IA em Saúde, Profiling e Proteção de Dados: tensões entre inovação tecnológica, biodireito e direitos fundamentais*

IA en Salud, Profiling y Protección de Datos: tensiones entre innovación tecnológica, bioderecho y derechos fundamentales

AI in Health, Profiling and Data Protection: tensions between technological innovation, biolaw and fundamental rights

IA in Salute, Profiling e Protezione dei Dati: tensioni tra innovazione tecnologica, biodiritto e diritti fondamentali

Bruno Nazih Nehme Nassar[1]
Mestrando do PPG em Direito da Saúde, Universidade Santa Cecília, Santos, SP, Brasil

Alexandre Rocha Almeida de Moraes[2]
Doutor, PPG em Direito da Saúde, Universidade Santa Cecília, Santos, SP, Brasil,

RESUMO: Contextualização: O avanço da inteligência artificial (IA) na saúde apresenta promessas de diagnósticos mais precisos e tratamentos individualizados, mas também gera relevantes tensões jurídicas e bioéticas. Os riscos advindos dessas tecnologias demandam revisões constantes do arcabouço normativo que as circunda. O presente artigo examina um desses riscos, investigando eventual insuficiência da Lei Geral de Proteção de Dados (LGPD) para lidar com desafios associados ao uso de dados sensíveis e técnicas de *profiling*, que representam ameaça à proteção da privacidade, à isonomia e ao livre desenvolvimento da personalidade. **Objetivo:** O objetivo do estudo é analisar criticamente a pretensa neutralidade algorítmica, identificar as fragilidades da regulação vigente e propor uma leitura consequencialista do conceito de dado pessoal, integrando-o aos princípios do Biodireito, em especial o da precaução. **Métodos**: A metodologia adotada foi dedutiva, com base em análise documental e revisão bibliográfica, nacional e internacional, além de exame comparativo com instrumentos normativos estrangeiros, como o Regulamento Geral de Proteção de Dados (GDPR) e o *Artificial Intelligence Act*, da União Europeia. **Resultados:** Os resultados demonstram que a LGPD apresenta lacunas relevantes, notadamente a exclusão de dados anonimizados de sua incidência, o que fragiliza a tutela da personalidade, bem como a ausência de restrições claras a decisões automatizadas com efeitos significativos. Evidenciam-se ainda riscos decorrentes da opacidade técnica e econômica dos sistemas de IA, que favorecem discriminações sutis e dificultam a responsabilização. **Conclusões:** Conclui-se que o direito brasileiro, ao privilegiar uma lógica reativa de controle, não oferece salvaguardas suficientes

---

* Esse trabalho foi apresentado originalmente no VII Congresso Internacional de Direito da Saúde, realizado em 23, 24 e 25 de outubro de 2025 na Universidade Santa Cecília (Unisanta). Em função da recomendação de publicação da Comissão Científica do Congresso, fez-se a presente versão.

1 Advogado, bacharel em Direito pela PUC/SP, Especialista em Direito Digital pela PUC/RS e em Direito Penal pela ESMP, mestrando em Direito da Saúde na Unisanta, com bolsa provida pela CAPES. CV: http://lattes.cnpq.br/0855052242442027. E-mail: bnnnassar@gmail.com. ORCID: https://orcid.org/0009-0001-6070-0514.

2 Promotor de Justiça do Ministério Público do Estado de São Paulo. Mestre e Doutor em Direito pela Pontifícia Universidade Católica de São Paulo CV: http://lattes.cnpq.br/9309967566132792. E-mail: aram.mp@gmail.com. ORCID: https://orcid.org/0000-0002-8374-5694.

para enfrentar os desafios da era digital, sendo imprescindível o alinhamento da LGPD a uma abordagem preventiva e consequencialista, a maior integração com princípios do Biodireito e a previsão de mecanismos robustos de transparência, auditabilidade e intervenção humana nos sistemas de IA em saúde.

Palavras-chave: Inteligência Artificial; LGPD; Biodireito; *Profiling*; Dados Sensíveis.

RESUMEN: Contextualización*: El avance de la inteligencia artificial (IA) en la salud presenta promesas de diagnósticos más precisos y tratamientos individualizados, pero también genera relevantes tensiones jurídicas y bioéticas. Los riesgos derivados de estas tecnologías exigen revisiones constantes del marco normativo que las rodea. El presente artículo examina uno de esos riesgos, investigando la eventual insuficiencia de la Ley General de Protección de Datos (LGPD) para afrontar los desafíos asociados al uso de datos sensibles y técnicas de profiling, que representan una amenaza a la protección de la privacidad, a la igualdad y al libre desarrollo de la personalidad.* ***Objetivo****: El objetivo del estudio es analizar críticamente la pretendida neutralidad algorítmica, identificar las fragilidades de la regulación vigente y proponer una lectura consecuencialista del concepto de dato personal, integrándolo a los principios del Bioderecho, en especial al de precaución.* ***Métodos****: La metodología adoptada fue deductiva, basada en análisis documental y revisión bibliográfica, nacional e internacional, además de un examen comparativo con instrumentos normativos extranjeros, como el Reglamento General de Protección de Datos (GDPR) y el Artificial Intelligence Act de la Unión Europea.* ***Resultados****: Los resultados demuestran que la LGPD presenta lagunas relevantes, en particular la exclusión de los datos anonimizados de su ámbito de aplicación, lo que debilita la tutela de la personalidad, así como la ausencia de restricciones claras a las decisiones automatizadas con efectos significativos. También se evidencian riesgos derivados de la opacidad técnica y económica de los sistemas de IA, que favorecen discriminaciones sutiles y dificultan la atribución de responsabilidades.* ***Conclusiones****: Se concluye que el derecho brasileño, al privilegiar una lógica reactiva de control, no ofrece salvaguardas suficientes para enfrentar los desafíos de la era digital, siendo imprescindible el alineamiento de la LGPD con un enfoque preventivo y consecuencialista, una mayor integración con los principios del Bioderecho y la previsión de mecanismos sólidos de transparencia, auditabilidad e intervención humana en los sistemas de IA en salud.*

Palabras clave: *Inteligencia Artificial; LGPD; Bioderecho; Profiling; Datos Sensibles.*

ABSTRACT: Context*: The advancement of artificial intelligence (AI) in healthcare brings promises of more accurate diagnoses and personalized treatments, but also generates significant legal and bioethical tensions. The risks arising from these technologies demand constant revisions of the regulatory framework surrounding them. This article examines one of these risks by investigating the potential insufficiency of the Brazilian General Data Protection Law (LGPD) to address challenges associated with the use of sensitive data and profiling techniques, which pose threats to privacy protection, equality, and the free development of personality.* ***Objective****: The aim of this study is to critically analyze the alleged algorithmic neutrality, identify weaknesses in the current regulation, and propose a consequentialist interpretation of the concept of personal data, integrating it into the principles of Biolaw, particularly the precautionary principle.* ***Methods****: The methodology adopted was deductive, based on documentary analysis and literature review, both national and international, as well as comparative examination of foreign regulatory instruments such as the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act of the European Union.* ***Results****: The findings show that the LGPD presents significant gaps, notably the exclusion of anonymized data from its scope, which undermines personality protection, as well as the absence of clear restrictions on automated decisions with significant effects. Risks also emerge from the technical and economic opacity of AI systems, which enable subtle forms of discrimination and hinder accountability.* ***Conclusions****: It is concluded that Brazilian law, by privileging a reactive control logic, does not provide sufficient safeguards to address the challenges of the digital age. It is therefore essential to align the LGPD with a preventive and consequentialist approach, to strengthen its integration with Biolaw principles, and to ensure robust mechanisms for transparency, auditability, and human intervention in healthcare AI systems.*

Keywords: *Artificial Intelligence; LGPD; Biolaw; Profiling; Sensitive Data.*

RIASSUNTO: Contestualizzazione*: L'avanzamento dell'intelligenza artificiale (IA) nella sanità porta con sé la promessa di diagnosi più accurate e trattamenti personalizzati, ma genera anche rilevanti tensioni giuridiche e bioetiche. I rischi derivanti da queste tecnologie richiedono revisioni costanti dell'impianto normativo che le circonda. Il presente articolo esamina uno di tali rischi, indagando la possibile insufficienza della Legge Generale sulla Protezione dei Dati (LGPD) nell'affrontare le sfide legate all'uso di dati sensibili e delle tecniche di profiling, che rappresentano una minaccia alla tutela della privacy, all'uguaglianza e al libero sviluppo della personalità.* ***Obiettivo****: L'obiettivo dello studio è analizzare criticamente la presunta neutralità algoritmica, individuare le fragilità della regolamentazione vigente e proporre una lettura consequenzialista del concetto di dato personale, integrandolo con i principi del Biodiritto, in particolare con*

quello di precauzione. ***Metodi****: La metodologia adottata è stata deduttiva, basata su analisi documentale e revisione bibliografica, sia nazionale che internazionale, oltre a un esame comparativo con strumenti normativi stranieri, come il Regolamento Generale sulla Protezione dei Dati (GDPR) e l'Artificial Intelligence Act dell'Unione Europea.* ***Risultati****: I risultati dimostrano che la LGPD presenta lacune rilevanti, in particolare l'esclusione dei dati anonimizzati dal suo campo di applicazione, che indebolisce la tutela della personalità, così come l'assenza di restrizioni chiare alle decisioni automatizzate con effetti significativi. Emergono inoltre rischi derivanti dall'opacità tecnica ed economica dei sistemi di IA, che favoriscono discriminazioni sottili e ostacolano l'attribuzione di responsabilità.* ***Conclusioni****: Si conclude che il diritto brasiliano, privilegiando una logica reattiva di controllo, non offre garanzie sufficienti per affrontare le sfide dell'era digitale. È quindi imprescindibile l'allineamento della LGPD a un approccio preventivo e consequenzialista, una maggiore integrazione con i principi del Biodiritto e la previsione di meccanismi solidi di trasparenza, verificabilità e intervento umano nei sistemi di IA in sanità.*

Parole chiave: *Intelligenza Artificiale; LGPD; Biodiritto; Profiling; Dati Sensibili.*

Introdução

Os séculos XX e XXI têm como marca distintiva vertiginosos saltos tecnológicos, mormente no que diz respeito a biotecnologias. No entanto, quaisquer avanços científicos vêm necessariamente acompanhados de questionamentos éticos e jurídicos relevantes quanto à sua aplicação, inclusive à luz daquilo que Beck convencionou chamar de "sociedade de riscos" (Beck, 2011).

Por isso, no campo da saúde, tomaram forma os campos da Bioética e do Biodireito.

A Bioética surge a partir de uma demanda teórica face os problemas éticos que as ciências biológicas passam a suscitar. Nesse sentido, Diego Garcia coloca que a Bioética surgiu por absoluta necessidade, em decorrência da revolução nas ciências biológicas e médicas, citando como marcos relevantes o descobrimento da biologia molecular (1950/1960), do código genético (1960) e da recombinação do DNA (1970) (Garcia, 2010, p. 472).

Assim, é a consolidação do conhecimento científico das ciências biológicas e médicas às ciências sociais, com o consequente fortalecimento da autonomia individual.

O Informe Belmont, ao final da década de 70, traça os princípios da Bioética: autonomia, beneficência e justiça. No entanto, a questão ainda se hospedava apenas no campo da moral. Em um segundo momento, essas demandas sociais efervescentes são absorvidas pelo Direito, em verdadeira expressão do tridimensionalismo (fato, valor e norma), observado por Reale (Reale, 1999).

Nasce o Biodireito, que trabalha com princípios próprios, que podem ser resumidos como: precaução, autonomia privada, responsabilidade e dignidade (Naves; Sá, 2023, posição 1.463).

Conforme destacam Naves e Sá, os impactos sociais decorrentes das inovações biomédicas, engenharia genética e altas tecnologias aplicadas à saúde foram decisivos para a criação de um novo microssistema jurídico, com princípios próprios, concebido como Biodireito (Naves; Sá, 2023, posição 919).

A natureza interdisciplinar dos problemas, a sobreposição de sistemáticas públicas e privadas, e a necessidade de respostas específicas a desafios novos, todos conduziram ao aperfeiçoamento desse ramo autônomo do Direito, cuja dialética clássica sempre foi o equilíbrio entre inovação tecnológica e proteção da saúde individual e coletiva.

Assim, o Direito moderno funciona (ou clama por funcionar) como um sistema aberto, perene a demandas sociais e a contribuições de outras áreas do conhecimento. A crise do positivismo foi precursora dessa nova conformação jurídica.

Atualmente, esse arcabouço jurídico na área da saúde se defronta com dois importantes conjuntos de problemas, que se entrelaçam: a gestão de dados pessoais relacionados à saúde, classificados como sensíveis pela Lei Geral de Proteção de Dados (LGPD) (art. 5º, II), e o emprego de sistemas de inteligência artificial (IA) nas áreas médicas.

Esses desafios contemporâneos testam de maneira ímpar a capacidade do sistema jurídico em apresentar soluções eficazes para problemas em constante e rápida evolução, bem como em dialogar com outras áreas do conhecimento, como estatística, ciência da computação, segurança da informação, cibernética etc.

Os benefícios prometidos pelo emprego de IA na saúde são promissores. Diagnósticos mais rápidos e precisos, identificação antecipada de riscos epidemiológicos, tratamentos individualizados e de melhor qualidade.

De fato, as promessas de um futuro edílico guiado por forças de inteligência artificial são tentadoras e movimentam uma indústria multibilionária, porém, ofuscam os riscos concretos inerentes a essas tecnologias, desde tutela da privacidade e proteção de dados pessoais, até proteção do princípio da isonomia, proteção do trabalhador em uma indústria crescentemente automatizada[3], ameaças ao meio ambiente e questionamentos da própria noção do que significa ser humano e aprender em uma era de culto a uma "inteligência" artificial.[4]

É especialmente preocupante um dos principais argumentos que embasa a proliferação dessas tecnologias, qual seja, a ideia de que sistemas de IA seriam mais objetivos e neutros do que seres humanos, de modo que a delegação de funções humanas à máquina tornará processos não só mais eficientes, como mais igualitários.

Por detrás dessas tecnologias, contudo, há interesses humanos, calcados em vieses econômicos, sociais e políticos, nada neutros. A opacidade inerente a esses sistemas que, como se verá, se desdobra em diversas camadas, dificulta a percepção desse maquinário.

De outro lado, uma das premissas da indústria da inteligência artificial é que toda experiência pode ser reduzida a dados que apenas estão aguardando para ser "minerados". Com

3 Muito olvidado que o art. 7º da Constituição prevê a "XXVII - proteção em face da automação, na forma da lei". O dispositivo, previsto desde a redação original da Constituição e que carece de regulação, é sintomático da sensibilidade do constituinte originário com um receio de substituição da massa trabalhadora, presente desde a Revolução Industrial. É temor que nunca se concretizou de maneira substancial, considerando que o surgimento de novas tecnologias, apesar de extinguir determinados postos de trabalho, historicamente veio acompanhado da criação de novas funções. Nada obstante, os avanços em inteligência artificial, que ameaçam substituir e enxugar até mesmo a massa de programadores hoje lhe sustenta, ainda não ofereceu respostas acalentadoras quanto a esse risco.

4 A indústria da tecnologia, encabeçada pelas conhecidas "Big Techs", nutre o mito de que sistemas não humanos são ou podem ser análogos a mentes humanas. Conforme Crawford, deflagra, essa perspectiva assume que a inteligência humana está ao alcance da indústria tecnológica, podendo ser emulada, bastando investimentos generosos em recursos e treinamento suficientes. A autora, então, provoca que: "(…) I argue that AI is neither artificial nor intelligent. Rather, artificial intelligence is both embodied and material, made from natural resources, fuel, human labor, infrastructures, logistics, histories, and classifications. AI systems are not autonomous, rational, or able to discern anything without extensive, computationally intensive training with large datasets or predefined rules and rewards. In fact, artificial intelligence as we know it depends entirely on a much wider set of political and social structures. And due to the capital required to build AI at scale and the ways of seeing that it optimizes AI systems are ultimately designed to serve existing dominant interests. In this sense, artificial intelligence is a registry of power" (Crawford, 2021, posição 123)

esse espírito, cada minúsculo detalhe da experiência humana, cada dado biométrico, cada hábito, cada livro já escrito, cada imagem já produzida, cada emoção, representam meros "*datasets*" que aguardam mineração. Nesse sentido, privacidade, intimidade e proteção de dados pessoais representam meros empecilhos a um plano desenvolvimentista de um aparato tecnológico.

Atualmente, até mesmo dados neurais se encontram ao alcance da indústria da tecnologia (Yuste, 2017), abrindo caminhos para um futuro mapeamento complexo do cérebro humano, de modo que nem mesmo o pensamento escaparia ao apetite de *Big Techs* por dados pessoais.

A coleta, tratamento e controle de dados pessoais, dessarte, se torna o novo recurso que dita dinâmicas de poder, criando as bases para aquilo que Zuboff chama de "capitalismo de vigilância" (Zuboff, 2021). Ainda, alimenta o fascínio pela construção de modelos preditivos com cada vez maior acurácia. Com dados pessoais como sua matéria prima, a indústria da tecnologia espera avaliar, prever e, quiçá, moldar, comportamentos de indivíduos e grupos. Esse controle ocorre em pequenas escalas, como em recomendações de conteúdo por plataformas de streaming ou marketplaces virtuais, até decisões de maior impacto, como avaliação de risco para concessão de crédito por instituições bancárias.

Técnicas de *profiling*, mediante decisões automatizadas impulsionadas por sistemas de inteligência artificial, cuja regulação é pouco explorada na LGPD, representam uma das maiores ameaças ao desenvolvimento da personalidade e liberdades individuais, apresentando lacunas perigosas, como no que diz respeito à conceituação de dado pessoal, que exclui de sua incidência dados anonimizados.

Em se tratando de dados sensíveis ligados à saúde, a questão é especialmente delicada considerando o alto risco de perfilamento que a má-gestão desses dados representa.

Diante desse cenário, o presente artigo busca questionar precisamente a pretensa neutralidade de sistemas de IA à luz de técnicas de *profiling*, contrastando-as com a doutrina especializada sobre o tema, com princípios do Biodireito, mormente o princípio da precaução, e com regras e princípios da LGPD.

Para tanto, a pesquisa perpassará três camadas. Primeiro, endereçará o mito da neutralidade algorítmica de sistemas de inteligência artificial e suas ameaças concretas ao princípio da isonomia. Em sequência, explorará o desenho jurídico de dados pessoais sensíveis ligados à saúde na LGPD e a regulação de técnicas de *profiling*. Por fim, à luz dos princípios do Biodireito, avaliará a consonância do arcabouço jurídico atual com as finalidades da proteção de dados pessoais na área da saúde, bem como eventuais propostas de incremento do sistema de proteção.

A metodologia adotada foi dedutiva, pautada na análise documental e revisão bibliográfica, incluindo livros e artigos científicos sobre privacidade digital, proteção de dados pessoais e direito da saúde, bem como pesquisa documental das normas jurídicas, nacionais e internacionais, e projetos de lei, atinentes ao tema, com destaque à LGPD, ao reporte sobre inteligência artificial da Organização Mundial da Saúde (OMS), ao PL/2.338 em trâmite no Congresso Nacional e à decisão do STF na Ação Direta de Inconstitucionalidade 6.387.

1 O mito da neutralidade algorítmica e os riscos da opacidade

Crawford engenhosamente compara o atual panorama da IA com um Atlas, justificando o nome de sua obra, "*The Atlas of AI*" (Crawford, 2021). Um Atlas é uma publicação constituída por uma coleção de mapas ou de cartas geográficas. É sabido que mesmo um dado tão pretensamente objetivo quanto o mapeamento sempre foi sujeito a enorme influência política.

Em agosto de 2025, a União Africana, organização que reúne todos os Estados africanos, aderiu à campanha *Correct The Map*[5] para que se deixe de utilizar a projeção de Mercator nos mapas-múndi. A projeção em questão, amplamente adotada mundo afora há séculos, torna maiores territórios próximos aos polos, ou seja, a América do Norte e a Europa, em relação àqueles situados perto da linha do Equador, como a África e a América do Sul.

Em 2024, o Instituto Brasileiro de Geografia e Estatística (IBGE) divulgou sua própria versão do mapa-múndi, onde o Brasil figura no centro. A medida foi alvo de críticas nas redes sociais, como se a versão alternativa do mapa agredisse algum fato objetivo.[6]

A própria noção de temporalidade na globalização já foi alvo de disputa política. O Meridiano de Greenwich, situado em Londres, é o meridiano principal oficial do mundo, adotado internacionalmente em 1884. Porém, nenhum elemento objetivo justifica a adoção do Reino Unido como marco 0 do tempo. Tanto é verdade que houve disputa quanto ao posto de meridiano inicial, sendo certo que a França recusou o Meridiano de Greenwich em 1884, optando por utilizar seu próprio meridiano, o Meridiano de Paris. Foi apenas em 1911 que os franceses aderiram à ficção dos ingleses e se ajustaram ao Meridiano de Greenwich.[7]

Um Atlas representa um recorte da realidade que serve a algum interesse. Países africanos podem buscar uma representação mais fidedigna da extensão de seus territórios, o Brasil pode querer colocar-se ao centro como exaltação nacional, países europeus e norte-americanos podem buscar uma falsa impressão de imensidão como demonstração de poder. Os próprios relógios que governam o mundo são parte de um recorte. Em todo caso, resta claro que as questões são inteiramente pautadas por interesses políticos, econômicos, históricos e culturais.

O mesmo deve ser reconhecido quando do estudo de sistemas de inteligência artificial.

Conforme destaca Burrell, as escolhas dos desenvolvedores do algoritmo ficam embutidas no modelo, incluindo definir *"(...) features, pre-classifying training data, and adjusting threshold and parameters*" (Burrell, 2016, p. 3). Essas decisões, nada neutras, se carentes de padrões éticos e jurídicos, podem facilmente conduzir à criação de um modelo eivado de preconceito.

O AI Act, normativa europeia para regular sistemas de inteligência artificial, traz provisões contundentes contra discriminação algorítmica por IA.[8] O PL 2338/2023, tentativa de regulamentação em trâmite no Congresso Nacional, traz regras semelhantes, destacando em seu art. 2º, V, que o desenvolvimento, a implementação e o uso de sistemas de inteligência artificial no Brasil têm como fundamentos "(...) a igualdade, a não discriminação, a pluralidade e o respeito aos direitos trabalhistas".

A experiência europeia demonstra que a opacidade algorítmica não pode ser enfrentada apenas por instrumentos de tutela reativa, como o direito de revisão individual assegurado pela LGPD. O *Artificial Intelligence Act* (AI Act), aprovado em 2024 pelo Parlamento Europeu, inaugura uma abordagem *ex ante*, impondo deveres específicos de transparência, auditabilidade e registro

5 Disponível em: <https://correctthemap.org/>. Acesso em: 23/09/2025.

6 Disponível em: <https://agenciagov.ebc.com.br/noticias/202505/qual-modo-de-ver-o-mundo-ibge-mapa-brasil-centro-sul-no-topo>. Acesso em: 23/09/2025.

7 Disponível em: <https://www.thegreenwichmeridian.org/tgm/artides.php?artide=10>. Acesso em: 23/09/2025.

8 Por exemplo: "*Article 5: Prohibited AI Practices (...) (b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm*".

público para sistemas de IA classificados como de "alto risco", categoria que abrange expressamente aplicações médicas.

O modelo europeu exige que fornecedores realizem avaliações de conformidade prévias e adotem medidas técnicas para explicar a lógica subjacente às decisões algorítmicas, inclusive em linguagem acessível. Trata-se de um contraste relevante em relação à LGPD, que se limita a prever a possibilidade de revisão posterior (art. 20), sem impor obrigações sistemáticas de explicabilidade ou auditoria independente. Nesse sentido, o arcabouço brasileiro ainda privilegia uma lógica de controle a posteriori, enquanto o regime europeu aposta em mecanismos preventivos de mitigação de riscos.

É, pois, central a preocupação quanto aos valores por trás de um sistema de IA, permitindo fiscalizar se o algoritmo se encontra de acordo com os valores constitucionais ou adota classificações ilícitas de grupos sociais ou indivíduos. Se argumenta que esse escopo é virtualmente impossível sem que seja endereçado o problema da opacidade desses sistemas.

Algoritmos não passam de representações abstratas de algum processo, calcados em modelos, um conjunto de *inputs* (entradas) que produzem *outputs* (saídas ou resultados) (O'Neil, 2021, p. 22). São, por definição, simplificações, generalizações, em detrimento da especificidade.[9] Por isso, "os pontos cegos de um modelo refletem o julgamento e prioridades de seus criadores" (O'Neil, 2021, p. 24).

Perceptível, assim, o potencial discriminatório dos sistemas.

Atualmente, o mercado de inteligência artificial, dentre diversos tipos de modelo, é em muito calcado em modelos de aprendizado de máquina ou *machine learning*. Esses modelos, de um modo geral, são do tipo discriminativo ou classificatório.

A função classificatória do modelo, por si só, não é ilícita. É certo que o art. 5º, *caput*, CR, presta genericamente o princípio da igualdade, porém, como ressalta Mello, em exegese uníssona da doutrina, o alcance do princípio não se restringe em nivelar os cidadãos diante de uma norma posta, "(...) mas que a própria lei não pode ser editada em desconformidade com a isonomia" (Mello, 2014, p. 9).

Em seu estudo paradigmático, Mello lecionou que não deve o operador do direito voltar seus olhos à discriminação em si, mas sim à compreensão do fator de discrímen que está por trás dela. Por isso, qualquer elemento (seja raça, sexo, orientação sexual etc.), pode ser escolhido pela lei como fator discriminatório, desde que verificado um "(...) vínculo de correlação lógica entre a peculiaridade diferencial acolhida por residente no objeto, e a desigualdade de tratamento em função dela conferida, desde que tal correlação não seja incompatível com interesses prestigiados na Constituição" (Mello, 2014, p. 17).

Assim, Mello concebeu verdadeira fórmula ou conjunto de critérios para avaliar se a discriminação quebra ou não a isonomia, passando por três etapas: (i) definir o elemento tomado como fator de desigualdade; (ii) demonstrar a correlação lógica abstrata entre o fator erigido em critério de discrímen e o tratamento desigual conferido; (iii) demonstrar a adequação jurídica entre essa correlação lógica e o sistema constitucional, seus interesses e finalidades (Mello, 2014, p. 21).

É dizer que a desigualdade pode ser positiva ou negativa. Inclusive, Boaventura de Sousa Santos aduz que, por vezes, o tratamento desigual não só é necessário, como é indispensável, haja

9 Ademais: "(...) Para criar um modelo, então, fazemos escolhas sobre o que é importante o bastante para ser induído, simplificando o mundo numa versão de brinquedo que possa ser facilmente entendida, e a partir da qual possamos inferir fatos e ações importantes. Esperamos que o modelo lide com apenas um trabalho e aceitamos que irá ocasionalmente agir como uma máquina ignorante com enormes pontos cegos" (O'Neil, 2021, p. 23).

vista que: "temos o direito a ser iguais sempre que a diferença nos inferioriza; temos o direito a ser diferentes sempre que a igualdade nos descaracteriza" (Santos, 2006, p. 316).

Mais recentemente, os avanços nos estudos da relação entre direito, igualdade e discriminação, deram surgimento a novas disciplinas jurídicas autônomas, como a noção de Direito Antidiscriminatório, objeto de extensa pesquisa por Moreira (Moreira, 2020, posição 574).

No que tange especificamente a sistemas de inteligência artificial, o mesmo raciocínio deve ser emulado desde a concepção do sistema. O sucesso e a licitude de uma classificação dependerão desde a qualidade dos dados que alimentam o sistema até os parâmetros desenvolvidos para orientar o algoritmo.

É ônus do desenvolvedor esclarecer quaisquer dúvidas a respeito do resultado da classificação projetada pelo algoritmo. A fim de fiscalizar a observância do preceito constitucional da isonomia, é preciso haver algum grau de claridade a respeito do funcionamento do modelo.

Esse desiderato entra em conflito com o alto grau de opacidade encontrada em mecanismos de classificação e ranking, como filtros de spam, buscadores, qualificação para seguro ou empréstimo, score de crédito etc., o que se traduz em um problema social.

Burrell, em estudo específico sobre opacidade, distingue ao menos três manifestações em algorítmicos de aprendizado de máquina: (i) intencional, por segredo corporativo ou de Estado; (ii) técnica, no sentido de falta de conhecimento técnico necessário para compreensão do mecanismo; ou (iii) de escala, decorrente da própria natureza e forma de aplicação de sistemas de *machine learning* em termos de usabilidade (Burrell, 2016).

De fato, parte da opacidade algorítmica é intencional, justificada pelo segredo comercial, decorrente do desejo de corporações ou Estados de manter alguma vantagem competitiva.

Porém, segundo Pasquale, a opacidade baseada em vantagem competitiva pode facilmente se tornar uma fachada para evitar regulações, manipular consumidores e conciliar padrões de discriminação (Pasquale, 2015).

Assim, uma das soluções possíveis para contornar essa forma de opacidade seria permitir a auditoria externa e independente do código ou mesmo, sem acesso ao código, auditorias sobre padrões de tomada de decisão visando identificar potenciais focos de risco discriminatórios (Nassar, 2025).

De outro lado, há opacidade por limitações técnicas. A escrita e leitura de códigos é uma habilidade especializada, tornando o algoritmo e sua tomada de decisão incompreensível para a maioria da população. Essa forma de opacidade é lógica e de alguma forma esperada, podendo, porém, ser contrabalanceada com maior transparência e explicações coloquiais sobre as conclusões do algoritmo.

Por fim, há opacidade pela escala de operação e aplicação de algoritmos. Essa forma de opacidade, que mais interessa ao presente estudo, decorre em parte do já conhecido *black box problem*[10] e, apesar de poder revelar-se como um efeito não intencional da tecnologia, significa um perigo concreto a seus usuários.

10 "*A technological 'black box' refers to human inability to grasp the inner workings of some technological systems. Even if humans can sometimes understand the inputs and outputs of a technological system, were they to view the inner workings of that system, they might find it incomprehensible. Accordingly, the person is unable to verify the integrity of the process used by the AI system to arrive at the output from the input. An explanation of connections in an artificial neural network is as unhelpful in understanding the system as is a neuron-by-neuron description of a human brain in understanding the reasons for a complex decision made by a human. This has led to interest in 'explainable' AI*" (Bell, 2002).

Algoritmos de *machine learning* servem como poderosos generalizadores e preditores. A acurácia desses algoritmos depende de grandes quantidades de dados (Burrell, 2016, p. 5).

Nas palavras de Burrell, "*(...) Machine learning is applied to the sorts of problems for which encoding an explicit logic of decision-making functions very poorly*" (Burrell, 2016, p. 6). Ou seja, cuida-se de tecnologia útil para situações nas quais a mão humana se mostra ineficiente ou insuficiente. Essas situações provavelmente envolvem escala, o tratamento de quantidade tão grande de informações que tomaria tempo demais para um humano ou um grupo de humanos examinar e classificar.

Nada obstante, o "racional" de uma máquina movida por modelos de inteligência artificial, por exemplo, por redes neurais, não gera automaticamente informações inteligíveis a um operador humano. Mais do que isso, o próprio processo de tomada de decisão da máquina assume tamanha complexidade que seus próprios desenvolvedores podem encontrar dificuldades em explicá-lo.

Um dos subprodutos dessa tecnologia, dessarte, é que a tradução de dados em modelos matemáticos para posterior conversão em informação compreensível por agentes humanos não é consequência automática.

Novamente, Burrell: "*(...) the opacity of machine learning algorithms is challenging at a more fundamental level. When a computer learns and consequently builds its own representation of a classification decision, it does so without regard for human comprehension. Machine optimizations based on training data do not naturally accord with human semantic explanations. (…)*" (Burrell, 2016, p. 10).

Isso decorre da própria ausência de consciência ou sensibilidade de um sistema de IA. Uma IA não "raciocina" no sentido humano da palavra, apesar de todos os esforços da comunidade tech em antropomorfizar IAs como forma de melhor comercializá-las ao grande público.

Por isso, há sérios riscos quando agentes públicos e privados tomam conclusões de modelos de inteligência artificial *prima facie*, de maneira acrítica, abrindo espaço para que os opacos sistemas de funcionamento interno da tecnologia passem a ser os verdadeiros tomadores de decisão da vida cotidiana, ao arrepio da ordem jurídica.

O ideal da *accountability*, muito difundido em normas internacionais sobre regulação de tecnologias, não passa de um dever de transparência, motivação e auditabilidade.

E, a partir de técnicas de *profiling*, o emprego a IA ganha maior escala. Atualmente, seria a Lei Geral de Proteção de Dados Pessoais (LGPD) o regramento responsável por regular e conter essas práticas no Brasil, mas há lacunas temerárias.

2 Construção de identidade pessoal e medidas de antidiscriminação na LGPD: as ameaças de técnicas de *profiling* movidas por IA

A LGPD foi a primeira positivação expressa do direito ao livre desenvolvimento da personalidade no ordenamento pátrio, constando como objeto de proteção da norma (art. 1º) e um dos fundamentos da disciplina da proteção de dados (art. 2º, VII).

Livre desenvolvimento significa o espaço necessário para que o indivíduo desenvolva o si próprio, explorando suas potencialidades com autonomia. Em uma acepção clássica, inclusive, como paradigma de liberdade negativa, era tido como um "direito à diferença" (Pinto, 1999).

Como coloca Martins, isso implica na necessidade de um contexto dialógico, "(...) em que a pessoa consiga se fazer ouvida e possa reivindicar uma identidade própria", sendo certo que (Martins, 2022, p. 25):

> um ambiente em que atores, sejam eles estatais ou privados, possuam um poder desproporcional sobre um indivíduo (ou um grupo), de forma que ele não tenha os meios para participar ativamente tanto da sua própria construção, quanto da construção desse ambiente, não é um ambiente em que o livre desenvolvimento da personalidade é materializado.

No entanto, a construção de identidade pessoal não se consubstancia em processo isolado. Marya Schechtman trabalha com a teoria da identidade narrativa, segundo a qual os acontecimentos passados, ações presentes e planos futuros de um indivíduo constituem a formação narrativa de sua identidade, sob processo de autonarrativa. Porém, a esse elemento primordialmente individual agrega o reconhecimento de terceiros sobre essa autonarrativa e a construção conjunta de narrativas (Schechtman, 2014). A partir desses outros elementos, a autora argumenta que não importa apenas a percepção sobre si, como também a percepção externa sobre essa narrativa.

Martins exemplifica. Uma pessoa X pode se identificar como financeiramente responsável, pagador de dívidas confiável e com hábitos de consumo responsáveis, mas se seu círculo social não reconhecer essa característica, dificilmente ela se tornará elemento constitutivo de sua identidade (Martins, 2022, p. 52). Essa inferência externa pode vir desde um círculo próximo, como familiares e amigos, até relações comerciais, como com o gerente de um banco. Nessa segunda hipótese, é esperado que a percepção do agente bancário sobre a organização financeira do cliente impacte seu acesso a crédito.

Fato é que o reconhecimento externo pode representar um risco ao livre desenvolvimento da personalidade caso a dissociação entre ele e a autonarrativa, ou a tentativa de sua construção, forem expressivos.

É estabelecido um diálogo na construção dessas duas narrativas, com possíveis interferências mútuas. Para tanto, crucial o controle do indivíduo sobre o fluxo de suas informações, permitindo que seja ele o corresponsável por sua narrativa, não apenas terceiros, muito menores agentes econômicos ou estatais.

Em realidade, como destaca Durante, o que importa é que essas duas perspectivas compitam em condições mínimas de justiça, a fim de que o indivíduo tenha ao menos a oportunidade de reivindicar uma narrativa própria, mediante demonstração de fatores que o algoritmo não captou ou não é capaz de captar (Durante, 2011, p. 606).

Isso implica em transparência, de modo que o titular do dado considerado em determinada análise por terceiros tenha conhecimento do que foi condicionante para determinada decisão, os critérios utilizados e possibilidade de contraponto.

Emerge, assim, uma tensão entre capacidade de controle de informações pessoais e acesso dessas informações por terceiros (Martins, 2022, p. 56). No contexto da LGPD, esse acesso se dá na forma do tratamento de dados pessoais.

O art. 5º, X, LGPD, conceitua tratamento de dados pessoais como toda operação realizada com dados pessoais, independente da complexidade ou se por meio físico ou digital.

O tratamento de dados pessoais pode ser e frequentemente é automatizado. Essa automatização diz respeito ao emprego de meios técnicos computacionais para realização do tratamento, que independe de intervenção humana. Essa automatização pode se configurar em diferentes graus, até "(...) um tratamento totalmente automatizado de aprendizado não supervisionado, como um sistema de classificação de consumidores a partir de hábitos comportamentais, configurando um grau muito elevado de automatização" (Martins, 2022, p. 95)

O desenvolvimento de sistemas de inteligência artificial, impulsionados por técnicas de *machine learning*, permitem que essa automatização alcance decisões cada vez mais complexas,

incluindo concessão de crédito bancário (Campos, 2021), concessão de liberdade condicional (Larson *et al.*, 2016) etc.

Nesse sentido, se confere certa liberdade de ação ao algoritmo, apesar de os processos internos poderem ser opacos para os próprios desenvolvedores, como já evidenciado.

A LGPD trata de decisões automatizadas em seu art. 20, prevendo o direito de revisão. Aduz que "o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses (...)". O legislador faz especial destaque a decisões que visam "definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade". Essa menção diz respeito à técnica de *profiling*, que será melhor elucidada adiante.

Importa que o controlador dos dados tem o dever de fornecer "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial" (§1º) e, caso não o faça, alegando segredo comercial e industrial, "(...) a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais" (§2º).

Corolário ao dispositivo acima, o art. 12, §2º, destaca que "poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada".

O regramento, em primeira vista, mostra-se razoável, pois sistemas de IA são passíveis de erros, incorrendo em falsos positivos ou falsos negativos. No entanto, há pontos de atenção.

Primeiro, porque "dado" não se confunde com "informação".

A informação é o conteúdo semântico extraído a partir de um processo de estruturação e interpretação de dados (Floridi, 2010).

A LGPD, porém, na superfície, preocupa-se apenas com o controle de dados, mas não da informação. O dado é uma condicionante para a informação, mas não o resultado, que advém de um processo de interpretação.

Para a proteção adequada do direito ao livre desenvolvimento, contudo, não basta o controle sobre o tratamento dos próprios dados pessoais, como alguma participação no processo de interpretação dos dados. Uma leitura superficial da LGPD, distante da teleologia do marco protetivo, ameaça um esvaziamento da norma em favor de uma mera aparência de proteção jurídica.

Outro alerta consiste nas próprias técnicas adotadas na estruturação dos dados colacionados pelo algoritmo, que além de opacas, pelos motivos já expostos no item anterior, são denunciadas pela doutrina especializada como imprecisas e excessivamente simplistas. Isso porque o mero cruzamento de variáveis pode anunciar correlações, mas não necessariamente relações de causalidade.

Em verdade, correlações podem ser úteis para o refinamento de perguntas de pesquisa, mas são insuficientes para a interpretação de dados. Um dos grandes males na indústria da inteligência artificial consiste precisamente na falsa crença de que quaisquer correlações de dados são suficientes para responder perguntas causais complexas (Pearl, 2017).

Gutwirth e Hildebrandt também alertam para os perigos dessa torsão de conceitos da estatística. Se, classicamente, a mensuração de uma correlação pode servir como indicativo de uma hipótese formulada, a contemporânea abordagem algorítmica plasmada por sistemas de IA considera a correlação em si como a informação necessária (Gutwirth; Hildebrandt, 2010).

Para tanto, os dados mais banais podem revelar uma infinidade de características individuais e, com base em métodos probabilísticos, gerar classificações por modelos de IA, separando indivíduos em grupos.

Por exemplo, há estudos no sentido de que, mediante técnicas de aprendizado de máquina, é possível que companhias como a Microsoft detectem doenças neurodegenerativas simplesmente a partir do tempo médio em buscas na internet, número de cliques em links, tremor do mouse etc. (White, 2015). Esses dados, inicialmente coletados com a finalidade de aperfeiçoar o sistema em si, por via oblíqua, permitem que a companhia tenha um conhecimento aprofundado sobre o estado de saúde seu usuário, possivelmente identificando uma condição de saúde grave antes de le próprio.

Nesse ponto, é relevante destacar que a LGPD define duas categorias de dados pessoais.

O art. 5º, I, define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável". Já o inciso II define outra categoria de dado pessoal, cujo tratamento jurídico no decurso da norma é mais rigoroso, na forma de dados pessoais sensíveis. Dado pessoal sensível é o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Quanto a essa distinção, importante frisar que não há definição apriorística sobre a natureza de um dado pessoal como sensível ou não sensível, sendo certo que a análise dessa categorização é contextual. Por exemplo, o CPF pode ser dado sensível ou não, conforme o contexto. O cadastro de um CPF em uma loja virtual atrai a definição como dado pessoal não sensível, mas se o mesmo cadastro ocorrer em uma farmácia, passa a ser considerado dado pessoal sensível, porque o tratamento se relaciona à saúde do indivíduo.

Ainda, a distinção tem como fundamento o maior potencial discriminatório dos dados elencados como sensíveis pelo legislador. A não-discriminação é um dos princípios elencados no art. 6º, IX, e devem ser rigorosamente observados os preceitos constitucionais já delineados no item anterior.

A saúde tem especial destaque no restante da norma. Além do rigor maior que a normativa já estabelece para dados pessoais sensíveis, dados relativos à saúde apresentam algumas limitações adicionais: (i) via de regra, é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica (art. 11, §4º), questão que vem gerando debate quanto à coleta e compartilhamento de dados por farmácias no Brasil e merece estudo à parte; (ii) é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários (art. 11, §5º), de modo que, a princípio, há uma vedação genérica na técnica de *profiling* para operadoras de planos de saúde quanto a esses fins.

Novamente, o escopo de proteção da LGPD aparenta ser adequado para os fins da norma, destacadamente quanto à limitação de técnicas de *profiling* para tratamentos de dados sensíveis ligados à saúde. Análise mais apurada, porém, revela outras fragilidades.

2.1 Definição de *profiling*, anonimização de dados e subterfúgios

A LGPD traz diversas definições em seu art. 5º, mas não define *profiling*. Essa atividade, porém, é mencionada nos arts. 12, §2º, e 20, *caput*. A partir desses dispositivos, é possível constatar

que a norma impõe rigor maior quando a atividade de tratamento de dados envolver formação de perfil comportamental do titular dos dados.

Uma proeminente definição de *profiling* é proposta por Hildebrandt (Hildebrandt, 2008, p. 19):

> The process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category.

Na perspectiva nacional, merece destaque o conceito de Martins (Martins, 2022, p. 152):

> Assim, pode-se entender o profiling como uma atividade que busca gerar novas informações a partir de um conjunto de dados iniciais. Em geral, esse processo é feito com a utilização de sistemas algorítmicos de aprendizado de máquina. Embora diferentes sistemas e técnicas possam trazer resultados e consequências distintas, no presente trabalho não iremos restringir a análise para alguma tecnologia específica, mas partiremos de uma análise funcional dos pressupostos, processos e consequências do profiling.
>
> (...) consiste em descobrir, gerar e criar informações sobre um sujeito a partir de um conjunto de dados, com o objetivo de avaliar e/ou prever suas características e comportamento. Nesse sentido, poder-se-ia argumentar que o profiling não é nada mais do que fazer generalizações e previsões sobre uma pessoa a partir de informações iniciais que se têm sobre ela.

Portanto, o *profiling* tem como características importantes o emprego usual de algoritmos de aprendizado de máquina (i.e., sistemas de IA), tem como consequência o perfilamento de indivíduos para construção de generalizações a seu respeito e divide indivíduos em grupos ou categorias a partir dessas generalizações.

Essas generalizações, em um segundo momento, podem ser instrumentalizadas de diversas formas. Por exemplo, ganha projeção o campo da publicidade comportamental, que, alimentada pela coleta de toda espécie de dado (hábitos de consumo, dados biométricos, idade, preferências alimentares, condições de saúde etc.), promete oferecer publicidades direcionadas a grupos com perfis que melhor correspondem ao produto.

A LGPD, seguindo o exemplo do regulamento europeu que lhe serviu de inspiração, apresenta alguns critérios de limitação para o *profiling*, com regras ainda mais rigorosas quando os dados pessoais forem sensíveis e ligados à saúde.

No entanto, o legislador agiu aquém da potencialidade lesiva dessas técnicas, pois excluiu de seu âmbito de proteção dados pessoais anonimizados.

Segundo o art. 12 da LGPD, dados anonimizados não serão considerados dados pessoais para os fins da norma, salvo quando o processo de anonimização for reversível.

A anonimização consiste na "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (art. 5º, XI).

O próprio conceito de dado pessoal, já exposto no item anterior, deflagra que o legislador condicionou o conceito jurídico de dado pessoal à possibilidade individualização a determinada pessoa natural. O mesmo ocorre no art. 12, §2º, que faz destaque à condição de a pessoa perfilada ser "identificada".

Os dispositivos acima partem de uma abstração de que, caso o dado não possa ser individualizado, porque bem-sucedido um procedimento de anonimização, seu tratamento não mais oferece risco ou dano jurídico ao indivíduo.

A presente pesquisa argumenta o contrário.

Conforme Martins, os termos "pessoa natural identificada ou identificável" e "se identificada" criam uma restrição incompatível com o regime da proteção de dados pessoais, especialmente dos sensíveis ligados à saúde. A proteção de dados pessoais não pode ser entendida como restrita à proteção contra a identificação por terceiros. Muito pelo contrário, "(...) a proteção de dados pessoais procedimentaliza regras para que os direitos fundamentais sejam garantidos em atividades de tratamento de dados" (Martins, 2022, p. 168).

Retomando o exemplo da publicidade comportamental, esta apenas demonstra como um eventual processo de anonimização não protege o indivíduo perfilado (Borgesius, 2016.). Mesmo que a publicidade não lhe seja inteiramente individualizada, a formação do perfil comportamental lhe alcança de toda forma. Pode aparentar ser situação inofensiva, mas o mesmo princípio se aplica para outros stores, como formação de scores de crédito, de probabilidade de reincidência em crimes ou precificação de seguros.

O mercado da saúde é um dos mais cobiçados nesse empreendimento (Garla, 2013) e, como exposto, ainda que a LGPD traga vedação genérica ao perfilamento por planos de saúde, a anonimização serve como mecanismo para contornar restrições. Em última medida, o consumidor ainda terá seus direitos fundamentais afetados. À companhia que perfila, pouco importa a identificabilidade de cada consumidor, importa apenas a maximização de lucros. Sandra Watcher argumenta que "o que importa é se o usuário se comporta de maneira semelhante o suficiente ao grupo suposto para ser tratado como um membro do grupo" (Wachter, 2019, p. 13.).

O potencial discriminatório, dessa forma, é atingido de maneira sutil, mas com alcance ainda mais expressivo.

É excessivo e equivocado o apego da LGPD a uma dimensão individual para conceituação jurídica de dado pessoal. Mais do que isso, é contraditório com os termos da própria norma.

A dimensão supraindividual se encontra expressamente prevista no art. 22 da norma, segundo o qual "a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva". O dispositivo insere a tutela de dados pessoais no centro do complexo mosaico do microssistema de tutela coletiva, inclusive com aproveitamento da teoria dos vasos comunicantes, e clama pela atuação do Ministério Público em juízo.

O contraste entre a lei nacional e a regulação jurídica europeia torna-se ainda mais evidente quando se observa justamente a disciplina do *profiling* no Regulamento Geral de Proteção de Dados da União Europeia (GDPR).

O aludido art. 22 do GDPR estabelece que os indivíduos têm o direito de não se submeter a decisões tomadas exclusivamente com base em tratamento automatizado de dados, incluindo o perfilamento, quando tais decisões produzirem efeitos jurídicos ou afetarem significativamente sua esfera pessoal.

Essa vedação só pode ser afastada em hipóteses excepcionais, como consentimento explícito, necessidade para execução contratual ou previsão legal específica. Ademais, mesmo nesses casos, o regulamento impõe salvaguardas obrigatórias, como a possibilidade de intervenção humana, o direito à explicação e a faculdade de contestação.

Diferentemente, a LGPD não prevê qualquer proibição genérica a decisões automatizadas com efeitos significativos, limitando-se a reconhecer ao titular o direito de revisão (§1º do art. 20), sem detalhar garantias adicionais. Tal lacuna normativa fragiliza a tutela da personalidade e expõe titulares, sobretudo em contextos sensíveis como o da saúde, a riscos de discriminação velada por sistemas algorítmicos.

Há, ainda, intersecções constantes entre a LGPD e o CDC, destacadas em diversas passagens da presente pesquisa. O Código de Defesa do Consumidor, que já trazia uma semente da proteção de dados de consumidores na forma de seus arts. 43 e seguintes, é fundamento normativo para a repressão de quase todos os exemplos de perfilamento listados acima, que atingem ao coletivo de consumidores vulneráveis, como perfilamento praticado por agências de publicidade, bancos, planos de saúde etc. Processos de anonimização não podem servir como escudo a essa necessidade de proteção

Por isso, o conceito de dado pessoal no Brasil merece uma revisão sistemática e teleológica. Por isso, autores proeminentes como Bioni optam por uma abordagem consequencialista quanto a essa conceituação, argumentando que (Bioni, 2021, p. 125):

> Se a premissa da causa regulatória da proteção de dados pessoais é tutelar o cidadão, que é cada vez mais exposto a tais tipos de práticas que afetam a sua vida, então, uma compartimentalização "dura" entre dados pessoais e dados anonimizados deixaria de fazer sentido. Em especial, quando está em questão a formação de perfis comportamentais que tem por objetivo precípuo influenciar de alguma forma a vida de uma pessoa, que está atrás de um dispositivo e pouco importa ser ela identificável ou não.
>
> Abre-se espaço, assim, para uma escolha normativa consequencialista. Não se normatiza apenas pela lente da conceituação mutualmente excludente entre dados pessoais e dados anônimos, mas, também, por meio da relação de causa e efeito que a mera atividade de tratamento de dados pode exercer sobre um indivíduo.

Essa abordagem conceitua dados pessoais e atrai a sistemática de proteção da norma jurídica, dessarte, com base no resultado do tratamento do dado, não na identificabilidade de seu titular. Em atividades de *profiling*, no mais das vezes, é irrelevante ao titular do dado se este é identificável ou não para o controlador, e sim os efeitos do perfilamento em sua vida, como quando é limitando seu acesso a bens e serviços essenciais ligados à saúde.

3 Resultados do atrito entre desenvolvimento tecnológico, direito à saúde e proteção de dados pessoais em sentido consequencialista

É certo que a Constituição da República de 1988 consagrou não só o direito à saúde (arts. 196 e seguintes) como também o desenvolvimento tecnológico.

Em seu art. 3º, II, destaca ser objetivo fundamental da República "garantir o desenvolvimento nacional". É competência comum dos entes federativos "proporcionar os meios de acesso à cultura, à educação, à ciência, à tecnologia, à pesquisa e à inovação" (art. 23, V, CR). Ao Sistema Único de Saúde compete "incrementar, em sua área de atuação, o desenvolvimento científico e tecnológico e a inovação" (art. 200, V, CR). E, se não bastasse, o constituinte dedicou capítulo inteiro apenas à ciência tecnologia e inovação a partir do art. 218, sendo que o "Estado promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação".

Destarte, é um dever constitucional, não uma faculdade, que o Estado brasileiro assegure as condições para que sua comunidade científica se encontre na vanguarda do desenvolvimento tecnológico global, mormente no setor de saúde.

É argumentável que a adoção de sistemas de inteligência artificial atende a esses critérios. O aperfeiçoamento de modelos preditivos, inexoravelmente, contribuirá para uma medicina mais moderna e eficiente, capaz de melhor atender a principiologia constitucional na área da saúde. Isso implicará no aumento da chance de cura, com diagnósticos mais precisos.

Autores como Abbott, inclusive, vislumbram um futuro em que a implementação de sistemas de IA agregará tanto à prática da medicina que se tornaria antiético a recusa no apoio de sistemas de diagnóstico mais seguros impulsionados por essas tecnologias (Abbott, 2020, p. 10).

Esses benefícios, porém, não podem ofuscar a necessária observância dos direitos humanos, direitos fundamentais e princípios caros ao Biodireito, como o princípio da precaução. Diversos riscos devem ser endereçados desde a concepção dessas tecnologias, incluindo a necessidade de regulamentações mais precisas, implicações na relação-médico paciente, potenciais imprecisões do algoritmo nos estágios iniciais da tecnologia, potenciais discriminatórios, proteção da privacidade e dados pessoais, acesso amplo às novas tecnologias a fim de evitar aumento de desigualdades, dentre outros.

Esse atrito entre desenvolvimento tecnológico e tutela da saúde, bem como todos os elementos que lhe são adjacentes, como os dados pessoais ligados à saúde, se fez presente no Brasil antes mesmo de a LGPD superar sua *vacatio legis*.

Foi o que ocorreu quando do julgamento, pelo STF, da constitucionalidade da Medida Provisória 954, editada em abril de 2020 pela Presidência da República no sentido de determinar o compartilhamento de dados entre as empresas de telefonia e o IBGE. Diante do isolamento social promovido em função da emergência sanitária do novo coronavírus (Covid-19), o Poder Executivo justificou a necessidade desse compartilhamento como forma de prezar pela saúde dos entrevistadores e entrevistados, de modo que as empresas de telefonia compartilhariam dados de seus usuários para viabilizar a realização de pesquisas estatísticas por esse meio, incluindo nome, número de telefone e endereço.

O STF foi instado a analisar a constitucionalidade dessa norma, através das ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, sob alegações de violação à dignidade da pessoa humana, privacidade, autodeterminação informativa e sigilo da correspondência e das comunicações telegráficas.

Como contexto adicional, a LGPD havia sido aprovada, mas ainda não se encontrava em vigor.

Foi suspensa liminarmente a eficácia da norma pela Ministra Rosa Weber, com posterior confirmação da decisão pelo plenário, com argumentos calcados na primazia da proteção de dados pessoais no caso concreto. O Ministro Gilmar Mendes, inclusive, pontuou em seu voto que (Brasil, 2020):

> A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa.

O enfrentamento da pandemia demonstrou a aptidão e interesse de agentes públicos e privados em empregar novas tecnologias, inclusive sistemas de IA, visando tornar a prática médica mais eficiente. Essas aplicações incluíram, como apontou Sousa, utilização de médicos e enfermeiros virtuais para atender dúvidas e orientar a população, utilização de algoritmos que para ajudar a entender o avanço do coronavírus, detecção de casos e prioridades de atendimentos em hospitais e direcionamento de recursos, análise de imagens de tomografias realizadas em pulmões para tentar diagnosticar a doença etc. (Sousa, 2020).

Essa aptidão, porém, se mostrou pouco engajada com a observância de princípios da bioética e do biodireito, tampouco com o recém aprovado arcabouço jurídico de proteção de dados pessoais. A pandemia ilustrou a dissociação crescente entre avanço tecnológico na saúde e regulação dos riscos inerentes a essa marcha.

A regulação de tecnologias disruptivas na área da saúde, que são extremamente dependentes no tratamento de dados pessoais sensíveis, deve ser inequivocamente pautada na precaução, pois há risco de dano grave ou irreversível dano à esfera coletiva e individual.

É princípio típico do Direito Ambiental, incorporado oficialmente no Brasil em 1992, por ocasião da Conferência das Nações Unidas sobre o Meio Ambiente e o Desenvolvimento (Rio- 92 ou ECO-92). Também pode ser implicitamente extraído do art. 225 da Constituição da República.

O art. 3º, item 3, do texto da Convenção-Quadro das Nações Unidas sobre Mudança do Clima, adotada em Nova Iorque, em 9 de maio de 1992, internalizada no Brasil através do Decreto Legislativo nº 1, de 3 de fevereiro de 1994, dispõe sobre a noção de precaução:

> 3. As Partes devem adotar medidas de precaução para prever, evitar ou minimizar as causas da mudança do clima e mitigar seus efeitos negativos. Quando surgirem ameaças de danos sérios ou irreversíveis, a falta de plena certeza científica não deve ser usada como razão para postergar essas medidas, levando em conta que as políticas e medidas adotadas para enfrentar a mudança do clima devem ser eficazes em função dos custos, de modo a assegurar benefícios mundiais ao menor custo possível. Para esse fim, essas políticas e medidas devem levar em conta os diferentes contextos socioeconômicos, ser abrangentes, cobrir todas as fontes, sumidouros e reservatórios significativos de gases de efeito estufa e adaptações, e abranger todos os setores econômicos. As Partes interessadas podem realizar esforços, em cooperação, para enfrentar a mudança do clima.

Precaução, no entanto, não se confunda com prevenção. Pode-se dizer que precaução amplia a proteção em relação à simples prevenção, porque se preocupa com a mera probabilidade, não certeza. Prevenção consiste na adoção de medidas para evitar danos conhecidos e esperados, ou seja, trabalha sob um juízo de certeza quanto à existência ou ocorrência do risco. Já a precaução trabalha com um juízo de probabilidade, vedando comportamentos que possivelmente apresentam risco sério e irreversível a dado bem jurídico, como ao meio ambiente ou a saúde.

Vê-se, portanto, que os princípios da precaução e da prevenção não servem de entrave ao desenvolvimento tecnológico, apenas buscam racionalizá-lo em uma era de riscos vertiginosos. A Constituição garante, sim, o desenvolvimento tecnológico, mas condizente com os demais direitos fundamentais e, acima de tudo, com a garantia da dignidade da pessoa humana.

A privacidade e, mais recentemente, a proteção de dados pessoais, são vistos por certos agentes econômicos como empecilho para o progresso tecnológico. Trata-se de perspectiva que se amolda perfeitamente aos arquétipos do capitalismo de vigilância descritos por Zuboff. Não há espaço para uma ordem jurídica de matriz humanista, que entroniza a dignidade da pessoa humana como metaprincípio, para permitir a mera objetificação e instrumentalização de seres humanos

para finalidades comerciais, independentemente das promessas vagas que essas tecnologias apresentam.

Os princípios da precaução e da prevenção são, portanto, caminhos valiosos para o enfrentamento da problemática, desde uma perspectiva de *privacy by design*. Machado e Mendes, em análise de propostas de perfilamento e dados agregados de geolocalização para fins de enfrentamento da pandemia do novo coronavírus no Brasil, seguiram precisamente essa linha argumentativa, destacando que, a título de prevenção, controladores devem conceber desde o início quaisquer atividades de tratamento de dados tendo em vista a observância das regras e princípios da LGPD (Machado; Mendes, 2020).

É orientação em linha com os documentos internacionais de *soft law* já redigidos sobre o tema. Em 2019, a Organização Mundial da Saúde (OMS) publicou reporte intitulado "*Ethical use of artificial intelligence: principles, guidelines, frameworksand human rights standards*", onde enumerou desafios éticos e de governança na implementação de IA na área da saúde, incluindo:

> *ensuring equitable access to AI and determining how AI is affected by, and affects the digital divide; preserving individual rights of autonomy, privacy, informed consent and freedom from bias and discrimination; ensuring understanding of how AI functions and makes decisions (transparency and explainability); ensuring equal access to databases for all users and not only those with more capacity to pay for access; preserving human control of AI; and strengthening public oversight and regulation of the private sector*

Tanto o AI Act quanto o GDPR demonstram que o ordenamento europeu busca alinhar inovação tecnológica com mecanismos robustos de proteção da pessoa humana.

O AI Act considera de **alto risco** qualquer aplicação de IA destinada a auxiliar diagnósticos ou procedimentos médicos, exigindo registro e monitoramento contínuo (art. 14).

Já o GDPR, em seu art. 9º, veda o tratamento de dados de saúde como regra geral, admitindo-o apenas em situações estritamente delimitadas, como consentimento explícito ou relevante interesse público.

No Brasil, a LGPD disciplina o tratamento de dados sensíveis (art. 11), mas admite hipóteses mais amplas e indeterminadas, além de excluir de sua incidência os dados anonimizados, mesmo quando empregados em atividades de perfilamento. Essa divergência demonstra que, enquanto a União Europeia impõe restrições preventivas e garantias materiais, o ordenamento brasileiro opera em chave mais permissiva e aberta, confiando em salvaguardas de difícil operacionalização prática.

Ainda no plano nacional, o Projeto de Lei 2.338/2023, que visa regulamentar sistemas de IA no País, considera em seu art. 14 do texto aprovado pela Comissão Especial como "de alto risco" o sistema de IA empregado para "VIII - aplicações na área da saúde para auxiliar diagnósticos e procedimentos médicos, quando houver risco relevante à integridade física e mental das pessoas".

São disposições promissoras, mas que estão fadadas à proteção jurídica insuficiente se não endereçadas de forma conjunta as limitações encontradas na LGPD no emprego de sistemas de *profiling*, que permitem até mesmo o uso de dados pessoais sensíveis para fins de perfilamento se empregados processos de anonimização. Nesse sentido, atualmente, sistemas de IA são empregados para o tratamento massificado de dados pessoais ligados à saúde, mas excluídos da regulação da LGPD, apesar de o usuário final de serviços ligados à saúde ser impactado com o perfilamento.

Conclusões

É falacioso o dilema, novamente muito difundido diante dos investimentos bilionários no setor de IA, que coloca inovação e proteção de direitos fundamentais em linha de disputa.

O constituinte originário brasileiro, desde 1988, já encerrou esse debate, esculpindo uma Constituição complexa que concilia diversos interesses, condizente com uma sociedade plural e preocupada com avançar tecnologicamente, mas de forma responsável e racional.

A proteção de dados pessoais, nessa toada, foi alçada expressamente ao status de direito fundamental, previsto no rol do art. 5º da Constituição da República: "LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)".

Não há dúvida no texto constitucional quanto à harmonia dessas regras e princípios. Os verdadeiros desafios se encontram em sua implementação.

As relações de causalidade envolvidas em violações de direitos fundamentais se tornaram cada vez mais sutis e invisíveis na era digital. A violação de privacidade ou atos de discriminação não dependem mais de interações físicas quando virtualizadas, de tal forma que a vítima pode sequer ter consciência da vulneração de seus direitos.

A perda de privacidade, consumo de dados pessoais e medidas discriminatórias por meio de algoritmos digitais, apesar de opacas, têm alcance expressivamente maior. Com um simples cadastramento em uma farmácia ou uma simples pesquisa na internet, todo indivíduo se torna potencial alvo de perfilamento algorítmico, impulsionado por sistemas de inteligência artificial.

A análise comparativa da regulação e projeto de regulação jurídica nacional com o direito comparado já existente evidencia que a União Europeia, por meio do GDPR e do AI Act, estrutura uma tutela mais abrangente e preventiva, conjugando a proteção de dados pessoais com regras específicas para sistemas de inteligência artificial. O Brasil, por sua vez, ainda mantém uma regulação fragmentada: a LGPD garante direitos fundamentais importantes, mas carece de disposições expressas sobre *profiling*, decisões automatizadas de alto impacto e auditorias de algoritmos.

Dessa forma, a exclusão de dados anonimizados de sua incidência amplia ainda mais a vulnerabilidade dos titulares. Para que o sistema nacional se aproxime do paradigma europeu, é necessário: (i) proibir decisões exclusivamente automatizadas que gerem efeitos jurídicos relevantes, salvo exceções claras e justificadas; (ii) exigir mecanismos de intervenção humana e explicabilidade em sistemas de IA de alto risco, em especial na saúde; (iii) prever auditorias independentes obrigatórias; e (iv) alinhar a atuação da Autoridade Nacional de Proteção de Dados (ANPD) com órgãos do setor de saúde. Apenas com tais medidas será possível conciliar desenvolvimento tecnológico e efetividade dos direitos fundamentais, conforme exige a Constituição da República.

Nesse esteio, três perigos se anunciam, conforme dissecou essa breve pesquisa.

Primeiro, o pretenso discurso de neutralidade e absoluta objetividade desses sistemas, em uma acepção quase messiânica da máquina, que entregaria à humanidade soluções para seus mais antigos problemas. Se demonstrou, por outro lado, a opacidade inerente a esses sistemas, que são facilmente suscetíveis a influências de vieses discriminatórios, mas apresentam graves problemas de auditabilidade, especialmente pelo usuário.

Segundo, a anonimização de dados pessoais como forma de escapar do âmbito de incidência da LGPD, mas ainda atingindo as consequências do *profiling* na esfera individual dos titulares dos dados. Em linha com a doutrina especializada sobre o tema, vê-se uma lacuna clara na LGPD, que se distancia de seu espírito supraindividual ao adotar conceitos excessivamente baseados na identificabilidade dos titulares de dados. No enxame digital, pouco importa a identificabilidade para fins de vigilância, controle e lucro.

Terceiro, a ausência de diálogo claro entre as normas de proteção de dados pessoais e de regulação de IA com princípios caros à bioética e ao biodireito, especialmente às noções de precaução e prevenção. A sociedade de riscos clama pela antecipação de medidas tendentes a proteger indivíduos e grupos, evitando riscos. No caso do desenvolvimento e aplicação de sistemas de IA, essa preocupação deve existir desde a concepção do algoritmo.

Esses perigos denunciam a fraqueza de um direito excessivamente autorreferencial. Torna, mais do que nunca, estéril um direito autopoiético, apegado a suas próprias formas e satisfeito com perfunctória reprodução de seus próprios conceitos e decisões, alheio à multidisciplinariedade indispensável para compreender e regular novos desafios na era digital.

Por isso, se defende uma reorientação do conceito de dados pessoais, adotando abordagem consequencialista, que atrai a proteção jurídica não a partir da identificabilidade do usuário, mas sim do impacto do tratamento dos dados em sua esfera jurídica. Essa interpretação teleológica e sistemática do conceito é imprescindível no que diz respeito a dados pessoais sensíveis ligados à saúde, visando alinhar o tratamento desses dados aos preceitos da bioética e do biodireito, bem como permitir a adequada fiscalização dos graves potenciais discriminatórios carregados por essas atividades.

AGRADECIMENTO

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES - Código de Financiamento 001 - ao primeiro autor.

Referências

BECK, Ulrich. **Sociedade de Risco: rumo a uma outra modernidade**. 2ª ed. São Paulo: Editora 34, 2011.

BELL, Felicity, *et al.* ***AI decision-making and the courts – a guide for judges, Tribunal Members and Court Administrators***. Aija, Australia, 2002. Disponível em: <https://aija.org.au/publications/ai-decision-making-and-the-courts-a-guide-for-judges-tribunal-members-and-court-administrators/>. Acesso em: 22/09/2025.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. 3ª ed. São Paulo: Forense, 2021.

BORGESIUS, Frederik Zuiderveen. ***Singling out people without knowing their names: behavioural targeting, pseudonymous data, and the new Data Protection Regulation***. Computer Law & Security Review, v. 32, n. 2, 2016, p. 256-271. Disponível em:

<https://www.sciencedirect.com/science/article/abs/pii/S0267364915001788>. Acesso em: 22/09/2025.

BRASIL. Assembleia Nacional Constituinte. **Constituição da República de 1988.** Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 22/09/2025.

BRASIL. Congresso Nacional. Decreto Legislativo nº 1, de 3 de fevereiro de 1994. **Convenção-Quadro das Nações Unidas sobre Mudança do Clima**. Disponível em: <https://www2.camara.leg.br/legin/fed/decleg/1994/decretolegislativo-1-3-fevereiro-1994-358285-publicacaooriginal-1-pl.html>. Acesso em: 22/09/2025.

BRASIL. Congresso Nacional. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor (CDC).** Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 22/09/2025.

BRASIL. Congresso Nacional. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 22/09/2025.

BRASIL. Congresso Nacional. **Projeto de Lei 2.338.** Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 22/09/2025.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Referendo na medida cautelar na Ação Direta de Inconstitucionalidade 6.387.** Relatora: Min. Rosa Weber, 07/05/2020. Brasília: STF, 2020. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em: 22/09/2025.

BURRELL, Jenna. ***How the machine 'thinks': Understanding opacity in machine learning algorithms***. Big Data & Society, January–June, 2016. Disponível em: <https://journals.sagepub.com/doi/10.1177/2053951715622512>. Acesso em: 22/09/2025.

DURANTE, Massimo. ***The Online Construction of Personal Identity Through Trust and Privacy***. Information, v. 2, n. 4, out. 2011. Disponível em: <https://www.mdpi.com/2078-2489/2/4/594>. Acesso em: 22/09/2025.

FLORIDI, Luciano. ***Information: a very short introduction***. Oxford: Oxford University Press, 2010.

GARCIA, Diego. **Pensar a bioética: metas e desafios**. São Paulo: São Camilo; Loyola, 2010.

GARLA, Satish *et al.* **What Do Your Consumer Habits Say About Your Health? Using Third-Party Data to Predict Individual Health Risk and Costs.** SAS Global Forum, 2013, Disponível em: <http://support.sas.com/resources/papers/proceedings13/170-2013.pdf>. Acesso em: 22/09/2025.

GUTWIRTH, Serge; HILDEBRANDT, Mireille. ***Some Caveats on Profiling***. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul. (Eds.). *Data Protection in a Profiled World*. Netherlands: Springer, 2010. Disponível em: <https://link.springer.com/chapter/10.1007/978-90-481-8865-9_2>. Acesso em: 22/09/2025.

HILDEBRANDT, Mireille. ***Defining Profiling: A New Type of Knowledge?*** In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (Eds.). *Profiling the European Citizen: Cross-Disciplinary Perspectives*. Cham: Springer Science, 2008. Disponível em: <https://link.springer.com/chapter/10.1007/978-1-4020-6914-7_2>. Acesso em: 22/09/2025.

LARSON, Jeff; MATTU, Surya; KIRCHNER Lauren; ANGWIN, Julia. ***How We Analyzed the COMPAS Recidivism Algorithm.*** Nova Iorque: ProPublica, 2016. Disponível em:

<https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. Acesso em: 22/09/2025.

MACHADO, Diego Carvalho; MENDES, Laura Schertel. **Tecnologias de perfilamento e dados agregados de geolocalização no combate à Covid-19 no Brasil**. Revista Brasileira de Direitos Fundamentais & Justiça, Belo Horizonte, v. 14, n. 1, p. 105-148, nov. 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1020/998>. Acesso em: 22/09/2025.

MARTINS, Pedro Bastos Lobo Profiling na Lei Geral de Proteção de Dado: desenvolvimento da personalidade em face da governamentalidade algorítmica. 1ª ed. São Paulo: Editora Foco, 2022.

MELLO, Celso Antônio Bandeira de. **O conteúdo jurídico do princípio da igualdade**. 3ª ed. São Paulo: Malheiros, 2014.

MOREIRA, Adilson José. **Tratado de Direito Antidiscriminatório**. São Paulo: Editora Contracorrente, 2020, edição digital.

NATIONAL COMMISSION FOR THE PROTECTION OF HUMAN SUBJECTS OF BIOMEDICAL AND BEHAVIORAL RESEARCH. ***The Belmont Report***. 1978. Disponível em: <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html>. Acesso em: 22/09/2025.

NAVES, Bruno Torquato de Oliveira; SÁ, Maria de Fátima Freire. **Bioética e Biodireito**. 6ª ed. São Paulo: Editora Foco, 2023, edição digital.

O'NEIL, Cathy. **Algoritmos de Destruição em Massa**. 1ª ed. São Paulo: Rua do Sabão, 2021.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. ***Ethical use of artificial intelligence: principles, guidelines, frameworks and human rights standards***. Disponível em: <https://www.jstor.org/stable/resrep35680.8?seq=1>. Acesso em: 22/09/2025.

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

PEARL, Judea. ***The Book of Why: The New Science of Cause and Effect***. Los Angeles: Ingram Publisher Services, 2017.

PINTO, Paulo Mota. **O Direito ao Livre Desenvolvimento da Personalidade**. In: PÁDUA RIBEIRO, Antônio de *et al*. Coimbra: Coimbra Editora, 1999.

REALE, Miguel. **Filosofia do direito**. 14ª ed. São Paulo: Saraiva, 1999.

SANTOS, Boaventura de Souza. **A gramática do tempo**. São Paulo: Cortez, 2006.

SOUSA, Maria Eliane Alves de. **Direitos humanos e princípios comuns entre inteligência artificial e direito à saúde**. Cadernos Ibero-Americanos de Direito Sanitário. 2020 jul./set.; 9(3): 26-48. Disponível em: <https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/658>. Acesso em: 22/09/2025.

UNIÃO EUROPEIA. Artificial **Intelligence Act (AI Act)**. Disponível em: <https://artificialintelligenceact.eu/article/5/#weglot_switcher>. Acesso em: 22/09/2025.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR).** Disponível em: <https://gdpr-info.eu/>. Acesso em: 22/09/2025.

WACHTER, Sandra. ***Affinity Profiling and Discrimination by Association in Online Behavioural Advertising***. Berkeley Technology Law Journal, v. 35, n. 2, p. 1-74, 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639>. Acesso em: 22/09/2025.

WHITE, Ryen; DORAISWAMI, Murali; HORVITZ, Eric. ***Detecting neurodegenerative disorders from web search signals***. Digital Medicine, v. 8 n. 1, p. 1-4, 2015. Disponível em: <https://www.nature.com/articles/s41746-018-0016-6#publish-with-us>. Acesso em: 22/09/2025.

YUSTE, Rafael *et al.* ***Four ethical priorities for neurotechnologies and AI***. Nature, v. 551, n. 7679, p. 159-163, 2017. Disponível em: <https://www.nature.com/articles/551159a>. Acesso em: 22/09/2025.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

NASSAR, Bruno Nazih Nehme; MORAES, Alexandre Rocha Almeida de. IA em Saúde, Profiling e Proteção de Dados: tensões entre inovação tecnológica, biodireito e direitos fundamentais. **Revista Brasileira de Direito Constitucional**, vol. 25, jan./dez. 2025), pp. 303-325. São Paulo: ESDC, 2025. ISSN: 1983-2303 (eletrônica).

Recebido em 03/10/2025

Aprovado em 25/10/2025

https://creativecommons.org/licenses/by/4.0/deed.pt-br