INTUITIO

PPGFil/UFFS | e-ISSN 1983-4012

DOI: http://doi.org/10.36661/1983-4012.2025v18n2.15075

SEÇÃO: Dossiê Vulnerabilidade e Humanidade

DIREITO, TECNOLOGIAS E VULNERABILIDADE: INTERSECÇÕES CONTEMPORÂNEAS

Law, Technologies and Vulnerability: Contemporary Intersections

Ricardo Rheingantz Abuchaim[1]

Resumo: O artigo analisa as interseções complexas entre ordenamentos jurídicos, avanços tecnológicos e estados de vulnerabilidade na contemporaneidade. Propõe uma taxonomia analítica tripartite das vulnerabilidades tecnológicas: material, moral e jurídica, demonstrando como essas dimensões interagem em uma perspectiva interseccional. Examina tipologias de vulnerabilidade no contexto digital, incluindo discriminação algorítmica, vigilância digital e exclusão sociotécnica. O trabalho discute diversas abordagens filosóficas para enfrentar os dilemas éticos da tecnologia, como deontologia, utilitarismo, teoria da justiça, abordagem das capacidades e ética do cuidado. Analisa paradigmas regulatórios emergentes, como legislações de proteção de dados, reinterpretação de direitos fundamentais e governança algorítmica. Conclui que o enfrentamento das vulnerabilidades tecnológicas requer abordagens pluralistas, contextualmente sensíveis e fundamentadas em uma compreensão relacional da vulnerabilidade que reconheça nossa interdependência compartilhada.

Palavras-chave: Ética da tecnologia. Filosofia do direito. Justiça digital. Regulação algorítmica. Vulnerabilidade tecnológica.

Abstract: The article analyzes the complex intersections between legal systems, technological advances, and states of vulnerability in contemporary society. It proposes a tripartite analytical taxonomy of technological vulnerabilities: material, moral, and legal, demonstrating how these dimensions interact from an intersectional perspective. It examines typologies of vulnerability in the digital context, including algorithmic discrimination, digital surveillance, and socio-technical exclusion. The work discusses various philosophical approaches to addressing the ethical dilemmas of technology, such as deontology, utilitarianism, theory of justice, capabilities approach, and ethics of care. It analyzes emerging regulatory paradigms, such as data protection legislation, reinterpretation of fundamental rights, and algorithmic governance. It concludes that addressing technological vulnerabilities requires pluralistic, contextually sensitive approaches grounded in a relational understanding of vulnerability that recognizes our shared interdependence.

Key-words Algorithmic regulation. Digital justice. Ethics of technology. Philosophy of law. Technological vulnerability.

[1] Procurador federal da Advocacia-Geral da União e engenheiro de software. Doutorando em filosofia pelo Programa de Pós-Graduação em Filosofia da Fundação Universidade Federal de Pelotas. rheingantz.abuchaim@gmail.com ORCID https://orcid.org/0009-0006-9802-6648.

1 Introdução

A tessitura complexa que entremeia as relações entre ordenamentos jurídicos, avanços tecnológicos e estados de vulnerabilidade constitui, indubitavelmente, um dos mais prementes desafios epistêmicos da contemporaneidade (Zuboff, 2019). Em um cenário de transformações sociotécnicas vertiginosas, somos convocados a perscrutar, com acuidade analítica, as ressonâncias que as inovações tecnológicas projetam sobre as estruturas jurídicas convencionais e, sobretudo, sobre os sujeitos e coletividades em situação de fragilidade (Benjamin, 2019).

A revolução informacional e a subsequente digitalização das relações sociais inauguram possibilidades inéditas de atuação humana, ao mesmo tempo em que urdem formas específicas de exposição a riscos e danos (Castells, 2011). Tais transformações demandam uma renovação do instrumental analítico das ciências jurídicas e sociais, capaz de apreender as particularidades dos fenômenos emergentes sem desconsiderar suas continuidades com estruturas de desigualdade historicamente consolidadas. A ubiquidade da vigilância digital, a discriminação algorítmica, a exclusão sociotécnica e a instrumentalização da subjetividade mediante tecnologias persuasivas configuram apenas algumas das manifestações contemporâneas dessa problemática, demandando respostas normativas que transcendam os paradigmas jurídicos tradicionais.

O presente artigo se propõe a examinar, sob um prisma filosófico-jurídico, a tríade conceitual formada por direito, tecnologia e vulnerabilidade, desvelando suas imbricações e tensões constitutivas. A hipótese central que orienta esta investigação sustenta que o enfrentamento adequado das vulnerabilidades tecnológicas contemporâneas requer não apenas ajustes regulatórios pontuais, mas uma compreensão aprofundada de seus fundamentos filosóficos e de suas manifestações interseccionais. Propõe-se, assim, uma abordagem que articule análise conceitual, reflexão normativa e exame de paradigmas regulatórios emergentes.

Do ponto de vista metodológico, este trabalho adota uma perspectiva interdisciplinar que conjuga métodos da filosofia do direito, da teoria política e dos estudos críticos da tecnologia. A investigação privilegia a análise conceitual das diferentes dimensões da vulnerabilidade tecnológica, o exame crítico de abordagens filosóficas relevantes para a compreensão dos dilemas éticos contemporâneos, e a avaliação de paradigmas regulatórios

emergentes à luz de critérios normativos explicitados ao longo do texto. Metodologicamente, recorremos tanto à análise bibliográfica de fontes primárias e secundárias quanto à construção de tipologias conceituais que sintetizam padrões recorrentes de vulnerabilização no contexto digital.

A estrutura argumentativa do artigo se desenvolve em quatro momentos distintos e complementares. Inicialmente, na seção 1, apresenta-se uma taxonomia tripartite das vulnerabilidades tecnológicas, distinguindo suas dimensões material, moral e jurídica, e demonstrando como essas dimensões interagem em uma perspectiva interseccional. A seção 2 examina tipologias específicas de vulnerabilidade no contexto digital contemporâneo, incluindo discriminação algorítmica, vigilância digital, exclusão sociotécnica e riscos associados a tecnologias emergentes. A seção 3 se concentra na fundamentação filosófica da problemática, privilegiando a abordagem das capacidades de Martha Nussbaum como matriz teórica principal para a análise das vulnerabilidades tecnológicas, sem desconsiderar suas articulações com outras perspectivas normativas relevantes. Por fim, a seção 4 analisa paradigmas regulatórios emergentes, examinando legislações de proteção de dados, reinterpretações de direitos fundamentais e mecanismos de governança algorítmica.

A relevância deste estudo se justifica pela urgência de desenvolver arcabouços conceituais e normativos adequados para lidar com os desafios éticos e jurídicos impostos pela aceleração tecnológica contemporânea, especialmente em um momento histórico marcado pela crescente dependência de sistemas algorítmicos em domínios críticos como justiça, saúde, educação e trabalho, tornando imperativa a reflexão sistemática sobre as formas pelas quais as tecnologias digitais podem tanto amplificar vulnerabilidades preexistentes quanto criar novas modalidades de vulnerabilização. O escopo deste trabalho abrange tanto a dimensão fenomenológica das vulnerabilidades tecnológicas contemporâneas quanto os arcabouços normativos desenvolvidos para seu enfrentamento, com particular atenção à abordagem das capacidades como perspectiva filosófica privilegiada para a análise dessas questões, considerando que a proteção efetiva dos direitos fundamentais em contextos digitais demanda não apenas inovações regulatórias como também o aprofundamento teórico das categorias conceituais que estruturam nossa compreensão das relações entre tecnologia, direito e vulnerabilidade. Mediante uma análise multidimensional e interdisciplinar, busca-se contribuir para a elaboração de perspectivas regulatórias que conciliem o potencial

emancipatório das inovações tecnológicas com a proteção de valores fundamentais como dignidade, autonomia e justiça (Amoore, 2020).

2 Taxonomia Analítica das Vulnerabilidades Tecnológicas: Dimensões Material, Moral e Jurídica

A compreensão adequada do fenômeno da vulnerabilidade tecnológica pressupõe o desenvolvimento de uma taxonomia que distinga suas diversas manifestações fenomenológicas. Propõe-se, parra tanto, uma tripartição analítica que identifica três dimensões fundamentais da vulnerabilidade no contexto sociotécnico contemporâneo: material, moral e jurídica (Fineman, 2008).

A *vulnerabilidade material* se refere à suscetibilidade a danos ou privações no plano das necessidades objetivas e dos recursos tangíveis; no contexto tecnológico, manifesta-se primariamente através de fenômenos como:

a) Precariedade infraestrutural: compreendendo a insuficiência ou inadequação do acesso a dispositivos, conexões e infraestruturas tecnológicas essenciais para a participação significativa na sociedade informacional, transcendendo mera ausência de equipamentos e abrangendo também a obsolescência prematura, a dependência de infraestruturas precárias e a vulnerabilidade a interrupções no fornecimento de serviços essenciais (Crawford, 2021).

b) Vulnerabilidade econômica digital: englobando a exposição desproporcional a exploração econômica mediada por tecnologias, incluindo práticas como precificação discriminatória algorítmica, monetização não-consentida de dados pessoais e sujeição a condições laborais deterioradas em virtude da automação e da precarização tecnológica do trabalho (Pistor, 2019).

c) Suscetibilidade patrimonial tecnológica: referindo-se à exposição aumentada a danos patrimoniais relacionados a fenômenos como fraudes digitais, violações de segurança informática e obsolescência programada. Esta faceta da vulnerabilidade material se intensifica em contextos marcados por assimetrias informacionais significativas entre provedores de tecnologias e usuários finais.

d) Exclusão sociotécnica: constituindo a manifestação mais abrangente da vulnerabilidade material no contexto tecnológico porque se caracteriza pela impossibilidade de acesso e apropriação significativa de recursos tecnológicos essenciais para a participação plena em esferas cada vez mais digitalizadas da vida social, econômica e política (Noble, 2018).

A vulnerabilidade material tecnológica se revela particularmente aguda em sociedades marcadas por desigualdades estruturais preexistentes, onde as assimetrias no acesso a recursos educacionais, econômicos e infraestruturais amplificam as disparidades na capacidade de apropriação significativa das tecnologias emergentes[2]. Em semelhantes

[2] Segundo investigação do ICL Notícias (disponível em https://iclnoticias.com.br/atg/inclusao-digital-no-brasil/, acesso em 14abr25), embora 156 milhões de brasileiros tenham se conectado à internet em 2023, persistem profundas desigualdades no acesso e na apropriação das tecnologias digitais. A pesquisa TIC Domicílios 2023, citada na reportagem, revela que o acesso à internet apresenta variações expressivas de acordo com a

contextos, a exclusão digital se sobrepõe a vulnerabilidades materiais preexistentes, configurando condições de marginalização multidimensional (FRASER, 2009).

A *vulnerabilidade moral,* a seu turno, concerne à suscetibilidade a violações da integridade existencial e da autonomia ética dos sujeitos. No âmbito tecnológico, ela se manifesta através de fenômenos como:

a) Erosão da autodeterminação informativa: consistindo na diminuição da capacidade de controle sobre informações pessoais e sobre a construção da própria identidade em ambientes digitais, redundado em práticas como a coleta indiscriminada de dados, a elaboração de perfis comportamentais sem consentimento significativo e a manipulação algorítmica de preferências (Véliz, 2020).

b) Vulnerabilidade à discriminação algorítmica: caracterizando-se pela exposição desproporcional a tratamentos discriminatórios mediados por sistemas algorítmicos, particularmente em contextos decisórios com impactos significativos sobre direitos fundamentais, como acesso a crédito, oportunidades educacionais e profissionais, e tratamento pelo sistema de justiça criminal (O'Neil 2016).

c) Instrumentalização da subjetividade: dizendo respeito à redução do sujeito à condição de mero meio para a consecução de finalidades alheias, especialmente econômicas, mediante a exploração de vulnerabilidades psicológicas e cognitivas por tecnologias de persuasão e manipulação comportamental (Zuboff, 2019).

d) Vulnerabilidade à vigilância: abarcando a exposição desproporcional a regimes de monitoramento e controle que comprometem a privacidade, a intimidade e a liberdade de expressão e associação. Esta faceta da vulnerabilidade moral se exacerba em contextos políticos autoritários ou em relação a grupos historicamente sujeitos a vigilância discriminatória (Rodotà, 2008).

e) Precarização da autonomia cognitiva: englobando a deterioração das condições necessárias para o exercício da reflexão crítica e da deliberação autônoma em ambientes informacionais caracterizados pela desinformação, pela polarização extrema e pela fragmentação epistêmica (Coeckelbergh, 2020).

---

renda: enquanto nas classes mais altas a conectividade atinge quase 100%, nas classes D e E esse percentual cai para 69%. A precariedade infraestrutural se concretiza também no dado de que 24% dos domicílios com renda igual ou inferior a um salário-mínimo dependem do compartilhamento de rede com vizinhos. A dimensão qualitativa da exclusão digital é evidenciada pelo fato de que 58% das pessoas conectadas utilizam a internet exclusivamente pelo telefone celular, com maior prevalência desse comportamento entre mulheres, pessoas negras e integrantes das classes D e E. Esse dado corrobora a tese do artigo sobre como vulnerabilidades tecnológicas se sobrepõem a outras formas de marginalização social.

Adicionalmente, reportagem do Sindicato dos Servidores e Empregados Públicos do Rio de Janeiro (disponível em https://sindsprevrj.org/exclusao-digital-e-problema-grave-e-ainda-nao-enfrentado-com-seriedade-pelos-governos-brasileiros/, acesso em 14abr25) aponta que, segundo a PNAD Contínua do IBGE, mais de 10,3 milhões de brasileiros não utilizam internet por não saberem se conectar à rede, sendo que 66% desse público corresponde a pessoas idosas com ensino fundamental incompleto. O mesmo estudo revela que apenas 30% da população brasileira possuem habilidades digitais básicas, como copiar arquivos ou enviar e-mails com anexos, enquanto somente 18% demonstram habilidades intermediárias e meros 4,2% possuem competências digitais avançadas. Esses dados ilustram com precisão o que o artigo denomina "exclusão epistemológica", fator constituinte da vulnerabilidade material.

A vulnerabilidade moral tecnológica adquire contornos particularmente complexos em virtude da opacidade epistêmica que caracteriza muitos sistemas tecnológicos contemporâneos[3]. A inescrutabilidade algorítmica, aliada às assimetrias informacionais entre desenvolvedores e usuários, dificulta a identificação e a contestação de práticas potencialmente lesivas à integridade moral dos sujeitos (Pasquale, 2015).

Por fim, a *vulnerabilidade jurídica* diz com a suscetibilidade a violações de direitos ou à inadequação dos mecanismos de proteção jurídica diante de riscos e danos emergentes. No contexto tecnológico, concretiza-se através de fenômenos como:

a) Lacunas normativas: compreendendo a ausência ou insuficiência de marcos regulatórios adequados para lidar com fenômenos sociotécnicos emergentes, resultando em zonas de desproteção jurídica. Isso se dá particularmente em áreas caracterizadas por inovação tecnológica acelerada, como inteligência artificial, biotecnologia e tecnologias de vigilância (Suzor, 2019).

b) Ineficácia dos mecanismos de cumprimento da lei: aduzindo à inadequação dos instrumentos tradicionais de implementação e fiscalização normativa diante da

[3] A vulnerabilidade moral encontra expressão contundente na reportagem do Olhar Digital sobre o vazamento de dados da empresa de inteligência artificial chinesa DeepSeek. O incidente expôs milhões de dados confidenciais, incluindo históricos de conversas de usuários, chaves de API e informações de *backend*. A gravidade do vazamento é ampliada pelo fato de os dados estarem em texto não criptografado, o que ilustra perfeitamente o conceito de "vulnerabilidade à vigilância". A facilidade com que pesquisadores conseguiram acesso irrestrito ao banco de dados demonstra as fragilidades dos sistemas de proteção e os riscos à autodeterminação informativa dos usuários. Disponível em https://olhardigital.com.br/2025/01/30/seguranca/deepseek-ia-chinesa-sofre-falha-critica-e-expoe-milhoes-de-dados-confidenciais/, acesso em 30mar25.

Em outra vertente da vulnerabilidade moral, a coluna "A vigilância das redes sociais e a intervenção da FTC" publicada no porta jurídico Migalhas (disponível em https://www.migalhas.com.br/coluna/direito-digital/415663/a-vigilancia-das-redes-sociais-e-a-intervencao-da-ftc, acesso em 04jan25) discute o uso indiscriminado e invasivo dos dados pessoais por plataformas de redes sociais. O texto relata como empresas como Facebook, Instagram, TikTok e Twitter ampliam suas capacidades de vigilância, utilizando algoritmos para monitorar comportamentos dos usuários em tempo real. Esse monitoramento comercial exemplifica com precisão o que o artigo denomina "instrumentalização da subjetividade", ou seja, a redução do sujeito à condição de mero meio para fins alheios mediante a exploração de vulnerabilidades psicológicas por tecnologias de persuasão comportamental.

Reportagem do Olhar Digital sobre o uso de inteligência artificial do Google para armas e vigilância (disponível em https://olhardigital.com.br/2025/02/06/videos/seu-direito-digital-uso-de-ia-do-google-para-armas-e-vigilancia/, acesso em 10fev25) evidencia como a remoção de restrições éticas por gigantes tecnológicos pode amplificar riscos relacionados à vigilância e à segurança, exemplificando a precarização dos limites éticos no desenvolvimento tecnológico.

Um estudo acadêmico apresentado pela Semantic Scholar (disponível em https://www.semanticscholar.org/paper/%E2%80%9CARKANGEL%E2%80%9D-E-RELA%C3%87%C3%95ES-PARENTAIS%3A-VIGIL%C3%82NCIA-E-AOS-Tobbin-Cardin/bde793555916c4c58b5e656d97acf20239e25d5d, acesso em 15mar25) analisa as repercussões aos direitos da personalidade em contextos de vigilância tecnológica, utilizando como ponto de partida o episódio "Arkangel" da série Black Mirror. A pesquisa demonstra como dispositivos tecnológicos de monitoramento podem representar vigilância excessiva e violar direitos a autonomia, privacidade e integridade psíquica. A análise corrobora a discussão proposta sobre como a vulnerabilidade moral tecnológica se manifesta na erosão de espaços de autonomia e privacidade, especialmente em relações assimétricas de poder. O estudo conclui que a proteção da dignidade humana e do livre desenvolvimento da personalidade exige limites claros ao uso de tecnologias de vigilância.

transnacionalidade, da complexidade técnica e da volatilidade que caracterizam os fenômenos tecnológicos contemporâneos.

c) Vulnerabilidade jurisdicional: revelando-se pela dificuldade de determinação da jurisdição competente e da legislação aplicável em contextos digitais transnacionais, resultando em obstáculos significativos ao acesso à justiça por vítimas de violações de direitos mediadas por tecnologias.

d) Assimetria de poder jurídico-tecnológico: englobando os desequilíbrios na capacidade de mobilização de recursos jurídicos para a proteção de interesses em contextos tecnológicos, manifesta em fenômenos como a captura regulatória por interesses corporativos, a imposição unilateral de termos de uso abusivos e o acesso desigual à representação jurídica especializada (Magrani, 2019).

e) Inadequação conceitual-normativa: compreendendo a insuficiência dos conceitos e categorias jurídicas tradicionais para apreender adequadamente fenômenos emergentes como responsabilidade algorítmica, propriedade sobre dados pessoais e identidade digital, resultando em distorções interpretativas que comprometem a tutela efetiva de direitos fundamentais (Mendes, 2014).

A vulnerabilidade jurídica tecnológica se faz sentir com particular intensidade em contextos caracterizados pela assimetria de recursos técnicos, econômicos e cognitivos entre atores corporativos transnacionais e usuários individuais ou coletividades locais. Nesses cenários, a complexidade técnica dos fenômenos tecnológicos, aliada à sua transnacionalidade intrínseca, engendra obstáculos significativos tanto à elaboração de marcos regulatórios adequados quanto à sua implementação efetiva[4].

[4] A vulnerabilidade jurídica, encontra evidência empírica na entrevista do advogado Ciro Torres Freitas ao Consultor Jurídico (disponível em https://www.conjur.com.br/2024-jul-02/sem-diagnostico-dos-impactos-da-ia-lei-geral-nao-e-melhor-caminho-diz-ciro-torres-freitas/, acesso em 16abr25). Segundo ele, o Brasil discute a criação de uma lei geral de inteligência artificial sem ter um diagnóstico satisfatório dos impactos dessa tecnologia no país. A ausência de um levantamento oficial sobre setores beneficiados, ganhos proporcionados e ameaças da IA ilustra perfeitamente o conceito de "lacunas normativas". O especialista adverte que essa falta de diagnóstico pode gerar o risco de que a futura lei "seja insuficiente para mitigar os efeitos indesejados da IA" e acabe "inibindo os potenciais benefícios dessa tecnologia". A complexidade do tema regulatório é destacada quando Freitas argumenta que "conhecer os impactos causados pela IA é algo fundamental para se definir prioridades, identificar lacunas na legislação atual e, a partir disso, delimitar o escopo de novas normas a serem criadas".

Reportagem do jornal O Globo sobre ataques cibernéticos contra o governo brasileiro apresenta dados alarmantes sobre a vulnerabilidade das instituições públicas (disponível em https://oglobo.globo.com/brasil/noticia/2025/01/02/vulnerabilidade-virtual-numero-de-ataques-ciberneticos-contra-o-governo-aumenta-tcu-ve-risco-de-vazamento.ghtml, acesso em 16abr25). Segundo auditoria do Tribunal de Contas da União (TCU), os órgãos públicos federais estão vulneráveis a ataques hackers, com risco de vazamento de dados classificado como "particularmente alarmante". O levantamento revelou que apenas 14 de 229 órgãos públicos federais haviam implementado mais de 70% das medidas de segurança recomendadas, ilustrando a ineficácia dos mecanismos de cumprimento normativo. O aumento de ataques cibernéticos, que no primeiro semestre de 2024 já havia superado o total de 2023, demonstra a intensificação das ameaças à segurança informacional do Estado. Complementarmente, pesquisa publicada pela Semantic Scholar sobre o futuro da governança de cibersegurança no Brasil aponta que a segurança da informação e a cibersegurança estão entre as vulnerabilidades de alto risco da administração pública brasileira, segundo relatório de 2022 do TCU (disponível em https://www.semanticscholar.org/paper/Qual-%C3%A9-o-futuro-da-governan%C3%A7a-de-

As dimensões material, moral e jurídica da vulnerabilidade tecnológica não operam de maneira isolada, mas configuram uma trama complexa de interações recíprocas. A vulnerabilidade material frequentemente potencializa a suscetibilidade a violações de caráter moral, enquanto a vulnerabilidade jurídica pode amplificar tanto a exposição a danos materiais quanto a violações da integridade moral dos sujeitos.

Essa perspectiva interseccional se revela fecunda para a compreensão de como determinados grupos sociais, situados na confluência de múltiplos eixos de opressão e marginalização, experimentam formas agudizadas de vulnerabilidade tecnológica. Minorias étnicas, mulheres, pessoas com deficiência, idosos, populações rurais, comunidades economicamente desfavorecidas e grupos linguisticamente minoritários, entre outros, frequentemente enfrentam barreiras específicas no acesso e na apropriação significativa das tecnologias digitais, ao mesmo tempo em que estão mais expostos a riscos como vigilância discriminatória, exploração econômica e violações de privacidade (Benjamin, 2019).

A interseccionalidade das vulnerabilidades tecnológicas demanda, por conseguinte, abordagens regulatórias igualmente multidimensionais, capazes de reconhecer e responder à complexidade das interações entre diferentes formas de vulnerabilização. A elaboração de marcos normativos eficazes nesse domínio pressupõe não apenas a compreensão técnica dos fenômenos emergentes, mas também uma sensibilidade apurada para as dinâmicas sociais, econômicas e culturais que determinam a distribuição diferencial da vulnerabilidade entre distintos sujeitos e coletividades.

Diante da complexidade dos fenômenos examinados, faz-se necessário explorar os fundamentos normativos que podem subsidiar uma resposta jurídica adequada às vulnerabilidades tecnológicas contemporâneas. Destacam-se, nesse contexto, quatro matrizes teóricas complementares: a ética da responsabilidade (JONAS, 2006), a teoria crítica da tecnologia (Feenberg, 2002), a abordagem das capacidades (NUSSBAUM, 2011) e a ética do cuidado (Tronto, 1993).

3 Configurações Empíricas da Vulnerabilidade Tecnológica: Discriminação Algorítmica, Vigilância e Exclusão Sociotécnica

A elaboração de tipologias conceituais que categorizam as diversas manifestações da vulnerabilidade no ecossistema digital contemporâneo se mostra fundamental para a subsequente teorização filosófica e jurídica. As configurações arquetípicas aqui examinadas não constituem casos empíricos específicos, e sim construtos teóricos que sintetizam padrões recorrentes de vulnerabilização mediados por tecnologias emergentes, permitindo uma apreensão mais sistemática desses fenômenos complexos.

---

ciberseguran%C3%A7a-no-Goldoni-Rodrigues/9415489442e0ceec015df10ae1851863a22acf9a, acesso em 16abr25). O estudo conclui que, apesar dos esforços para securitizar o ciberespaço, o Brasil possui "uma coleção ampla, porém desconexa, de documentos, cuja maturidade de implementação não está clara".

A preponderância crescente de sistemas algorítmicos em processos decisórios que impactam direitos fundamentais constitui um fenômeno disruptivo que redefine as relações entre sujeitos, instituições e normatividade jurídica. Sob a aparência de neutralidade técnica, tais sistemas frequentemente reproduzem e amplificam vieses discriminatórios preexistentes, cuja genealogia remonta tanto às assimetrias presentes nos dados de treinamento quanto às escolhas valorativas implícitas nas métricas de otimização algorítmica (Mittelstadt et al., 2016). A incorporação desses sistemas em domínios como justiça criminal, concessão de crédito e recrutamento profissional redunda em formas específicas de vulnerabilidade para grupos historicamente marginalizados, cujas particularidades existenciais frequentemente escapam às categorias estatísticas hegemônicas (Noble, 2018).

A opacidade epistêmica dos algoritmos mais sofisticados, particularmente aqueles fundamentados em aprendizado profundo *(deep learning),* colide frontalmente com princípios jurídicos fundamentais, como transparência administrativa, devido processo legal e direito à explicação[5] (Wachter, Mittelstadt e Floridi, 2017). A vulnerabilidade resultante decorre da impossibilidade prática de contestação efetiva de decisões algorítmicas adversas, comprometendo garantias processuais basilares do Estado Democrático de Direito. Simultaneamente, os modelos de microdirecionamento comportamental exploram vulnerabilidades cognitivas e psicológicas específicas para maximizar engajamento, consumo ou comportamentos politicamente relevantes. A assimetria informacional entre plataformas tecnológicas e usuários individuais, aliada ao desenvolvimento de técnicas sofisticadas de personalização e persuasão, cria formas inéditas de manipulação que desafiam concepções tradicionais de autonomia e consentimento (Zuboff, 2019).

As estruturas arquetípicas de vigilância digital constituem outro elemento essencial para a compreensão das vulnerabilidades tecnológicas contemporâneas. A ubiquidade da coleta de dados, a interoperabilidade crescente entre sistemas de monitoramento e a sofisticação das técnicas de análise preditiva engendram um ecossistema de visibilidade

[5] O direito à explicação, no âmbito jurisdicional e doutrinário contemporâneo, consubstancia-se na prerrogativa inalienável do cidadão de obter esclarecimentos pormenorizados e inteligíveis acerca de decisões que lhe afetem o *status* jurídico, mormente quando tais deliberações advêm de sistemas automatizados ou mecanismos algorítmicos decisórios. Tal garantia fundamental se encontra insculpida no arcabouço normativo de tutela de dados pessoais, adquirindo notória relevância ante o inexorável avanço tecnológico e a consequente proliferação de decisões automatizadas que potencialmente cerceiam direitos subjetivos dos administrados. No ordenamento pátrio, a Lei Geral de Proteção de Dados Pessoais estatui expressamente a faculdade do titular dos dados de requisitar a revisão de decisões tomadas exclusivamente por meio de tratamento automatizado de seus dados pessoais, consoante preceituado pelo legislador ordinário (art. 20, cabeça e §§ 1º e 2º da lei n.13.709/18). De modo análogo, o Regulamento Geral sobre a Proteção de Dados da União Europeia consagra disposições congêneres, não obstante persistam controvérsias hermenêuticas quanto à extensão e aplicabilidade de tal direito. A *ratio essendi* do direito à explicação reside na salvaguarda da transparência decisória, viabilizando o exercício do contraditório e da ampla defesa mediante impugnação de decisões reputadas injustas pelo jurisdicionado, além de propiciar a identificação e subsequente mitigação de eventuais discriminações ou enviesamentos sistêmicos. Constitui, ademais, corolário lógico dos princípios basilares do devido processo legal e do acesso à justiça, porquanto a inteligibilidade dos fundamentos decisórios se afigura *conditio sine qua non* para o pleno exercício do direito de defesa e da contestação de atos potencialmente lesivos à esfera jurídica individual.

assimétrica com profundas implicações para a privacidade e para a liberdade individual e coletiva. A vigilância comercial expansiva, caracterizada pela extração massiva de dados pessoais para fins de monetização publicitária e precificação discriminatória, reconfigura profundamente as relações entre corporações e consumidores, redundando em vulnerabilidades específicas para indivíduos com características psicográficas ou sociodemográficas atípicas (Solove, 2008).

Os regimes de vigilância estatal, potencializados por tecnologias como reconhecimento facial, interceptação massiva de comunicações e análise de redes sociais, estabelecem desequilíbrio assombroso entre o poder de monitoramento do Estado e a capacidade de autodeterminação informativa dos indivíduos (Rodotà, 2008), gerando vulnerabilidades particulares para ativistas políticos, jornalistas, minorias étnicas e outros grupos tradicionalmente sujeitos a escrutínio governamental desproporcional, flertando com uma censura velada. Paralelamente, a vigilância interpessoal facilitada por tecnologias digitais se materializa em fenômenos como *digital stalking*[6], compartilhamento não consensual de imagens íntimas e monitoramento abusivo no contexto de relações domésticas. A miniaturização de dispositivos de captura, a facilidade de compartilhamento e a persistência temporal das informações digitais criam vulnerabilidades específicas para vítimas potenciais de violência de gênero, assédio e outras formas de abuso interpessoal (Véliz, 2020).

A inserção diferencial de indivíduos e coletividades no ecossistema digital cria assimetrias de poder, conhecimento e oportunidades que transcendem a mera questão do acesso material a dispositivos e conexões. A exclusão infraestrutural, caracterizada pela impossibilidade ou precariedade do acesso físico a tecnologias digitais essenciais, aflora tanto na escala geográfica - como no caso de áreas rurais e periferias urbanas desprovidas de conectividade adequada - quanto na dimensão socioeconômica, através das barreiras financeiras que obstaculizam a aquisição e atualização de dispositivos e serviços digitais por populações vulnerabilizadas (Castells, 2011).

---

[6] O *digital stalking*, também denominado ciberperseguição ou *stalking* cibernético, é conduta delituosa caracterizada pela perseguição sistemática, reiterada e indesejada de outrem mediante o emprego de tecnologias digitais e recursos telemáticos, em flagrante violação à intimidade, privacidade e tranquilidade psíquica da vítima. Tal comportamento antijurídico se materializa por intermédio de variadas modalidades de interação virtual, abrangendo, *inter alia,* o monitoramento não consentido de atividades *online*, o envio compulsivo de mensagens eletrônicas, a disseminação de conteúdos difamatórios em plataformas digitais, bem como a intrusão em dispositivos informáticos alheios mediante técnicas de engenharia social ou exploração de vulnerabilidades cibernéticas. No ordenamento jurídico pátrio, a tipificação de tal conduta encontra-se positivada na Lei nº 14.132/2021, que alterou o Código Penal para incluir o art. 147-A, instituindo o crime de perseguição ou *stalking lato sensu*, abarcando sua manifestação no ambiente digital. A *mens legislatoris,* ao introduzir tal dispositivo, visou a tutelar não apenas a incolumidade física do ofendido, mas precipuamente sua integridade psíquica e moral, frequentemente vulneradas pelas práticas ciberpersecutórias. Impende ressaltar que a comprovação do elemento subjetivo do tipo, consubstanciado no dolo específico de perturbar a esfera de privacidade da vítima, afigura-se requisito indispensável à caracterização do ilícito em comento, distinguindo-o de meros aborrecimentos ou interações digitais inofensivas, à luz dos princípios da fragmentariedade e subsidiariedade que norteiam o Direito Penal.

As discrepâncias de capital cultural, habilidades técnicas e letramento digital fundamentam uma exclusão epistemológica que afeta desproporcionalmente certos grupos sociais. A complexidade crescente das interfaces tecnológicas, aliada à rapidez de sua evolução, gestaciona vulnerabilidades específicas para grupos com acesso limitado a educação formal de qualidade, idosos, pessoas com deficiências cognitivas e indivíduos com baixos níveis de alfabetização convencional (Bauman, 2001). Simultaneamente, a invisibilidade ou representação distorcida de determinados grupos sociais nos sistemas de classificação e recomendação que estruturam o ambiente informacional contemporâneo configura uma exclusão algorítmica persistente. A sub-representação de certas categorias sociais nos conjuntos de dados utilizados para treinar sistemas algorítmicos resulta em seu funcionamento subótimo para esses grupos, criando ciclos de retroalimentação que amplificam marginalizações preexistentes[7] (Crawford, 2021).

As estruturas de governança que regulam o desenvolvimento e a implementação de tecnologias emergentes também criam vulnerabilidades específicas para grupos com limitada capacidade de influência política e econômica. A captura regulatória por interesses corporativos se manifesta na influência desproporcional de conglomerados tecnológicos sobre a elaboração de marcos normativos que disciplinam suas próprias atividades. A complexidade técnica dos fenômenos digitais, aliada à assimetria informacional entre reguladores e entidades reguladas, cria vulnerabilidades específicas para o interesse público quando contraposto a imperativos de maximização de lucro e expansão de mercado (Suzor, 2019).

A descontinuidade entre o caráter territorialmente delimitado da soberania estatal e a natureza globalmente distribuída das infraestruturas digitais engendra lacunas de governança

[7] A sub-representação de grupos sociais em conjuntos de dados de treinamento para sistemas algorítmicos tem sido amplamente documentada como fator crítico para a geração de resultados discriminatórios e a perpetuação de desigualdades estruturais. Estudos empíricos demonstram que a escassez de dados representativos de minorias raciais, de gênero ou socioeconômicas leva a modelos de *machine learning* com precisão reduzida para esses grupos, além de reproduzir estereótipos históricos. Esse fenômeno não apenas compromete a eficácia técnica dos algoritmos, mas também cria ciclos viciosos nos quais decisões automatizadas reforçam exclusões preexistentes, ampliando disparidades em setores como justiça criminal, saúde e oportunidades econômicas. A sub-representação ocorre quando determinados grupos sociais aparecem em proporção significativamente menor nos dados de treinamento em relação à sua presença na população real. Esse desequilíbrio deriva frequentemente de: 1) vieses históricos institucionalizados em bancos de dados que refletem discriminações passadas, como registros policiais com sobre-representação de grupos racializados; 2) desigualdades no acesso a tecnologias na coleta seletiva de informações por dispositivos menos presentes em comunidades de baixa renda, como no caso do aplicativo *Street Bump* em Boston, que subnotificava buracos em bairros pobres devido à menor posse de *smartphones* avançados; 3) dinâmicas de exclusão digital onde populações marginalizadas têm menor presença em plataformas online que servem como fontes primárias para treinamento de modelos de linguagem. Em problemas de classificação binária, como diagnósticos médicos ou detecção de fraudes, a classe minoritária (ex.: pacientes com câncer) pode corresponder a menos de 1% dos registros, levando modelos a ignorar padrões críticos. Esses estudos estão disponíveis em https://journals.sagepub.com/doi/10.1177/23328584241258741, https://www.scielo.br/j/eb/a/QkXT9mpFFmbDPyH9Gc4y3zS/, https://news.mit.edu/2024/researchers-reduce-bias-ai-models-while-preserving-improving-accuracy-1211 e https://www.dtibr.com/post/discrimina%C3%A7%C3%A3o-algor%C3%ADtmica-origens-conceitos-e-perspectivas-regulat%C3%B3rias-parte-1, todos acessados em 16abr25.

que podem ser estrategicamente exploradas por atores poderosos, em detrimento de indivíduos e coletividades com limitada mobilidade jurisdicional. A tecnicidade excessiva dos debates sobre política tecnológica, aliada à polarização e à fragmentação do ambiente informacional, obstaculiza a participação significativa da cidadania em decisões fundamentais sobre o desenvolvimento e implementação de tecnologias com profundos impactos sociais, econômicos e culturais (Latour, 2012).

A aceleração da inovação tecnológica, aliada à convergência entre diferentes domínios como inteligência artificial, biotecnologia, nanotecnologia e computação quântica, apresenta desafios inéditos para os marcos conceituais e normativos tradicionais. Os sistemas avançados de inteligência artificial generativa, com sua capacidade de produzir conteúdo multimodal indistinguível daquele criado por humanos, produzem riscos específicos relacionados a desinformação, manipulação de mercados, erosão da confiança epistêmica e automação de atividades criminosas, criando vulnerabilidades particulares para instituições democráticas, mercados regulados e populações com limitada literacia midiática (Solove, 2024).

A convergência entre biotecnologia e tecnologias digitais introduz vulnerabilidades de nova ordem. A democratização de técnicas como edição genética, aliada ao desenvolvimento de sistemas computacionais capazes de projetar organismos com características predeterminadas, cria riscos inéditos relacionados a biossegurança, privacidade genética e distribuição desigual de benefícios e ônus da revolução biotecnológica. Concomitantemente, a incorporação crescente de sistemas digitais na infraestrutura crítica e no tecido corporal humano - manifesta em dispositivos médicos implantáveis, próteses neuronais e interfaces cérebro-máquina - produz riscos específicos relacionados à segurança cibernética, autonomia corporal e privacidade cognitiva, criando vulnerabilidades particulares para populações com condições médicas específicas e para usuários precoces dessas tecnologias transformadoras (Haraway, 2025).

As tipologias conceituais aqui delineadas, embora não esgotem a complexidade dos fenômenos examinados, proporcionam um arcabouço analítico preliminar para a compreensão sistemática das vulnerabilidades tecnológicas contemporâneas. A identificação desses padrões arquetípicos de vulnerabilização mediada por tecnologias emergentes constitui passo fundamental para a subsequente elaboração de respostas filosóficas, jurídicas e políticas que promovam uma distribuição mais equitativa dos benefícios e riscos do desenvolvimento tecnológico.

O exame dessas tipologias evidencia a insuficiência de abordagens meramente técnicas ou procedimentais para a compreensão e o enfrentamento das vulnerabilidades geradas ou amplificadas por tecnologias emergentes. Fazem-se necessárias, como procuraremos demonstrar nas seções subsequentes, reflexões filosóficas aprofundadas que problematizem os fundamentos éticos e epistemológicos das relações entre direito, tecnologia e vulnerabilidade.

4 Perspectivas Ético-Filosóficas

As questões suscitadas pelos casos analisados demandam um exame meticuloso das matrizes filosóficas que podem subsidiar uma compreensão mais profunda das interconexões entre ordenamentos jurídicos, desenvolvimento tecnológico e estados de vulnerabilidade. Nesta seção, exploram-se potencialidades e limitações de diferentes abordagens filosóficas para o enfrentamento dos dilemas éticos contemporâneos relacionados à tecnologia, privilegiando o diálogo entre tradições deontológicas e consequencialistas, bem como a contribuição da ética do cuidado e das teorias de justiça para esse debate.

A contraposição entre perspectivas deontológicas, centradas na conformidade das ações a princípios morais universalizáveis, e abordagens consequencialistas, que avaliam a correção moral a partir dos resultados produzidos, revela-se particularmente profícua no exame das questões tecnológicas. O imperativo categórico em sua formulação clássica - "age apenas segundo uma máxima tal que possas ao mesmo tempo querer que ela se torne lei universal" -, oferece parâmetros valiosos para a avaliação ética de inovações tecnológicas[8]. Sob esse prisma, tecnologias que instrumentalizam seres humanos, reduzindo-os a meros meios para a consecução de finalidades alheias, revelar-se-iam intrinsecamente imorais, independentemente de seus eventuais benefícios práticos.

A aplicação do formalismo deontológico ao domínio tecnológico enfrenta, contudo, desafios consideráveis, particularmente em contextos caracterizados pela incerteza epistêmica quanto aos impactos futuros de determinadas inovações. A impossibilidade de prever, com razoável segurança, todas as consequências potenciais de tecnologias emergentes compromete a operacionalização do teste de universalização proposto, que pressupõe um conhecimento abrangente das implicações de determinada conduta.

As abordagens consequencialistas, exemplificadas pelo utilitarismo, deslocam o foco avaliativo dos princípios subjacentes às ações para seus efeitos concretos sobre o bem-estar coletivo. Essa tradição filosófica, ao privilegiar a maximização da utilidade social como critério moral fundamental, proporciona ferramentas conceituais relevantes para a análise de políticas tecnológicas, permitindo comparações entre diferentes cenários regulatórios com base em seus impactos agregados sobre o bem-estar. Não obstante, o cálculo utilitário enfrenta limitações significativas quando confrontado com a complexidade e a imprevisibilidade das

[8] O Imperativo Categórico, apresentado por Immanuel Kant em sua obra "Fundamentação da Metafísica dos Costumes" (1785), possui diversas formulações que expressam o mesmo princípio moral fundamental de diferentes perspectivas. A *Fórmula da Lei Universal* orienta que ajamos apenas segundo uma máxima que possamos querer que se torne lei universal, estabelecendo assim um critério de universalização para nossas ações morais. Já a *Fórmula da Humanidade* nos direciona a tratar a humanidade, tanto em nossa pessoa quanto na de qualquer outro, sempre como fim em si mesma e nunca meramente como meio, reconhecendo o valor intrínseco de cada ser racional. A *Fórmula da Autonomia,* por sua vez, enfatiza que devemos agir de modo que nossa vontade possa se considerar legisladora universal através de suas máximas, destacando a importância da autonomia moral. Por fim, a *Fórmula do Reino dos Fins* propõe que ajamos segundo máximas que possam simultaneamente ter valor de leis universais para um possível reino dos fins, concebendo uma comunidade ideal de seres racionais unidos por leis morais comuns. Todas as formulações refletem diferentes aspectos do mesmo princípio ético fundamental, que busca estabelecer uma base racional e universal para a moralidade, independente de consequências ou interesses particulares.

tecnologias contemporâneas, cuja dinâmica evolutiva frequentemente escapa aos modelos preditivos convencionais (MULGAN, 2009).

A teoria da justiça como equidade apresenta contribuições significativas para o exame das questões distributivas relacionadas à tecnologia. O experimento mental da "posição original", no qual indivíduos racionais, desprovidos de conhecimento sobre sua posição social específica, deliberam acerca dos princípios fundamentais de justiça, propicia um ponto de vista imparcial a partir do qual se podem avaliar as disparidades no acesso e nos benefícios das inovações tecnológicas. O "princípio da diferença", que admite desigualdades apenas na medida em que beneficiem os membros menos favorecidos da sociedade, oferece um parâmetro normativo robusto para a crítica de tecnologias que exacerbam disparidades sociais preexistentes (Rawls, 2016).

A abordagem das capacidades, como alternativa ao formalismo contratualista, proporciona instrumentos teóricos particularmente adequados para a análise da exclusão digital. Ao compreender a justiça não como a distribuição equitativa de bens primários, mas como a garantia de capacidades fundamentais que possibilitam uma vida digna, essa perspectiva desloca o foco da mera provisão material de recursos tecnológicos para as condições efetivas de apropriação significativa dessas tecnologias. Sob esse prisma, políticas de inclusão digital deveriam visar não apenas à universalização do acesso a dispositivos e conexões, como também à promoção de capacidades que permitam a utilização autônoma e crítica das tecnologias digitais (Nussbaum, 2011).

A ética do cuidado introduz no debate tecnológico considerações fundamentais acerca da interdependência humana e da responsabilidade relacional. Ao contestar o paradigma liberal do sujeito autônomo e autossuficiente, essa corrente filosófica enfatiza a vulnerabilidade constitutiva dos seres humanos e a centralidade das relações de cuidado para a vida social. Aplicada ao contexto tecnológico, a ética do cuidado sugere a necessidade de políticas regulatórias que priorizem a proteção dos sujeitos mais vulneráveis e que reconheçam a dimensão relacional das tecnologias digitais (Tronto, 1993).

As reflexões sobre a ética da responsabilidade diante do poder tecnológico contemporâneo complementam esse quadro teórico, introduzindo a dimensão temporal e intergeracional na avaliação ética das inovações. De acordo com essa perspectiva, o alcance e a irreversibilidade potencial das transformações tecnológicas modernas impõem um novo imperativo categórico: "age de tal maneira que os efeitos de tua ação sejam compatíveis com a permanência de uma vida humana autêntica na Terra". Essa formulação, ao enfatizar a responsabilidade para com as gerações futuras, propicia fundamentos éticos sólidos para políticas precaucionais no âmbito do desenvolvimento tecnológico (Jonas, 2006).

A teoria crítica da tecnologia, ao propor uma análise que contesta tanto o determinismo tecnológico quanto o instrumentalismo ingênuo, oferece importantes subsídios para a compreensão da dimensão política das escolhas tecnológicas. Segundo essa corrente, as tecnologias não são neutras porque incorporam valores e relações de poder específicos, que podem ser contestados e transformados mediante processos de democratização

tecnológica. Essa perspectiva ressalta a importância da participação pública na governança tecnológica, particularmente de grupos tradicionalmente excluídos dos processos decisórios nesse âmbito (Feenberg, 2002).

No contexto latino-americano, as abordagens da filosofia da libertação e da pedagogia do oprimido fornecem instrumentos teóricos valiosos para a análise crítica da colonialidade tecnológica. Essas correntes enfatizam a necessidade de tecnologias situadas, que respondam às necessidades e aspirações de comunidades locais, contrapondo-se à imposição acrítica de modelos tecnológicos desenvolvidos em contextos hegemônicos (Dussel, 2012; Freire, 2019).

O exame dessas diferentes perspectivas filosóficas evidencia a complexidade inerente aos dilemas éticos suscitados pelas tecnologias contemporâneas, sugerindo a necessidade de abordagens pluralistas que integrem elementos de diferentes tradições teóricas. Mais do que a adesão dogmática a uma única corrente filosófica, o enfrentamento adequado das questões relacionadas à vulnerabilidade tecnológica demanda um diálogo contínuo entre distintas perspectivas normativas, atento às especificidades contextuais e às vozes dos sujeitos diretamente afetados pelas inovações tecnológicas.

As diferentes perspectivas filosóficas examinadas nesta seção - desde abordagens deontológicas e consequencialistas até teorias da justiça, a abordagem das capacidades e a ética do cuidado - evidenciam a complexidade dos fundamentos normativos que podem orientar respostas adequadas às vulnerabilidades tecnológicas contemporâneas. A tradução desses princípios filosóficos em arranjos institucionais e marcos regulatórios concretos constitui o desafio central que a seção seguinte busca enfrentar, examinando como o direito contemporâneo tem respondido aos dilemas éticos e práticos suscitados pelas tecnologias disruptivas e avaliando as potencialidades e limitações dessas respostas jurídicas à luz das considerações normativas aqui desenvolvidas.

5 Perspectivas Jurídicas

A análise dos paradigmas regulatórios que emergem como resposta aos desafios impostos pelas tecnologias disruptivas se mostra fundamental para a compreensão das possibilidades e limitações do direito contemporâneo diante da aceleração tecnológica. Observa-se, nas últimas décadas, uma proliferação de iniciativas normativas voltadas à disciplina jurídica das novas tecnologias, refletindo tanto a preocupação institucional com seus potenciais impactos deletérios quanto o reconhecimento da insuficiência dos arcabouços regulatórios tradicionais para lidar com fenômenos sociotécnicos inéditos.

No âmbito da proteção de dados pessoais, o estabelecimento de legislações abrangentes como o Regulamento Geral de Proteção de Dados europeu (GDPR em inglês)[9] e a Lei Geral de Proteção de Dados brasileira (LGPD)[10] exemplifica uma tendência regulatória fundada no reconhecimento da autodeterminação informativa como direito fundamental.

[9] Disponível em https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html , acesso em 15mar25.

[10] Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm , acesso em 15mar25.

Esses diplomas normativos, ao estabelecerem princípios como a minimização de dados, a limitação de finalidade e a transparência no tratamento de informações pessoais, buscam restabelecer um equilíbrio de poder entre indivíduos e entidades que processam seus dados, mitigando vulnerabilidades informacionais (BIONI, 2018).

A efetividade desse modelo regulatório, contudo, enfrenta desafios significativos. A assimetria de conhecimentos entre usuários comuns e corporações tecnológicas complexifica a operacionalização do consentimento informado como base legítima para o tratamento de dados, enquanto a transnacionalidade dos fluxos informacionais dificulta a aplicação territorial de legislações protetivas. Ademais, o contraste entre a velocidade de desenvolvimento tecnológico e a relativa lentidão dos processos legislativos tradicionais ocasiona lacunas normativas que podem comprometer a tutela efetiva dos direitos em questão (Doneda, 2019).

A reinterpretação dos direitos fundamentais à luz dos desafios tecnológicos contemporâneos constitui outro aspecto crucial da interpenetração entre direito e tecnologia. Direitos consolidados como a privacidade, a liberdade de expressão e a igualdade adquirem novas dimensões no contexto digital, demandando adaptações hermenêuticas que preservem seu núcleo axiológico enquanto respondem a realidades sociotécnicas inéditas. O reconhecimento jurisprudencial de direitos emergentes, como o "direito ao esquecimento"[11] e o "direito à explicação" em decisões automatizadas, exemplifica esse processo de atualização interpretativa, que busca conciliar a estabilidade dos sistemas jurídicos com a dinamicidade do desenvolvimento tecnológico (Floridi, 2013).

A questão da responsabilidade civil e penal no contexto da automação e da inteligência artificial suscita desafios teóricos e práticos de particular complexidade. Os modelos tradicionais de responsabilização, fundamentados na culpabilidade individual e na causalidade direta, mostram-se insuficientes diante de sistemas sociotécnicos caracterizados por cadeias causais complexas e pela distribuição difusa de agência entre múltiplos atores humanos e não-humanos. A opacidade algorítmica dos sistemas de inteligência artificial mais sofisticados, particularmente aqueles baseados em aprendizado de máquina, dificulta a identificação precisa dos fatores determinantes de eventuais danos, comprometendo a aplicação de critérios convencionais de responsabilização (Mittelstadt et al., 2016).

[11] O denominado "direito ao esquecimento" constitui expressão da autodeterminação informativa que transcende a mera tutela da privacidade, configurando-se como prerrogativa existencial *sui generis* que faculta ao indivíduo requerer a supressão de dados pretéritos que, não obstante verídicos, ocasionam constrangimentos desproporcionais à luz do transcurso temporal. Impende ressaltar, contudo, que tal constructo normativo, não obstante sua sustentação doutrinária sobre os pilares da dignidade da pessoa humana e do livre desenvolvimento da personalidade, não encontra guarida no ordenamento pátrio desde o paradigmático julgamento do Tema 786 de Repercussão Geral pelo Supremo Tribunal Federal, que, por maioria, refutou a tese de sua compatibilidade com o sistema constitucional brasileiro, assentando a impossibilidade de obstar a divulgação de fatos verídicos, ainda que desabonadores. A decisão pretoriana, de efeito vinculante e eficácia *erga omnes,* cristalizou o entendimento de que a memória coletiva e o direito à informação preponderam sobre eventuais pretensões individuais de oblívio compulsório, ressalvada a tutela específica contra ilícitos autônomos que possam decorrer da forma ou do contexto da divulgação, mediante instrumentos jurídicos diversos que não importem em censura informativa de dados historicamente relevantes (disponível em https://jurisprudencia.stf.jus.br/pages/search/sjur446557/false, acessado em 29abr25).

Diferentes abordagens têm sido propostas para enfrentar esse desafio regulatório. Modelos de responsabilidade objetiva, que dispensam a comprovação de culpa e enfatizam o nexo causal entre atividade e dano, oferecem vantagens em termos de proteção das vítimas; entretanto, podem desestimular inovações tecnológicas benéficas. Abordagens baseadas na teoria do risco, que atribuem responsabilidade ao agente que introduz tecnologias potencialmente perigosas no meio social, equilibram a necessidade de reparação com a preservação de incentivos à inovação responsável. A emergência de modelos híbridos, que combinam elementos de diferentes tradições jurídicas, reflete a complexidade inerente à regulação de tecnologias cujos impactos escapam às categorias tradicionais do pensamento jurídico.

A tensão entre inovação tecnológica e princípios jurídicos consolidados se materializa com particular intensidade no debate sobre regulação *ex ante versus* regulação *ex post.* Abordagens precaucionais, que enfatizam a prevenção de danos potencialmente irreversíveis mediante controles prévios rigorosos, confrontam-se com perspectivas mais permissivas, que privilegiam a experimentação tecnológica e reservam a intervenção regulatória para o momento posterior à constatação de danos concretos. Essa tensão reflete divergências mais profundas acerca do papel do direito na sociedade contemporânea e de sua relação com o desenvolvimento tecnológico (Suzor, 2019).

O constitucionalismo digital oferece uma perspectiva teórica relevante para a compreensão dessas tensões. Segundo essa corrente, o ambiente digital, caracterizado pela fragmentação, pela descentralização e pela autogovernança, desafia pressupostos fundamentais do constitucionalismo moderno, como a centralidade do Estado-nação e a distinção clara entre esferas pública e privada. A preservação dos ideais normativos do constitucionalismo em um contexto radicalmente transformado pela tecnologia digital demandaria, nessa perspectiva, a elaboração de novos arranjos institucionais e princípios regulatórios, capazes de responder à complexidade e à transnacionalidade das relações mediadas por tecnologias emergentes (Celeste, 2018).

A abordagem da regulação por implementação ou *design,* que busca incorporar valores e princípios jurídicos no próprio desenho de sistemas tecnológicos, representa uma tentativa promissora de conciliar inovação e proteção de direitos fundamentais. Ao deslocar parte do ônus regulatório para a fase de concepção das tecnologias, essa perspectiva busca prevenir danos potenciais antes de sua ocorrência, alinhando incentivos econômicos com imperativos éticos e jurídicos. Iniciativas como *Privacy by Design (PbD)* e *Value Sensitive Design (VSD)*[12]

[12] *Privacy by Design* e *Value Sensitive Design* são duas abordagens complementares para o desenvolvimento ético de tecnologias. *Privacy by Design* defende a incorporação da privacidade desde o início do desenvolvimento de produtos e serviços, através de medidas proativas em vez de reativas. *Value Sensitive Design* amplia essa perspectiva ao considerar como os valores humanos fundamentais (como autonomia, bem-estar e justiça) podem ser integrados sistematicamente durante todo o processo de design tecnológico. Ambas as metodologias reconhecem que os valores e princípios éticos devem ser elementos estruturais do *design,* e não apenas considerações posteriores, resultando em tecnologias que respeitam a dignidade e os direitos dos usuários.

exemplificam essa tendência, que encontra respaldo teórico na formulação "code is law" - o código é lei (Floridi, 2013).

A governança algorítmica, compreendida como o conjunto de arranjos institucionais, normas e práticas que orientam o desenvolvimento e a implementação de sistemas algorítmicos, emerge como domínio regulatório estratégico na sociedade contemporânea. A elaboração de princípios éticos para inteligência artificial, exemplificada por iniciativas como as "Diretrizes Éticas para uma IA Confiável" da União Europeia[13], busca estabelecer parâmetros normativos para o desenvolvimento responsável dessas tecnologias. Não obstante, a tradução desses princípios abstratos em mecanismos regulatórios concretos e eficazes permanece um desafio considerável, demandando a articulação entre diferentes modalidades de regulação -- estatal, autorregulação privada e regulação técnica (Coeckelbergh, 2020).

No contexto específico da vulnerabilidade digital, abordagens regulatórias interseccionais, atentas às múltiplas dimensões da desigualdade social, tornam-se particularmente necessárias. A proteção efetiva de sujeitos e grupos vulneráveis no ambiente digital demanda não apenas regras formalmente igualitárias, mas também mecanismos compensatórios que reconheçam e mitiguem disparidades estruturais no acesso e na apropriação de tecnologias (FRASER, 2009). Nessa perspectiva, o direito à inclusão digital passa de mero corolário do princípio da igualdade formal a verdadeira expressão de um compromisso substantivo com a justiça social no contexto da sociedade informacional.

A experiência regulatória internacional evidencia a diversidade de abordagens possíveis para o enfrentamento dos desafios tecnológicos contemporâneos. O modelo europeu, caracterizado por uma regulação abrangente e principiológica, contrasta com a abordagem setorial e minimalista tradicionalmente adotada nos Estados Unidos, enquanto países emergentes como Brasil e Índia desenvolvem modelos híbridos que buscam conciliar a proteção de direitos fundamentais com particularidades socioeconômicas locais. Essa pluralidade regulatória, se por um lado dificulta a harmonização internacional de normas, por outro possibilita experimentações institucionais valiosas para o aprimoramento dos mecanismos de governança tecnológica.

A análise das perspectivas jurídicas aqui empreendida explicita tanto o potencial transformador do direito diante dos desafios tecnológicos contemporâneos quanto suas limitações inerentes[14]. A efetividade dos mecanismos jurídicos tradicionais depende, crescentemente, de sua articulação com outras modalidades regulatórias - técnicas,

[13] Disponível em https://www.consilium.europa.eu/pt/policies/artificial-intelligence/, acesso em 15mar25.

[14] Artigo publicado pela Semantic Scholar sobre o direito fundamental à proteção de dados pessoais analisa as externalidades da economia digital que implicam restrições às liberdades e à autodeterminação informacional. O estudo reconhece a vulnerabilidade do titular de dados pessoais em um cenário de assimetria informacional, propondo a utilização de instrumentos da tutela coletiva para reprimir a "normatividade tecnológica da economia digital". A análise converge com a discussão presente no artigo sobre a inadequação conceitual-normativa dos marcos jurídicos tradicionais para lidar com fenômenos emergentes. O estudo destaca a necessidade de interpretação das normas de proteção de dados de forma a reconhecer a vulnerabilidade estrutural dos titulares frente ao poder econômico e informacional das entidades que processam seus dados. Disponível em https://www.semanticscholar.org/paper/Direito-fundamental-%C3%A0-prote%C3%A7%C3%A3o-de-dados-pessoais%3A-a-Macedo/c3b49804ef4502c48d90c2a1d47be53f5f6c0989, acesso em 16abr25.

mercadológicas, sociais - em um contexto de governança policêntrica e multinível. Mais do que um conjunto estático de normas, o direito contemporâneo se apresenta como processo dinâmico de aprendizagem institucional, que busca responder à complexidade e à imprevisibilidade das transformações sociotécnicas mediante a constante revisão de seus pressupostos fundamentais (Magrani, 2019).

5 Considerações Finais

A exploração multidimensional das interfaces entre ordenamentos jurídicos, avanços tecnológicos e estados de vulnerabilidade, empreendida ao longo deste ensaio, evidencia a complexidade inerente a esse campo de investigação, irredutível a abordagens disciplinares estanques ou a soluções técnicas simplificadoras. Os dilemas éticos, jurídicos e políticos suscitados pela aceleração tecnológica contemporânea demandam, como procuramos demonstrar, perspectivas integradoras que articulem diferentes tradições de pensamento e que reconheçam a indissociabilidade entre questões normativas e questões empíricas nesse domínio (Amoore, 2020).

As reflexões desenvolvidas não pretendem oferecer respostas definitivas para os complexos dilemas suscitados pela intersecção entre direito, tecnologia e vulnerabilidade, e sim contribuir para um debate público informado e crítico sobre questões que afetam, de maneira crescente, a vida de indivíduos e coletividades em todo o mundo. A construção de uma sociedade tecnológica mais justa e democrática demanda um compromisso coletivo contínuo com a reflexão crítica e com a experimentação institucional, guiadas por valores como a dignidade humana, a solidariedade e a sustentabilidade.

O reconhecimento da vulnerabilidade como condição ontológica compartilhada, longe de conduzir ao fatalismo ou à resignação, apresenta-se como ponto de partida para a elaboração de práticas e arranjos institucionais que mitiguem formas evitáveis de sofrimento e vulnerabilização. Nesse sentido, a vulnerabilidade se revela não apenas como problema a ser superado, mas como condição existencial que fundamenta éticas do cuidado e da responsabilidade, necessárias para a convivência humana significativa em um mundo crescentemente tecnológico (Fineman, 2008).

A complexidade e a dinamicidade das questões abordadas sugerem a necessidade de uma vigilância epistêmica contínua, que reconheça o caráter provisório e situado de nossas compreensões atuais e que se mantenha aberta a reformulações substantivas diante de transformações sociotécnicas imprevisíveis. Essa postura de humildade epistêmica, combinada com um compromisso ético robusto com a promoção da dignidade humana, desponta como diretriz fundamental para navegarmos os desafios tecnológicos do presente e do futuro próximo.

Em síntese, a intersecção entre direito, tecnologia e vulnerabilidade desvela cenário de latitude epistêmica para reflexões filosóficas e experimentações institucionais que busquem conciliar o potencial emancipatório das inovações tecnológicas com a proteção de valores fundamentais como a justiça, a autonomia e a solidariedade. O enfrentamento das

vulnerabilidades tecnológicas contemporâneas demanda abordagens pluralistas e contextualmente sensíveis, que reconheçam tanto a especificidade das diferentes formas de vulnerabilização quanto suas raízes estruturais comuns em assimetrias de poder econômico, político e epistêmico (Feenberg, 2008).

A tecnologia, enquanto produto da criatividade e da intencionalidade humanas, permanece aberta a reconfigurações que podem tanto amplificar quanto mitigar vulnerabilidades existentes. O direito, como instrumento de mediação social e expressão de valores comunitários, possui papel crucial nesse processo de reconfiguração, estabelecendo limites legítimos à exploração mercantil e estatal de vulnerabilidades e promovendo condições institucionais para o desenvolvimento de tecnologias inclusivas e emancipatórias. A realização desse potencial regulatório, contudo, depende da contínua renovação crítica dos pressupostos epistemológicos, metodológicos e axiológicos que fundamentam a normatividade jurídica, em diálogo permanente com outras formas de conhecimento e com as experiências concretas dos sujeitos afetados pelas transformações tecnológicas.

Ao concluir esta análise, reafirmamos o caráter inevitavelmente político e valorativo das escolhas tecnológicas, contestando tanto o determinismo fatalista quanto o otimismo ingênuo que frequentemente caracterizam os debates públicos sobre tecnologia. A construção de futuros tecnológicos mais justos e democráticos demanda o engajamento crítico e criativo de diversas vozes e perspectivas, em um processo contínuo de deliberação pública que não se restrinja a especialistas técnicos ou políticos profissionais, mas que incorpore significativamente as experiências e aspirações daqueles historicamente excluídos dos processos decisórios nesse âmbito (Feenberg, 2002).

A vulnerabilidade, compreendida não como fragilidade a ser superada, porém como condição existencial compartilhada que fundamenta relações éticas de cuidado e responsabilidade, põe-se como horizonte normativo fundamental para repensar nossas relações com as tecnologias e para orientar processos de inovação tecnológica mais atentos as necessidades e aspirações de diferentes sujeitos e coletividades. Essa compreensão relacional da vulnerabilidade, ao contestar o ideal moderno do sujeito autônomo e autossuficiente, propicia bases conceituais fecundas para a crítica de tecnologias que exacerbam o individualismo possessivo e para a construção de alternativas tecnológicas que reconheçam e fortaleçam nossos vínculos de interdependência (Tronto, 1993).

Os desafios tecnológicos do século XXI, em sua complexidade e magnitude sem precedentes, convidam-nos a reimaginar radicalmente nossas instituições políticas e jurídicas, nossas práticas sociais e culturais, e nossos pressupostos filosóficos fundamentais. O enfrentamento desses dilemas tecnocientíficos demanda não apenas inovações técnicas ou regulatórias pontuais, como também transformações profundas em nossas concepções de conhecimento, de poder e de comunidade, orientadas pela busca incessante de formas de convivência que conciliem o florescimento individual com a sustentabilidade ecológica e com a justiça social (Jonas, 2006).

Que as reflexões aqui desenvolvidas possam contribuir, ainda que modestamente, para esse necessário e urgente processo de reimaginação coletiva de nossos futuros tecnológicos possíveis.

Referências

AMOORE, Louise. *Cloud Ethics:* Algorithms and the Attributes of Ourselves and Others. Durham: Duke University Press, 2020;

BAUMAN, Zygmunt. *Modernidade Líquida.* Rio de Janeiro: Zahar, 2001;

BENJAMIN, Ruha. *Race After Technology:* Abolitionist Tools for the New Jim Code. Cambridge: Polity Press, 2019;

BIONI, Bruno. *Proteção De Dados Pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2018;

CASTELLS, Manuel. *A Sociedade Em Rede.* São Paulo: Paz e Terra, 2011;

COECKELBERGH, Mark. *Ai Ethics.* Cambridge: MIT Press, 2020;

CELESTE, Edoardo. Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges. In *Hiig Discussion Paper Series* n. 2018-02, 2018;

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:* fundamentos da lei geral de proteção de dados. São Paulo: Thomson Reuters Brasil, 2019;

DUSSEL, Enrique. *Ética Da Libertação Na Idade Da Globalização E Da Exclusão*. 4ª ed. Petrópolis: Vozes, 2012;

FEENBERG, Andrew. *Transforming Technology:* A Critical Theory Revisited. New York: Oxford University Press, 2002;

FEENBERG, Andrew. *Questioning Technology.* London: Routledge, 2008;

FINEMAN, Martha Albertson. The Vulnerable Subject: Anchoring Equality in the Human Condition. In *Yale Journal Of Law & Feminism,* v. 20, n. 1, 2008;

FLORIDI, Luciano. *The Ethics Of Information.* Oxford: Oxford University Press, 2013;

FRASER, Nancy. *Scales Of Justice:* Reimagining Political Space in a Globalizing World. New York: Columbia University Press, 2009;

FREIRE, Paulo. *Pedagogia Do Oprimido.* 84.ed. Rio de Janeiro/São Paulo: Paz e Terra, 2019;

HARAWAY, Donna. Manifesto Ciborgue: Ciência, tecnologia e feminismo-socialista no final do século XX. In SILVA, Tomaz Tadeu da (organizador). *Antropologia Do Ciborgue:* As vertigens do pós-humano. Belo Horizonte: Autêntica, 2025;

JONAS, Hans. *O Princípio Responsabilidade:* Ensaio de uma ética para a civilização tecnológica. Rio de Janeiro: Contraponto, 2006;

LATOUR, Bruno. *Reagregando O Social:* Uma introdução à Teoria do Ator-Rede. Salvador: EDUFBA, 2012;

MAGRANI, Eduardo. *Entre Dados E Robôs:* Ética e Privacidade na Era da Hiperconectividade. Porto Alegre: Arquipélago Editorial, 2019.

MENDES, Laura Schertel. *Privacidade, Proteção De Dados E Defesa Do Consumidor:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014;

MITTELSTADT, Brent Daniel *et alii.* The Ethics of Algorithms: Mapping the Debate. In *Big Data & Society***,** v. 3, n. 2, 2016;

MULGAN, Tim. *Future People:* A Moderate Consequentialist Account of our Obligations to Future Generations. Oxford: Oxford University Press, 2009;

NOBLE, Safiya Umoja. *Algorithms Of Oppression:* How Search Engines Reinforce Racism. New York: NYU Press, 2018;

NUSSBAUM, Martha. *Creating Capabilities:* The Human Development Approach. Cambridge: Harvard University Press, 2011;

O'NEIL, Cathy. *Weapons Of Math Destruction:* how big data increases inequality and threatens democracy. New York: Crown, 2016;

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

PISTOR, Katharina. *The Code Of Capital:* How the Law Creates Wealth and Inequality. Princeton: Princeton University Press, 2019;

RAWLS, John. *Uma Teoria Da Justiça.* 4.ed. São Paulo: Martins Fontes, 2016;

RODOTÀ, Stefano. *A Vida Na Sociedade Da Vigilância:* A privacidade hoje. Rio de Janeiro: Renovar, 2008;

SOLOVE, Daniel J. *Understanding Privacy.* Cambridge: Harvard University Press, 2008;

SOLOVE, Daniel J. Artificial Intelligence and Privacy. In *Gwu Legal Studies.* Research Paper n. 2024-36, disponível em https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=4713111#, acessado em 02fev25;

SUZOR, Nicolas P. Lawless. *The Secret Rules That Govern Our Digital Lives.* Cambridge: Cambridge University Press, 2019;

TRONTO, Joan C. *Moral Boundaries:* A Political Argument for an Ethic of Care. New York: Routledge, 1993;

VÉLIZ, Carissa. *Privacy Is Power:* Why and How You Should Take Back Control of Your Data. London: Bantam Press, 2020;

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*, v. 7, n. 2, p. 76-99, 2017;

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism:* The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019.

Recebido em: 30/04/2025
Aprovado em: 07/11/2025
Publicado em: 02/12/2025