INTELIGÊNCIA ARTIFICIAL E PROTEÇÃO DE DADOS: DESAFIOS REGULATÓRIOS À LUZ DA LGPD

Arthur Perussini Viana[1]

Augusto Martins de Jesus[2]

RESUMO: O presente artigo analisa os desafios jurídicos decorrentes do avanço da inteligência artificial (IA), com foco na proteção de dados pessoais e na necessidade de estruturar mecanismos regulatórios capazes de acompanhar tecnologias de aprendizado de máquina. Examina-se, ainda, o caso do bloqueio temporário do ChatGPT na Itália, ocorrido em 2023, como estudo de caso útil para compreender os limites e possibilidades de aplicação da Lei Geral de Proteção de Dados (LGPD) no Brasil. A partir de uma análise teórico-dogmática e do exame de precedentes nacionais e internacionais, identificam-se lacunas regulatórias, tensões com direitos fundamentais e barreiras para a fiscalização das decisões automatizadas. O estudo conclui que a IA demanda uma regulação flexível, interdisciplinar e dinâmica, capaz de mitigar riscos e fortalecer a autonomia informacional dos titulares. Por fim, aponta-se que o tema permanece aberto a investigações futuras, dada sua complexidade e constante evolução tecnológica.

Palavras-chave: Inteligência Artificial. Proteção de Dados. Regulação Algorítmica. LGPD. GDPR.

INTRODUÇÃO

O crescimento acelerado da inteligência artificial (IA) transformou profundamente a sociedade contemporânea, ampliando a eficiência de processos, a automação de tarefas e a capacidade de análise de grandes volumes de dados. No campo jurídico, tais inovações têm provocado impactos significativos, sobretudo no que diz respeito à proteção de dados pessoais, à transparência das decisões automatizadas e à responsabilidade derivada de sistemas autônomos. Diante desse cenário, surge a necessidade de repensar instrumentos normativos, institucionais e doutrinários para garantir que a evolução tecnológica esteja alinhada aos direitos fundamentais e aos valores do Estado Democrático de Direito.

[1] Graduando em Direito pela Fundação Educacional de Fernandópolis (FEF).E-mail: arthurperussini@gmail.com

[2] Professor da Fundação Educacional de Fernandópolis (FEF), onde atua como orientador acadêmico. Mestre em Jornalismo pela Universidade Estadual de Ponta Grossa. Bacharel em Jornalismo pela Universidade do Estado de Minas Gerais, em Direito pelo Centro Universitário de Votuporanga (Unifev) e em Publicidade e Propaganda pela Cruzeiro do Sul Virtual (Universidade de Franca – Unifran). Especialista em Lei Geral de Proteção de Dados e em Direito Público (Faculdade Legale). E-mail: augustodejesus@fef.edu.br

O objeto deste estudo consiste em analisar os desafios jurídicos emergentes da utilização de sistemas de IA, com destaque para o tratamento de dados pessoais e a regulação de decisões automatizadas. Para tanto, examina-se de forma aprofundada o caso do bloqueio temporário do ChatGPT na Itália, ocorrido em 2023, como exemplo emblemático da aplicação do Regulamento Geral de Proteção de Dados (GDPR) a modelos generativos. Trata-se de um caso que demonstra como autoridades reguladoras europeias têm buscado enfrentar riscos decorrentes de tecnologias que aprendem de modo contínuo, operam com opacidade e apresentam potencial de impacto massivo na esfera informacional dos usuários.

A justificativa da pesquisa reside na atualidade e relevância do tema. A IA deixou de ser um fenômeno futurista e tornou-se elemento estruturante de políticas públicas, relações sociais, práticas empresariais e processos jurisdicionais. No Brasil, a ausência de uma legislação específica sobre IA faz com que a LGPD desempenhe função central na regulação de sistemas automatizados. Assim, compreender seus limites e potencialidades torna-se fundamental para garantir segurança jurídica, promover proteção efetiva aos titulares e orientar o desenvolvimento ético e responsável de novas tecnologias. Além disso, os debates internacionais, especialmente no âmbito da OCDE, da UNESCO e da União Europeia, evidenciam que o país precisa alinhar-se a padrões globais de governança digital.

A problemática que orienta esta investigação pode ser sintetizada na seguinte pergunta: de que maneira o ordenamento jurídico brasileiro, especialmente por meio da LGPD, pode enfrentar os desafios impostos pelos sistemas de inteligência artificial, garantindo transparência, responsabilidade e proteção dos dados pessoais? A resposta a essa questão envolve a análise de lacunas normativas, requisitos de governança, instrumentos de fiscalização e os riscos associados a decisões algorítmicas opacas.

Para orientar a discussão, o estudo adota os seguintes objetivos: a) examinar os principais desafios jurídicos relacionados à regulação da IA; b) analisar o papel da proteção de dados pessoais como mecanismo de controle e responsabilização; c) investigar o caso do bloqueio do ChatGPT na Itália e suas possíveis lições para o Brasil; d) avaliar a capacidade da LGPD de prevenir abusos, garantir direitos e promover governança algorítmica.

A pesquisa apresenta caráter qualitativo, de natureza teórico-dogmática, fundamentada em bibliografia especializada e em documentos normativos nacionais e internacionais. Seu alcance abrange a compreensão de como sistemas de IA, ao operarem de forma opaca e autônoma, desafiam estruturas jurídicas tradicionais, exigindo respostas normativas adaptativas e multidisciplinares. A estrutura do trabalho organiza-se em três capítulos principais. O primeiro analisa os desafios jurídicos da regulação da IA, abordando lacunas

normativas, problemas de responsabilidade civil, impactos éticos e tensões com direitos fundamentais. O segundo capítulo trata da relação entre IA e proteção de dados pessoais, destacando princípios, riscos, deveres dos agentes de tratamento e limites da transparência algorítmica. O terceiro capítulo apresenta o estudo de caso do bloqueio do ChatGPT na Itália, examinando as medidas impostas pelo regulador europeu e discutindo possíveis implicações para a aplicação da LGPD no Brasil. Ao final, apresentam-se as considerações finais, que sintetizam os achados da pesquisa e indicam caminhos para estudos futuros.

1. INTELIGÊNCIA ARTIFICIAL, COMPLEXIDADE E LACUNAS NORMATIVAS: TENSÕES CONTEMPORÂNEAS DO DIREITO

O avanço da tecnologia de inteligência artificial (IA) tem introduzido novas questões jurídicas que desafiam profundamente a aplicação das normas existentes. A rápida evolução desses sistemas cria lacunas significativas no marco regulatório contemporâneo, dificultando a adaptação das estruturas legais tradicionais. Como observa Mireille Hildebrandt (2016), o Direito moderno foi construído com base na previsibilidade e na racionalidade humana, ao passo que a IA opera com lógica probabilística e aprendizado adaptativo, características que tensionam os modelos regulatórios clássicos. Assim, normas formuladas para realidades estáveis muitas vezes não contemplam peculiaridades da IA, como autonomia decisória, mutabilidade algorítmica e aprendizado contínuo. A falta de legislação específica compromete a interpretação e implementação das normas, ocasionando uma aplicação imprecisa e, por vezes, insuficiente.

A lacuna regulatória se manifesta concretamente em diferentes cenários. O uso de IA na previsão de sentenças e apoio a decisões judiciais, por exemplo, enfrenta dificuldades devido à ausência de transparência no processo decisório algorítmico. Como destaca Frank Pasquale (2015), sistemas opacos, as chamadas black box algorithms, operam sem explicitar suas lógicas internas, inviabilizando a auditabilidade e dificultando a compatibilização com princípios jurídicos como motivação e devido processo legal. Em outro campo, veículos autônomos expõem lacunas nas normas de trânsito, que não preveem a responsabilização em acidentes decorrentes de decisões tomadas por sistemas autônomos, evidenciando o descompasso entre inovação tecnológica e ordenamento jurídico.

A dificuldade em acompanhar o ritmo acelerado do desenvolvimento tecnológico torna evidente a necessidade de revisão urgente das leis. Bruno Bioni (2021) ressalta que a proteção de dados pessoais deve ser entendida como mecanismo de governança da

informação, especialmente em um contexto de opacidade algorítmica e assimetrias informacionais crescentes. Assim, normas criadas para outros contextos exigem reinterpretação e atualização, o que se torna ainda mais complexo devido ao caráter global da IA. A atuação de empresas transnacionais e a circulação internacional de dados impõem desafios adicionais de coordenação regulatória, agravados pela diversidade de interpretações jurídicas entre diferentes países, como observa Luciano Floridi (2018) ao discutir a necessidade de ecossistemas regulatórios harmonizados.

A insegurança jurídica resultante dessas lacunas compromete políticas públicas e dificulta a construção de um marco regulatório robusto. Em muitos casos, sistemas legais vigentes não possuem mecanismos adequados para lidar com consequências de ações autônomas da IA, especialmente quando danos decorrem de decisões tomadas sem intervenção humana direta. A evolução contínua das tecnologias torna difícil definir responsabilidades legais, gerando o que Andrew Selbst e Solon Barocas (2018) chamam de problema da responsabilidade algorítmica, em que a causalidade se fragmenta entre desenvolvedores, datasets, operadores e modelos autônomos.

O uso de IA no processamento de dados pessoais é outro exemplo relevante. Algoritmos utilizados por empresas de tecnologia para segmentação comportamental apresentam desafios à aplicação da Lei Geral de Proteção de Dados (LGPD). A capacidade adaptativa dos modelos dificulta o controle sobre finalidades, bases legais e compatibilidade de tratamentos sucessivos. Danilo Doneda (2019) já alertava que a autodeterminação informativa depende da clareza sobre fluxos de dados, algo comprometido quando algoritmos evoluem sem intervenção humana clara.

A complexidade das tecnologias de IA exige normas flexíveis e eficazes. A adaptação normativa pressupõe processo contínuo de revisão e diálogo entre Direito e tecnologia, o que nem sempre acompanha a velocidade das inovações. Além disso, a falta de conhecimento técnico adequado entre legisladores e reguladores compromete a elaboração de dispositivos eficientes. Kate Crawford (2021) aponta que a governança algorítmica envolve conhecimentos interdisciplinares que ultrapassam o escopo jurídico tradicional, demandando cooperação intensa com cientistas de dados e engenheiros de software.

O contexto internacional agrega desafios adicionais. A ausência de uniformidade nas abordagens regulatórias entre países gera fragmentação normativa, impondo custos operacionais e jurídicos a empresas que atuam globalmente. Organismos internacionais, como a OCDE e a UNESCO (2021), defendem a construção de princípios universais para orientar o uso ético da IA, mas a implementação concreta ainda é incipiente. Sem harmonização

mínima, conflitos entre legislações nacionais tendem a se intensificar.

O monitoramento das práticas de IA enfrenta obstáculos decorrentes da própria dinâmica da tecnologia. Sistemas que aprendem continuamente tornam obsoletos mecanismos estáticos de fiscalização. Para Virgílio Almeida e Ana Paula Bialer (2020), a governance-by-design, isto é, mecanismos de governança incorporados desde o desenvolvimento — é indispensável para garantir controle efetivo.

A atribuição de responsabilidade civil em danos causados por sistemas autônomos representa outro ponto crítico. Modelos tradicionais de culpa e nexo causal nem sempre se adequam a agentes artificiais parcialmente imprevisíveis. A literatura internacional, incluindo autores como Ryan Calo (2015), destaca a necessidade de repensar categorias clássicas de imputação em contextos de autonomia algorítmica.

A evolução tecnológica exige, portanto, uma regulação flexível e adaptativa. Sistemas de IA modificam seu comportamento ao longo do tempo, dificultando previsões normativas amplas e exigindo mecanismos de revisão periódica. A eficácia regulatória dependerá da superação das barreiras identificadas e da criação de normas capazes de equilibrar inovação e proteção de direitos fundamentais. A colaboração entre juristas, engenheiros, entidades reguladoras e organismos internacionais será essencial para esse processo.

A regulação da IA enfrenta, em suma, desafios significativos decorrentes de sua rápida evolução, complexidade técnica e impacto transversal sobre diferentes setores. A construção de um marco regulatório eficaz demanda revisão constante das normas e coordenação multissetorial, garantindo que a inovação ocorra em consonância com valores jurídicos essenciais, como segurança, responsabilidade, transparência e proteção de dados pessoais.

2. PRIVACIDADE E DECISÕES ALGORÍTMICAS: ENSAIOS SOBRE A APLICAÇÃO DA LGPD

O uso de inteligência artificial (IA) para o processamento de dados pessoais apresenta desafios significativos relacionados à privacidade e à proteção dos direitos dos indivíduos. A coleta e o tratamento automatizado dessas informações podem gerar riscos à autodeterminação informativa, especialmente quando não há transparência sobre as finalidades envolvidas. Como observa Danilo Doneda (2019), a proteção de dados pessoais é um instrumento essencial para assegurar que o titular mantenha controle sobre seus fluxos informacionais, o que se torna particularmente complexo em ambientes altamente automatizados.

O consentimento, tradicionalmente considerado um dos principais fundamentos jurídicos para o tratamento de dados, encontra novos limites diante da utilização de algoritmos de aprendizado de máquina. A complexidade técnica dos modelos torna mais difícil garantir que o consentimento seja realmente livre, informado e específico. Bruno Bioni (2021) destaca que, em sistemas automatizados, o consentimento perde eficácia quando o titular não compreende plenamente como seus dados serão utilizados ou quando há reuso para finalidades não originalmente informadas. A capacidade da IA de modificar autonomamente seus critérios de análise amplia esse risco.

A transparência, princípio basilar tanto da Lei Geral de Proteção de Dados (LGPD) quanto de marcos internacionais como o GDPR, é igualmente desafiada. Sistemas de IA frequentemente operam como "caixas-pretas", dificultando a explicação dos motivos que levam a determinadas decisões automatizadas. Como afirma Frank Pasquale (2015), a opacidade algorítmica ameaça a prestação de contas e compromete direitos fundamentais, especialmente quando decisões automatizadas impactam esferas sensíveis como crédito, emprego, saúde e segurança pública.

Nesse contexto, o tratamento automatizado de dados pessoais deve observar os dispositivos legais aplicáveis, especialmente a LGPD. A legislação prevê direitos como o acesso aos dados, a retificação, a eliminação e, fundamentalmente, o direito à revisão de decisões automatizadas (art. 20). Esse direito está alinhado ao que Mireille Hildebrandt (2016) denomina "direito à contestação algorítmica", isto é, a possibilidade de questionar decisões baseadas exclusivamente em processamento automatizado.

Também as implicações éticas do uso da IA merecem atenção. Sistemas algorítmicos podem intensificar desigualdades nas tomadas de decisão, sobretudo quando replicam vieses existentes nos bancos de dados utilizados para treinamento. Autores como Cathy O'Neil (2016) alertam que algoritmos tendem a amplificar discriminações se não forem cuidadosamente supervisionados, gerando impactos assimétricos sobre grupos vulneráveis. Nesse cenário, definir claramente a responsabilidade pelo funcionamento e pelos resultados dos sistemas torna-se indispensável.

A supervisão regulatória e a adoção de práticas preventivas, como a realização de Relatórios de Impacto à Proteção de Dados Pessoais (art. 38 da LGPD), surgem como mecanismos essenciais para reduzir riscos. Segundo Laura Schertel Mendes (2020), a avaliação prévia de riscos é componente central da governança de dados, funcionando como instrumento para identificar vulnerabilidades e garantir que o desenvolvimento de sistemas de IA observe princípios de privacidade desde sua concepção.

Outro aspecto indispensável é o princípio da minimização de dados, que determina a coleta apenas das informações estritamente necessárias à finalidade pretendida. No contexto da IA, esse princípio ganha relevância porque a tendência à coleta massiva de dados ("data maximization") aumenta a exposição indevida de titulares e amplia o risco de violações. Luciano Floridi (2018) destaca que práticas excessivas de coleta fragilizam modelos de governança e ampliam potenciais danos.

A segurança da informação também desempenha papel central no tratamento de dados pessoais em sistemas de IA. Técnicas como criptografia, anonimização e privacy by design buscam mitigar riscos e assegurar a integridade das informações. Conforme argumenta Virgílio Almeida (2020), a complexidade dos sistemas digitais exige abordagens contínuas de monitoramento, capazes de detectar falhas e incidentes antes que comprometam direitos fundamentais.

A capacitação de profissionais responsáveis pelo desenvolvimento e operação de sistemas de IA é igualmente necessária. Sem conhecimento técnico adequado, torna-se inviável implementar medidas eficazes de conformidade. Conforme defende Ronaldo Lemos (2019), a governança digital exige a articulação entre saberes jurídicos e tecnológicos, o que demanda formação interdisciplinar.

A governança de dados, portanto, surge como um mecanismo indispensável para assegurar o cumprimento das normas, estabelecer controles claros sobre o ciclo de vida dos dados e minimizar riscos de violações. Esse processo inclui políticas internas de gestão, auditorias, mecanismos de revisão e padrões de segurança alinhados à legislação vigente.

O direito à explicação, reconhecido em diversos ordenamentos internacionais e debatido no Brasil, reforça a exigência de que algoritmos sejam compreensíveis e auditáveis. Para Andrew Selbst (2018), a explicabilidade não é apenas uma questão técnica, mas uma garantia jurídica essencial para o exercício de direitos fundamentais. A ausência de explicabilidade dificulta a responsabilização e compromete a transparência.

Outro desafio é o compartilhamento de dados entre diferentes sistemas de IA. Embora isso possa ampliar a eficiência e a qualidade dos serviços digitais, exige rigoroso cumprimento de normas de segurança, especialmente quando o tratamento envolve dados pessoais sensíveis. A interoperabilidade tecnológica, se não alinhada às normas de proteção de dados, pode aumentar a superfície de risco.

O princípio da responsabilidade ativa — ou accountability — impõe aos controladores o dever de adotar medidas preventivas para minimizar riscos. Para Juliano Maranhão (2021), a responsabilidade ativa é condição necessária para que modelos de IA sejam projetados e

operados com segurança, evitando abusos e falhas.

A atuação dos órgãos reguladores, como a Autoridade Nacional de Proteção de Dados (ANPD), é crucial. A imposição de sanções, a elaboração de guias orientativos e a emissão de regulamentos específicos fortalecem a conformidade das empresas. No entanto, a eficácia regulatória depende também da capacidade técnica das autoridades públicas, aspecto apontado por Zuboff (2019) como um dos maiores desafios contemporâneos. Medidas como anonimização, pseudonimização e limitação de acesso são fundamentais, mas sua eficácia depende da impossibilidade de reidentificação, o que exige padrões técnicos elevados. A literatura recente, como Solove e Schwartz (2021), ressalta que técnicas mal implementadas podem oferecer falsa sensação de segurança.

Diante desses desafios, a relação entre IA e proteção de dados exige constante revisão, aprimoramento normativo e vigilância permanente. Os direitos dos titulares precisam ser resguardados em um ambiente tecnológico complexo e em rápida evolução. Assim, o equilíbrio entre inovação e proteção de dados deve ser continuamente aperfeiçoado por meio de regras claras, fiscalização eficiente e práticas éticas. A proteção da privacidade é resultado de esforços integrados entre governos, empresas e sociedade civil.

A análise realizada demonstra que, à medida que a IA avança, a aplicação das normas existentes exige interpretação flexível e compreensão aprofundada das implicações tecnológicas. A complexidade do cenário regulatório demanda abordagem colaborativa e interdisciplinar, sob pena de gerar insegurança jurídica e fragilizar direitos fundamentais. O desafio central é garantir que a inovação ocorra de forma responsável, transparente e alinhada ao Estado Democrático de Direito.

3. O PRECEDENTE REGULATÓRIO ITALIANO E SUA CONTRIBUIÇÃO PARA O DEBATE BRASILEIRO SOBRE IA

Em março de 2023, a Autoridade Italiana de Proteção de Dados (Garante per la Protezione dei Dati Personali) determinou a suspensão temporária do funcionamento do ChatGPT em território italiano. A medida foi motivada por supostas violações ao Regulamento Geral de Proteção de Dados (GDPR), especialmente no que se refere à ausência de base legal adequada para o tratamento de dados pessoais, à insuficiência de transparência sobre a lógica algorítmica empregada e à inexistência de mecanismos de verificação etária. Como observa Cecilia Álvarez Rigaudias (2023), o GDPR estabelece parâmetros rigorosos sobre finalidade, necessidade e proporcionalidade, elementos de difícil compatibilização com

modelos de IA generativa que utilizam grandes massas de dados para aperfeiçoamento contínuo.

As determinações impostas à desenvolvedora do ChatGPT incluíram a explicitação detalhada dos dados coletados, das finalidades do tratamento e dos critérios utilizados pelo sistema para gerar respostas, o que está alinhado ao princípio da transparência previsto no art. 5 do GDPR. Além disso, o órgão exigiu a implementação de ferramentas que assegurassem o exercício dos direitos dos titulares, como acesso, retificação, oposição e exclusão, em consonância com o que Paul Schwartz e Daniel Solove (2021) definem como "arquiteturas de accountability informacional". Também foi determinada a adoção de mecanismos eficazes de verificação de idade, em razão do risco de acesso por menores a conteúdos potencialmente inadequados.

A decisão italiana tornou-se um dos primeiros precedentes regulatórios envolvendo sistemas de IA generativa em larga escala. Para Luciano Floridi (2023), o caso demonstrou que modelos de aprendizado profundo, apesar de sua natureza inovadora, estão sujeitos aos mesmos princípios normativos que regem qualquer operação de tratamento de dados pessoais. Além disso, a medida evidenciou o caráter preventivo das autoridades europeias, que atuam de acordo com o modelo de regulação orientado por risco — abordagem amplamente discutida por Brent Mittelstadt (2016) ao tratar de impactos algorítmicos.

No contexto brasileiro, embora a Lei Geral de Proteção de Dados (LGPD) não trate expressamente da regulação de sistemas de inteligência artificial, seus dispositivos são plenamente aplicáveis ao tratamento automatizado. O art. 20 da Lei nº 13.709/2018 assegura ao titular o direito à revisão de decisões tomadas unicamente com base em processamento automatizado, o que representa um mecanismo essencial de contestação algorítmica. Em 2024, o Superior Tribunal de Justiça analisou situação envolvendo o desligamento de um motorista de aplicativo com base em decisão automatizada, reconhecendo a necessidade de permitir ao titular a compreensão da lógica empregada — interpretação coerente com o que Danilo Doneda (2019) denomina “autodeterminação informativa”.

Além disso, o art. 38 da LGPD prevê a obrigatoriedade de avaliação de impacto à proteção de dados pessoais (RIPD) em operações que apresentem risco elevado aos titulares. Relatórios dessa natureza são considerados, por Laura Schertel Mendes (2020), instrumentos essenciais de governança e responsabilização. O art. 55-J, por sua vez, autoriza a Autoridade Nacional de Proteção de Dados (ANPD) a impor medidas corretivas, incluindo suspensão ou proibição parcial de operações de tratamento — prerrogativa que guarda semelhança com a atuação do regulador italiano.

A ANPD tem competência para editar orientações técnicas, normativas e recomendações voltadas à aplicação da LGPD em contextos de inteligência artificial. Embora ainda não existam diretrizes específicas sobre IA generativa, documentos como o Planejamento Estratégico 2023–2024 indicam que o tema está entre as prioridades futuras. Como enfatiza Ronaldo Lemos (2023), o Brasil precisa desenvolver marcos regulatórios capazes de dialogar com fenômenos tecnológicos emergentes, sem comprometer a inovação.

A natureza transnacional do tratamento de dados realizado por sistemas como o ChatGPT demanda articulação entre diferentes regimes regulatórios. A harmonização internacional é essencial para evitar conflitos normativos e assegurar segurança jurídica. O Brasil integra a Global Privacy Assembly (GPA), fórum de cooperação que reúne autoridades de proteção de dados de diversos países. Documentos internacionais, como os Princípios de Inteligência Artificial da OCDE (2019) e a Recomendação da UNESCO sobre Ética da IA (2021), estabelecem padrões reconhecidos globalmente e influenciam a atuação das autoridades nacionais.

À luz do caso italiano, é possível propor medidas de aprimoramento para a aplicação da LGPD a sistemas de IA generativa. Entre elas, destaca-se a exigência de explicações claras e compreensíveis sobre a lógica de funcionamento dos algoritmos, conforme debatido por Hildebrandt (2016). Também seria recomendável definir critérios objetivos para a revisão de decisões automatizadas, incentivar a elaboração de relatórios de impacto algorítmico e promover políticas de transparência desde a fase de projeto (privacy by design e ethics by design). A promoção de códigos de conduta e mecanismos de autorregulação pode complementar a atuação estatal, seguindo práticas já difundidas em outros países.

A suspensão do ChatGPT na Itália representa um marco regulatório relevante na aplicação do GDPR a sistemas de IA. A decisão baseou-se em fundamentos legais sólidos, reforçando que operações automatizadas devem respeitar direitos fundamentais e limites normativos. No Brasil, embora a LGPD ofereça um arcabouço jurídico aplicável, sua efetividade depende da capacidade técnica e institucional da ANPD para interpretar, fiscalizar e orientar o uso responsável dessas tecnologias. Em última análise, a proteção de dados pessoais permanece intrinsecamente ligada à regulação do uso de sistemas automatizados e ao compromisso do Estado com a defesa dos direitos dos titulares.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste artigo demonstrou que a inteligência artificial representa um dos maiores desafios contemporâneos para o Direito, especialmente no que se refere à proteção de dados pessoais e à transparência das decisões automatizadas. Os três eixos abordados, desafios regulatórios, proteção de dados e estudo de caso internacional, evidenciam que a regulação da IA exige um modelo normativo capaz de conciliar inovação tecnológica, eficiência operativa e preservação dos direitos fundamentais.

Os resultados obtidos indicam que, embora a LGPD não tenha sido concebida especificamente para regular sistemas de IA, seu conjunto de princípios, direitos e obrigações oferece instrumentos importantes para enfrentar riscos associados ao tratamento automatizado. O direito à revisão de decisões automatizadas, a exigência de avaliação de impacto, o princípio da transparência e a responsabilização dos agentes de tratamento são mecanismos centrais para limitar abusos e fortalecer a autonomia informacional dos titulares. No entanto, sua efetividade depende da capacidade técnica e institucional da ANPD, da cooperação entre órgãos públicos e da adoção de políticas corporativas robustas de governança algorítmica.

O estudo de caso do bloqueio do ChatGPT na Itália reforça a importância de abordagens regulatórias preventivas, orientadas por risco e alinhadas a padrões internacionais. O precedente europeu mostra que modelos de IA generativa não estão fora do alcance das normas de proteção de dados, devendo observar requisitos de finalidade, proporcionalidade, transparência e garantia de direitos. Para o Brasil, o caso oferece lições relevantes sobre a necessidade de fortalecer instrumentos regulatórios, aprimorar a fiscalização e estabelecer critérios objetivos de funcionamento para sistemas automatizados.

Apesar dos avanços, a pesquisa também evidencia limites. Trata-se de um tema recente, tecnicamente complexo e em constante transformação, o que impede conclusões definitivas. Muitas questões permanecem em aberto, como a definição de responsabilidade civil em sistemas autônomos, a governança de modelos que aprendem continuamente e os critérios de explicabilidade para algoritmos de alta complexidade. Essas lacunas indicam amplo campo para futuras investigações, tanto no âmbito acadêmico quanto no desenvolvimento de políticas públicas.

Além dessas conclusões, é importante reconhecer as dificuldades enfrentadas ao longo da pesquisa, especialmente no que diz respeito ao acesso à literatura especializada. Embora a produção acadêmica sobre inteligência artificial e regulação venha crescendo, ela

ainda é relativamente escassa no contexto brasileiro, concentrando-se majoritariamente em estudos iniciais, relatórios técnicos e obras de caráter introdutório. Observa-se, ainda, que grande parte das pesquisas consolidadas sobre governança algorítmica, proteção de dados e impactos sociais da IA encontra-se em língua inglesa, o que, embora não represente um obstáculo intransponível, impõe desafios adicionais à revisão bibliográfica, à atualização conceitual e ao acompanhamento das discussões internacionais. Essa limitação evidencia a necessidade de ampliar a produção científica nacional sobre o tema e reforça a importância de que novas pesquisas aprofundem aspectos específicos, contribuindo para o fortalecimento do debate jurídico no país.

Os objetivos propostos foram, portanto, alcançados, ainda que de forma parcial, dadas as limitações próprias de um tema emergente. O artigo contribui para o debate sobre a regulação da IA no Brasil ao oferecer uma análise crítica, articulada e fundamentada sobre desafios normativos, proteção de dados e governança algorítmica. Espera-se que o estudo sirva de base para pesquisas posteriores, tanto em cursos de pós-graduação quanto em programas de mestrado e doutorado, contribuindo para a construção de um marco normativo sólido e alinhado aos valores democráticos.

REFERÊNCIAS BIBLIOGRÁFICAS

ÁLVAREZ RIGAUDIAS, Cecilia. **Artificial Intelligence and Data Protection:** Challenges under the GDPR. Madrid: IE Law School, 2023.

ALMEIDA, Virgílio. **Governança algorítmica e os desafios da regulação digital.** Revista Brasileira de Políticas Públicas, Brasília, v. 10, n. 2, 2020.

ALMEIDA, Virgílio; BIALER, Ana Paula. **Governança de algoritmos:** desafios e caminhos. Revista Brasileira de Políticas Públicas, Brasília, v. 10, n. 2, 2020.

BAROCAS, Solon; SELBST, Andrew D. **Big Data's Disparate Impact.** California Law Review, v. 104, p. 671–732, 2016.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. São Paulo: Thomson Reuters Brasil, 2021.

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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 maio 2025.

CALO, Ryan. **Robotics and the Lessons of Cyberlaw.** California Law Review, v. 103, p. 513–563, 2015.

CRAWFORD, Kate. **Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence.** New Haven: Yale University Press, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da disciplina no contexto brasileiro. 2. ed. Rio de Janeiro: Renovar, 2019.

FLORIDI, Luciano. **Soft Ethics and the Governance of the Digital**. Philosophy & Technology, v. 31, p. 1–8, 2018.

FLORIDI, Luciano. **The Ethics of Artificial Intelligence.** Cambridge: Cambridge University Press, 2023.

HILDEBRANDT, Mireille. **Smart Technologies and the End(s) of Law:** Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar, 2016.

LEMOS, Ronaldo. **Direito, tecnologia e democracia.** Rio de Janeiro: FGV Editora, 2019.

LEMOS, Ronaldo. Inteligência Artificial e Regulação: desafios emergentes. **Revista de Direito, Tecnologia e Sociedade**, Brasília, v. 9, n. 1, 2023.

MARANHÃO, Juliano. **Responsabilidade civil por sistemas de inteligência artificial.** São Paulo: Revista dos Tribunais, 2021.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Revista dos Tribunais, 2020.

MITTELSTADT, Brent. **Auditing for Transparency in Algorithmic** Decision-Making. Communications of the ACM, v. 59, n. 10, p. 40–43, 2016.

O'NEIL, **Cathy. Weapons of Math Destruction:** How Big Data Increases Inequality and Threatens Democracy. New York: Crown, 2016.

OCDE. OECD **Principles on Artificial Intelligence.** Paris: Organisation for Economic Co-operation and Development, 2019.

PASQUALE, Frank. **The Black Box Society:** The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press, 2015.

SCHWARTZ, Paul; SOLOVE, Daniel. **Privacy Law:** Fundamentals. New York: Wolters Kluwer, 2021.

SELBST, Andrew D.; BAROCAS, Solon. **Regulating Big Data Algorithms.** Harvard Journal of Law & Technology, v. 31, n. 2, p. 1–34, 2018.

UNESCO. Recomendação sobre a Ética da Inteligência Artificial. Paris: UNESCO, 2021.
UNIÃO EUROPEIA. **Regulamento (UE) 2016/679** do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral de Proteção de Dados (GDPR). Jornal Oficial da União Europeia, 4 maio 2016.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. New York: PublicAffairs, 2019.