Desafios regulatórios da LGPD diante do uso de inteligência artificial em incidentes de vazamentos de dados

Regulatory challenges of the LGPD in the face of the use of artificial intelligence in data breach incidents

Igor Duarte Maia[1]
Leonardo Silva de Oliveira Bandeira[2]

COMO CITAR
MAIA, Igor Duarte; BANDEIRA, Leonardo Silva de Oliveira. Desafios regulatórios da LGPD diante do uso de inteligência artificial em incidentes de vazamentos de dados. In: OLIVEIRA, Emanuelle Góes (org.). **Desafios do Direito Contemporâneo**: volume 16. Rio Branco: Momento Jurídico, 2026. p. 64-94. ISBN 978-65-978356-4-5.

RESUMO

Introdução. O presente estudo trata dos desafios regulatórios impostos pela Lei Geral de Proteção de Dados Pessoais (LGPD) frente ao uso da inteligência artificial (IA) em incidentes de vazamento de dados, com ênfase nas lacunas normativas e na opacidade algorítmica. **Objetivo.** Diante desse contexto, procedeu-se o estudo considerando a suficiência do arcabouço normativo brasileiro para enfrentar as novas dinâmicas de risco tecnológico, discorrendo sobre a aplicabilidade prática da LGPD, a responsabilização em ambientes complexos e as exigências para o Relatório de Impacto à Proteção de Dados (RIPD). **Método.** Através do embasamento teórico e análise documental, produziu-se uma análise comparativa da legislação brasileira com o Regulamento Geral sobre a Proteção de Dados (GDPR) e o *AI Act* da União Europeia, com exame da jurisprudência do Superior Tribunal de Justiça sobre reparação de danos em incidentes de vazamento. **Resultados.** A adoção de sistemas de IA evidenciou limitações estruturais na LGPD, dentre elas, destaca-se

[1] Discente do 8º período do curso de bacharelado em Direito pelo Centro Universitário UNINORTE.
[2] Docente do curso de bacharelado em Direito do Centro Universitário Uninorte. Especialista em Direito Civil, Docência do Ensino Superior e Legal Operations: Dados, IA e Performance Jurídica (PUC/PR). Coordenador do NEAD/Uninorte. Advogado (Casas, Ricardo, Bandeira & Soares Advocacia). E-mail: leonardo.bandeira@uninorteac.com.br.

a ausência de parâmetros procedimentais que assegurem a efetividade do direito de revisão de decisões automatizadas, bem como a necessidade de regulamentação específica para sistemas de alto risco. **Conclusão.** Dessa forma, é imperativa a articulação da LGPD com um marco normativo específico para IA e o fortalecimento institucional da Autoridade Nacional de Proteção de Dados (ANPD) para assegurar a proteção efetiva dos titulares.

Palavras-chave: LGPD. Inteligência artificial. Vazamento de dados. Regulação. Proteção de dados.

ABSTRACT

Introduction. This study deals with the regulatory challenges imposed by the General Data Protection Law (LGPD) regarding the use of artificial intelligence (AI) in data breach incidents, with emphasis on regulatory gaps and algorithmic opacity. **Objective.** In this context, the study considered the sufficiency of the Brazilian regulatory framework to face the new dynamics of technological risk, discussing the practical applicability of the LGPD, accountability in complex environments and the requirements for the Data Protection Impact Report (DPIA). **Method.** Through theoretical grounding and documentary analysis, a comparative analysis was produced between Brazilian legislation and the General Data Protection Regulation (GDPR) and the AI Act of the European Union, with an examination of the case law of the Superior Court of Justice on damages in data breach incidents. **Results.** The adoption of AI systems has revealed structural limitations in the LGPD, among which stands out the absence of procedural parameters ensuring the effectiveness of the right to review automated decisions, as well as the need for specific regulation of high-risk systems. **Conclusion.** Therefore, it is imperative to articulate the LGPD with a specific regulatory framework for AI and to strengthen the National Data Protection Authority (ANPD) institutionally in order to ensure effective protection of data subjects.

Keywords: LGPD. Artificial intelligence. Data breach. Regulation. Data protection.

INTRODUÇÃO

A expansão das relações sociais e econômicas no ambiente digital ampliou a circulação e o tratamento de dados pessoais, tornando cada vez mais necessária a existência de mecanismos jurídicos capazes de acompanhar as transformações tecnológicas. No Brasil, a Lei Geral de Proteção de

Dados Pessoais, Lei n.º 13.709/2018, consolidou um marco geral de proteção dos dados pessoais e estabeleceu princípios e deveres voltados à segurança, à prevenção, à transparência e à responsabilização dos agentes de tratamento (Brasil, 2018). A evolução da inteligência artificial, contudo, acrescenta novas dificuldades a esse regime, especialmente pela capacidade dos sistemas automatizados de processar grandes volumes de informações, estabelecer relações entre diferentes bases de dados e produzir resultados cuja lógica nem sempre é facilmente compreendida. Em situações de vazamento, essas características podem ampliar a quantidade de pessoas atingidas, dificultar a identificação das causas do incidente e tornar mais complexa a definição dos responsáveis pelos danos ocasionados.

Este trabalho tem como objetivo analisar os desafios regulatórios enfrentados pela LGPD diante do uso de inteligência artificial em incidentes de vazamento de dados, com atenção especial aos mecanismos de prevenção, responsabilização e reparação. Busca-se examinar se as disposições atualmente existentes conseguem responder às particularidades dos sistemas de IA, sobretudo diante da opacidade algorítmica, da dificuldade de atribuição de responsabilidade quando participam diferentes agentes da cadeia tecnológica e dos riscos decorrentes do processamento e da inferência de informações pessoais. A análise também considera a proteção de dados como direito fundamental e instrumento de garantia da autodeterminação informacional, ultrapassando a compreensão de que a tutela jurídica se limita à preservação da privacidade.

A questão que orienta a pesquisa é a seguinte: os mecanismos de prevenção, responsabilização e reparação previstos na LGPD são suficientes para enfrentar as particularidades dos vazamentos de dados pessoais relacionados ao uso de sistemas de inteligência artificial? Para responder a esse questionamento, será desenvolvida pesquisa qualitativa, fundamentada em revisão bibliográfica e documental, com análise da legislação brasileira, da produção doutrinária, de documentos da Autoridade Nacional de Proteção de Dados, da jurisprudência dos tribunais superiores e das propostas legislativas relacionadas à regulamentação da inteligência arti-

ficial. Também será realizada análise comparativa com o Regulamento Geral sobre a Proteção de Dados da União Europeia, conhecido como GDPR, e com o *AI Act*, buscando identificar soluções regulatórias que possam contribuir para a compreensão das limitações e das possibilidades do modelo brasileiro. A relevância dessa comparação decorre das diferenças entre uma regulação voltada predominantemente à proteção dos dados pessoais e outra que disciplina diretamente os sistemas de inteligência artificial segundo diferentes níveis de risco.

A necessidade dessa discussão torna-se ainda mais evidente diante das limitações identificadas na aplicação da LGPD a sistemas automatizados. Embora a lei estabeleça deveres relacionados à segurança e à prevenção e assegure ao titular o direito de revisão de decisões tomadas exclusivamente com base em tratamento automatizado, permanecem questões quanto ao conteúdo dessa revisão, à explicabilidade dos sistemas e à atribuição de responsabilidade em situações envolvendo múltiplos agentes tecnológicos. Nesse contexto, as discussões conduzidas pela ANPD e a tramitação do Projeto de Lei n.º 2.338/2023, aprovado pelo Senado Federal em dezembro de 2024 e submetido à revisão da Câmara dos Deputados, demonstram a busca por mecanismos regulatórios capazes de complementar a proteção existente e estabelecer parâmetros mais específicos para o desenvolvimento e a utilização da inteligência artificial no país (Brasil, 2023a). O projeto adota uma abordagem baseada em diferentes níveis de risco e prevê obrigações progressivas de conformidade, aproximando-se, em determinados aspectos, do modelo adotado pelo *AI Act*.

A pesquisa pretende contribuir para o debate jurídico acerca da capacidade do ordenamento brasileiro de proteger os titulares diante de novas formas de tratamento automatizado de dados. Ao examinar as potencialidades e as limitações da LGPD frente aos vazamentos relacionados à inteligência artificial, busca-se oferecer uma análise que auxilie os operadores do Direito na compreensão dos desafios de prevenção, responsabilização e reparação, bem como na reflexão sobre os caminhos necessários

para o desenvolvimento de um ambiente digital que concilie inovação tecnológica, segurança e proteção dos direitos fundamentais.

1 DADOS PESSOAIS: FUNDAMENTOS JURÍDICOS E EVOLUÇÃO NORMATIVA

Compreender o conceito de dado pessoal é o ponto de partida de qualquer análise sobre a LGPD. A lei o define como "informação relacionada a pessoa natural identificada ou identificável" (Brasil, 2018, art. 5.º, I). A definição é funcionalmente ampla: não exige que o dado identifique alguém de forma direta, bastando que, combinado a outras informações disponíveis, permita fazê-lo, amplitude que assume especial relevância diante dos sistemas de inteligência artificial, capazes de cruzar grandes volumes de dados e reidentificar indivíduos mesmo em bases formalmente anonimizadas. A lei distingue, ainda, os dados comuns dos dados sensíveis, definidos no artigo 5.º, inciso II, como aqueles referentes à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação sindical, à saúde ou à vida sexual, bem como os dados genéticos e biométricos (Brasil, 2018). Essa categoria exige proteção reforçada porque sua exposição gera risco qualificado de discriminação e dano de difícil reparação: para algoritmos de triagem, reconhecimento facial ou análise de crédito, a manipulação de dados sensíveis sem base legal adequada representa violação cujas consequências ultrapassam a dimensão patrimonial e atingem a dignidade da pessoa.

Doneda (2019) distingue dado de informação com precisão conceitual relevante: o dado é o elemento bruto; a informação nasce quando esse dado é processado e contextualizado, adquirindo significado. Nissenbaum (2010) complementa essa análise ao propor o conceito de integridade contextual, segundo o qual a privacidade não é violada simplesmente pela divulgação de informações sigilosas, mas quando o fluxo de dados contraria as normas vigentes no contexto em que foram originalmente coletados. Aplicado à IA, esse conceito revela que dados migram de contexto para contexto de forma invisível, tornando cada nova utilização potenci-

almente uma violação adicional, ainda que juridicamente imperceptível à luz dos marcos normativos tradicionais. Solove (2006) oferece, por sua vez, uma taxonomia útil das violações de privacidade, distinguindo coleta indevida, processamento não autorizado e disseminação prejudicial, o que permite identificar com precisão onde a IA amplifica os riscos regulatórios.

A proteção jurídica dos dados pessoais tem raízes históricas que remontam ao debate oitocentista sobre privacidade. Warren e Brandeis (1890) foram os primeiros a sistematizar o direito à privacidade no *common law* americano, antecipando o problema do controle sobre informações pessoais. No plano internacional, a Declaração Universal dos Direitos Humanos consagrou, em seu artigo 12, a proteção contra interferências arbitrárias na vida privada (Organização das Nações Unidas, 1948); as primeiras leis de proteção de dados surgiram na Europa ocidental na década de 1970, com Alemanha e Suécia na vanguarda; e, em 1980, as Diretrizes da Organização para a Cooperação e Desenvolvimento Econômico sistematizaram os princípios que ainda hoje orientam a legislação global (OCDE, 1980). A Convenção n.º 108 do Conselho da Europa, aberta à assinatura em 1981, constituiu o primeiro tratado internacional juridicamente vinculante em matéria de proteção de dados pessoais, consagrando a coleta leal, a finalidade determinada, a proporcionalidade e a vedação ao tratamento de categorias especiais de dados sem garantias adequadas (Conselho da Europa, 1981), princípios que influenciaram diretamente a elaboração da LGPD brasileira (Doneda, 2019).

Nesse mesmo período firmou-se o precedente fundador da matéria. Ao julgar, em 15 de dezembro de 1983, a constitucionalidade da lei do recenseamento populacional, no célebre *Volkszählungsurteil*, o Tribunal Constitucional Federal alemão reconheceu o direito à autodeterminação informacional como projeção do livre desenvolvimento da personalidade e da dignidade humana, assentando que cabe ao indivíduo decidir sobre a divulgação e o emprego dos dados que lhe dizem respeito (Alemanha, 1983). O julgado forneceu o substrato teórico sobre o qual se construiu o

moderno direito à proteção de dados em escala global (Doneda, 2019; Mendes, 2021).

No Brasil, a Constituição Federal (Brasil, 1988), por meio da Emenda Constitucional n.º 115, de 10 de fevereiro de 2022, inseriu no artigo 5.º o inciso LXXIX, consagrando o direito à proteção dos dados pessoais como direito fundamental autônomo (Brasil, 2022a). Doneda (2019, p. 44) sintetiza o alcance dessa transformação:

> A proteção de dados pessoais não se confunde com a proteção da privacidade, ainda que com ela se relacione de forma íntima. Trata-se de um direito autônomo, cujo objeto é o controle pelo indivíduo das informações que lhe dizem respeito, independentemente de seu caráter reservado ou público. O dado pessoal é, nessa perspectiva, uma projeção da própria personalidade humana no espaço informacional, e sua instrumentalização sem o consentimento ou o conhecimento do titular representa uma violação da dignidade que o ordenamento jurídico não pode tolerar.

Mendes (2021) destaca que a constitucionalização impõe ao intérprete a obrigação de conferir efetividade material ao direito, o que exige atualização permanente dos instrumentos normativos diante das transformações tecnológicas. Essa dimensão objetiva, reconhecida também por Doneda (2011) em trabalho anterior ao advento da LGPD, obriga o Estado a conformar toda a ordem jurídica ao imperativo de proteger os dados pessoais como bem jurídico de relevância coletiva. Para Bioni (2020), o conteúdo desse direito vai além do consentimento individual: envolve a construção de estruturas institucionais e normativas capazes de limitar o poder dos agentes de tratamento e proteger os titulares de danos que, com frequência, eles próprios não percebem ter sofrido.

A proteção de dados no contexto da IA apresenta, ainda, uma dimensão coletiva que a LGPD não capta plenamente em suas disposições individuais. Quando sistemas algorítmicos tomam decisões sobre grupos, ao negar crédito a pessoas de determinadas regiões ou ao perfilar usuários com base em comportamentos coletivos, o dano não se resolve pela tutela

individual do titular. Frazão e Cueva (2021) apontam que essa dimensão coletiva dos danos algorítmicos exige novas formas de representação processual e novos instrumentos de reparação, como a ação civil pública e a regulação preventiva. A ausência de disposições específicas sobre responsabilidade coletiva na LGPD representa lacuna relevante que os projetos de lei em tramitação precisarão endereçar.

2 O MARCO CIVIL DA INTERNET E A PROTEÇÃO DE DADOS NO BRASIL

A Lei n.º 12.965, de 23 de abril de 2014, o Marco Civil da Internet, precedeu a LGPD como principal instrumento normativo do ambiente digital brasileiro. Sua elaboração resultou de processo colaborativo coordenado pelo Ministério da Justiça, com participação de cidadãos, especialistas e organizações da sociedade civil, configurando, segundo Lemos (2014), o primeiro exemplo bem-sucedido de legislação participativa em larga escala no país; o contexto político também foi determinante, pois as revelações de Edward Snowden sobre programas de vigilância em massa dos Estados Unidos pressionaram o governo a dar resposta normativa urgente à questão da soberania digital. Já em seu artigo 3.º, a lei estabeleceu a proteção da privacidade e dos dados pessoais como fundamentos do uso da internet no Brasil (Brasil, 2014), escolha principiológica deliberada e politicamente disputada, que representou o reconhecimento de que privacidade e proteção de dados são condições estruturais para a confiança na rede, sem as quais a democracia digital não se sustenta (Lemos, 2014).

No plano da privacidade, o artigo 7.º estabeleceu direitos relevantes aos usuários, entre eles:

> I — inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; II — inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...] VII — não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; [...] X — exclusão definitiva dos dados

> pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes (Brasil, 2014).

O artigo 11 foi pioneiro ao afirmar a territorialidade da lei brasileira no ambiente digital: mesmo serviços sediados no exterior ficam sujeitos à legislação nacional quando coletam dados de brasileiros ou operam em território nacional (Brasil, 2014). Esse dispositivo antecipou, ainda que de forma incipiente, o debate que o GDPR europeu tornaria central em 2018 e que permanece relevante para a regulação de sistemas de IA desenvolvidos fora do país, mas utilizados para processar dados de titulares brasileiros. No campo da responsabilidade civil, por sua vez, o artigo 19 adotou modelo subsidiário, pelo qual o provedor de aplicações apenas responde por danos decorrentes de conteúdo de terceiros após descumprir ordem judicial de remoção. Esse modelo, concebido para a dinâmica do conteúdo gerado pelo usuário, revelou-se inadequado para os casos de violação de dados pessoais. Ao julgar o Tema 533 da repercussão geral, o Supremo Tribunal Federal reconheceu a inconstitucionalidade parcial e progressiva do dispositivo, admitindo hipóteses de responsabilização dos provedores independentemente de ordem judicial quando o conteúdo manifestamente ilícito não for tornado indisponível, e sinalizando que o modelo original era insuficiente para responder aos danos graves gerados no ambiente digital (Brasil, 2025b).

As insuficiências do Marco Civil como instrumento de proteção de dados eram estruturais: o escopo da lei limitava-se ao ambiente de internet, excluindo setores como saúde, finanças e telecomunicações; não havia autoridade regulatória especializada, tampouco sistema sancionatório robusto; e a lei não disciplinava o ciclo completo do dado, da coleta à eliminação. O escândalo Cambridge Analytica, revelado em março de 2018, tornou essas limitações inegáveis ao demonstrar que dados de dezenas de milhões de usuários, coletados sob aparência de legitimidade por meio de um aplicativo de testes de personalidade, podiam ser desviados para fins radicalmente distintos, incluindo a manipulação eleitoral por meio de

perfilamento psicográfico baseado em IA (Cadwalladr; Graham-Harrison, 2018).

A relação entre o Marco Civil e a LGPD é de complementaridade normativa, não de substituição. A LGPD derrogou os dispositivos do Marco Civil que tratavam especificamente de proteção de dados pessoais, mas não suprimiu as disposições sobre neutralidade de rede, liberdade de expressão e responsabilidade civil dos provedores por conteúdo de terceiros. Para incidentes de segurança envolvendo dados pessoais, a LGPD é a lei aplicável; para o regime de guarda de registros de conexão e de acesso a aplicações, o Marco Civil conserva plena relevância. Bioni (2020) destaca que a articulação entre os dois diplomas é indispensável para a compreensão integral do regime de proteção de dados no país, especialmente nas situações em que o tratamento de dados se dá em plataformas digitais sujeitas, simultaneamente, às obrigações de ambos.

3 VAZAMENTOS DE DADOS: CONCEITO, TIPOLOGIA E IMPACTOS

3.1 CONCEITO LEGAL E TIPOLOGIA DOS INCIDENTES DE SEGURANÇA

A LGPD trata os incidentes de vazamento sob a rubrica de "incidente de segurança", definido como qualquer situação acidental ou ilícita que resulte em destruição, perda, alteração, comunicação ou acesso não autorizado a dados pessoais (Brasil, 2018, art. 48). A amplitude da definição tem virtude e risco: abarca tanto ataques externos deliberados quanto falhas internas de configuração e erros humanos, mas gera imprecisão sobre quais eventos efetivamente disparam o dever de notificação à ANPD, abrindo margem para que controladores posterguem a comunicação de incidentes de menor gravidade aparente.

Do ponto de vista da origem, os incidentes se dividem entre ataques externos, como *ransomware*, *phishing* e exploração de vulnerabilidades de *software*, e fatores internos, como erros de funcionários, configurações inadequadas ou uso malicioso de acessos privilegiados. Quanto ao tipo de dado comprometido, incidentes que expõem dados sensíveis pro-

duzem impactos mais graves e duradouros, com potencial de discriminação e chantagem de difícil reparação. Anderson *et al.* (2019) documentaram que os custos econômicos dos incidentes vão muito além das multas regulatórias, alcançando a erosão da confiança institucional e o dano reputacional de longo prazo.

3.2 A INTELIGÊNCIA ARTIFICIAL COMO MULTIPLICADOR DO DANO E COMO INSTRUMENTO DE DEFESA

A IA ocupa, no cenário dos incidentes de segurança, uma posição que o legislador de 2018 não poderia ter antecipado com precisão. Quando está do lado do atacante, ou quando o descuido na sua implementação expõe milhões de registros simultaneamente, ela é o multiplicador do dano: um único modelo de linguagem comprometido pode tornar públicas informações que, em décadas anteriores, teriam exigido o vazamento de centenas de sistemas independentes para alcançar a mesma escala. Quando está do lado da defesa, detectando padrões anômalos em tempo real e respondendo a ataques com velocidade que nenhum analista humano alcançaria, a mesma tecnologia é parte essencial da solução. Regular apenas a exposição ao risco, ignorando esse potencial defensivo, resultaria em marco normativo incompleto: a legalidade da IA na segurança de dados não pode ser avaliada apenas pela ameaça que representa, mas pela função que desempenha no ecossistema mais amplo de proteção.

A adoção de sistemas de IA no tratamento de dados pessoais agrava o cenário em duas dimensões. A primeira é quantitativa: o volume de dados processados é significativamente maior, o que amplia o escopo do dano em caso de vazamento. A segunda é qualitativa: a capacidade inferencial dos algoritmos pode transformar dados formalmente anonimizados em informações identificáveis. Narayanan e Shmatikov (2008) demonstraram que bases comportamentais anonimizadas podem ser reidentificadas com alta precisão a partir de informações auxiliares publicamente disponíveis. Isso significa que a exclusão do dado anonimizado do âmbito de proteção da LGPD, prevista no artigo 12, pode ser insuficiente

quando o tratamento envolve tecnologias com capacidade de reidentificação.

3.3 INCIDENTES DE GRANDE ESCALA E A DIMENSÃO COLETIVA DO DANO

O Brasil é cenário recorrente de incidentes de grande escala. O mais expressivo ocorreu em janeiro de 2021, com a exposição de dados de mais de 220 milhões de brasileiros, incluindo pessoas falecidas, abrangendo CPF, renda estimada, pontuação de crédito e endereço, em base composta por dezenas de conjuntos distintos de informações (Valente, 2021). A origem nunca foi formalmente apurada, o que ilustra um problema sistêmico: quando dados circularam por múltiplos agentes ao longo do tempo, a identificação do controlador responsável torna-se tarefa de elevada complexidade. O Relatório de Atividades da ANPD referente a 2022 registrou crescimento significativo nas notificações de incidentes, sinalizando tanto maior frequência dos eventos quanto amadurecimento na cultura de cumprimento das obrigações de comunicação (ANPD, 2022).

As consequências dos vazamentos não se restringem ao plano individual. Rodotà (2008) argumenta que a privacidade se transformou em condição essencial para o exercício da liberdade: sem o controle sobre as próprias informações, o indivíduo torna-se vulnerável à vigilância, ao controle e à discriminação, perdendo autonomia tanto no espaço público quanto no privado. Nessa perspectiva, um vazamento de dados não é mero incidente técnico, mas uma agressão às condições mínimas de exercício da dignidade humana. No plano coletivo, incidentes de grande escala corroem a confiança nas instituições, afetam a disposição dos cidadãos para participar da economia digital e criam externalidades negativas para o desenvolvimento de modelos de negócio baseados em dados.

3.4 DEVERES DE COMUNICAÇÃO E LIMITES OPERACIONAIS DA RESPOSTA A INCIDENTES

As obrigações legais do controlador em caso de incidente estão disciplinadas no artigo 48 da LGPD:

> O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1.º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I — a descrição da natureza dos dados pessoais afetados; II — as informações sobre os titulares envolvidos; III — a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados; IV — os riscos relacionados ao incidente; V — os motivos da demora, no caso de a comunicação não ter sido imediata; e VI — as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (Brasil, 2018, art. 48).

A Resolução CD/ANPD n.º 15, de 24 de abril de 2024, regulamentou os procedimentos de comunicação, fixando o prazo de três dias úteis para que o controlador notifique a ANPD e os titulares afetados, contados do conhecimento de que o incidente afetou dados pessoais (ANPD, 2024, art. 6.º e 9.º). O descumprimento sujeita o controlador às sanções do artigo 52 da LGPD, que incluem multa de até 2% do faturamento, limitada a R$ 50 milhões por infração (Brasil, 2018).

O prazo de três dias úteis, embora represente avanço normativo, enfrenta desafios práticos nas organizações brasileiras. Muitas empresas de médio e pequeno porte não dispõem de equipes de resposta a incidentes estruturadas, nem de sistemas de monitoramento contínuo que permitam a detecção e o registro do incidente no intervalo legalmente exigido. Bioni (2020) observa que a proteção efetiva de dados pessoais depende não apenas da existência de normas, mas da capacidade das organizações de internalizá-las em seus processos operacionais, o que implica um papel educativo e orientador da ANPD que vai além de sua função sancionatória.

4 LEGISLAÇÃO DE PROTEÇÃO DE DADOS: LGPD, GDPR E PROJETOS SOBRE IA

4.1 A ESTRUTURA PRINCIPIOLÓGICA DA LGPD E AS TENSÕES COM A INTELIGÊNCIA ARTIFICIAL

A Lei n.º 13.709/2018 unificou sob um marco geral a proteção de dados pessoais no Brasil, superando a fragmentação das regulações setoriais anteriores. Sua estrutura organiza-se em torno dos dez princípios do artigo 6.º, quais sejam: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, que funcionam como vetores interpretativos de toda a lei e como parâmetros de avaliação da licitude das práticas de tratamento (Brasil, 2018). Para sistemas de IA, os princípios da transparência, da necessidade e da não discriminação apresentam tensões regulatórias particularmente agudas.

Entre os dez princípios, o da não discriminação merece atenção especial no contexto da IA. O inciso IX do artigo 6.º veda o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos. Para algoritmos de decisão de crédito, seleção de candidatos ou triagem de benefícios sociais, esse princípio é frequentemente desafiado de forma indireta: o modelo pode não utilizar explicitamente raça ou gênero como variável, mas produzir resultados sistematicamente discriminatórios por meio de variáveis correlatas, como CEP, nível educacional ou padrões de consumo. Esse fenômeno, denominado discriminação algorítmica indireta, não encontra resposta específica na LGPD, que não estabelece obrigação de auditoria ou avaliação de impacto discriminatório para sistemas automatizados. Frazão e Cueva (2021) identificam essa lacuna como uma das principais fragilidades do quadro normativo atual.

4.2 BASES LEGAIS, SEGURANÇA E GOVERNANÇA DESDE A CONCEPÇÃO

O artigo 7.º elenca as bases legais que legitimam o tratamento de dados, entre as quais o consentimento, o cumprimento de obrigação legal, a execução contratual, o legítimo interesse e a proteção do crédito (Brasil, 2018). Doneda (2019) destaca que o modelo plural de bases legais representa evolução em relação ao sistema centrado exclusivamente no consentimento, mas cria desafios próprios: um modelo de aprendizado de máquina treinado com dados coletados sob uma finalidade específica pode produzir inferências que vão além do escopo original, gerando problemas de adequação que a lei não resolve expressamente.

No campo da segurança, o artigo 46 impõe a obrigação central de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas:

> 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. § 1.º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis (Brasil, 2018, art. 46).

O artigo 49 complementa esse dispositivo ao exigir que os sistemas de tratamento sejam estruturados segundo requisitos de segurança e boas práticas de governança desde sua concepção, o que remete ao conceito de *privacy by design*, central no GDPR europeu. Para sistemas de IA, implementar esse padrão é particularmente desafiador, dada a dificuldade de prever e controlar os comportamentos de modelos complexos em condições reais de operação (Mendes, 2021).

4.3 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E O DÉFICIT DE CAPACIDADE INSTITUCIONAL

A ANPD, transformada em autarquia de natureza especial pela Medida Provisória n.º 1.124, de 13 de junho de 2022 (Brasil, 2022b), é responsável por fiscalizar o cumprimento da lei, editar normas complementares e apreciar petições de titulares. Em seu Relatório de Atividades de 2022, a autoridade reconheceu que a adoção da IA demanda interpretação da LGPD em consonância com os princípios da finalidade, da transparência e da responsabilização (ANPD, 2022, p. 7). Frazão e Cueva (2021) advertem, porém, que a efetividade regulatória da ANPD depende de capacidade técnica e independência política ainda em consolidação, o que cria um déficit estrutural entre as exigências da lei e a capacidade real de sua execução.

4.4 O GDPR E O AI ACT COMO REFERÊNCIAS COMPARATIVAS

O GDPR europeu, em vigor desde maio de 2018, é a principal referência comparativa da LGPD. Mendes (2021) registra que o Brasil adotou o modelo europeu, mas enfrenta dificuldades adicionais diante da carência de infraestrutura regulatória e da ausência de previsões específicas sobre IA. A diferença mais relevante para os fins deste trabalho está no artigo 22 do GDPR: o titular tem direito de não ser submetido a decisões baseadas exclusivamente em tratamento automatizado que produzam efeitos jurídicos ou que o afetem de forma significativa, com garantias procedimentais detalhadas (União Europeia, 2016). O artigo 20 da LGPD prevê o direito de revisão de decisões automatizadas em termos mais genéricos, sem especificar o conteúdo mínimo dessa revisão, lacuna que fragiliza sensivelmente a proteção do titular.

Além do GDPR, a União Europeia aprovou o *AI Act*, consubstanciado no Regulamento (UE) 2024/1689, adotado em 13 de junho de 2024 e publicado no Jornal Oficial da União Europeia em 12 de julho de 2024, que classifica sistemas de IA por níveis de risco e impõe obrigações específicas de conformidade, auditabilidade e transparência para as categorias de

maior risco (União Europeia, 2024). O regulamento europeu distingue os sistemas de risco inaceitável, proibidos, como as técnicas de manipulação cognitiva e a identificação biométrica em massa em espaços públicos, dos sistemas de alto risco, que incluem avaliação de crédito, recrutamento automatizado e triagem de benefícios sociais, e que ficam sujeitos a obrigações de registro, documentação técnica, gestão de riscos e supervisão humana. Ao disciplinar diretamente os sistemas de IA, e não apenas o tratamento dos dados que processam, o *AI Act* representa mudança de paradigma em relação ao modelo de proteção de dados: enquanto o GDPR e a LGPD incidem sobre as consequências do tratamento, o regulamento europeu incide sobre as ferramentas em si, antes mesmo que o dano ocorra, precisamente o que falta ao quadro normativo brasileiro.

4.5 OS PROJETOS BRASILEIROS DE REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL

No plano nacional, o Projeto de Lei n.º 2.338, de 2023, propõe abordagem baseada em risco semelhante à do *AI Act*, classificando sistemas de IA em categorias de risco excessivo, alto risco, risco limitado e risco mínimo, com obrigações progressivas de conformidade; aprovado pelo Senado Federal em 10 de dezembro de 2024, o texto foi remetido à Câmara dos Deputados, onde permanece em exame (Brasil, 2023a). Antes dele, o Projeto de Lei n.º 21, de 2020, aprovado pela Câmara dos Deputados em setembro de 2021, adotava linguagem mais principiológica e menos operacional (Brasil, 2020).

O Senado Federal, contudo, optou por construir projeto próprio em vez de deliberar sobre o texto aprovado pela Câmara, o que resultou, por anos, na coexistência de duas propostas com filosofias regulatórias distintas, encerrada apenas quando o Projeto de Lei n.º 21, de 2020, foi declarado prejudicado em razão da aprovação do substitutivo ao Projeto de Lei n.º 2.338, de 2023. Essa sobreposição reproduziu, no plano da regulação da IA, o mesmo problema de fragmentação normativa que motivou a criação da própria LGPD quase uma década antes. Sem articulação entre o

projeto em tramitação e a lei de proteção de dados, o resultado provável é a geração de insegurança jurídica e o enfraquecimento de ambos os marcos (Frazão; Cueva, 2021).

5 DESAFIOS REGULATÓRIOS DA LGPD DIANTE DA INTELIGÊNCIA ARTIFICIAL

A LGPD foi aprovada em 2018, antes que sistemas de IA generativa, reconhecimento facial em larga escala e modelos preditivos de risco se tornassem infraestrutura operacional corrente. As lacunas que se identificam a seguir não constituem propriamente vícios de técnica legislativa, mas refletem o descompasso estrutural entre o ritmo da inovação tecnológica e a cadência dos processos normativos. Sua identificação rigorosa constitui premissa metodológica para qualquer proposta de aperfeiçoamento do marco regulatório vigente.

5.1 OPACIDADE ALGORÍTMICA E OS LIMITES DO DEVER DE TRANSPARÊNCIA

O problema da opacidade algorítmica é o mais visível. O princípio da transparência, previsto no artigo 6.º, inciso VI, exige que os agentes de tratamento forneçam informações claras e acessíveis sobre o tratamento realizado (Brasil, 2018). Para modelos de aprendizado profundo com dezenas de milhões de parâmetros, essa exigência esbarra em obstáculo técnico estrutural: nem os próprios desenvolvedores conseguem explicar, em termos compreensíveis, por que o algoritmo chegou a determinada conclusão. Goodman e Flaxman (2017) demonstraram que o "direito à explicação" pressuposto em legislações como o GDPR enfrenta limites técnicos reais; a área de *Explainable AI* (XAI) busca supri-los com métodos como LIME e SHAP, mas sem solução satisfatória para os sistemas mais complexos.

5.2 O DIREITO DE REVISÃO DO ARTIGO 20 E O DÉFICIT DE PARÂMETROS PROCEDIMENTAIS

O artigo 20 da LGPD assegura ao titular o direito de revisão de decisões tomadas exclusivamente com base em tratamento automatizado, prevendo, em seu § 2.º, a possibilidade de auditoria pela ANPD para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (Brasil, 2018). O problema está na ausência de parâmetros mínimos: a lei não especifica o que deve conter essa revisão, quais informações o controlador deve prestar ao titular nem quais padrões de explicabilidade os sistemas precisam atender. Sem esses parâmetros, o direito corre o risco de ser cumprido apenas formalmente, sem que o titular tenha acesso real às razões da decisão que o afetou. O GDPR, nos artigos 13, 14 e 22, é mais exigente ao requerer "informações significativas sobre a lógica envolvida" no tratamento automatizado (União Europeia, 2016). Doneda (2019) adverte que a proteção de dados deve ser compreendida como processo contínuo de adaptação normativa e institucional, e que a lei sozinha não basta para enfrentar os desafios tecnológicos.

Para que o direito previsto no artigo 20 seja efetivo, e não meramente formal, a ANPD precisaria estabelecer padrões mínimos de explicabilidade por categoria de sistema. Em decisões de concessão de crédito, por exemplo, poderia exigir que o modelo indique ao menos as principais variáveis que contribuíram para o resultado desfavorável ao titular. Não se trata de exigência estranha ao ordenamento: a Lei n.º 12.414, de 9 de junho de 2011, que disciplina os bancos de dados de adimplemento, já assegura ao cadastrado o direito de "conhecer os principais elementos e critérios considerados para a análise de risco", resguardado o segredo empresarial, bem como o de solicitar a revisão de decisão realizada exclusivamente por meios automatizados (Brasil, 2011, art. 5.º, IV e VI). O que se propõe é a generalização desse parâmetro setorial para as demais hipóteses de tratamento automatizado de alto impacto.

5.3 RESPONSABILIZAÇÃO CIVIL EM CADEIAS ALGORÍTMICAS

A responsabilização em ambientes de IA apresenta dificuldade estrutural distinta. A LGPD trabalha com as categorias de controlador e operador, pressupondo que as decisões sobre o tratamento são tomadas por pessoas ou organizações identificáveis. Sistemas de aprendizado de máquina, porém, tomam decisões a partir de padrões extraídos de enormes volumes de dados de treinamento, podendo produzir resultados que os desenvolvedores não previram. Em um incidente que envolva múltiplos atores, o desenvolvedor do modelo, a empresa que o implementou e o provedor de infraestrutura em nuvem, a atribuição de responsabilidade pode ser extraordinariamente complexa. Mulholland (2019) demonstra que o nexo de causalidade é particularmente problemático nesse contexto: a cadeia entre a conduta humana e o dano sofrido pela vítima é frequentemente mediada por decisões algorítmicas opacas, cuja lógica não é inteiramente conhecida nem controlada pelo operador ou pelo desenvolvedor, criando um déficit de imputação que as teorias clássicas da causalidade não estão preparadas para suprir sem adaptações dogmáticas significativas.

A dificuldade, contudo, não é inteiramente inédita, e a doutrina civilista brasileira oferece chaves de solução anteriores ao debate sobre algoritmos. Schreiber (2015) descreve a erosão dos filtros tradicionais da reparação, a culpa e o nexo causal, como tendência estrutural da responsabilidade civil contemporânea, acompanhada da diluição dos danos entre os agentes em melhor posição para suportá-los e preveni-los. Lida à luz dos incidentes envolvendo IA, essa análise sugere que o déficit de imputação apontado por Mulholland (2019) não reclama necessariamente a criação de categoria dogmática inédita, mas a intensificação de um movimento que a responsabilidade civil já vinha realizando: deslocar o eixo da imputação da conduta individual para a organização da atividade. Miragem (2021), na mesma direção, sustenta que a responsabilidade objetiva fundada no risco da atividade permite imputar o dano a quem organiza o em-

preendimento e dele se beneficia economicamente, independentemente da identificação do elo específico da cadeia em que a falha se produziu, solução compatível com o regime dos artigos 42 e 44 da LGPD e apta a evitar que a complexidade técnica se converta em imunidade prática. A divergência entre os autores não é de fundamento, mas de ênfase: enquanto Mulholland (2019) enfatiza a insuficiência das categorias causais clássicas, Schreiber (2015) e Miragem (2021) sugerem que o instrumental da responsabilidade objetiva, corretamente manejado, já oferece resposta ao problema, cabendo ao legislador apenas explicitá-la.

A responsabilidade objetiva adotada pela LGPD tem, nesse sentido, o mérito de impedir que a complexidade técnica sirva de escudo para a irresponsabilização. Contudo, a lei não disciplina especificamente os casos em que o sistema atua de forma autônoma e imprevisível. Doshi-Velez *et al.* (2017) identificam três dimensões que os marcos regulatórios precisam enfrentar: a responsabilização técnica (auditabilidade dos sistemas), a legal (atribuição de deveres e sanções) e a ética (alinhamento com valores sociais). A LGPD avança principalmente na segunda dimensão, deixando as outras sem resposta normativa satisfatória.

5.4 A JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA SOBRE DANO MORAL EM INCIDENTES DE VAZAMENTO

A insuficiência dos parâmetros legais manifesta-se com nitidez na jurisprudência sobre a reparação dos danos decorrentes de vazamento de dados, campo em que o Superior Tribunal de Justiça já produziu orientação relevante. Em um primeiro momento, ao julgar o Agravo em Recurso Especial n.º 2.130.619/SP, a Segunda Turma firmou entendimento restritivo: o vazamento de dados pessoais comuns, tais como nome, endereço, filiação e data de nascimento, não gera dano moral presumido, incumbindo ao titular a demonstração do prejuízo efetivamente sofrido (Brasil, 2023b). O acórdão distinguiu expressamente os dados comuns dos dados sensíveis, sinalizando que a natureza da informação exposta é determinante para a aferição do dano.

A orientação evoluiu de modo significativo. Ao julgar o Recurso Especial n.º 2.121.904/SP, a Terceira Turma reconheceu que o vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida acarreta responsabilidade objetiva da seguradora, com dano moral presumido, dispensada a demonstração de dolo ou culpa e a prova do prejuízo concreto, em fundamentação que articula a LGPD ao Código de Defesa do Consumidor (Brasil, 2025a). A leitura conjunta dos dois precedentes revela um critério em construção: a presunção do dano acompanha a gravidade intrínseca da informação exposta e o grau de vulnerabilidade que a exposição produz.

Esse critério, embora funcional para os incidentes convencionais, mostra-se frágil quando confrontado com os vazamentos mediados por inteligência artificial. Se, como demonstram Narayanan e Shmatikov (2008), a capacidade inferencial dos sistemas permite reidentificar titulares a partir de bases formalmente anonimizadas, a fronteira entre dado comum e dado sensível, que a jurisprudência elegeu como divisor de águas para a presunção do dano, deixa de ser estável: um conjunto de dados comuns pode, submetido a tratamento algorítmico, revelar informações de saúde, orientação sexual ou convicção política que jamais foram diretamente coletadas. A consequência prática é relevante: a aferição do dano tende a depender não apenas da natureza formal do dado vazado, mas do potencial inferencial do tratamento a que ele pode ser submetido, dimensão que nem a LGPD nem os precedentes examinados enfrentam expressamente. O ponto reforça a conclusão de Schreiber (2015) e Miragem (2021) quanto à necessidade de deslocar o eixo da imputação para a organização da atividade, e não para a caracterização casuística do dano.

5.5 DISCRIMINAÇÃO ALGORÍTMICA E A INSUFICIÊNCIA DA TUTELA INDIVIDUAL

A questão ética talvez seja o ponto mais frágil dos marcos regulatórios em vigor. Quando um sistema é treinado com dados que carregam desigualdades históricas, ele tende a repetir esses padrões e, em muitos ca-

sos, a torná-los ainda mais nítidos. A LGPD, por sua vez, foi pensada para proteger o dado de cada titular isoladamente, o que limita sua capacidade de responder a prejuízos que atingem coletividades inteiras, sem que se possa apontar um único indivíduo lesado. Esse vazio se torna particularmente preocupante em situações como processos de contratação, análise de crédito e decisões judiciais apoiadas por ferramentas automatizadas, nas quais o impacto sobre grupos vulneráveis pode passar despercebido pelo arcabouço legal existente.

5.6 GOVERNANÇA PREVENTIVA E O RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

A governança preventiva é outra frente de insuficiência. O artigo 38 da LGPD prevê que a ANPD poderá determinar ao controlador a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), instrumento cujo conteúdo mínimo é definido em seu parágrafo único e que, nos termos do artigo 10, § 3.º, pode ser exigido especialmente quando o fundamento do tratamento for o legítimo interesse (Brasil, 2018). O GDPR vai além: torna o relatório obrigatório sempre que o tratamento provavelmente resultar em alto risco aos titulares, hipótese que abrange expressamente decisões automatizadas em larga escala (União Europeia, 2016). Enquanto no modelo europeu a avaliação de impacto é condição prévia para que sistemas de alto risco entrem em operação, no Brasil ela depende de determinação da ANPD, tornando-se instrumento reativo. Abrams (2020) argumenta que a avaliação de impacto é o instrumento de governança preventiva mais efetivo disponível, pois força as organizações a identificar e mitigar riscos antes que os sistemas causem dano.

A experiência europeia oferece parâmetros relevantes. O Information Commissioner's Office (2025), autoridade britânica de proteção de dados, sistematizou hipóteses de obrigatoriedade da avaliação de impacto que incluem o emprego de tecnologias inovadoras, entre elas a inteligência artificial, o tratamento de categorias especiais de dados em larga escala, a adoção de decisões automatizadas com efeitos relevantes sobre o

acesso a serviços e oportunidades e o tratamento de dados de crianças ou de outros públicos vulneráveis. Tais hipóteses não foram incorporadas, em termos expressos, à regulamentação brasileira. Como consequência, empresas que operam justamente os sistemas mais sensíveis podem, no plano formal, prosseguir suas atividades sem jamais elaborar uma avaliação de impacto, sem que a ANPD tenha, até o presente, editado regulamentação específica destinada a suprir essa lacuna (Mendes, 2021).

5.7 SÍNTESE DAS INSUFICIÊNCIAS E PROPOSIÇÕES DE APERFEIÇOAMENTO

A análise sistemática da LGPD à luz da realidade dos sistemas automatizados permite identificar quatro insuficiências estruturais. A primeira, de maior densidade, reside no silêncio normativo quanto à inteligência artificial: a lei sequer menciona expressamente o tema, o que impõe aos agentes de tratamento e aos operadores do direito o recurso à analogia em um domínio no qual tanto os pressupostos técnicos quanto a doutrina jurídica permanecem em estágio de elaboração. A essa insuficiência inicial somam-se outras três: o direito de revisão previsto no artigo 20 carece de parâmetros procedimentais que lhe assegurem efetividade; o RIPD mantém natureza facultativa, embora a obrigatoriedade prévia se imponha como exigência razoável em hipóteses de tratamento de alto risco; e a ANPD, dotada de estrutura humana e orçamentária reduzida, é instada a fiscalizar tecnologias cuja complexidade ultrapassa, em muitos aspectos, sua atual capacidade institucional.

A superação dessas insuficiências exige a articulação da LGPD com um marco normativo específico sobre inteligência artificial. Não se cogita, todavia, da edição de um diploma autônomo e desconectado, mas de norma que dialogue com os princípios já consolidados pela LGPD e enderece as lacunas identificadas neste estudo. Paralelamente, faz-se necessária a edição, pela ANPD, de regulamentação complementar que defina, no mínimo, o conteúdo material do dever de explicação previsto no artigo 20, sob pena de reduzi-lo a garantia meramente formal. Impõe-se, ademais, a

previsão de obrigatoriedade do RIPD nas hipóteses de tratamento automatizado de alto risco, independentemente de prévia determinação da autoridade no caso concreto. Nenhuma dessas providências, contudo, produzirá os efeitos almejados sem o efetivo fortalecimento institucional da ANPD, mediante dotação orçamentária compatível e quadro técnico especializado em ciência de dados e segurança da informação. A efetividade da norma jurídica, em última análise, depende da capacidade institucional para sua aplicação.

CONSIDERAÇÕES FINAIS

A análise empreendida ao longo deste trabalho permite concluir que a Lei Geral de Proteção de Dados Pessoais representa o mais importante avanço normativo já realizado pelo ordenamento jurídico brasileiro em matéria de proteção da privacidade informacional. Sua aprovação, em 2018, encerrou um período de fragmentação regulatória e inseriu o Brasil no circuito internacional dos países que reconhecem a proteção de dados como questão central da agenda jurídica contemporânea. A posterior elevação desse direito ao patamar constitucional, por força da Emenda Constitucional n.º 115, de 2022, consolidou esse processo de amadurecimento institucional (Brasil, 2022a).

A pesquisa demonstrou, contudo, que essa estrutura apresenta limitações claras quando confrontada com a realidade dos sistemas de inteligência artificial. As lacunas identificadas não decorrem de imprecisão legislativa, mas do descompasso entre o tempo do direito e o tempo da tecnologia. Concentram-se em quatro frentes: a ausência de regulamentação específica para a inteligência artificial, a fragilidade operacional do direito à explicabilidade previsto no artigo 20, o caráter facultativo do Relatório de Impacto à Proteção de Dados Pessoais e as limitações institucionais da Autoridade Nacional de Proteção de Dados.

O exame da jurisprudência do Superior Tribunal de Justiça confirmou esse diagnóstico a partir da prática judiciária. A evolução que vai do

entendimento restritivo firmado no Agravo em Recurso Especial n.º 2.130.619/SP (Brasil, 2023b) ao reconhecimento do dano moral presumido no Recurso Especial n.º 2.121.904/SP (Brasil, 2025a) demonstra que os tribunais vêm construindo, por via pretoriana, critérios de reparação que a lei não fornece. Esse critério, ancorado na distinção entre dados comuns e dados sensíveis, tende, porém, a perder estabilidade diante da capacidade inferencial dos sistemas automatizados, o que reforça a necessidade de parâmetros normativos expressos.

A análise comparativa com o quadro europeu evidenciou que a articulação entre o GDPR e o *AI Act* representa modelo de coerência normativa que o Brasil ainda não conseguiu replicar. A tramitação prolongada e sobreposta dos projetos de lei sobre inteligência artificial, sem coordenação efetiva entre eles e sem articulação com a LGPD, reproduziu a fragmentação que motivou a criação da lei de proteção de dados quase uma década antes.

A pergunta que orientou esta investigação, sobre a suficiência da LGPD para enfrentar os desafios trazidos pela inteligência artificial nos incidentes de vazamento de dados, recebe resposta matizada. A lei é suficiente para a maioria dos casos de tratamento de dados pessoais e oferece base principiológica sólida sobre a qual se pode construir a resposta aos desafios da automação. Não é suficiente, contudo, quando se trata de sistemas de inteligência artificial complexos, decisões automatizadas de alto impacto e contextos em que a opacidade algorítmica inviabiliza o cumprimento substantivo do princípio da transparência.

REFERÊNCIAS

ABRAMS, Martin. **The accountability gap**: why privacy accountability is broken and how to fix it. Washington, DC: Future of Privacy Forum, 2020.

ALEMANHA. Bundesverfassungsgericht (Primeiro Senado). **Volkszählungsurteil**: BVerfGE 65, 1; 1 BvR 209/83 e outros. Reconhecimento do direito à autodeterminação informacional. Karlsruhe, 15 dez. 1983.

ANDERSON, Ross et al. Measuring the changing cost of cybercrime. In: WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY, 18., 2019, Boston. **Proceedings** [...]. Boston: WEIS, 2019. Disponível em: https://weis2019.econinfosec.org/. Acesso em: 10 mar. 2025.

ANPD. **Relatório de atividades 2022**. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2022. Disponível em: https://www.gov.br/anpd/. Acesso em: 20 set. 2025.

ANPD. **Resolução CD/ANPD n.º 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: Autoridade Nacional de Proteção de Dados, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aprova-o-regulamento-de-comunicacao-de-incidente-de-seguranca. Acesso em: 30 abr. 2025.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. **[Constituição (1988)]**. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 mar. 2025.

BRASIL. **Emenda Constitucional n.º 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022a. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 10 mar. 2025.

BRASIL. **Lei n.º 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 20 ago. 2026.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 mar. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://

www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 set. 2025.

BRASIL. **Medida Provisória n.º 1.124, de 13 de junho de 2022**. Transforma a Autoridade Nacional de Proteção de Dados em entidade da administração pública federal indireta, submetida a regime autárquico especial. Brasília, DF: Presidência da República, 2022b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/mpv/mpv1124.htm. Acesso em: 15 abr. 2025.

BRASIL. **Projeto de Lei n.º 21, de 2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 20 ago. 2026.

BRASIL. **Projeto de Lei n.º 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Brasília, DF: Senado Federal, 2023a. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 15 abr. 2025.

BRASIL. Superior Tribunal de Justiça (2. Turma). **Agravo em Recurso Especial n.º 2.130.619/SP**. Vazamento de dados pessoais. Dados comuns. Dano moral presumido. Impossibilidade. Necessidade de comprovação do dano efetivo. Relator: Min. Francisco Falcão, 7 de março de 2023. Brasília, DF: Superior Tribunal de Justiça, 2023b. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/. Acesso em: 20 ago. 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial n.º 2.121.904/SP**. Vazamento de dados pessoais sensíveis. Contrato de seguro de vida. Responsabilidade objetiva do fornecedor. Dano moral presumido. Relatora: Min. Nancy Andrighi, 11 de fevereiro de 2025. Brasília, DF: Superior Tribunal de Justiça, 2025a. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/. Acesso em: 20 ago. 2026.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n.º 1.057.258/MG** (Tema 533 da repercussão geral). Inconstitucionalidade parcial e progressiva do art. 19 da Lei n.º 12.965/2014. Relator: Min. Luiz Fux, 26 de junho de 2025. Brasília, DF: Supremo Tribunal Federal, 2025b. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=533. Acesso em: 10 jul. 2025.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**,

London, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 20 ago. 2026.

CONSELHO DA EUROPA. **Convenção n.º 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. Estrasburgo: Conselho da Europa, 28 jan. 1981. Disponível em: https://rm.coe.int/1680078b39. Acesso em: 20 ago. 2026.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DOSHI-VELEZ, Finale et al. **Accountability of AI under the law**: the role of explanation. Cambridge: Berkman Klein Center for Internet & Society, Harvard University, 2017. Disponível em: https://dash.harvard.edu/handle/1/34372584. Acesso em: 12 mar. 2025.

FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021.

GOODMAN, Bryce; FLAXMAN, Seth. European Union regulations on algorithmic decision-making and a "right to explanation". **AI Magazine**, Menlo Park, v. 38, n. 3, p. 50-57, 2017.

INFORMATION COMMISSIONER'S OFFICE. **When do we need to do a DPIA?** Wilmslow: ICO, 2025. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/. Acesso em: 24 ago. 2026.

LEMOS, Ronaldo. O Marco Civil como símbolo do desejo por inovação no Brasil. In:

LEITE, George Salomão; LEMOS, Ronaldo (org.). **Marco Civil da Internet**. São Paulo: Atlas, 2014.

MENDES, Laura Schertel. **LGPD comentada**: Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709/2018. 2. ed. São Paulo: Revista dos Tribunais, 2021.

MIRAGEM, Bruno. **Responsabilidade civil**. 2. ed. Rio de Janeiro: Forense, 2021.

MULHOLLAND, Caitlin. Responsabilidade civil e processos decisórios autônomos em sistemas de Inteligência Artificial (IA): autonomia, imputabilidade e

responsabilidade. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Robust de-anonymization of large sparse datasets. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 29., 2008, Oakland. **Proceedings** [...]. Los Alamitos: IEEE Computer Society, 2008. p. 111-125.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

OCDE. **Guidelines on the protection of privacy and transborder flows of personal data**. Paris: Organização para a Cooperação e Desenvolvimento Econômico, 1980. Disponível em: https://legalinstruments.oecd.org/public/doc/114/114.en.pdf. Acesso em: 20 ago. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Adotada e proclamada pela Resolução n.º 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Paris: ONU, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 20 ago. 2026.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação à diluição dos danos. 6. ed. São Paulo: Atlas, 2015.

SOLOVE, Daniel J. A taxonomy of privacy. **University of Pennsylvania Law Review**, Philadelphia, v. 154, n. 3, p. 477-564, 2006.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – GDPR). **Jornal Oficial da União Europeia,** Luxemburgo, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679. Acesso em: 20 ago. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024**. Estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial – AI Act). Jornal Oficial da União Europeia, Luxemburgo, 12 jul. 2024. Disponível em: https://eur-

lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689. Acesso em: 20 ago. 2025.

VALENTE, Jonas. OAB pede investigação do vazamento de dados de 220 milhões de pessoas. **Agência Brasil**, Brasília, DF, 28 jan. 2021. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2021-01/oab-pede-investigacao-do-vazamento-de-dados-de-220-milhoes-de-pessoas. Acesso em: 20 ago. 2026.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193-220, dez. 1890.