1 INTRODUÇÃO

A ascensão da inteligência artificial (IA) tem provocado transformações profundas no ecossistema digital, sobretudo pela automatização de decisões e pelo uso massivo de dados pessoais em plataformas digitais. Alimentados por algoritmos complexos, esses sistemas frequentemente operam de forma opaca, dificultando a compreensão dos critérios utilizados em processos decisórios automatizados. Essa característica amplia riscos de violações à privacidade, discriminações e vazamentos de dados, colocando em evidência o desafio de conciliar inovação tecnológica com a proteção dos direitos fundamentais dos indivíduos.

Nesse cenário, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018, alterada pela Lei nº 13.853/2019) representou um marco normativo relevante no Brasil, ao estabelecer princípios e garantias para o tratamento de dados pessoais. Contudo, a sofisticação técnica da inteligência artificial evidencia limitações dessa legislação diante da realidade dos sistemas algorítmicos. Além da LGPD, este estudo dialoga com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR – 2016/679), o *Artificial Intelligence Act* (AI Act – 2024) e o Projeto de Lei nº 2.338/2023 em tramitação no Brasil, que buscam oferecer respostas regulatórias específicas para os desafios da IA.

Diante desse contexto, formula-se o seguinte problema de pesquisa: em que medida a LGPD é suficiente para garantir a proteção dos direitos fundamentais dos indivíduos no contexto do uso massivo de dados por sistemas de inteligência artificial, e quais mecanismos regulatórios e de governança podem ser adotados para suprir suas limitações?

O objetivo geral do trabalho é analisar os desafios e limitações da LGPD diante da complexidade da IA, discutindo a pertinência de um marco regulatório específico que aborde riscos e impactos sociais decorrentes do tratamento automatizado de dados. Como objetivos específicos, busca-se: (i) investigar os riscos associados à opacidade algorítmica e ao vazamento de dados; (ii) discutir a relevância do *compliance* algorítmico como instrumento de transparência e conformidade legal; (iii) apresentar *frameworks* de governança de dados, como o DAMA-DMBOK e o COBIT, e sua aplicabilidade; e (iv) propor uma abordagem integrada que combine medidas legais, técnicas e organizacionais para fortalecer a governança de dados no Brasil.

Metodologicamente, o estudo adota uma abordagem qualitativa, de caráter exploratório-descritivo, utilizando o método dedutivo. A pesquisa foi desenvolvida a partir de levantamento bibliográfico e documental, com base em marcos normativos nacionais e internacionais, literatura acadêmica e relatórios técnicos sobre inteligência artificial e proteção

de dados, além da análise de casos emblemáticos de falhas de *compliance* e vazamentos de dados em plataformas digitais.

O trabalho está dividido em três seções, além desta introdução e da conclusão. A seção 2 examina os limites da LGPD diante dos desafios da inteligência artificial, com ênfase na opacidade algorítmica, nos riscos de discriminação e nos vazamentos de dados. A seção 3 aborda o conceito e a importância do *compliance* algorítmico, explorando estratégias de mitigação de riscos, proteção da privacidade e *frameworks* de governança de dados. A seção 4 analisa as perspectivas regulatórias nacionais e internacionais, destacando o GDPR, o AI Act europeu e o Projeto de Lei nº 2.338/2023 no Brasil.

A relevância deste estudo reside na necessidade de construir um ambiente digital em que a inovação tecnológica esteja alinhada à proteção de direitos fundamentais, oferecendo subsídios ao debate contemporâneo sobre a regulação da inteligência artificial no Brasil e à formulação de políticas públicas e práticas organizacionais mais responsáveis.

2 A LGPD FRENTE À INTELIGÊNCIA ARTIFICIAL

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) surge como marco normativo essencial no ordenamento jurídico brasileiro, estabelecendo princípios, fundamentos e garantias voltados ao tratamento de dados pessoais. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a lei assegura direitos fundamentais como a portabilidade, a exclusão de dados e a revisão de decisões automatizadas (BRASIL, 2018). Tais dispositivos representam avanços significativos, sobretudo em um cenário em que os dados pessoais se consolidaram como recursos estratégicos de alto valor econômico e social.

No entanto, a evolução tecnológica, em especial com a consolidação da inteligência artificial (IA), expõe os limites práticos da LGPD. A utilização de algoritmos complexos e técnicas de *machine learning*[1] ampliou exponencialmente a capacidade de coleta, processamento e análise de informações pessoais. Esse contexto revela tensões regulatórias que desafiam a efetividade da legislação, sobretudo no que se refere à transparência, responsabilização e proteção da autodeterminação informativa.

[1] *Machine learning* (aprendizagem de máquina) é um ramo da inteligência artificial (IA) que permite que os sistemas de computador aprendam a partir de dados e tomem decisões ou façam previsões sem serem explicitamente programados para cada tarefa. O processo envolve treinar um algoritmo em um grande conjunto de dados para que ele possa identificar padrões e correlações. Uma vez treinado, o algoritmo pode aplicar o conhecimento adquirido a novos dados, melhorando seu desempenho ao longo do tempo. É a base de muitas tecnologias modernas, como sistemas de recomendação (Netflix, Spotify), reconhecimento de imagem e fala (Google Photos, Siri) e carros autônomos.

2.1 Opacidade Algorítmica e Limitações da LGPD

A chamada opacidade algorítmica, também conhecida como “caixa-preta da IA”, refere-se à dificuldade ou mesmo impossibilidade de compreender os critérios de decisão empregados por sistemas automatizados. Esse fenômeno decorre, em grande medida, da complexidade técnica de modelos de aprendizado profundo, como redes neurais artificiais, que processam grandes volumes de dados em múltiplas camadas internas, tornando os resultados pouco ou nada explicáveis para usuários e até mesmo para especialistas (PASQUALE, 2016).

Essa ausência de explicabilidade desafia frontalmente os princípios de transparência e *accountability*[2], previstos na LGPD. O art. 20 da lei estabelece o direito do titular de dados à revisão de decisões automatizadas, assegurando que processos baseados exclusivamente em algoritmos possam ser questionados (BRASIL, 2018). Todavia, a falta de clareza quanto aos critérios utilizados pelos sistemas compromete a efetividade desse dispositivo legal, uma vez que, se o próprio funcionamento do algoritmo não é inteligível, a revisão se torna meramente formal e não substancial.

A opacidade algorítmica não é apenas um desafio técnico, mas também jurídico e social. Do ponto de vista jurídico, ela impede a efetiva responsabilização de agentes de tratamento, já que muitas vezes não é possível identificar quem é responsável por determinada decisão ou qual critério levou a um resultado específico. Do ponto de vista social, a falta de explicabilidade fragiliza a confiança dos indivíduos no ambiente digital, reduzindo a percepção de segurança e de proteção de seus direitos fundamentais.

Casos de discriminação algorítmica evidenciam a gravidade do problema. Algoritmos utilizados em processos seletivos ou na concessão de crédito podem reproduzir vieses presentes nos dados de treinamento, resultando em decisões injustas que afetam diretamente grupos vulneráveis. A ausência de transparência dificulta a contestação dessas decisões, perpetuando desigualdades e violando o princípio da não discriminação, implícito na LGPD e explícito em tratados internacionais de direitos humanos.

2.2 Riscos Associados ao Uso Massivo de Dados

[2] *Accountability* (responsabilização) é a obrigação de aceitar a responsabilidade por ações, decisões e seus resultados, com a disposição de justificar o que foi feito. O conceito vai além de apenas "ter responsabilidade", pois implica em ser passível de punição ou recompensa com base no que foi entregue. É um pilar para a transparência, confiança e bom desempenho em diversos contextos, sejam pessoais, profissionais ou governamentais.

A utilização intensiva de dados pessoais em sistemas de inteligência artificial gera uma série de riscos à privacidade, à segurança da informação e à própria dignidade da pessoa humana. Isso ocorre porque tais tecnologias dependem de grandes volumes de dados para treinar e aperfeiçoar seus modelos, o que potencializa tanto os benefícios quanto as vulnerabilidades inerentes ao processo.

Um dos riscos mais evidentes é o de vazamento de dados em larga escala, que serão abordados mais a frente nesse artigo. Tais incidentes expõem informações sensíveis e fragilizam a confiança social no ambiente digital. Esses eventos revelam a insuficiência dos mecanismos previstos pela LGPD, que embora estabeleça princípios de segurança e prevenção (arts. 6º e 46), carece de instrumentos regulatórios e técnicos específicos para lidar com a complexidade das ameaças contemporâneas. Nesse sentido, a lei sozinha não consegue prevenir vulnerabilidades decorrentes da escala e da interconectividade dos sistemas de IA, os quais demandam medidas adicionais de governança e monitoramento.

Outro risco relevante é a discriminação algorítmica, que ocorre quando vieses presentes nos dados de treinamento são reproduzidos ou até mesmo ampliados pelos sistemas. Isso se dá porque os algoritmos aprendem padrões a partir de informações históricas, que muitas vezes carregam desigualdades estruturais. Como consequência, decisões automatizadas podem reforçar estereótipos ou práticas discriminatórias em áreas críticas, como processos seletivos, concessão de crédito, políticas de segurança pública e até mesmo no acesso a serviços de saúde.

A ausência de transparência na tomada de decisão algorítmica agrava o problema, pois dificulta que os indivíduos afetados compreendam ou questionem os critérios utilizados. Tal cenário contraria o princípio da não discriminação e da autodeterminação informativa, previstos na LGPD, e compromete a proteção de direitos fundamentais.

2.3 A Necessidade de Complementariedade Normativa

É crescente a percepção de que a LGPD não é suficiente para regular os riscos específicos associados à inteligência artificial. Isso ocorre porque ela foi concebida em um contexto de proteção de dados pessoais de caráter geral, sem considerar as particularidades dos sistemas algorítmicos, como a opacidade, a possibilidade de discriminação e a dificuldade de atribuição de responsabilidades.

Nesse sentido, especialistas e organismos internacionais têm defendido a adoção de instrumentos normativos complementares, voltados a assegurar maior transparência,

explicabilidade e supervisão humana sobre as decisões automatizadas (WEHANDLE, 2023). A implementação de mecanismos regulatórios adicionais é fundamental para garantir que a inovação tecnológica esteja alinhada a valores éticos e jurídicos, evitando a ampliação de desigualdades ou a violação de direitos fundamentais.

No cenário internacional, destaca-se o Artificial Intelligence Act (AI Act), aprovado pela União Europeia em 2024. Essa norma estabelece um marco regulatório abrangente para a IA, introduzindo a classificação dos sistemas conforme o grau de risco — mínimo, limitado, alto ou inaceitável — e impondo requisitos diferenciados às chamadas "IAs de alto risco". Entre as obrigações previstas, incluem-se: a necessidade de supervisão humana, a gestão da qualidade de dados, a produção de documentação técnica auditável e a adoção de mecanismos de transparência e explicabilidade (UNIÃO EUROPEIA, 2024).

Além disso, o AI Act prevê sanções expressivas em caso de descumprimento, que podem alcançar até 35 milhões de euros ou 7% do faturamento global da empresa infratora, reforçando a natureza vinculante do compliance algorítmico no contexto europeu (UNIÃO EUROPEIA, 2024). Essa experiência normativa evidencia a importância de associar instrumentos legais a práticas concretas de fiscalização e responsabilização, de modo a reduzir riscos sistêmicos decorrentes do uso de IA.

Para o Brasil, a experiência europeia pode servir como referência, mas não deve ser simplesmente reproduzida. É necessário adaptar as diretrizes internacionais à realidade nacional, considerando as especificidades socioeconômicas, o nível de maturidade tecnológica e os desafios institucionais do país. Nesse sentido, o Projeto de Lei nº 2.338/2023, em tramitação no Congresso Nacional, representa um passo relevante ao propor um marco regulatório específico para a inteligência artificial, inspirado no modelo europeu, mas ajustado às demandas locais (BRASIL, 2025).

3 COMPLIANCE ALGORÍTMICO E GOVERNANÇA DE DADOS

A transição para uma economia digital impulsionada por dados e algoritmos redefiniu os perímetros da governança corporativa e da conformidade regulatória. Nesta seção, a análise se aprofunda na intersecção entre os sistemas de decisão automatizada, as estruturas de governança de dados e o arcabouço normativo da LGPD. O objetivo é a demonstração de que o compliance algorítmico não é um exercício estático de conformidade legal, mas uma disciplina dinâmica e contínua, intrinsecamente ligada à gestão de riscos, à proteção da privacidade e que age com proeminência na resposta a incidentes. A conformidade eficaz, portanto, emerge como um resultado direto de uma governança de dados madura e proativa.

3.1 Conceito e relevância do compliance algorítmico

Uma definição abrangente de compliance algorítmico o estabelece como o conjunto de processos, políticas, controles internos e mecanismos de supervisão que uma organização implementa para assegurar que seus sistemas de IA e de decisão automatizada operem em estrita conformidade com as leis e regulamentações, além de padrões éticos aplicáveis, que posteriormente serão expostos.

Essa abordagem ultrapassa a simples adequação normativa, exigindo que os princípios de conformidade estejam enraizados na missão, visão e valores da organização, e possibilitando uma coerência fundamental entre as práticas operacionais e os princípios éticos declarados (LIMA; GARRIDO[3], 2022).

[3] LIMA, Ricardo Alves de; GARRIDO, Guilherme Leite. Lei Geral de Proteção de Dados Pessoais (LGPD) e compliance: um panorama da adequação normativa para organizações contemporâneas. Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, v. 17, n. 1, e68680, 2022. ISSN 1981-3694. DOI: 10.5902/1981369468680. Disponível em: https://doi.org/10.5902/1981369468680. Acesso em: 23 set. 2025.

A relevância do compliance algorítmico tornou-se crítica com a ascensão de tecnologias baseadas em *big data*[4] e *machine learning*, que intensificaram a preocupação com a perpetuação de vieses e discriminações por meio de sistemas automatizados. Nesse cenário, a implementação de um programa de compliance algorítmico robusto é vital para diversos fins estratégicos. Primeiramente, visa à mitigação de riscos legais e financeiros, evitando as sanções administrativas previstas na LGPD, que podem alcançar multas de até 2% do faturamento da empresa. Em segundo lugar, atua na proteção da reputação corporativa, pois a ocorrência de erros, vieses ou resultados discriminatórios em algoritmos pode infligir danos severos e, por vezes, irreparáveis à marca e à confiança do público (IBM, 2023). E mais importante, o compliance algorítmico é um mecanismo salutar e essencial para a garantia de direitos fundamentais, assegurando que as decisões automatizadas não violem preceitos constitucionais como a dignidade da pessoa humana, a privacidade e o princípio da não discriminação (GONÇALVES[5], 2025).

3.2 Estratégias de mitigação de riscos e proteção da privacidade

A mitigação de riscos em sistemas algorítmicos exige uma abordagem estruturada que identifique as ameaças intrínsecas a essas tecnologias e implemente estratégias proativas e contínuas para neutralizá-las. O foco principal recai sobre os vieses discriminatórios e a falta de transparência, desafios que podem ser endereçados por meio de metodologias como o *Privacy by Design* e práticas de governança robustas.

Os riscos associados aos sistemas algorítmicos são complexos e multifacetados. O mais proeminente é o viés algorítmico, que se manifesta quando um sistema de IA produz resultados que sistematicamente favorecem ou prejudicam determinados grupos de indivíduos de forma desproporcional. As origens desse viés são diversas.

---

[4] *Big Data* é um conjunto de técnicas e processos de tratamento de dados caracterizado pelos chamados "5 Vs": volume (grande quantidade de dados), velocidade (geração e processamento em tempo real), variedade (diferentes formatos estruturados e não estruturados), veracidade (confiabilidade) e valor (extração de conhecimento útil). O Big Data permite identificar padrões e prever comportamentos, sendo amplamente utilizado em marketing e segurança.

[5] GONÇALVES, Rafaela Vilela; BARBARESCO, Rogério Ananias. Discriminação em algoritmos de inteligência artificial: estudo da LGPD como mecanismo de controle dos vieses discriminatórios. Revista Científica da UNIFENAS, Alfenas, v. 6, n. 8, p. 150-160, 19 dez. 2024. ISSN 2596-3481. Disponível em: https://orcid.org/0009-0003-2501-7749. Acesso em: 24 set. 2025.

Há de se salientar 2 tipos mais comuns: o viés de preconceito, ou *prejudice bias*, que ocorre quando estereótipos, preconceitos e suposições sociais errôneas, presentes na sociedade, são refletidos e codificados nos dados de treinamento do algoritmo; e o viés de Amostra, ou *sample/selection bias*, que surge quando os dados utilizados para treinar o modelo não são representativos da população sobre a qual ele irá operar (IBM[6], 2023).

A falta de transparência, frequentemente descrita como o problema da "caixa preta", é um outro risco significativo, onde muitos sistemas de IA, especialmente os baseados em redes neurais profundas, operam de maneira opaca, tornando muito difícil para humanos compreenderem a lógica e os fatores que levaram a uma decisão específica.

Essa opacidade representa um obstáculo formidável para a responsabilização, a identificação de erros e a contestação de decisões injustas (L. C. SALLES[7], 2024). A LGPD busca mitigar esse risco através do princípio da transparência (art. 6º, inciso VI) e do direito à revisão de decisões automatizadas (art. 20), que implicitamente demanda um certo grau de explicabilidade (E-DIREITO[8], 2025).

A abordagem mais eficaz para a gestão de riscos algorítmicos é a prevenção, e estratégias proativas são implementadas desde as fases iniciais de concepção e desenvolvimento do sistema. A metodologia *Privacy by Design (PbD)* é a pedra angular dessa abordagem, da qual foi concebida para que a privacidade e a proteção de dados sejam incorporadas de forma nativa e por padrão (*by default*) em todos os processos, produtos e sistemas, a *PbD* evita que a proteção de dados seja tratada como um adendo ou uma correção tardia (CAPTAIN COMPLIANCE[9], 2024; BLOG CONVISOAPPSEC[10], 2019). A LGPD internaliza esse conceito em seu art. 46, ao exigir que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas "desde a fase de concepção do produto ou do serviço até a sua execução".

---

[6] IBM. *O que é viés da IA?* IBM, 22 dez. 2023. Disponível em: https://www.ibm.com/br-pt/think/topics/ai-bias. Acesso em: 23 set. 2025.

[7] L. C. SALLES. *Alguns exemplos de perigos reais oriundos do mau uso da IA*. L.C. Salles, 2024. Disponível em: https://www.lcsalles.com.br/post/alguns-exemplos-de-perigos-reais-oriundos-do-mau-uso-da-ia. Acesso em: 17 set. 2025.

[8] E-DIREITO. *LGPD: Direito à Explicação em Decisões Automatizadas*. E-Direito, 12 set. 2025. Disponível em: https://e-direito.com/2025/09/12/lgpd-direito-a-explicacao-em-decisoes-automatizadas/. Acesso em: 16 set. 2025.

[9] CAPTAIN COMPLIANCE. *Privacy by Design LGPD: The Ultimate Guide for Businesses*. Captain Compliance, 14 maio 2024. Disponível em: https://captaincompliance.com/education/privacy-by-design-lgpd/. Acesso em: 19 set. 2025.

[10] BLOG CONVISOAPPSEC. *Privacy by Design and Data Security*. Conviso, 2019. Disponível em: https://blog.convisoappsec.com/en/privacy-by-design-and-data-security/. Acesso em: 15 set. 2025.

Outras estratégias proativas incluem a formação de **e**quipes de desenvolvimento diversas**,** pois a inclusão de profissionais de diferentes áreas do conhecimento, gêneros, etnias e origens socioeconômicas é crucial para identificar e questionar vieses que poderiam passar despercebidos por equipes homogêneas (FGV CEPI[11], 2024). Além disso, a realização de um diagnóstico e mapeamento de riscos no início de qualquer projeto de IA permite uma avaliação abrangente das áreas de vulnerabilidade, a identificação dos tipos específicos de riscos algorítmicos e a definição de níveis de prioridade para a alocação de recursos de mitigação.

O treinamento e a conscientização de todos os colaboradores envolvidos no ciclo de vida da IA também são essenciais. Eles devem receber formação específica sobre proteção de dados, ética em IA e seus papéis individuais na identificação e mitigação de riscos.

A causa raiz da maioria dos vieses discriminatórios reside em dados de treinamento inadequados, que refletem preconceitos históricos ou falhas de representação. Casos emblemáticos, como a ferramenta de recrutamento da Amazon que penalizava currículos com termos associados a mulheres (L. C. SALLES, 2024), e o algoritmo COMPAS[12], que atribuía maior risco de reincidência a réus negros (DIO, 2025; MCKINSEY, 2019), demonstram que o algoritmo simplesmente aprende os padrões discriminatórios presentes nos dados. A LGPD, em seu princípio da qualidade dos dados (Art. 6º, inciso V), exige que os dados tratados sejam precisos e revisados constantemente.

3.3 Vazamentos de dados e seus efeitos sociais

O cenário de segurança de dados no Brasil é alarmante, marcado por incidentes de grande escala que expõem a vulnerabilidade de infraestruturas críticas e afetam milhões de cidadãos. A análise desses eventos e de suas consequências revela impactos que transcendem as perdas financeiras diretas, atingindo as esferas social e psicológica dos indivíduos e impulsionando uma evolução na resposta regulatória e na jurisprudência sobre danos morais.

---

[11] FGV CEPI. *Os muitos desafios da mitigação de vieses no desenvolvimento de algoritmos*. Medium, 2024. Disponível em: https://fgvcepi.medium.com/os-muitos-desafios-da-mitiga%C3%A7%C3%A3o-de-vieses-no-desenvolvimento-de-algoritmos-83a48888e734. Acesso em: 22 set. 2025.

[12] Algoritmo *COMPAS* é uma ferramenta algorítmica de avaliação de risco criminal (*Correctional Offender Management Profiling for Alternative Sanction*s), desenvolvida pela empresa *Northpointe*. É utilizada para prever a probabilidade de reincidência de acusados ou condenados. Tornou-se exemplo emblemático de opacidade e vieses algorítmicos, pois estudos (como o da ProPublica, 2016) apontaram que ele superestimava riscos para pessoas negras e subestimava para brancas, evidenciando o problema da discriminação algorítmica.

O Brasil também figura consistentemente entre os países com maior volume de dados vazados no mundo, onde os incidentes de segurança tornaram-se mais frequentes e sofisticados, atingindo grandes corporações, instituições financeiras e órgãos governamentais, o que demonstra uma fragilidade sistêmica (FIA, 2025).

Em 2021, ocorreu o episódio que ficou conhecido como o "Mega Vazamento do Fim do Mundo", considerado à época o maior já registrado no Brasil. Estima-se que 223 milhões de pessoas tiveram informações expostas, incluindo CPF, nome completo, data de nascimento, endereço, fotos de rosto, renda, dados de veículos e escolaridade, entre outros.

O caso ganhou esse apelido justamente pelo volume inédito de informações, que alcançou praticamente toda a população brasileira, incluindo pessoas já falecidas. A gravidade do episódio levou à atuação da Secretaria Nacional do Consumidor (Senacon) e do Procon-SP, que notificaram a Serasa para prestar esclarecimentos quanto à origem dos dados e às medidas de contenção adotadas. O roubo de identidade é uma das principais causas de perdas financeiras no Brasil, com um prejuízo médio estimado em mais de R$5.700 por vítima em 2024 (IDENTY.IO[13], 2025; CLEAR.SALE[14], 2025).

Tratando do cenário internacional, em junho de 2025, segundo reportagem da revista *Forbes*, foi identificado o maior vazamento de dados da história: cerca de 16 bilhões de senhas e credenciais foram expostas, atingindo plataformas como Apple, Google, Facebook, Telegram, GitHub, além de serviços governamentais de diferentes países. Diferentemente de incidentes anteriores, que em grande medida se baseavam na reciclagem de bancos de dados já comprometidos, esse caso envolveu informações inéditas, coletadas por meio de malwares do tipo *infostealer* (FORBES, 2025).

[13] IDENTY.IO. *Brasil perdeu mais de R$ 297,7 bilhões devido a fraudes em 2024; roubo de identidade é uma das principais causas*. Identy.io, 2025. Disponível em: https://www.identy.io/brasil-perdeu-mais-de-r-2977-bilhoes-devido-a-fraudes-em-2024-roubo-de-identidade-e-uma-das-principais-causas/. Acesso em: 20 set. 2025.

[14] CLEAR.SALE. *Roubo de identidade: o que é, como acontece e como prevenir*. Clear.Sale, 2025. Disponível em: https://br.clear.sale/blog/roubo-de-identidade. Acesso em: 16 set. 2025.

Em muitos casos, autoridades e empresas frequentemente minimizam o risco de vazamentos de dados cadastrais, classificando-os como "não sensíveis" e de "baixo impacto" (AGÊNCIA BRASIL[15], 2025). Os dados vazados são mais do que suficientes para a aplicação de golpes que afetam em muito a vida dos cidadãos. A jurisprudência inicial do STJ refletiu essa visão ao exigir prova de dano concreto para esses casos, mas a realidade demonstra que a combinação de dados aparentemente comuns é precisamente o que os fraudadores necessitam para construir narrativas críveis e aplicar golpes de engenharia social (STJ, 2023).

O "paradoxo do dado não sensível" reside no fato de que informações de baixo risco isoladamente, quando agregadas e contextualizadas, tornam-se uma ferramenta de alto impacto para o crime, cujo dano à vítima, posteriormente, enfrenta dificuldades para comprovar em juízo. Adicionalmente, os vazamentos de dados criam um "resíduo tóxico" digital que pode ser reaproveitado para fins ainda mais nefastos, como a alimentação de sistemas de IA discriminatórios, que resultam em incidentes massivos, como o de 2021 e o "Mother of All Breaches" (MOAB), cujo efeito disponibilizou vastos conjuntos de dados na *dark web*.

A questão da reparação por danos morais tem sido objeto de intenso debate na jurisprudência brasileira. Inicialmente, em 2023, o STJ, no julgamento do AREsp 2.130.619, firmou o entendimento de que o vazamento de dados pessoais comuns (não sensíveis) não gera, por si só, um dano moral presumido (*in re ipsa*), e, portanto, caberia ao titular dos dados comprovar o efetivo prejuízo sofrido para ter direito à indenização (LOPES[16], 2025).

Contudo, decisões mais recentes indicam uma evolução nesse entendimento. No REsp 2.147.374, o STJ decidiu que a ocorrência de um ataque hacker não isenta a empresa de sua responsabilidade, rejeitando a tese de "culpa exclusiva de terceiro" quando há falha no dever de segurança do agente de tratamento (DATA PRIVACY BRASIL[17], 2024). Mais significativamente, em fevereiro de 2025, o julgamento do REsp 2.121.904 sinalizou uma mudança de posicionamento ao reconhecer o dano moral presumido em um caso de vazamento, inaugurando um entendimento que valoriza a angústia e a violação da expectativa de privacidade do titular, independentemente da comprovação de prejuízo material subsequente.

---

[15] AGÊNCIA BRASIL. *BC informa que total de chaves Pix vazadas chega a 46,8 milhões*. Agência Brasil, 24 jul. 2025. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2025-07/bc-informa-que-total-de-chaves-pix-vazadas-chega-468-milhoes. Acesso em: 19 set. 2025.

[16] LOPES, Roberta Castilho Andrade. STJ reconhece dano moral presumido em vazamento de dados pessoais. MIGALHAS, 29 maio 2025. Disponível em: https://www.migalhas.com.br/depeso/431132/stj-reconhece-dano-moral-presumido-em-vazamento-de-dados-pessoais. Acesso em: 26 set. 2025.

[17] DATA PRIVACY BRASIL. *Mudou tudo? STJ decide sobre resp. civil em vazamento de dados*. Data Privacy Brasil, 13 dez. 2024. Disponível em: https://dataprivacy.com.br/mudou-tudo-stj-decide-sobre-resp-civil-em-vazamento-de-dados/. Acesso em: 15 set. 2025.

3.4 Frameworks de governança de dados: DAMA-DMBOK e COBIT

Para construir um programa de compliance algorítmico e de proteção de dados que seja robusto, auditável e alinhado aos preceitos da LGPD, as organizações necessitam de estruturas metodológicas consolidadas. Os *frameworks*[18] DAMA-DMBOK e COBIT 2019 destacam-se como os principais guias para a implementação de uma governança de dados e de TI eficaz, fornecendo o ferramental conceitual e prático para a conformidade.

DAMA-DMBOK (*Data Management Body of Knowledge*): Desenvolvido pela *DAMA International,* o DMBOK é um *framework* globalmente reconhecido que estabelece um corpo de conhecimento e melhores práticas para a gestão de dados, onde a sua filosofia central é tratar os dados como um ativo estratégico da organização, cujo valor deve ser maximizado e cujos riscos devem ser minimizados (ATLAN[19], 2025; BLR DATA[20], 2019.).

O guia fornece uma linguagem comum e uma estrutura para gerenciar os dados ao longo de todo o seu ciclo de vida. Funda-se em princípios como governança de dados, que, considerada a função central que orienta todas as outras, é definida como o exercício de autoridade e controle (planejamento, monitoramento e execução) sobre os ativos de dados.

Também tem como premissa a segurança de dados, onde foca na proteção dos dados contra acesso não autorizado e uso indevido, assegurando os pilares de confidencialidade, integridade e disponibilidade.

O princípio de qualidade de dados visa garantir que os dados sejam precisos, consistentes, completos e adequados ao seu propósito e a implementação de controles de qualidade de dados é fundamental para mitigar vieses algorítmicos, que frequentemente se originam de dados de treinamento falhos ou não representativos (DAMA INTERNATIONAL, 2020).

COBIT (*Control Objectives for Information and Related Technologies*): Desenvolvido pela ISACA[21], o COBIT é um *framework* de governança e gestão de tecnologia da informação corporativa cujo objetivo primordial é alinhar as estratégias de TI com os objetivos de negócio, garantindo a criação de valor, a otimização de riscos e a gestão eficiente de recursos.

---

[18] No campo da governança e da tecnologia, frameworks são estruturas metodológicas e normativas que organizam princípios, processos e boas práticas a fim de orientar a gestão. Diferem-se de leis ou regulamentos, pois não são obrigatórios, mas servem como modelos de referência reconhecidos.

[19] ATLAN. *The DAMA-DMBOK Framework for Data Management*. Atlan, 2025. Disponível em: https://atlan.com/dama-dmbok-framework/. Acesso em: 22 set. 2025.

[20] BLR DATA. *LGPD impulsiona Governança de Dados*. BLR Data, 2019. Disponível em: https://www.blrdata.com.br/single-post/lgpd-impulsiona-governan%C3%A7a-de-dados. Acesso em: 20 set. 2025.

[21] ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, 2018. Disponível em: https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf. Acesso em: 17 set. 2025.

O COBIT 2019 estabelece seis princípios fundamentais para o sistema de governança: prover valor às partes interessadas, adotar uma abordagem holística, manter o sistema de governança dinâmico, diferenciar governança de gestão, adaptar-se às necessidades da empresa e implementar um sistema de governança de ponta a ponta (*end-to-end*).

4 PERSPECTIVAS REGULATÓRIAS

A insuficiência de marcos normativos de caráter geral, como a LGPD, para endereçar os riscos sistêmicos e as especificidades técnicas da inteligência artificial impulsionou uma nova onda regulatória em escala global. A tendência observada é a evolução de leis de proteção de dados para frameworks específicos, desenhados para governar o ciclo de vida dos sistemas de IA com base em uma estratificação de riscos. Esta seção analisa os paradigmas internacionais que moldam o debate, como o Regulamento Geral sobre a Proteção de Dados (GDPR) e o *AI Act* da União Europeia. E examina como o Brasil, por meio do PL nº 2.338/2023 e do fortalecimento da Agência Nacional de Proteção de Dados (ANPD), se posiciona nesse cenário, se adaptando e inovando a partir de modelos estrangeiros.

4.1 Marcos internacionais: GDPR e AI Act como Paradigmas Globais

A trajetória regulatória da União Europeia oferece um estudo de caso sobre a maturação da governança de tecnologias emergentes. O GDPR estabeleceu as fundações baseadas em direitos individuais, enquanto o *AI Act* construiu sobre elas uma estrutura de governança proativa e focada nos sistemas tecnológicos em si.

O GDPR da União Europeia foi pioneiro ao estabelecer um regime robusto para a proteção de dados pessoais, e serviu de inspiração direta para a LGPD brasileira. No que tange à IA, seu dispositivo mais relevante é o artigo 22, que consagra o direito do titular de não ser sujeito a uma decisão baseada exclusivamente em tratamento automatizado, incluindo a definição de perfis (*profiling*), que produza efeitos jurídicos ou o afete significativamente de modo similar (UNIÃO EUROPEIA, 2016). Este artigo representa a primeira tentativa legislativa de mitigar os riscos da "tirania do algoritmo", garantindo um ponto de contestação para o indivíduo.

A estrutura do GDPR, embora fundamental e robusta, revelou suas limitações diante da crescente complexidade e opacidade dos sistemas de IA. O modelo de governança proposto é essencialmente reativo, ou seja, coloca o ônus sobre o indivíduo para contestar uma decisão após sua ocorrência. Exercer esse direito de forma eficaz pressupõe a capacidade de compreender a lógica da decisão, o que se torna uma barreira quase intransponível diante de modelos de "caixa-preta". Essa assimetria informacional e técnica evidenciou a necessidade de um novo paradigma regulatório, que deslocasse o foco da reparação individual *ex-post* para a governança sistêmica *ex-ante*.

O *Artificial Intelligence Act*, ou AI Act, aprovado pela União Europeia em 2024, materializa essa mudança de paradigma. Trata-se da primeira regulação horizontal e abrangente para a IA no mundo, estabelecendo um padrão global que influenciou, inclusive, o debate legislativo no Brasil. Sua inovação central é a adoção de uma abordagem proporcional baseada em risco, que impõe obrigações graduais conforme o potencial de dano de um sistema de IA à saúde, à segurança e aos direitos fundamentais. Essa metodologia permite regular estritamente as aplicações de alto impacto sem sufocar a inovação em áreas de baixo risco.

O AI Act da União Europeia também estabelece uma tipologia de quatro categorias de risco para sistemas de inteligência artificial, definindo diferentes níveis de restrição e obrigações regulatórias. Em primeiro lugar, enquadram-se no risco inaceitável as práticas consideradas incompatíveis com os direitos fundamentais e a segurança das pessoas, razão pela qual são terminantemente proibidas. Nessa categoria situam-se, por exemplo, os sistemas de pontuação social aplicados por governos, a manipulação cognitiva de indivíduos vulneráveis e a coleta indiscriminada de imagens faciais destinadas à formação de bases de dados de reconhecimento.

Em seguida, os sistemas de alto risco constituem o núcleo central da regulação, abrangendo aplicações cujo mau funcionamento pode gerar consequências graves, como no controle de tráfego aéreo, nos processos de recrutamento, na análise de crédito ou na administração da justiça. Para tais sistemas, o legislador europeu impõe um conjunto de exigências ex-ante, entre as quais se destacam: a implementação de gestão de riscos, a utilização de dados de treinamento de alta qualidade, a elaboração de documentação técnica auditável, a manutenção de *logs*[22] para rastreabilidade, a previsão de supervisão humana e a observância de elevados padrões de robustez, precisão e cibersegurança.

[22] Logs são registros automáticos e cronológicos de eventos ou operações realizadas por um sistema, armazenados para fins de rastreabilidade, auditoria, monitoramento de segurança e diagnóstico técnico.

Tratando dos sistemas de risco limitado, como *chatbots*[23] e *deepfakes*[24], não são proibidos, mas devem observar deveres de transparência. Nesse caso, importa informar ao usuário, de modo claro, que está interagindo com uma máquina ou diante de conteúdo gerado artificialmente, garantindo-lhe condições para uma decisão consciente.

Por fim, no nível de risco mínimo, encontram-se a maioria das aplicações de uso corrente, como filtros de spam e sistemas de recomendação em jogos eletrônicos. Embora isentos de obrigações legais específicas, tais sistemas são incentivados a aderir voluntariamente a códigos de conduta e boas práticas, de modo a reforçar a confiança pública no uso da inteligência artificial (UNIÃO EUROPEIA, 2024).

4.2 O Projeto de Lei nº 2.338/2023 no Brasil

O Brasil, seguindo a tendência internacional, busca construir seu próprio marco legal para a inteligência artificial. O PL nº 2.338/2023 representa o esforço mais consolidado nessa direção, propondo um modelo que, embora inspirado na experiência europeia, apresenta características próprias que refletem as particularidades do ecossistema tecnológico e jurídico nacional.

A estrutura do PL 2.338/2023 é explicitamente inspirada no modelo de risco do *AI Act* europeu. O projeto também classifica os sistemas de IA com base no risco, dedicando atenção especial aos sistemas de "alto risco". A definição de alto risco no texto do PL abrange finalidades análogas às do *AI Act*, como a aplicação em infraestruturas críticas, avaliação de crédito, elegibilidade para serviços públicos, recrutamento e seleção, e uso em atividades de persecução penal (INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO, 2025).

Para os sistemas de alto risco, o projeto estabelece um conjunto de deveres para os "agentes de inteligência artificial" (fornecedores e operadores), que incluem a adoção de medidas de governança, a realização de testes para garantir a confiabilidade e a segurança, e, notadamente, a elaboração de uma "avaliação de impacto algorítmico" antes da implementação do sistema. Além do mais, o PL estabelece um robusto rol de direitos para as pessoas afetadas pelos sistemas de IA, que expande e detalha as garantias já previstas na LGPD. (BRASIL, 2023).

---

[23] Chatbots são programas de computador baseados em inteligência artificial capazes de interagir com usuários por meio de linguagem natural, simulando diálogos humanos em interfaces de texto ou voz.

[24] Deepfakes são conteúdos sintéticos, geralmente imagens, áudios ou vídeos, que são gerados ou manipulados por técnicas de aprendizado profundo (*deep learning*), capazes de produzir representações altamente realistas, mas potencialmente enganosas.

Apesar das semelhanças estruturais, o PL brasileiro não é uma mera transposição do regulamento europeu. Uma análise comparativa detalhada revela uma adaptação deliberada do modelo, refletindo uma filosofia regulatória distinta. Uma das divergências mais significativas reside na distribuição de responsabilidades, pois enquanto o *AI Act* adota uma abordagem mais vertical, concentrando a maior parte das obrigações no fornecedor do serviço, o PL 2.338/2023 opta por uma estratégia mais horizontal. O texto brasileiro impõe um número maior de obrigações compartilhadas entre os diversos atores da cadeia de valor. mais ampla (INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO, 2025).

Essa "tropicalização" do modelo regulatório parece ser uma resposta estratégica à complexidade das cadeias de suprimento de tecnologia no Brasil. Ao tornar a responsabilidade mais coletiva, o legislador busca fechar brechas onde a responsabilização poderia ser diluída ou evadida, incentivando um maior nível de diligência em todo o ecossistema.

4.3 Agência Nacional de Proteção de Dados (ANPD)

A eficácia de qualquer marco regulatório depende de uma autoridade fiscalizadora com capacidade institucional, autonomia técnica e legitimidade. No Brasil, a ANPD emerge como a instituição central para a governança não apenas de dados, mas de todo o ecossistema digital, incluindo a inteligência artificial. Criada para zelar pela aplicação da LGPD, a ANPD viu seu escopo de atuação naturalmente se expandir para o campo da IA, dado que o funcionamento desses sistemas é intrinsecamente dependente do tratamento de dados pessoais. A Agência tem abraçado esse papel de forma proativa, e mesmo antes da aprovação de um marco legal específico para IA, a ANPD já vinha exercendo sua competência regulatória sobre o tema.

Em 2025, publicou a Nota Técnica nº 12, consolidando os resultados de uma tomada de subsídios sobre o Artigo 20 da LGPD (decisões automatizadas), sinalizando os caminhos para a futura regulamentação do tema. (AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS[25], 2023).

[25] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Nota Técnica nº 12/2025/CON1/CGN/ANPD. Consolidação das contribuições recebidas na Tomada de Subsídios sobre decisões automatizadas. Brasília, DF: ANPD, 2025.

O reconhecimento da expertise e da centralidade da ANPD culminou na proposta, contida no texto do PL 2.338/2023 aprovado pelo Senado, de designá-la como o órgão coordenador do futuro Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA). Essa escolha estratégica visa garantir a convergência regulatória entre a proteção de dados e a governança da IA, evitando a fragmentação de competências e a criação de sobreposições normativas que poderiam gerar insegurança jurídica (BRASIL, 2023).

Essa ampliação de mandato ocorre em um momento de fortalecimento institucional da própria ANPD, conforme a MP nº 1.317, que transformou a Autoridade Nacional de Proteção de Dados na Agência Nacional de Proteção de Dados. Essa mudança não é meramente nominal, pois ela consolida a ANPD como uma autarquia de natureza especial, nos moldes das demais agências reguladoras brasileiras, conferindo-lhe autonomia funcional, técnica, decisória, administrativa e financeira (BRASIL[26], 2025).

5 CONCLUSÃO

A trajetória analisada neste artigo demonstra uma transição inequívoca: da proteção de dados como um fim em si mesma para a governança de dados como o alicerce para uma regulação mais ampla e complexa da inteligência artificial. A LGPD inaugurou uma nova cultura de privacidade e responsabilidade no Brasil, mas a velocidade e a profundidade das transformações impulsionadas pela IA exigem uma arquitetura normativa e institucional mais sofisticada. A conclusão deste estudo sintetiza os principais achados, reitera as limitações do arcabouço atual e propõe um modelo integrado de *compliance* algorítmico como caminho para conciliar inovação tecnológica com a salvaguarda dos direitos fundamentais.

O presente estudo confirmou a hipótese central de que a LGPD, apesar de seu caráter principiológico e de sua importância como marco fundador, é estruturalmente insuficiente para endereçar os desafios únicos impostos pelos sistemas de inteligência artificial avançada. A opacidade algorítmica, o potencial de discriminação embutido nos modelos e a escala das ameaças à segurança da informação em um ecossistema de *big data* extrapolam o escopo de uma legislação de proteção de dados de caráter geral.

---

[26] BRASIL. *Medida Provisória nº 1.317, de 17 de setembro de 2025. Altera a Lei nº 13.709, de 14 de agosto de 2018, para tratar da Agência Nacional de Proteção de Dados, a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, transforma cargos no âmbito do Poder Executivo federal, e dá outras providências. Diário Oficial da União*, Brasília, DF, 18 set. 2025.

As limitações da LGPD frente à IA não residem em seus princípios, que permanecem válidos e essenciais, mas em seus instrumentos. O direito à revisão de decisões automatizadas, previsto no artigo 20, por exemplo, corre o risco de se tornar um "direito sem remédio" quando confrontado com a complexidade de modelos de *machine learning* do tipo "caixa-preta". A ausência de uma explicação inteligível sobre a lógica da decisão esvazia a capacidade do titular de contestá-la de forma substancialmente suficiente.

A perspectiva para o fortalecimento da governança de dados no Brasil reside, portanto, não na substituição da LGPD, mas em sua articulação sinérgica com o futuro marco legal da IA. O PL nº 2.338/2023 atuará como um instrumento de operacionalização dos princípios da LGPD no contexto algorítmico. Ele traduz conceitos abstratos como "não discriminação", "segurança" e "transparência" em requisitos concretos e auditáveis para sistemas de IA, como a exigência de avaliações de impacto algorítmico, a implementação de medidas para mitigação de vieses e a garantia de supervisão humana efetiva. O elo que garantirá a eficácia dessa sinergia é a ANPD. Consolidada como uma agência reguladora, de maneira recente, por meio da MP nº 1.317/2025 e designada como o órgão central de governança da IA, a ANPD terá a capacidade institucional para interpretar e aplicar ambos os marcos de forma coesa.

Para que as organizações naveguem com sucesso neste novo cenário regulatório, é imperativo abandonar abordagens fragmentadas de conformidade e adotar um modelo holístico de *compliance* algorítmico. Este modelo deve ser integrado e multifacetado, abrangendo as dimensões jurídica, organizacional e técnica, podendo ser dividido em 3 pilares.

O primeiro pilar refere-se à conformidade jurídico-regulatória unificada, segundo a qual as organizações devem desenvolver programas de *compliance* capazes de mapear e integrar as obrigações previstas tanto na LGPD quanto no futuro marco regulatório da inteligência artificial. Nesse ínterim, torna-se imprescindível que equipes jurídicas e de conformidade compreendam a intersecção entre os dois regimes normativos, e importa observar, por exemplo, que a exigência constante do PL de utilização de conjuntos de dados de treinamento de qualidade e representativos não constitui apenas um dever regulatório em matéria de IA, mas igualmente um meio de concretizar o princípio da qualidade dos dados previsto na LGPD (art. 6º, inciso V). De igual modo, a documentação técnica obrigatória para sistemas de alto risco deve ser estruturada de modo a servir também como evidência para o RIPD[27], ampliando a sinergia entre os instrumentos.

[27] RIPD é a sigla para Relatório de Impacto à Proteção de Dados Pessoais, instrumento previsto na LGPD (art. 38), destinado a documentar os riscos e medidas de mitigação relacionados ao tratamento de dados pessoais em atividades empresariais ou institucionais.

O segundo pilar está relacionado à governança organizacional e ética, evidenciando que a conformidade não pode restringir-se a uma função meramente legal, mas deve estar incorporada à estrutura decisória das instituições.

Sob essa ótica, propõe-se a constituição de comitês de ética em IA ou conselhos de revisão algorítmica, compostos de forma multidisciplinar e dotados de autoridade para aprovar, condicionar ou vetar projetos com base em avaliações que ultrapassem a estrita legalidade, contemplando aspectos éticos e de impacto social. Também sob essa perspectiva, o RIPD, já previsto na LGPD, deve evoluir para um relatório de impacto de IA mais abrangente, destinado a avaliar não apenas riscos à privacidade, mas também potenciais efeitos discriminatórios, manipulatórios ou outros danos a direitos fundamentais, em conformidade com a exigência de avaliação de impacto algorítmico constante do PL 2.338/2023.

O terceiro pilar, por sua vez, diz respeito aos controles técnicos e operacionais (*compliance by design*), responsáveis por traduzir os princípios jurídicos e éticos em práticas concretas, integrando a conformidade ao ciclo de vida do desenvolvimento tecnológico. Portanto, recomenda-se a adoção de *frameworks* internacionalmente reconhecidos, como o *AI RMF* do *NIST*, o qual fornece diretrizes para a implementação de controles operacionais.

Ao adotar essa abordagem integrada, as organizações transformarão o *compliance* de um exercício reativo e puramente legalista em uma função estratégica e proativa. A conformidade algorítmica, assim concebida, torna-se um pilar da inovação responsável, garantindo que o desenvolvimento tecnológico no Brasil avance em harmonia com os valores éticos e os direitos fundamentais que definem uma sociedade democrática.

REFERÊNCIAS

ALMADA, Marco; MARANHÃO, Juliano Souza de Albuquerque. Decisões automatizadas e o direito à revisão na Lei Geral de Proteção de Dados. *Revista de Direito Público da Economia – RDPE*, Brasília, v. 20, n. 106, p. 385-413, abr./jun. 2023.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Mapa de Temas Prioritários 2024-2025*. Brasília, DF: ANPD, 2023.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Análise Preliminar do Projeto de Lei nº 2.338/2023, que dispõe sobre o uso da Inteligência Artificial*. Brasília, DF: ANPD, 2023.

BRASIL. Congresso. Senado Federal. *Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial*. Brasília, DF: Senado Federal, 2023.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União*, Brasília, DF, 15 ago. 2018.

DAMA INTERNATIONAL. *DAMA DMBOK2 GUIDE*. DAMA International, 2020. Disponível em: https://opusmgt.files.wordpress.com/2020/04/dmbok-dama-overview-20200405.pdf. Acesso em: 18 set. 2025.

DIO. *Viés Algorítmico: Desafios, Problemas e Soluções na Inteligência Artificial*. DIO, 19 fev. 2025. Disponível em: https://www.dio.me/articles/vies-algoritmico-desafios-problemas-e-solucoes-na-inteligencia-artificial. Acesso em: 21 set. 2025.

DONEDA, D.; ALMEIDA, V. What Is Algorithm Governance? IEEE Internet Computing, [s.l.], v. 20, n. 4, p. 60-63, jul./ago. 2016. Disponível em: https://www.computer.org/csdl/magazine/ic/2016/04/mic2016040060/13rRUyekJ2d. Acesso em: 7 jul. 2025.

FENATI. *Maior vazamento de dados da história*. Fenati, 2024. Disponível em: https://fenati.org.br/maior-vazamento-de-dados-da-historia/. Acesso em: 19 set. 2025.

FIA. *Vazamento de dados: o que é, riscos, tipos e como evitar*. FIA, 2025. Disponível em: https://fia.com.br/blog/vazamento-de-dados/. Acesso em: 23 set. 2025.

IADB. *Auditoria algorítmica para sistemas de tomada de decisão ou suporte à decisão*. Banco Interamericano de Desenvolvimento, 2022. Disponível em: https://publications.iadb.org/publications/portuguese/document/Auditoria-algoritmica-para-sistemas-de-tomada-de-decis%C3%A3o-ou-suporte-a-decis%C3%A3o.pdf. Acesso em: 19 set. 2025.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO (ITS Rio). *Matriz comparada de obrigações: PL 2338/2023 vs. EU AI act*. Rio de Janeiro: ITS Rio, 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *AI Risk Management Framework (AI RMF 1.0).* Gaithersburg: NIST, 2023.

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2016.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). *Agravo em Recurso Especial nº 2.130.619.* Relator: Ministro Francisco Falcão. Brasília, DF, 2023.

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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia*, L 119/1, 4 maio 2016.

UNIÃO EUROPEIA. *Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial).* Bruxelas, 2024.