III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I

T255
Tecnologias disruptivas, direito e proteção de dados I [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Cildo Giolo Junior, Fausto Santos de Morais e Suelen Carls – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-417-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Governança, regulação e o futuro da inteligência artificial.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I

Apresentação

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 3 discute os impactos das tecnologias destrutivas no campo jurídico, com foco na aplicação da Lei Geral de Proteção de Dados e nas novas fronteiras da privacidade digital. As apresentações analisam o papel da inovação, da transparência e da responsabilidade jurídica em contextos digitais complexos. O grupo contribui para o debate sobre como a tecnologia pode ser aliada na proteção da dignidade humana e da segurança informacional.

DESAFIOS DA LGPD FRENTE À INTELIGÊNCIA ARTIFICIAL: OPACIDADE ALGORÍTMICA E CAMINHOS PARA O COMPLIANCE

THE CHALLENGES OF BRAZIL'S LGPD IN THE AGE OF ARTIFICIAL INTELLIGENCE: ALGORITHMIC OPACITY AND REGULATORY COMPLIANCE STRATEGIES

Tiago de Lima Mascarenhas Santos [1]
Jéssica Fachin [2]
Álvaro Campelo Fonseca [3]

Resumo

A Lei Geral de Proteção de Dados Pessoais (LGPD) trouxe avanços significativos à proteção de dados no Brasil, mas enfrenta desafios diante da complexidade dos sistemas de inteligência artificial (IA). Este artigo analisa as limitações da LGPD frente à opacidade algorítmica e propõe o compliance algorítmico como estratégia essencial à transparência e à conformidade. Examina-se o Projeto de Lei nº 2.338/2023, inspirado no AI Act europeu, e sua relevância na regulação da IA. Também são discutidos frameworks de governança de dados como o DAMA-DMBOK e o COBIT, fundamentais para assegurar proteção, ética e responsabilidade no ambiente digital.

Palavras-chave: Lgpd, Inteligência artificial, Opacidade algorítmica, Governança de dados, Compliance algorítmico

Abstract/Resumen/Résumé

The Brazilian General Data Protection Law (LGPD) marked significant progress in data protection but faces limitations amid the complexity of artificial intelligence (AI) systems. This article analyzes LGPD's shortcomings regarding algorithmic opacity and highlights algorithmic compliance as a key strategy for ensuring transparency and legal conformity. It examines Bill No. 2,338/2023, inspired by the European AI Act, as a step toward AI regulation in Brazil. Additionally, it discusses data governance frameworks such as DAMA-DMBOK and COBIT, which are essential for promoting data protection, ethics, and accountability within digital environments increasingly influenced by automated decision-making.

Keywords/Palabras-claves/Mots-clés: Lgpd, Artificial intelligence, Algorithmic opacity, Data governance, Algorithmic compliance

---

[1] Estudante de graduação em Direito pela Universidade de Brasília (UnB).

[2] Em estágio pós-doutoral na UnB. Doutora em Direito Constitucional pela PUCSP, mestre em ciência jurídica pela UENP. Especialista em Direito Constitucional Contemporâneo e Direito Processual Civil pelo IDCC.

[3] Estudante de graduação em Direito pela Universidade de Brasília (UnB).

1. Introdução

A ascensão da inteligência artificial (IA) tem transformado profundamente o ecossistema digital, promovendo a automatização de decisões e o uso massivo de dados pessoais em plataformas digitais. Esses sistemas, alimentados por algoritmos complexos, operam frequentemente de forma opaca, dificultando a identificação dos critérios utilizados nas decisões automatizadas e ampliando os riscos de violações à privacidade, discriminações e vazamentos de dados.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD) representou um avanço normativo relevante ao estabelecer princípios e garantias para o tratamento de dados no Brasil. No entanto, a sofisticação técnica das tecnologias baseadas em IA tem evidenciado as limitações da LGPD frente à realidade dos sistemas algorítmicos, exigindo a adoção de mecanismos complementares de governança e responsabilização.

A proposta do *compliance* algorítmico surge como resposta a essa lacuna, buscando assegurar que as soluções baseadas em IA operem em conformidade com os marcos legais, princípios éticos e padrões de transparência. Ferramentas como o *EU AI Act Compliance Checker*, inspiradas no *AI Act* europeu, ilustram caminhos viáveis para o monitoramento preventivo da conformidade algorítmica e oferecem subsídios importantes para o debate regulatório no Brasil.

2. Problema de pesquisa

Diante do avanço dos sistemas de inteligência artificial e da crescente opacidade nas decisões automatizadas, em que medida a Lei Geral de Proteção de Dados Pessoais (LGPD) é suficiente para garantir a proteção dos direitos fundamentais dos indivíduos no contexto do uso massivo de dados por sistemas de IA, e quais mecanismos regulatórios e de governança podem ser adotados para suprir suas limitações?

3. Objetivos

O presente artigo tem como objetivo principal analisar os desafios e limitações da Lei Geral de Proteção de Dados Pessoais (LGPD) frente à crescente complexidade dos sistemas de inteligência artificial (IA), bem como discutir a necessidade de um marco regulatório específico que aborde os riscos e impactos sociais decorrentes do uso massivo e automatizado de dados pessoais.

Além disso, o artigo pretende: investigar os riscos associados à opacidade algorítmica e ao vazamento de dados em sistemas de IA; discutir a importância do compliance algorítmico

como instrumento para garantir a transparência, a auditabilidade e a conformidade legal das decisões automatizadas; apresentar frameworks consolidados de governança de dados, como o DAMA-DMBOK e o COBIT, e sua relevância na estruturação de políticas internas e controles organizacionais eficazes; e propor uma abordagem integrada que combine medidas legais, técnicas e organizacionais para o fortalecimento da governança de dados no Brasil.

Ao cumprir esses objetivos, o artigo busca contribuir para o debate sobre a construção de um ecossistema digital ético, seguro e comprometido com a proteção dos direitos fundamentais dos indivíduos no contexto da inteligência artificial.

4. Método

O presente estudo adota uma abordagem qualitativa, com método de pesquisa dedutivo e caráter exploratório-descritivo. Foram utilizados procedimentos de pesquisa bibliográfica e documental, a partir da análise de marcos normativos, estudos acadêmicos e diretrizes internacionais sobre inteligência artificial e proteção de dados. Também foram examinados casos emblemáticos de vazamento de dados que evidenciam falhas de *compliance* e ausência de controle sobre algoritmos utilizados em plataformas digitais.

5. Discussão

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) representou um importante marco regulatório no Brasil, ao estabelecer princípios e direitos fundamentais no tratamento de dados pessoais. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD trouxe inovações como o direito à portabilidade, à exclusão de dados e à revisão de decisões automatizadas, como previsto em seu art. 20.

Entretanto, os sistemas de inteligência artificial (IA) trouxeram à tona uma nova realidade quanto ao uso de dados pessoais, principalmente pela potencialização dos algoritmos, que são definidos como um conjunto de códigos destinados à realização de uma tarefa, utilizando dados de entrada (*inputs*) para gerar resultados (*outputs*), que são traduzidos como recomendações nas redes sociais, por exemplo (DONEDA; ALMEIDA, 2016). A utilização massiva desses sistemas em plataformas digitais amplia significativamente a coleta e o tratamento de dados pessoais, muitas vezes de forma automatizada e sem a devida transparência quanto aos critérios envolvidos nas decisões.

Essa dinâmica desafia a estrutura da LGPD, devido a chamada opacidade algorítmica (ou "caixa-preta" da IA)[1], que torna difícil identificar quem é o responsável pelas decisões e como elas são tomadas, o que compromete o princípio da autodeterminação informativa, estabelecido no art. 2°, inciso II da LGPD.

Embora a LGPD represente um avanço fundamental, cresce a percepção de que ela não é suficiente para regular os riscos e impactos sociais da inteligência artificial. Isso tem motivado o debate em torno da criação de um novo marco legal específico para a IA no Brasil, atualmente em discussão por meio do Projeto de Lei nº 2338/2023, em tramitação na Câmara dos Deputados, inspirado no *AI Act*[2] (2024) que classifica os sistemas de IA em diferentes categorias de riscos e impõe requisitos para a implementação das chamadas "IAs de alto risco".

Nesse contexto, o texto do Projeto de Lei nº 2338/2023 propõe avanços importantes na proteção dos direitos dos indivíduos diante dos impactos gerados por sistemas de inteligência artificial. Dentre os dispositivos previstos, o Art. 5º delineia um conjunto de direitos fundamentais aplicáveis às pessoas ou grupos afetados, independentemente do grau de risco da tecnologia envolvida.

Nesse diapasão, surge a discussão acerca dos riscos de vazamento de dados em decorrência dessa utilização desenfreada de dados pessoais. Recentemente, pesquisadores da Cybernews identificaram o que pode ser considerado o maior vazamento de dados da história, expondo cerca de 16 bilhões de credenciais de login e senhas de usuários vinculados a plataformas como Apple, Google, Facebook, Telegram, GitHub, além de serviços governamentais (FORBES, 2025). As consequências incluem desde *phishing*[3] altamente segmentado até invasões automatizadas em contas, pois os dados seguem o padrão "URL + login + senha", facilitando os ataques.

---

[1] A opacidade algorítmica refere-se à dificuldade ou impossibilidade de compreender como determinados algoritmos tomam decisões, seja pela complexidade técnica dos modelos (como redes neurais profundas), pela falta de transparência dos desenvolvedores ou pela ausência de mecanismos legais que garantam o direito à explicação. Essa "caixa-preta" tecnológica compromete a accountability e impede que os indivíduos afetados compreendam ou contestem decisões automatizadas, especialmente quando envolvem impactos significativos sobre seus direitos. (PASQUALE, 2016.)

[2] O AI Act é o regulamento da União Europeia sobre inteligência artificial, aprovado em 2024, que estabelece um marco legal para o desenvolvimento, comercialização e uso de sistemas de IA no território europeu. A norma classifica os sistemas de IA conforme o grau de risco e impõe obrigações específicas, sobretudo para as chamadas IAs de alto risco, como transparência, supervisão humana, gerenciamento de dados e documentação técnica. O objetivo central do AI Act é garantir que as tecnologias de IA respeitem os direitos fundamentais, a segurança e a confiança dos cidadãos europeus (UNIÃO EUROPEIA, 2024).

[3] Phishing é uma técnica de engenharia social utilizada por cibercriminosos para enganar usuários e induzi-los a fornecer dados sensíveis, como senhas, números de cartões de crédito ou informações bancárias. Normalmente, essas fraudes ocorrem por meio de mensagens falsas que imitam comunicações legítimas de empresas, bancos ou instituições públicas, redirecionando as vítimas para sites falsos que coletam seus dados sem consentimento (CERT.br, 2023).

Frente a esse cenário, a adoção do *compliance* algorítmico surge como medida estratégica essencialíssima, na medida em que se trata de um conjunto de diretrizes, práticas e mecanismos que visam assegurar a conformidade operacional dos sistemas de inteligência artificial com a legislação vigente, mantendo padrões éticos e transparentes, e preservando o direito à auditabilidade. Isso inclui a adoção do princípio do *privacy by design*[4] até a implementação dos processos de explicabilidade algorítmica, permitindo a verificação das decisões automatizadas por partes interessadas e órgãos reguladores.

Para a efetivação do *compliance* algorítmico, são necessárias ações integradas, tais como:

- Prévia de riscos: análise e resolução de potenciais riscos de vazamento dos dados e violações à privacidade;
- Mapeamento do fluxo de dados: compreensão das cadeias operacionais, por onde são transmitidos e utilizados os dados pessoais, transparecendo todas as partes por onde os dados confluem e permitindo a prevenção de riscos;
- Mitigação de viés: evitar que quaisquer conteúdos gerados possam, em alguma medida, demonstrar alguma percepção particular, de modo a operar os dados de modo imparcial;
- Auditorias técnicas, revisão periódica dos modelos e capacitação constante das equipes envolvidas: este tripé garante a segurança e a concomitância dos mecanismos e procedimentos de um determinado sistema com a legislação vigente (WEHANDLE, 2023)

Em paralelo, faz-se mister discutir os caminhos para fortalecer a governança de dados, havendo um comprometimento da alta gestão, por via da definição clara de papéis e responsabilidades e a possibilidade da rastreabilidade dos dados utilizados. Todos esses pontos precisam estar sujeitos à padrões internacionais consagrados, como o *FAIR (Findable, Accessible, Interoperable, Reusable* - no português - Localizável, acessível, interoperável, reutilizável)[5], garantindo o uso ético e salutar dos dados (GOV.BR, 2024). Alguns determinados *Frameworks*[6] estruturados de governança oferecem diretrizes e premissas das

[4] Privacy by design é o conceito de se desenvolver programas cuja operação e funcionalidade tenha a privacidade como preceito fundamental, bem como a preservação da privacidade durante todo o ciclo de vida dos dados pessoais (TERRACAP, 2025).
[5] Os princípios FAIR surgem durante a conferência "Jointly Designing a Data FAIRPORT", nos países baixos, ocorrida em 2014, e foram publicados em 2016, com o objetivo de fornecer um guia para a gestão de dados, valorizando a identificação, acessibilidade, qualificação e pluralidade dos atributos de um determinado dado (UCOIMBRA, 2025).
[6] Frameworks são estruturas de trabalho que embasam a construção de softwares de maneira eficiente, via modulação, padronização e ferramentas de desenvolvimento (EBAC, 2023).

quais parte-se a gestão de dados corporativos e, conformidade com objetivos estratégicos e exigências normativas. É o caso do *DAMA-DMBOK* e do *COBIT*.

- *DAMA-DMBOK (Data Management Body of Knowledge)*

Centrado em 11 áreas de conhecimento reunidas, a utilidade do mecanismo reside em possibilitar a formalização de políticas e papéis, assim como assegurar um certo grau de consistência normativa no tratamento de dados pessoais, em conformidade com legislações como a LGPD e a GDPR. (DAMA INTERNATIONAL, 2017)

- *COBIT (Control Objectives for Information and Related Technologies)*

Diferentemente do *DAMA-DMBOK*, cuja especificidade são os dados propriamente ditos, o COBIT amplia suas funções ao se orientar por metas de valor e riscos empresariais. “Avaliar, Dirigir e Monitorar” e “Planejar e Construir" são os domínios utilizados por este *framework* para formular seus objetivos com efeitos estratégicos e alinhamento às legislações e regulações vigentes. (ISACA, 2018).

A existência de *frameworks* consolidados demonstra uma resposta das empresas de tecnologia em se adequarem à modelos de governança de dados que garantam transparência e redução de riscos. A GDPR desempenhou uma missão de ser uma legislação inovadora, da qual não apenas outras legislações se derivaram, como no caso da LGPD, mas começou-se a debater de maneira mais proeminente a maneira de certa forma “obscura” com a qual as empresas de tecnologia manejam os dados, e ainda o fazem.

6. Resultados

A análise realizada demonstrou que os mecanismos atualmente previstos na Lei Geral de Proteção de Dados Pessoais (LGPD) apresentam limitações relevantes diante da crescente complexidade dos sistemas de inteligência artificial (IA). Nesse contexto, o Projeto de Lei nº 2.338/2023 revelou-se um importante avanço no enfrentamento dessas lacunas normativas, ao propor um conjunto de direitos fundamentais aplicáveis a qualquer pessoa impactada por sistemas de IA, independentemente do grau de risco envolvido. No entanto, a concretização dessas garantias dependerá da construção de uma estrutura de governança algorítmica sólida, capaz de viabilizar o cumprimento efetivo das normas propostas.

A investigação demonstrou, ainda, que a efetividade do *compliance* algorítmico vai além do mero atendimento formal às exigências legais. É imprescindível que ele seja sustentado por processos técnicos bem definidos. Nesse sentido, a adoção de *frameworks* internacionais como o DAMA-DMBOK e o COBIT revela-se essencial.

Adicionalmente, o estudo do *AI Act*, evidenciou uma abordagem regulatória significativamente mais avançada. O regulamento impõe obrigações rígidas, como a implementação de sistemas internos de gestão da qualidade, a certificação de produtos por meio da marcação CE[7], a produção de documentação técnica auditável e a atuação ativa de autoridades reguladoras nacionais e europeias. Soma-se a isso a previsão de sanções expressivas em caso de descumprimento, que podem alcançar até 35 milhões de euros ou 7% do faturamento anual da empresa infratora. A introdução de instrumentos práticos, como o sistema obrigatório de avaliação e gestão da conformidade, consolida a natureza vinculante do *compliance* algorítmico e institui um modelo de supervisão ativa e contínua.

Por fim, conclui-se que o fortalecimento da governança de dados no Brasil requer uma abordagem verdadeiramente integrada, que combine medidas legais, organizacionais e tecnológicas. Isso implica, entre outros pontos, a definição clara de papéis e responsabilidades, a estruturação de políticas internas de controle, a criação de repositórios seguros e organizados, o uso de métricas de maturidade e o investimento em infraestrutura interoperável. Apenas com essa base robusta será possível concretizar as promessas normativas do *compliance* algorítmico e assegurar, de forma efetiva, a proteção dos direitos fundamentais no ambiente digital.

7. Referências

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 17 de março de 2025. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília: Senado Federal, 2025. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 7 jul. 2025.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. *Phishing e outros golpes*. São Paulo: CERT.br, 2023. Disponível em: https://cartilha.cert.br/fasciculos/#phishing-golpes. Acesso em: 7 jul. 2025.

DAMA INTERNATIONAL. DAMA-DMBOK: Data Management Body of Knowledge. 2. ed. New Jersey: Technics Publications, 2017.

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:

[7] Marcação *CE*, ou *Conformité Européenne*, é uma marca que os fabricantes e fornecedores de produtos e serviços utilizam para indicar que um produto cumpre as normas de conformidade legal relevantes da União Europeia (UE) em termos de segurança, saúde e proteção ambiental. O sistema é aplicável a todo o Espaço Econômico Europeu e só se aplica aos produtos abrangidos pela legislação da UE que requer a aposição da marcação CE (EUR-LEX, 2008).

https://www.computer.org/csdl/magazine/ic/2016/04/mic2016040060/13rRUyekJ2d. Acesso em: 7 jul. 2025.

EBAC. Framework SEO: O que é, como usar e principais ferramentas. EBAC Online, 2023. Disponível em: https://ebaconline.com.br/blog/framework-seo. Acesso em: 7 jul. 2025.

EU ARTIFICIAL INTELLIGENCE ACT COMPLIANCE CHECKER. Disponível em: https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/. Acesso em: 8 jul. 2025.

FORBES BRASIL. *Maior vazamento de dados da história expõe 16 bilhões de senhas – e o mundo quase não percebeu*. 25 jun. 2025. Disponível em: https://forbes.com.br/forbes-tech/2025/06/maior-vazamento-de-dados-da-historia-expoe-16-bilhoes-de-senhas-e-o-mundo-quase-nao-percebeu/. Acesso em: 5 jul. 2025.

GOVERNO FEDERAL. Governança de Dados - Estratégia de Governo Digital. Governo Digital – gov.br, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados. Acesso em: 7 jul. 2025.

ISACA. COBIT 2019 Framework: Governance and Management Objectives. Rolling Meadows: ISACA, 2018.

PASQUALE, Frank. *The black box society: the secret algorithms that control money and information*. Cambridge, MA: Harvard University Press, 2016.

TERRACAP. O que é Privacy by Design e Privacy by Default? Agência de Desenvolvimento do Distrito Federal, 2023. Disponível em: https://www.terracap.df.gov.br/index.php/listagem-faq/78-lgpd-lei-geral-de-protecao-de-dados-pessoais/196-53-o-que-e-privacy-by-design-e-privacy-by-default. Acesso em: 7 jul. 2025.

UNIVERSIDADE DE COIMBRA. Princípios FAIR. UC Open Science, 2023. Disponível em: https://www.uc.pt/openscience/sobre/acesso-aberto/fair/#:~:text=Os%20Princ%C3%ADpios%20FAIR%20foram%20publicados,do%20ecossistema%20da%20Ci%C3%AAncia%20Aberta. Acesso em: 7 jul. 2025.

UNIÃO EUROPEIA. Marcação CE. EUR-Lex, [s.d.]. Disponível em: https://eur-lex.europa.eu/PT/legal-content/glossary/ce-marking.html. Acesso em: 8 jul. 2025.

UNIÃO EUROPEIA. Regulation (EU) 2024/1689 [...] (Artificial Intelligence Act). *Official Journal of the European Union*, L 2024/1689, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689. Acesso em: 7 jul. 2025.

WEHANDLE. Compliance e machine learning: uma revolução na gestão de riscos. *Blog Wehandle*, 2023. Disponível em: https://wehandle.com.br/blog/compliance-e-machine-learning-uma-revolucao-na-gestao-de-riscos/. Acesso em: 7 jul. 2025.