdos que incitem atos antidemocráticos, discurso de ódio ou que façam uso de deepfakes.

Proteção de dados pessoais: proibição de pessoas jurídicas e pessoas naturais venderem cadastro de endereços eletrônicos e banco de dados pessoais. O cadastro de dados pessoais de contato, detido de forma legítima por pessoa natural, poderá ser cedido gratuitamente a partido político, federação, coligação, candidata ou candidato, condicionando-se o uso lícito na campanha à obtenção prévia de consentimento expresso e informado dos destinatários.

Portanto, a moderação de conteúdo, o dever de cuidado imposto às plataformas digitais e a proteção de dados pessoais, além do uso de IA, assumem centralidade em 2026, funcionando como parâmetro de prevenção e responsabilização em ambiente eleitoral. Espera-se maior exigência sobre políticas internas, sistemas de detecção, transparência algorítmica e controle do uso de IA e impulsionamento político.

IMPACTOS – O cenário eleitoral digital no Brasil conta com modelo de responsabilidade compartilhada, impondo a partidos, candidatos, coligações, agências, fornecedores tecnológicos e plataformas digitais deveres de transparência, rastreabilidade, identificação de conteúdo sintético, governança preventiva e controles técnicos contínuos. Isso exige revisão imediata de estratégias de comunicação política, contratos com terceiros e políticas de uso de dados e IA, com foco em compliance eleitoral e proteção de dados para o período de disputa eleitoral.

SOBRE NÓS

Direito,
Inovação
& Tecnologia

No VLK, **o Direito não é barreira**. É impulso para **inovar, viabilizar negócios** e construir uma sociedade mais próspera e justa.

Somos uma **boutique de Direito Digital** movida por **entregas que fazem a diferença**.

Conciliamos:

» Riscos e oportunidade;

» Complexidade e clareza; e

» Proteção e progresso.

Não importa o quão ousado seja o projeto: **faremos acontecer**, com segurança e **quebrando formalismos desnecessários**, nas seguintes áreas:

» Proteção de Dados Pessoais

» Governança Ética e Responsável de IA

» Cibersegurança e Resposta a Incidentes

» Legal Marketing e Propriedade Intelectual

» Regulação de Tecnologia

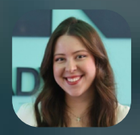
» Contencioso Estratégico

AUTORES

Rony Vainzof
rony@vlklaw.com.br

Caio Lima
caio@vlklaw.com.br

Gisele Karassawa
gisele@vlklaw.com.br



Carolina Rector
carolina.rector@vlklaw.com.br

Tayná Araújo
tayna.araujo@vlklaw.com.br