WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Inovação e direitos fundamentais: análise crítica do PL nº 2.338/2023 de regulação da IA no Brasil

Innovation and fundamental rights: a critical appraisal of Brazil's AI Regulation Bill no. 2338/2023

Carlos Roberto Weber Sobrinho[1]
Lucas Gondim Chaves Regis[2]

Recebido em: 03.09.2025
Aprovado em: 26.08.2026

RESUMO

O presente artigo examina criticamente o Projeto de Lei nº 2.338/2023, como marco regulatório emergente da Inteligência Artificial (AI) no Brasil. O objetivo é avaliar a capacidade da proposta legislativa de equilibrar, de forma juridicamente consistente, o imperativo da inovação tecnológica e a tutela efetiva dos direitos fundamentais, especialmente no que concerne à privacidade, à não discriminação e ao devido processo legal. Metodologicamente, adota-se uma abordagem analítico-crítica, confrontando a matriz de riscos adotada no projeto com as categorias de vulneração de direitos previamente mapeadas pela literatura e pela experiência comparada. A análise de dispositivos específicos - notadamente aqueles relativos à transparência, avaliação de impacto, mitigação de vieses e responsabilidade civil - permitiu identificar avanços importantes, como a adoção de um regime de responsabilidade objetiva e a incorporação de princípios de governança algorítmica. Entretanto, também foram evidenciadas lacunas relevantes, como a indeterminação conceitual acerca de sistemas de "alto risco", a fragilidade de mecanismos de auditoria, bem como a permissão excepcional para vigilância biométrica em espaços públicos. Conclui-se que, embora o PL nº 2.338/2023 represente um passo significativo rumo à regulação democrática da IA, sua eficácia normativa dependerá da superação de ambiguidades e da introdução de salvaguardas mais robustas, de modo a garantir reparação efetiva e prevenir práticas que fragilizem a esfera pública e o núcleo essencial dos direitos fundamentais.

Palavras-chave: Inteligência Artificial, Direitos Fundamentais, Responsabilidade Civil.

[1] Graduado em Biomedicina (2007), Mestre em Patologia (2010) e Doutor em Medicina Tropical (2012) pela Universidade Federal de Pernambuco. Professor adjunto de Medicina Tropical - UFPE, graduando em Direito. E-mail: carlos.sobrinho@ufpe.br. Lattes: http://lattes.cnpq.br/2327087430076889. Orcid: https://orcid.org/0000-0002-2188-6061

[2] Advogado, Mestre e Doutorando em Direito pela Universidade Católica de Pernambuco – UNICAP. E-mail: lucasgchaves@gmail.com. Lattes: http://lattes.cnpq.br/8252151327151375. Orcid: https://orcid.org/0000-0001-9882-5147.

CC BY

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

ABSTRACT

This paper provides a critical examination of Legislative Proposal No. 2.338/2023, as an emerging regulatory framework for Artificial Intelligence (AI) in Brazil. The central objective is to assess the extent to which the legislative proposal is capable of balancing, in a legally consistent manner, the imperative of technological innovation with the effective protection of fundamental rights, particularly in relation to privacy, non-discrimination, and due process of law. Methodologically, the study employs an analytical-critical approach, confronting the risk-based model adopted by the bill with categories of rights infringements previously identified in scholarly literature and in comparative regulatory experiences. The analysis of specific provisions—most notably those concerning transparency, impact assessments, bias mitigation, and civil liability—reveals significant progress, including the adoption of a strict liability regime and the incorporation of principles of algorithmic governance. Nevertheless, it also exposes important shortcomings, such as the conceptual indeterminacy surrounding "high-risk" systems, the fragility of auditing mechanisms, and the exceptional authorization for biometric surveillance in public spaces. It is concluded that, although Bill No. 2.338/2023 constitutes a meaningful step toward democratic regulation of AI, its normative effectiveness will depend on overcoming such ambiguities and introducing stronger safeguards to ensure effective redress and to prevent practices that may undermine the public sphere and the essential core of fundamental rights.

Keywords: Artificial Intelligence, Fundamental Rights, Civil Liability

1 INTRODUÇÃO

A expansão da inteligência artificial (IA) inaugura cenário paradigmático em que inovação tecnológica e tutela de direitos fundamentais se entrecruzam. Se, por um lado, os sistemas algorítmicos ampliam eficiência, racionalizam recursos e abrem novas fronteiras econômicas e sociais, por outro, geram riscos sistêmicos à privacidade, à igualdade e às instituições democráticas. A literatura adverte que a regulação da IA não pode restringir-se à lógica da inovação, devendo incorporar salvaguardas normativas para mitigar efeitos deletérios em direitos constitucionais estruturantes (Veale; Borgesius, 2021).

Nesse contexto, a experiência brasileira revela-se singular: além de acompanhar a tendência regulatória internacional, sobretudo a matriz europeia, exige soluções normativas compatíveis com um ordenamento marcado por desigualdades estruturais, assimetrias informacionais e fragilidades institucionais. Uma regulação demasiado aberta

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

tende a converter-se em enunciado simbólico, incapaz de enfrentar a complexidade técnico-social dos sistemas algorítmicos, ao passo que um regime excessivamente restritivo pode asfixiar a inovação ainda incipiente no país. O equilíbrio entre tais polos constitui tarefa hermenêutica e legislativa de elevada complexidade (Wachter; Mittelstadt; Floridi, 2017, p. 2-3; Selbst, 2021, p. 5).

No Brasil, o debate adquire relevo com a tramitação do Projeto de Lei nº 2.338/2023, que busca estabelecer marco normativo específico para a IA. A proposta, embora avance ao incorporar princípios como transparência, não discriminação e *accountability* (Responsabilização e Prestação de Contas-RPC) [3], revela fragilidades na concretização de tais diretrizes em normas efetivas (Selbst, 2021, p. 4–5).

A investigação ora apresentada examina criticamente em que medida o texto legal em discussão harmoniza inovação tecnológica e proteção de direitos fundamentais. Adota-se análise jurídico-crítica, confrontando a matriz de riscos do PL nº 2.338/2023 com os eixos de vulnerabilidade de direitos fundamentais previamente identificados. Essa abordagem articula exame dogmático dos dispositivos normativos com aportes da literatura especializada e experiências comparadas, permitindo avaliar a densidade normativa do projeto, suas potencialidades e insuficiências, bem como as lacunas que comprometem sua aptidão para sustentar regime simultaneamente fomentador da inovação e garantista da dignidade humana e dos valores democráticos.

2 HISTORICIDADE E IMPERATIVO DA INOVAÇÃO TECNOLÓGICA

A trajetória da humanidade tem sido reiteradamente marcada por transformações tecnológicas de natureza disruptiva, capazes de remodelar profundamente a organização social, a dinâmica econômica e a própria estrutura do Estado. Se a Primeira Revolução Industrial (1RI) encontrou na máquina a vapor o seu símbolo paradigmático, a Segunda (2RI) foi impulsionada pela eletricidade, e a Terceira (3RI) pela informática e pela

[3] Permite a transparência, a efetiva possibilidade de controle, contestação e correção de decisões automatizadas no âmbito judicial (Pecego; Teixeira, 2024, p. 5).

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

digitalização inicial dos processos produtivos. O século XXI, por sua vez, inaugura a Quarta Revolução Industrial (4RI), que se desdobra como fenômeno de complexidade e abrangência sem precedentes, tendo a Inteligência Artificial (IA) como seu vetor mais expressivo e transformador (Werner, 2019, p. 16-18, Siqueira; Lara, 2021, p. 302-303). A IA diferencia-se dos símbolos anteriores pela velocidade, amplitude de impactos e profundidade das transformações sociais (Werner, 2019, p. 14-18). Ao integrar tecnologias físicas, digitais e biológicas, redefine mecanismos de governança e impõe releitura de paradigmas jurídicos.

A IA não se limita à condição de mero recurso instrumental, mas deve ser concebida como uma *General Purpose Technology* (GPT) [4] . Assim como a eletrificação foi decisiva para a urbanização moderna, a IA expandiu-se em múltiplos domínios, da saúde às finanças, agricultura e gestão pública (Emmert-Streib, 2021, p. 285). Essa pervasividade e irreversibilidade inviabilizam sua contenção absoluta. O Direito, nesse cenário, não deve atua como barreira repressiva, mas como instância de racionalização normativa capaz de alinhar tecnologia e valores constitucionais. Sua tarefa central é reinterpretar institutos consolidados à luz da 4RI, assegurando conformidade ética, segurança e compatibilidade com a dignidade humana (Siqueira; Lara, 2020, p. 307).

A consolidação da IA como vetor de transformação social, econômica e política impõe imperativo estratégico ao Estado brasileiro. Permanecer como mero receptor de tecnologias compromete a soberania digital e perpetua dependência estrutural. Exige-se, portanto, protagonismo do poder público, em sinergia com academia e setor produtivo, para estruturar ecossistema nacional de IA baseado em diretrizes claras e políticas consistentes (Siqueira; Lara, 2020, p. 308). É importante destacar que o debate em torno da regulação da IA tende a concentrar-se em seus riscos potenciais, obscurecendo, não raras vezes, a magnitude dos benefícios concretos que a tecnologia é capaz de proporcionar. Para que a análise crítica seja verdadeiramente imparcial e epistemologicamente rigorosa, é necessário ressaltar, preliminarmente, os impactos

[4] Caracterizada pela pervasividade; melhoramento dinâmico e inovação de inovação. Trata-se de categoria de tecnologia cunhada pela teoria econômica para designar inovações estruturantes que irradiam efeitos transversais e multiplicadores em diversos setores (Bresnahan; Trajtenberg, 1995, p.84).

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

positivos da IA, no intuito de justificar tanto a urgência de um marco legal específico, quanto evitar uma interpretação equivocada do texto de modo a ser percebido como meramente tecnofóbico ou obscurantista.

Economicamente, a IA é instrumento de incremento de eficiência e produtividade. Na indústria, otimiza cadeias logísticas, previne falhas, reduz custos e automatiza tarefas repetitivas, liberando capital humano para funções estratégicas. No Brasil, tais benefícios podem ampliar a produtividade empresarial e reforçar a posição global do país. Na saúde, a IA mostra ganhos expressivos. A análise de grandes bases de dados com precisão superior à humana revoluciona diagnósticos e tratamentos. Ribeiro et al. (2020, p. 2) demonstram que redes neurais auxiliam no diagnóstico automatizado de eletrocardiogramas, acelerando triagens e reduzindo erros. No SUS, a IA pode prever demandas, otimizar recursos e personalizar tratamentos, elevando expectativa e qualidade de vida (Zuliane; Rachid; Fornazin, 2024, p. 11).

A administração pública também é campo fértil para a IA. Sistemas inteligentes aprimoram alocação de recursos, previnem fraudes e agilizam serviços (Sobrinho; Dias; Gianordoli, 2025, p. 22295). Fernandes e Carvalho (2018, p. 378) evidenciam ganhos de eficiência na gestão documental, enquanto Oliveira e Reis (2023, p. 17) destacam sua aplicação nos Tribunais de Contas, ampliando transparência e racionalidade no uso do erário. Na sustentabilidade, a IA é ferramenta crucial para monitoramento e preservação ambiental. Freitas (2023) ressalta a necessidade de equilibrar desenvolvimento tecnológico e preservação, destacando sua contribuição para uma economia verde e resiliente.

Tais exemplos confirmam a centralidade da IA para desenvolvimento e soberania. Atrasar-se na corrida tecnológica compromete a autonomia nacional e expõe o país a regulações externas. Um marco regulatório robusto sinaliza seriedade institucional e atratividade a investimentos, estimulando startups e consolidando nichos como o *agrotech*[5] (Fernandes; CARVALHO, 2018, p. 380).

[5] Conceito associado à agricultura inteligente em que tecnologias digitais permitem comunicação, monitoramento e gerenciamento em tempo real (Correia et al. 2023, p. 22-23).

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Reconhece-se que a inovação tecnológica, orientada por justiça social, pode reduzir desigualdades e ampliar inclusão. Ao democratizar serviços essenciais, a IA torna-se instrumento de modernização estatal. Contudo, tais promessas não são automáticas: a mesma tecnologia que gera ganhos também ameaça privacidade, autonomia e direitos fundamentais. Impõe-se, portanto, governança ética e ordenamento jurídico que assegurem a dignidade humana conforme a Constituição de 1988 (COSTA, 2024, p. 8-9).

3 RISCOS DA IA À TUTELA DE DIREITOS FUNDAMENTAIS

Precipuamente, para uma análise robusta é *sine qua non* entender a classificação dos tipos de IA. Embora não uniforme, pode ser organizada em dois eixos complementares: pelo grau de autonomia e pelas técnicas computacionais empregadas. No primeiro eixo, fala-se em IA fraca ou estreita (*narrow* AI), voltada para tarefas específicas, como reconhecimento de voz ou diagnósticos médicos; IA geral (AGI), ainda em estágio hipotético, que seria capaz de replicar a versatilidade cognitiva humana; e IA superinteligente, conceito teórico que projeta sistemas com capacidades superiores às humanas em praticamente todas as áreas do conhecimento. Já no segundo, há a IA simbólica, baseada em regras, e a conexionista, que utiliza redes neurais e *machine learning* (Aprendizado de Maquinas – AM)[6] para análise de padrões em grande quantidade de dados, sobretudo via *deep learning* (Aprendizado Profundo - AP)[7], núcleo das inovações atuais (Barroso; Mello, 2024, p. 10-11; Xiong et al., 2024, p. 2).

Destaca-se a inteligência artificial generativa, que emprega modelos probabilísticos — como transformers e redes neurais profundas — para criar conteúdos originais a partir de grandes bases de dados. Diferente da IA convencional, que apenas

[6] Campo da IA que permite que sistemas aprendam e melhorem a partir da experiência, sem programação explícita. Em vez de serem programados, analisam grandes quantidades de dados, identificam padrões e a partir disso tomam decisões ou fazem previsões (Goodfellow; Bengio; COURVILLE, 2016, p. 8).

[7] Utiliza redes neurais artificiais com múltiplas camadas hierárquicas para identificar padrões complexos em grandes volumes de dados, servindo de base para avanços recentes da IA, especialmente a generativa (Goodfellow; Bengio; Courville, 2016, p. 8).

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

classifica ou prevê, a generativa produz textos, imagens, músicas e até vozes de modo autônomo, muitas vezes indistinguível da produção humana (Sengar et al., 2024, p. 23662). Essa capacidade abre potencialidades para educação, saúde e economia criativa, mas também desafios ético-jurídicos ligados à autoria, manipulação de informações e autenticidade digital (Chowdhury et al., 2025, p. 9). É manifestação emblemática da 4RI, que requer políticas de fomento e regulação preventiva para proteção dos direitos fundamentais.

Cabe ressaltar que as distinções de IA não são meramente técnicas, mas possuem relevância normativa e política. Sistemas de IA cujo escopo é limitado demandam ordenamento jurídico de padrões proporcionais e de menor intensidade; já os autônomos e generativos exigem arcabouço normativo robusto, atento a opacidade, manipulação e responsabilidade difusa (Pasquale, 2015, p. 8, 16; Selbst, 2021, p. 120). A tipologia não é mera técnica: projeta consequências jurídicas, pois obrigações de governança, responsabilidade civil e direitos de explicação dependerão do tipo em análise. Compreender tais diferenças é condição para avaliar criticamente o alcance de qualquer regulação democrática.

O uso indiscriminado da IA, sobretudo da generativa, suscita preocupações adicionais. A alegada neutralidade algorítmica é ilusória: sistemas são produtos de escolhas humanas e dados marcados por desigualdades. Como adverte Noble (2018, p. 1-2), ao automatizar conhecimento, algoritmos cristalizam e amplificam desigualdades sob aparência de neutralidade. Essa afirmação revela a natureza paradoxal da IA: ao mesmo tempo em que promete racionalidade e precisão, pode perpetuar práticas discriminatórias sob a legitimidade de uma suposta objetividade matemática. A opacidade de sistemas de AM, verdadeiras "caixas-pretas", dificulta o escrutínio público, a responsabilização institucional e o devido processo legal, inviabilizando a contestação e a reparação de eventuais danos (Pasquale, 2015, p. 16; Wachter; Mittelstadt; Floridi, 2017, p. 75–76). Isso implica injustiças normalizadas, com vieses transformados em parâmetros técnicos dotados de legitimidade científica e jurídica (Noble, 2018, p. 1-2). Decisões de impacto - como crédito, benefícios sociais e seleções - tornam-se automatizadas sem transparência suficiente (Crawford; Schultz, 2014, p. 101). Essa naturalização da discriminação,

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

aplicada em escala massiva, é risco grave em contextos desiguais como o brasileiro. Esse viés algorítmico ameaça diretamente o princípio constitucional da isonomia (art. 5º, caput, CF/88) (Barocas; Selbst, 2016, p. 674).

Além dos riscos a desigualdade, a IA compromete privacidade e autodeterminação informativa. A exploração de dados massivos, muitas vezes sem consentimento livre e informado, converte experiências humanas em ativos mercantilizados, violando o núcleo essencial do direito à privacidade (Gosain et al., 2024, p. 10385). A vigilância algorítmica pervasiva cria um estado de monitoramento permanente e, consequentemente, assimetrias entre aplicadores e indivíduos (Pasquale, 2015, p. 3-4). Essa dinâmica ameaça a autodeterminação informativa e fragiliza a defesa contra exploração abusiva, convertendo privacidade em privilégio restrito. A ausência de controle efetivo sobre o ciclo de vida dos dados reforça tais riscos (Gosain *et al*., 2024, p. 10385).

No âmbito do devido processo legal, a aplicação de IA em decisões que afetam a esfera jurídica dos indivíduos — como em matéria penal ou administrativa — desafia os princípios do contraditório e da ampla defesa (art. 5º, LV, CF/88). A ausência de explicação efetiva converte cidadãos em objetos de decisões tecnicistas e ininteligíveis (Goodman; Flaxman, 2017, p. 3-6). Crawford e Schultz (2014, p. 110) sustentam que devido processo legal exige mais que eficiência: requer transparência, responsabilidade e contestação.

A ameaça à autonomia da vontade e à liberdade de pensamento (art. 5º, IV, VI e VIII, CF/88) é particularmente evidente diante de sistemas de recomendação e *microtargeting*[8], que personalizam ambientes informacionais e canalizam decisões por mecanismos persuasivos, sutis e quase imperceptíveis, contornando a deliberação racional e comprometendo a autodeterminação dos indivíduos (Papakyriakopoulos et al., 2018, p. 4). A filtragem algorítmica fomenta câmaras de eco, nas quais usuários consomem informações alinhadas às próprias crenças, o que reduz diversidade

[8] Microtargeting é um "processo estratégico que visa influenciar eleitores por meio da transmissão direta de estímulos, que são formados com base nas preferências e características de um indivíduo" (Papakyriakopoulos *et al*., 2018, p. 2).

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

informacional e acentua polarização (Cinelli et al., 2021, p. 1-3). Tais mecanismos podem manipular eleições e comprometer liberdades de expressão e pensamento.

Esse quadro de fragilidades constitui preâmbulo para exame dogmático-jurídico e doutrinário equânime e imparciais da norma em tramitação, servindo como pilares para a crítica subsequente.

Em síntese, os riscos da IA abrangem dimensões múltiplas e incidem sobre direitos fundamentais - da opacidade à erosão da privacidade, da desigualdade à manipulação da autonomia - exigindo respostas jurídicas ancoradas em proporcionalidade, transparência e responsabilidade. Esses desafios tensionam garantias constitucionais e impõem conciliar inovação e salvaguarda de direitos. Mais que normativo, é dilema político e filosófico sobre até que ponto a liberdade pode ser condicionada por sistemas opacos. O enfrentamento dessas tensões definirá não só a regulação da IA, mas os rumos da democracia e da cidadania no século XXI.

4 EFICÁCIA NORMATIVA NA TUTELA DOS DIREITOS FUNDAMENTAIS: PROJETO DE LEI Nº 2.338/23

O Brasil tem se posicionado ativamente no acompanhamento das discussões internacionais concernentes à governança da IA, incluindo influências de iniciativas legislativas como *AI Act Europe*. Em uma análise incipiente, o PL nº 2.338/23 possui arcabouço normativo fundado em princípios centrais - crescimento inclusivo; liberdade de decisão e de escolha; participação e supervisão humana efetiva; não discriminação; justiça, equidade e inclusão; transparência, explicabilidade, inteligibilidade e auditabilidade; devido processo legal, contestabilidade e contraditório; rastreabilidade das decisões; prestação de contas, responsabilização e reparação integral de danos; prevenção, precaução e mitigação; não maleficência e proporcionalidade. No entanto, tais princípios encontram entraves técnicos inerentes a própria tecnologia para serem efetivamente capazes de tutelar os bens jurídicos a que se propõem.

O Projeto de Lei nº 2.338/23 adota, como eixo central de sua arquitetura normativa, o modelo de regulação baseada em riscos, inspirado diretamente na legislação

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

europeia. O Capítulo III (Arts. 12 a 16) distingue os sistemas de IA em duas categorias: risco excessivo (vedados, art. 13) e alto risco (art. 14), impondo obrigações graduais conforme o potencial de dano. A lógica visa compatibilizar inovação e tutela de direitos fundamentais, evitando tanto a hipertrofia normativa quanto a omissão regulatória. Como sublinham Veale e Borgesius (2021, p. 147), a matriz de riscos pretende oferecer proporcionalidade e equilíbrio.

Todavia, o regime revela fragilidades. A mais evidente é a indefinição do conceito de "alto risco" que, embora exemplificada no art. 14, permanece permeada por cláusulas abertas cuja concretização depende de regulamentação infralegal pelo Executivo (art. 15). Essa abertura transfere à Administração ampla margem normativa, expondo o sistema a captura regulatória e instabilidade interpretativa (Barroso; Mello, 2024, p. 89). A ausência de critérios técnicos objetivos compromete a previsibilidade e gera insegurança jurídica, como já advertia a doutrina ao criticar modelos de responsabilidade fundados em categorias elásticas de risco (Araujo, 2012, p. 6). Além disso, a dependência de atos do Executivo reduz o espaço deliberativo do Legislativo, criando um déficit democrático-regulatório. Como notam Filho e Zaganelli (2021, p. 5), a regulação da IA não pode prescindir de balizas normativas claras, sob pena de desequilibrar a posição da vítima frente ao poder econômico dos desenvolvedores. Soma-se a isso a tensão entre a gradação de riscos e a tradição brasileira de responsabilidade objetiva, cujo núcleo é a reparação integral. Nesta seara Salles e Costa (2023, p. 4) pertinentemente advertem que a responsabilidade civil, além de reparatória, deve cumprir função preventiva, contendo os potenciais lesivos da tecnologia.

Por outro lado, a experiência europeia, consubstanciada no Regulamento (UE) 2024/1689, revela uma arquitetura normativa que limita a discricionariedade do Executivo na definição de sistemas de alto risco. Diferentemente do PL nacional, o legislador europeu estabeleceu uma lista taxativa de aplicações de alto risco, vinculadas a setores sensíveis como saúde, transporte e segurança pública, sujeita a revisões periódicas. Ao delimitar previamente o campo de incidência, reforça a segurança jurídica da regulação, preservando a adaptabilidade mediante anexos atualizáveis por atos delegados, submetidos a controle do Parlamento e do Conselho da União Europeia. Ao

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

circunscrever juridicamente essas categorias, o modelo europeu evita a captura regulatória e mitiga a indeterminação conceitual que fragiliza a proposta brasileira (Veale; Borgesius, 2021, p. 10; Costa, 2024, p. 18 e 27). Para o contexto brasileiro, impõe-se solução análoga: positivar em lei um rol de aplicações de alto risco**,** sujeito a revisão periódica pelo Congresso Nacional com base em relatórios técnicos da autoridade reguladora, de modo a conciliar previsibilidade normativa e adaptabilidade regulatória **e** reafirmar a reserva legal em matéria de restrição de direitos fundamentais.

Em análise preliminar de eficácia na tutela da Privacidade e da Autodeterminação Informativa, o Capítulo III do PL destaca-se pela dedicação aos "Direitos dos Titulares", o que deve ser destacado como um avanço conceitual inquestionável. O Art. 11 consagra o "direito à explicação", determinando que o usuário tenha acesso a "informações claras e adequadas" sobre a lógica envolvida na decisão automatizada. No entanto, além dos entraves tecnológicos já observados, a redação é notavelmente imprecisa. O texto não especifica o conteúdo mínimo dessa explicação, nem estabelece se deve ser técnica (explicando o algoritmo) ou causal (explicando os fatores decisórios). Em suma, sem definição clara de base jurídica e deveres correspondentes, um 'direito à explicação' tende a carecer de força executória: seu escopo pode até ser interpretado, mas a existência do direito deve estar fora de dúvida, e os deveres do controlador precisam ser clarificados com precisão para que sanções sejam legítimas (Wachter; Mittelstadt; Floridi, 2017, p. 93).

O Art. 12, §3º prevê exceções à transparência para proteger segredo comercial e propriedade intelectual, sendo este um ponto particularmente problemático. A ausência de um teste de proporcionalidade explícito para invocar tal exceção cria uma brecha perigosa. O argumento do segredo comercial tornou-se o cavalo de Troia da opacidade algorítmica, permitindo que empresas obscureçam práticas discriminatórias ou antiéticas sob o manto da proteção da propriedade intelectual (Pasquale, 2015, p. 193). A mera remissão à LGPD (Art. 5º, II) também se mostra insuficiente, uma vez originalmente não se destina a enfrentar a complexidade das cadeias de processamento algorítmico e a opacidade inerente aos modelos de AM.

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

O Art. 4º, II, bem como o Art. 9º, IV, através do princípio da não-discriminação impõe aos agentes a obrigação de adotar medidas para mitigar vieses ilícitos. Contudo, o PL peca por ser excessivamente principiológica, falhando em estabelecer mecanismos concretos de RPC. A obrigação de mitigar vieses é inócua sem a previsão concomitante de auditorias algorítmicas independentes e obrigatórias para sistemas de alto risco. A mitificação de vieses requer mais do que boa-fé; requer verificação externa, auditoria de *datasets* (Conjunto de Dados - CD) e testes de estresse contínuos, elementos ausentes no texto legal (Selbst, 2021, p. 123).

A questão da representatividade dos dados de treinamento, crucial em um país marcado por profundas desigualdades como o Brasil, é tratada de forma tangencial. A avaliação de impacto algorítmico (AIA), exigida para usos de alto risco, não determina, no plano legal, um diagnóstico específico sobre a representatividade e a diversidade dos dados; a metodologia mínima fixada limita-se a prever avaliação de riscos e benefícios aos direitos fundamentais, medidas de mitigação e exame de sua efetividade, sem menção expressa a auditorias de composição de bases (art. 25, §1º). Essa omissão é grave, pois sistemas treinados com dados que sub-representam ou distorcem grupos marginalizados inevitavelmente perpetuarão e amplificarão essas mesmas distorções no mundo real (Noble, 2018, p. 54). Embora o Capítulo de governança imponha aos agentes deveres de mitigar e prevenir vieses discriminatórios e de documentar testes de acurácia, robustez, confiabilidade e segurança, tais comandos não se convertem em obrigação legal de auditar representatividade dos conjuntos de treinamento, validação e teste (art. 18, I, b, c e e). Isso fragiliza a capacidade de prevenção ante a discriminações, precisamente onde elas tendem a emergir: na seleção e curadoria dos dados (Noble, 2018, p. 54).

O "*direito à revisão humana das decisões*", um pilar fundamental para o devido processo legal tem fulcro no Art. 6º, II e III do PL. O PL dedica dispositivo específico à isto para prevenir ou minimizar riscos, inclusive em usos indevidos razoavelmente previsíveis (art. 8º). Contudo, o texto aprovado não explicita salvaguardas institucionais indispensáveis à efetividade dessa revisão — como autoridade decisória, independência e expertise técnica suficiente para contrapor a lógica do modelo. Sem essas garantias, a

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

revisão corre o risco de degradar-se a rito formal, incapaz de alterar resultados ou interromper inferências danosas (Kaminski, 2019, p. 201).

O regime de responsabilidade civil proposto pelo PL n° 2.338/23 constitui um dos pilares mais críticos de sua arquitetura normativa, refletindo a tensão irreconciliável entre a necessidade de reparação de danos complexos e a dificuldade de imputação de responsabilidade em cadeias algorítmicas descentralizadas. Uma inquestionável fragilidade é o foco excessivo na responsabilidade civil *ex-post*, em detrimento de uma abordagem mais proativa de gestão de riscos. Isto é, a ênfase em soluções que atuam somente após a ocorrência do dano pode ser manifestamente insuficiente (Divino, 2024, p. 49 e 57). O regime de responsabilidade civil delineado no Capítulo V do projeto apresenta lacunas conceituais e contradições sistemáticas que merecem exame crítico aprofundado. A preservação da dicotomia tradicional entre responsabilidade subjetiva e objetiva, conjugada com a mera remissão às regras do Código Civil e do Código de Defesa do Consumidor, revela-se insuficiente para enfrentar os desafios específicos da responsabilização por danos causados por sistemas inteligentes autônomos.

A definição de quem é o "*aplicador*" (Art. 4º, VII) e o estabelecimento da sua responsabilidade objetiva (Art. 35, caput) configuram aparente avanço na proteção das vítimas. Embora o PL opte pela responsabilização objetiva do aplicador, a concepção restritiva do termo ainda gera déficit de RPC, sobretudo no contexto de AM, uma vez que sistemas de IA são fruto de cadeias produtivas complexas, envolvendo desde programadores de algoritmos até curadores de CD, integradores e usuários finais. Estes agentes detêm distintas expertises e habilidades, podendo gerar diferentes aportes, danos e responsabilidades. Essa variedade de papeis acrescenta alguns graus de dificuldade à regulação da matéria e toda esta complexidade transcende os paradigmas clássicos da responsabilidade civil (Barroso; Mello, 2024, p. 11). Como demonstram Filho e Zaganelli (2021, p. 195), "*a investigação levantada é justamente a respeito de casos em que não se tem como saber se há uma falha individual em questão*", configurando-se o que a doutrina denomina de "*lacuna na responsabilidade civil*" (*liability gap*).

O Art. 35 mantém a responsabilidade civil no âmbito das relações de consumo sujeita às regras do Código de Defesa do Consumidor, enquanto o Art. 36 preserva a

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

aplicabilidade do Código Civil para as demais hipóteses. Esta abordagem conservadora ignora as especificidades dos sistemas de IA que, como ressalta a literatura especializada, "*podem funcionar e ser usadas conforme o planejado, mas ainda causam uma lesão que nem o consumidor nem o fabricante previram*" (Filho; Zaganelli, 2021, p. 196). O cerne reside na autonomia decisória dos sistemas de AM, que dotam máquinas com capacidade de "*se aperfeiçoarem independente da vontade de seus programadores, podendo agir de acordo com as suas decisões*" (Sales; Costa, 2023, p. 6). Esta característica fundamental desafia a lógica tradicional da imputação, baseada na previsibilidade e controlabilidade dos riscos. Assim, ao estabelecer critérios genéricos para definição do regime de responsabilidade civil, considerando "*o nível de autonomia do sistema de IA e o seu grau de risco*" e "*a natureza dos agentes envolvidos*", o Art. 36 ainda perpetua a insegurança jurídica que o projeto deveria eliminar.

O PL não aborda adequadamente a questão dos danos imprevisíveis decorrentes da operação normal de sistemas de IA. Como alertam Filho e Zaganelli (2021, p. 197), "*os atos imprevisíveis realizados por sistemas de inteligência artificial potencializam a dúvida no que concerne à indagação a respeito da possibilidade de responsabilizar um sistema autônomo por um ato imprevisível*". A imprevisibilidade não constitui, necessariamente, excludente de responsabilidade quando se trata de atividades de risco. Contudo, no contexto de sistemas de IA, a imprevisibilidade assume contornos qualitativamente distintos, pois deriva não de falhas operacionais, mas da própria funcionalidade projetada do sistema.

A aplicação da teoria da causalidade adequada, consagrada no Art. 403 do Código Civil, revela-se particularmente problemática no contexto de sistemas de IA dotados de capacidade de autoaprendizagem. Como explica Araújo (2012, p. 8), segundo esta teoria, "*o dever de reparar apenas ocorre quando o dano é efeito imprescindível de determinada causa*", sendo que "*a causa direta e imediata não é sempre a mais próxima do dano, mas a que necessariamente o ensejou em um juízo de proximidade lógica*". Esta dificuldade reside na natureza dos sistemas de AP, que operam através de "*múltiplas redes e processadores* [que] *administrem as informações e estabeleçam correlações simultaneamente*" (Barroso; Mello, 2024, p. 9). Então, gera uma opacidade algorítmica

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

que torna extremamente difícil, quando não impossível, estabelecer a relação de causalidade necessária entre a conduta humana e o dano resultante.

O Art. 37 representa um avanço ao prever a inversão do ônus da prova "*quando a vítima for hipossuficiente ou quando as características de funcionamento do sistema de IA tornarem excessivamente oneroso para a vítima provar os requisitos da responsabilidade civil*". Esta previsão encontra respaldo teórico na doutrina do risco da atividade, segundo a qual, em empreendimentos de elevado potencial lesivo, a simples criação do perigo já seria suficiente para justificar a transferência do ônus probatório àquele que se beneficia da atividade (Araújo, 2012, p. 8).

É inteligível então que o dispositivo reconhece implicitamente as dificuldades probatórias inerentes à responsabilização por danos causados por sistemas de IA. Esta previsão legal alinha-se com a tendência contemporânea de "*objetivização de diversos regimes de imputação*" (Sales; Costa, 2023, p. 12), reconhecendo que "*a incidência do princípio constitucional da solidariedade* [art. 3º, I, da CF/88] *neste campo levou à compreensão de que o direito da vítima a ser reparada sobrepõe-se, axiologicamente, à garantia de liberdade do ofensor*".

Entretanto, a mera inversão do ônus probatório não resolve o problema fundamental da opacidade algorítmica. Esta abordagem ainda mantém intacta a estrutura conceitual da responsabilidade civil individual, a qual ignora as características sistêmicas dos riscos associados à IA, que demandam soluções coletivizadoras do risco. A experiência europeia aponta para a necessidade de implementação de seguros obrigatórios para sistemas de alto risco. Assim, a obrigatoriedade na contratação de seguro de responsabilidade é justificada pelo fato de o potencial danoso dos incidentes provocados pela IA tender a extrapolar a esfera individual e por isso, devem ser difundidos na sociedade brasileira (Sales; Costa, 2023, p. 13-16; Júnior, 2023, p. 193).

O PL não incorpora esta perspectiva, mantendo-se restrito ao paradigma da responsabilidade individual, representado então, oportunidade perdida de implementar mecanismos de distribuição de riscos mais adequados às características sistêmicas dos danos causados por IA.

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

O Art. 32 do PL apresenta uma redação excessivamente genérica uma vez que prevê que os desenvolvedores devem "*cooperar, na medida de sua participação, com os demais agentes de IA*" para "*permitir uma mitigação adequada dos riscos*". A ausência de critérios objetivos para definir o alcance dessa cooperação cria margem excessiva de discricionariedade judicial e insegurança jurídica para os agentes econômicos. O dispositivo estabelece deveres comportamentais sem correlação clara com o regime de responsabilidade civil delineado no capítulo V. Esta desarticulação normativa compromete a coerência sistemática do projeto, gerando dúvidas sobre as consequências jurídicas do descumprimento dos deveres de cooperação.

Para colmatar as fragilidades do arcabouço normativo proposto quanto a responsabilidade civil, tem-se aventado a necessidade de modificações estruturais no art. 36 do PL. Defende-se, em primeiro lugar, a positivação de uma responsabilidade solidária entre todos os integrantes da cadeia de fornecimento — operadores, desenvolvedores e integradores — ao menos no tocante aos sistemas de alto risco, com critérios objetivos delimitados para definir o alcance dessa cooperação de modo a assegurar à vítima um polo passivo robusto e eficaz, independentemente da intricada causalidade interna típica desses ecossistemas tecnológicos. Em segundo plano, surge a necessidade de mudança no Art. 37, que prevê inversão dinâmica do ônus probatório nas ações regressivas. No entanto, esta inversão é condicionada, seja pela hipossuficiência da vítima ou onerosidade de comprobatória do posso passivo.

A alteração pertinente é de que a inversão dinâmica do ônus da prova seja regra e não exceção, principalmente porque "*a violação do direito à prova pode implicar, de um lado, a inutilidade da ação judiciária, caracterizando, assim, violação oculta à garantia de acesso útil à justiça, restringindo-se indevidamente o exercício de um direito fundamental*" (Gondinho, 2007, p. 242). Acrescente-se a isso a pertinência de vincular expressamente o regime de responsabilidade civil ao cumprimento dos deveres de *due diligence*, tais como a realização de auditorias, a manutenção de documentação técnica e a observância de padrões mínimos de transparência previstos em outros capítulos do diploma, o que permitiria criar uma presunção relativa de culpa em caso de descumprimento. Isso porque a implementação de regime de responsabilidade estrita para

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

determinadas categorias de sistemas de IA, independentemente de culpa e com presunção absoluta de causalidade, representaria avanço significativo, mas é preciso cautela uma vez que a imprescindibilidade da regulação envolve riscos - sendo necessário equilibrar proteção das vítimas com incentivos à inovação (Araújo, 2012, p. 16). Esta presunção mínima de culpa é importante uma vez que que:

> ...a abolição total do conceito da culpa vai dar num resultado antissocial e amoral, dispensando a distinção entre o lícito e o ilícito, ou desatendendo à qualificação da boa ou má conduta, uma vez que o dever de reparar tanto corre para aquele que procede da conformidade da lei, quanto para aquele outro que age ao seu arrepio (Pereira, 2012, P. 391 *apud* Araújo, 2012, p. 6).

Ademais, sustenta-se a conveniência de instituir um fundo setorial de garantia, a ser custeado por contribuições compulsórias de desenvolvedores e operadores de sistemas de alto risco, a fim de assegurar a reparação em hipóteses de insolvência ou de impossibilidade de delimitação causal precisa, nos moldes do que já se verifica em regimes de responsabilidade por acidentes de consumo e ambientais. A proposta de criação de um fundo setorial demanda análise de suas implicações práticas no contexto brasileiro. Tal mecanismo permitiria socializar os riscos inerentes a sistemas de IA de alto risco, garantindo reparação mesmo quando o responsável é insolvente ou de difícil identificação[9], principalmente nos casos em que multiplicidade de agentes envolvidos compromete a eficácia do modelo clássico de responsabilidade civil. (Venzon, 2017, p. 18-19; p. 30-33; 41-42).

Todavia, a implementação de tal fundo no Brasil exigiria enfrentar desafios regulatórios e econômicos consideráveis. Em termos regulatórios, seria necessário definir com precisão a base de financiamento — se por contribuições compulsórias proporcionais ao faturamento das empresas desenvolvedoras e operadoras, ou por percentuais incidentes sobre contratos de fornecimento de sistemas de IA — evitando onerar excessivamente startups e pequenas empresas. Economicamente, haveria o risco de repasse dos custos ao

[9] O Fundo de Defesa de Direitos Difusos (FDD), criado pela Lei nº 7.347/1985, constitui precedente nacional relevante ao destinar indenizações para a recomposição de bens coletivos, garantindo reparação mesmo quando o responsável é desconhecido ou insolvente (Venzon, 2017, p. 30-33; 41-42).

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

consumidor final, o que poderia comprometer a acessibilidade da tecnologia. O foco de atenção deve ser direcionado ao modelo de governança institucional de um eventual fundo setorial voltado à reparação de danos decorrentes da inteligência artificial. A experiência brasileira em responsabilidade civil demonstra que a eficácia de regimes compensatórios depende diretamente da existência de órgãos com autonomia técnica, dotados de instrumentos de fiscalização e transparência, capazes de resistir a desvios de finalidade ou tentativas de captura política. A ausência desses elementos compromete a função reparatória do instituto e reduz a efetividade da proteção jurídica (Filho; Zaganelli, 2021, p. 515).

No plano econômico, o desafio está em evitar que a estrutura de financiamento se converta em obstáculo ao desenvolvimento tecnológico. Para lidar com esse dilema, parte da literatura especializada propõe mecanismos que promovam a distribuição coletiva dos riscos, como seguros obrigatórios e fundos compensatórios. Essas soluções permitem que os custos sejam partilhados entre os diversos agentes da cadeia de desenvolvimento e operação de sistemas de IA, prevenindo a transferência integral do ônus às vítimas e calibrando as contribuições de acordo com o nível de risco de cada aplicação (Melo, 2024, p. 58). Assim, a concepção normativa de um fundo setorial deve harmonizar dois objetivos centrais: garantir a reparação ainda que, "*o sistema securitário não afasta a responsabilidade civil, sendo apenas mecanismo complementar para sua concretização*" (Melo, 2024, p. 61) e, ao mesmo tempo, preservar a viabilidade da inovação tecnológica, mediante uma governança plural e um desenho econômico equitativo.

O PL em sua redação final, incorporou previsão expressa no art. 13, inciso IV, que veda o uso de sistemas de identificação biométrica em tempo real em espaços públicos, mas admite exceções como investigação criminal com ordem judicial, busca de vítimas, flagrante delito e cumprimento de mandados. Embora o dispositivo tenha buscado calibrar a proibição com hipóteses de necessidade estrita, tais aberturas permanecem problemáticas, pois podem ampliar o alcance da vigilância algorítmica em ambientes coletivos e comprometer direitos fundamentais. Foi demonstrado que tecnologias de big data expandem a "discrição de vigilância", permitindo monitoramento sem suspeita concreta. Nesse sentido, a combinação entre exceções legais e capacidade técnica

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

favorece a normalização da vigilância, produzindo efeitos inibidores sobre a privacidade, a liberdade de expressão e o direito de reunião. Assim, a exigência de autorização judicial ou de enquadramento taxativo não constitui salvaguarda suficiente, especificamente porque dispositivos excepcionais tendem a se consolidar na prática securitária, ampliando a discricionariedade estatal e fragilizando as bases do Estado Democrático de Direito. (JOH, 2015, p. 3-4, p. 6-7).

Outrossim, o projeto apresenta omissões significativas no tocante à regulação de práticas de *microtargeting político* em plataformas digitais. Do ponto de vista jurídico e ético, esta pratica levanta preocupações sobre manipulação comportamental, erosão da autonomia decisória e fragilização do debate público informado, configurando um risco significativo para a integridade dos processos democráticos. Embora classificadas como sistemas de "risco limitado", a ausência de previsão representa, assim, uma lacuna estratégica de relevante gravidade para a proteção da esfera pública. Por isso, a adição normativa para coibir especificamente faz-se inquestionavelmente necessário.

Sem o acolhimento dos ajustes aqui aparentados, principalmente no que tange ao regime de responsabilidade civil delineado no PL nº 2.338/2023, ousa-se afirmar que o diploma a partir do documento incorre no erro de permanecer como elegante construção teórica, porém de eficácia diminuta diante da complexidade empírica dos danos algorítmicos, frustrando, em última instância, sua finalidade precípua. Tais críticas remete ao contraste entre a experiência brasileira e a normativa europeia, a que já prevê mecanismos de responsabilização compartilhada para sistemas de alto risco, incluindo auditorias independentes, documentação obrigatória e obrigações específicas de mitigação de risco.

5 CONSIDERAÇÕES FINAIS

A investigação desenvolvida permitiu constatar que o Projeto de Lei nº 2.338/2023 enfrenta o dilema central de estruturar um regime jurídico para a IA que preserve o dinamismo inovador sem relativizar o núcleo essencial dos direitos fundamentais. O percurso analítico evidenciou um desenho normativo que acerta na

WB EDUCAÇÃO
DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

direção ao eleger princípios de transparência, não discriminação, contestabilidade e prestação de contas, mas que, na forma como está positivado, ainda não entrega a densidade necessária para gerar segurança, previsibilidade e efetividade.

A adoção de um modelo graduado de riscos parece compatível com a proporcionalidade, mas a indefinição de conceitos-chave e a discricionariedade ao Executivo ampliam a indeterminação e comprometem deveres, sanções e eficácia preventiva, fragilizando a coerência do diploma. O direito à explicação e à revisão humana é avanço relevante, mas sem parâmetros claros corre o risco de se tornar mera formalidade. A ressalva ampla a segredos comerciais amplia a opacidade e compromete a contestabilidade de decisões automatizadas. A governança algorítmica proposta permanece excessivamente principiológica.

Sistemas de alto risco exigem auditorias independentes, rastreabilidade e avaliação de representatividade dos dados; sem isso, a mitigação de vieses torna-se promessa frágil. A responsabilidade civil, por sua vez, revela a dificuldade de adaptar categorias clássicas a danos gerados por cadeias tecnológicas fragmentadas. A responsabilização objetiva do aplicador é positiva, mas insuficiente diante de fluxos causais opacos e papéis distribuídos. A ausência de mecanismos de socialização de riscos, como seguros obrigatórios ou fundos compensatórios, mantém a vítima em posição vulnerável. Vincular o regime de imputação ao cumprimento de deveres de diligência — documentação, auditorias e transparência — é indispensável para transformar a prevenção em realidade e a reparação em garantia efetiva. No campo das liberdades públicas, a identificação biométrica admite exceções que normalizam a vigilância, enquanto o silêncio sobre direcionamento político mantém vulnerável a esfera pública. Ambos exigem contenção normativa mais rigorosa.

Dessas constatações decorre uma agenda: fechar categorias de alto risco, definir conteúdo do direito à explicação, impor auditorias independentes, avaliar representatividade dos dados, vincular responsabilidade à diligência e restringir exceções em vigilância e manipulação política.

A consolidação de um marco normativo para a IA no Brasil não deve ser vista como ponto final, mas como etapa de um processo dinâmico. A velocidade da inovação

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

impõe revisões periódicas e diálogo constante entre legislador, sociedade e comunidade científica.

O futuro exigirá não apenas ajustes pontuais, mas a capacidade de o direito reinventar suas próprias categorias para enfrentar novas formas de risco. O verdadeiro desafio é transformar a regulação em instrumento de emancipação social, capaz de articular soberania tecnológica, desenvolvimento econômico e proteção inegociável da dignidade humana.

REFERÊNCIAS

ARAÚJO, Vera Dias de. **Responsabilidade em razão do risco da atividade**. Rio de Janeiro: Escola da Magistratura do Estado do Rio de Janeiro – EMERJ, 2012. Artigo científico apresentado como exigência do Curso de Pós-Graduação lato sensu em Direito do Consumidor e Responsabilidade Civil. Disponível em: https://emerj.tjrj.jus.br/files/pages/revistas/direito_do_consumidor_e_responsabilidade_civil/edicoes/n1novembro2012/pdf/VeraDiasdeAraujo.pdfhttps://emerj.tjrj.jus.br/files/pages/revistas/direito_do_consumidor_e_responsabilidade_civil/edicoes/n1novembro2012/pdf/VeraDiasdeAraujo.pdf . Acesso em: 11 jul. 2025.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review**, v. 104, n. 3, p. 671–732, 2016. Disponível em: https://doi.org/10.15779/Z38BG31. Acesso em: 05 ago. 2025.

BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol. **Revista Direito e Práxis**, Rio de Janeiro, v. 15, n. 4, p. 1-45, 2024. Disponível em: https://doi.org/10.1590/2179-8966/2024/84479. Acesso em: 01 ago. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2023].

BRASIL. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília: Congresso Nacional, 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2366532 . Acesso em: 12 abr. 2025.

BRESNAHAN, Timothy F.; TRAJTENBERG, Manuel. General Purpose Technologies: Engines of Growth? **Journal of Econometrics**, v. 65, n. 1, p. 83-108, 1995. DOI: 10.1016/0304-4076(94)01598-T. Disponível em:

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

https://www.sciencedirect.com/science/article/pii/030440769401598T. Acesso em: 20 ago. 2025.

CAPPI, Cyril; CHAPDELAINE, Camille; GARDES, Laurent; JENN, Eric; LEFÈVRE, Baptiste; PICARD, Sylvaine; SOUMARMON, Thomas. **Dataset Definition Standard (DDS)**. arXiv:2101.03020 [cs.DB], p. 1-12, jan. 2021. Disponível em: https://arxiv.org/pdf/2101.03020 . Acesso em: 01 ago. 2025.

CHOWDHURY, Shamsul; DAS, Ananya; RAHMAN, Md. Mahmudur; SARKER, Tanjina; HOSSAIN, Md. Monir; AKTER, Farzana. Artificial intelligence in education, healthcare, and creative economy: opportunities and challenges**. Journal of Digital Innovation and Emerging Technologies**, v. 3, n. 1, p. 1-15, 2025. Disponível em: https://www.genesispcl.com/wp-content/uploads/CSER-Vol-2-I-1-p-19-31.pdf . Acesso em: 20 ago. 2025.

CINELLI, Matteo; DE FRANCISCI MORALES, Gianmarco; GALEAZZI, Alessandro; QUATTROCIOCCHI, Walter; STARNINI, Michele. Echo chambers on social media: A comparative analysis. **Proceedings of the National Academy of Sciences**, v. 118, n. 9, p. 1-8, 2021. Disponível em: https://arxiv.org/pdf/2004.09603 .Acesso em: 17 jun. 2025.

CORREIA, Tamires Partélli; MENDES, Éber Lopes; SILVA, Sheldon William; MELO, Tuane Ferreira. Tecnologia e produção agrícola: uma interface promissora e de gestão. **Agriculturae**, v. 5, n. 1, p. 20-27, jan./jun. 2023. Disponível em: https://cognitionis.inf.br/index.php/agriculturae/article/view/224/188 . Acesso em: 05 jul. 2025.

COSTA, Lívia Trucharte. As novas regulações da inteligência artificial: considerações acerca do PL nº 2.338/2023 sob a luz do EU AI ACT e o modelo “risk based”. 2024. 98 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Escola de Direito, Fundação Getúlio Vargas, São Paulo, 2024.

CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework To Redress Predictive Privacy Harms. **Boston College Law Review**, v. 55, n. 1, p. 93-128, 2014. Disponível em: https://bclawreview.bc.edu/articles/620/files/63ae71f65c8fc.pdf . Acesso em: 08 abr. 2025.

DIVINO, Sthéfano Bruno Santos. Inteligência artificial, danos e responsabilidade: da tutela ética à tutela jurídica. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 33, n. 3, p. 45-77, jul./set. 2024. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/967/692 . Acesso em: 11 jul. 2025.

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

EMMERT-STREIB, Frank. From the Digital Data Revolution Toward a Digital Society: Pervasiveness of Artificial Intelligence. **MAKE**, v. 3, n. 1, p. 284-298, mar. 2021. Disponível em: https://doi.org/10.3390/make3010014 . Acesso em: 06 mai. 2025.

FILHO, Douglas Luis Binda; ZAGANELLI, Margareth Vetis. Responsabilidade civil e inteligência artificial: quem responde por danos ocasionados por sistemas inteligentes autônomos? **Revista de Direito, Tecnologia e Inovação**, v. 3, n. 1, p. 1-25, 2021. Disponível em: https://ojs.revistadcs.com/index.php/revista/article/view/2805/2191 . Acesso em: 11 jul. 2025.

FREITAS, L. L. Qual o Impacto da Inteligência Artificial no Meio Ambiente?. **Software Mata Nativa**, 2023. Disponível em: https://matanativa.com.br/__trashed/. Acesso em: 11 ago. 2025.

GODINHO, Robson Renault. A distribuição do ônus da prova na perspectiva dos direitos fundamentais. **Revista do Ministério Público**. Rio de Janeiro: MPRJ, n. 26, p. 233-251, jul./dez. 2007. Disponível em: https://www.mprj.mp.br/documents/20184/2740997/Robson_Renault_Godinho.pdf . Acesso em: 05 de jul. 2025.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. **Deep Learning**. Cambridge: MIT Press, 2016. Disponível em: https://www.deeplearningbook.org/ . Acesso 03 ago. 2024.

GOODMAN, B.; FLAXMAN, S. European Union regulations on algorithmic decision-making and a "right to explanation". **AI Magazine**, v. 38, n. 3, p. 50–57, 2017. Disponível em: https://doi.org/10.1609/aimag.v38i3.2741. Acesso 03 ago. 2024.

GOSAIN, Trisha; BHATIA, Kavya; SHARMA, Rashi. *et al*. Artificial Intelligence and the Privacy Paradox: Challenges and Opportunities in Legal Adaptations. **Educational Administration: Theory and Practice**, v. 30, n. 5, p. 10384–10394, 2024. Disponível em: https://ijsra.net/sites/default/files/IJSRA-2024-2510.pdf . Acesso em: 18 jul. 2025.

JOH, Elizabeth E. The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing. **Harvard Law & Policy Review** (forthcoming), 2015. UC Davis Legal Studies Research Paper No. 473. Disponível em: https://ssrn.com/abstract=2680266. Acesso em: 14 jul. 2025.

KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, p. 189–218, 2019. Disponível em: https://doi.org/10.15779/Z38TD9N83H. Acesso em: 15 ago. 2025

LINDOSO, Maria Cristine Branco. O processo decisório na era do Big Data: como novos mecanismos de processamento de dados através de algorítmos interferem nas tomadas de decisão. In: FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (Coord.). **Tecnologia jurídica & direito digital: II**

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Congresso Internacional de Direito, Governo e Tecnologia – 2018. Belo Horizonte: Fórum, 2018. p. 367-381. ISBN 978-85-450-0584-1.

MELO, Gustavo da Silva. Inteligência artificial e responsabilidade civil: uma análise do anteprojeto do Marco Legal da Inteligência Artificial e do Projeto de Lei 2338/2023. **Revista IBERC**, v. 7, n. 1, p. 49-65, jan./abr. 2024. Disponível em: https://doi.org/10.37963/iberc.v7i1.271. Acesso em: 12 jul. 2023.

NOBLE, S. U. **Algorithms of Oppression: How Search Engines Reinforce Racism**. New York: New York University Press, 2018. Disponível em: https://files.commons.gc.cuny.edu/wp-content/blogs.dir/6105/files/2019/01/SAFIYA-NOBLE.pdf . Acesso em: 03 jun. 2025.

OLIVEIRA, Allen Kardec Feitosa; REIS, Rafael Fernando Mendes. Inteligência Artificial e o princípio da eficiência administrativa: o sistema Sapiens como instrumento de auxílio eficiente à advocacia pública**. Revista da PGE-MS**, Campo Grande, MS, n. 19, p. 11-27, 2023. Disponível em: https://www.pge.ms.gov.br/wp-content/uploads/2023/12/Revista-PGE-19-Allen.pdf. Acesso em: 04 ago. 2025.

PAPAKYRIAKOPOULOS, Orestis; HEGELICH, Simon; SHAHREZAYE, Morteza; MEDINA SERRANO, Juan Carlos. Social media and microtargeting: political data processing and the consequences for Germany. **Big Data & Society**, v. 5, n. 2, p. 1-15, jul./dez. 2018. Disponível em: https://doi.org/10.1177/2053951718811844. Acesso em 02 ago. 2025.

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

PECEGO, Daniel Nunes; TEIXEIRA, Raphael Lobato Collet Janny. Inteligência Artificial no Judiciário: da opacidade à explicabilidade das decisões judiciais**. Revista da Faculdade de Direito da UERJ**, Rio de Janeiro, n. 43, p. 1-22, 2024. Disponível em: https://doi.org/10.12957/rfd.2024.87850. Acesso em: 05 mai. 2025.

PEREIRA, Caio Mario da Silva. Instituição de Direito Civil. 11. ed. Rio de Janeiro:Forense,2000, p.391.

RIBEIRO, Antônio H.; RIBEIRO, Manoel Horta; PAIXÃO, Gabriela M. M.; OLIVEIRA, *et al*. Automatic diagnosis of the 12-lead ECG using a deep neural network. **Nature Communications**, v. 11, n. 1, article 1760, 2020. DOI: 10.1038/s41467-020-15432-4. Disponível em: https://www.nature.com/articles/s41467-020-15432-4.pdf. Acesso em: 01 jun. 2025.

SELBST, Andrew D. An institutional view of algorithmic impact assessments. **Harvard Journal of Law & Technology**, v. 35, p. 117-192, 2021. UCLA School of Law, Public

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Law Research Paper n. 21-25. Disponível em: https://ssrn.com/abstract=3867634. Acesso em: 03 mai. 2025.

SENGAR, Sandeep Singh; HASAN, Affan Bin; KUMAR, Sanjay. *et al*. Generative artificial intelligence: a systematic review and applications**. Multimedia Tools and Applications**, v. 84, p. 23661-23700, 2025. Disponível em: https://link.springer.com/article/10.1007/s11042-024-20016-1 . Acesso em: 20 ago. 2025.

SILVA, Luana Nunes da. **Transformando a Saúde com Big Data e Inteligência Artificial: Uma Análise Abrangente**. 2024. 48 f. Trabalho de Conclusão de Curso (Graduação em Engenharia Biomédica) – Universidade Federal de Pernambuco, Recife, 2024.

SIQUEIRA, Dirceu Pereira; LARA, Fernanda Corrêa Pavesi. Quarta revolução industrial, inteligência artificial e a proteção do homem no direito brasileiro**. Revista Meritum**, Belo Horizonte, v. 15, n. 4, p. 300-311, 2020. Disponível em: https://revistas.pucminas.br/index.php/meritum/article/view/8223 . Acesso em: 10 jun. 2025.

SOBRINHO, Hananda de Freitas; DIAS, Taciana de Lemos; GIANORDOLI, Victor. Inteligência Artificial: desafios da administração pública para capacitar os servidores no uso de IA. **Aracê**, São José dos Pinhais, v. 7, n. 5, p. 22289-22321, 2025. DOI: 10.56238/arev7n5-081. Disponível em: https://periodicos.newsciencepubl.com/arace/article/download/4880/6817/19303. Acesso em: 08 jul. 2025.

VEALE, M.; BORGESIUS, F. Z. Demystifying the Draft EU Artificial Intelligence Act. **Computer Law & Security Review**, v. 44, p. 105-152, 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852. Acesso em: 15 ago. 2025.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, [s. l.], 28 dez. 2016. Disponível em: https://doi.org/10.2139/ssrn.2903469. Acesso em: 03 mai. 2025.

WERNER, Deivid Augusto. **A Quarta Revolução Industrial e a Inteligência Artificial: um estudo sobre seus conceitos, reflexos e possível aplicação no Direito**. 2019. 211 f. Dissertação (Mestrado em Direito) – Universidade do Vale do Rio dos Sinos – UNISINOS, Porto Alegre, 2019.

XIONG, Haoyi; WANG, Shuo; ZHAO, Zhengyu; YANG, Yi; CHEN, Yiqi; SUN, Yizhou; YU, Philip S.; YANG, Qiang. Converging paradigms: the synergy of symbolic

DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

and connectionist AI in LLM-empowered autonomous agents. 2024. Disponível em: https://arxiv.org/pdf/2407.08516v1 . Acesso em 01 ago 2025.

ZULIANE, Mateus; RACHID, Raquel; FORNAZIN, Marcelo. Digital Health in the Brazilian National Health System (SUS). **Interface – Comunicação, Saúde, Educação**, Botucatu, SP, v. 28, e230597, 2024. Disponível em: https://www.scielosp.org/article/icse/2024.v28/e230597/en/. Acesso em: 15 ago. 2025.