UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE CIÊNCIAS JURÍDICAS

FACULDADE DE DIREITO DO RECIFE

CAROLINA GOMES PUGLIESI BRANCO

LIMITAÇÕES DO HABEAS DATA E DA LGPD NO USO DE INTELIGÊNCIA ARTIFICIAL PELO ESTADO BRASILEIRO

Recife

2025

CAROLINA GOMES PUGLIESI BRANCO

LIMITAÇÕES DO HABEAS DATA E DA LGPD NO USO DE INTELIGÊNCIA ARTIFICIAL PELO ESTADO BRASILEIRO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito parcial para a obtenção do título de bacharela em Direito.

Orientadora: Antonella Bruna Machado Torres Galindo

Recife

2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Branco, Carolina Gomes Pugliesi.
LIMITAÇÕES DO HABEAS DATA E DA LGPD NO USO DE INTELIGÊNCIA ARTIFICIAL PELO ESTADO BRASILEIRO / Carolina Gomes Pugliesi Branco. - Recife, 2025.
65

Orientador(a): Antonella Bruna Machado Torres Galindo
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, Direito - Bacharelado, 2025.
Inclui referências.

1. Direito Constitucional. 2. Inteligência Artificial. 3. Constitucionalismo Digital. 4. Opacidade Algoritmica. 5. Habeas Data. 6. Lei Geral de Proteção de Dados. I. Galindo, Antonella Bruna Machado Torres . (Orientação). II. Título.

340 CDD (22.ed.)

CAROLINA GOMES PUGLIESI BRANCO

LIMITAÇÕES DO HABEAS DATA E DA LGPD NO USO DE INTELIGÊNCIA ARTIFICIAL PELO ESTADO BRASILEIRO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito parcial para a obtenção do título de bacharel(a) em Direito.

Aprovado em: 15/12/2025.

BANCA EXAMINADORA

Profº. Dra. Antonella Bruna Machado Torres Galindo
(Orientadora)

Universidade Federal de Pernambuco

Profº. Thácylla Dantas (Examinador Interno)
Universidade Federal de Pernambuco

Profº. Marcela Gama (Examinador Externo)

Universidade Federal de Pernambuco

AGRADECIMENTOS

À Jana e Jaime, meus pais, que me deram raízes firmes e asas seguras. Foram eles que construíram, com cuidado e sacrifício, o chão sobre o qual pude caminhar, tropeçar, aprender e finalmente chegar até aqui. Nada do que escrevo ou sou existiria sem o abrigo do amor deles.

À Soninha, minha segunda mãe, e aos meus irmãos, Rafael e Marina Branco, por serem lar em todas as formas possíveis. À Vini, meu amor, afilhado, sobrinho, por me dar esperança e vontade de construir pra você um mundo mais justo.

À Anna Bia e a Diego, meus primos-irmãos, companheiros de vida que me acompanharam no crescimento e nas descobertas. À minha família, que sempre me sustentou em lugares onde as palavras não alcançam. Às minhas tias Myriam e Simone, e à minha tia-madrinha Rosana, que são para mim exemplos vivos de coragem, luta e generosidade.

À minha família de santo, meus irmãos, e em especial Mãe Dai e Pai Mateus, por me ensinarem que espiritualidade também é pertencimento, comunidade e cuidado. Obrigada por moldarem minha força e por me guiarem quando os caminhos pareceram turvos.

Aos meus amigos, e família que escolhi, os “Fixos”, Aninha, Clara, Cláudia, Douglas, Duda, Guilherme, Ironildo, Shampoo, Malu, Victor Vinicius e Yasmin, agradeço pela escuta paciente, pelas conversas que me atravessaram, pela leveza que colocaram nos dias difíceis e por todo apoio que nunca me faltou. Obrigada por serem minha torcida mais fiel e por acolherem até as “palestrinhas” que nasceram das minhas inquietações.

À Iasmim Grosso, minha grande amiga e parceira em todos esses anos de FDR, por me mostrar tantos caminhos possíveis e me ensinar o que de fato é existência política.

A Victor Trajano, meu amado, presença luminosa que me acompanha mesmo nas sombras. Obrigada por segurar minha mão nas crises, por me lembrar do meu próprio valor e por ser descanso quando tudo ao redor parecia exaustão.

Aos meus gatinhos, Gil e Gadu, e também a Gal e Narinha, que hoje brilham como estrelinhas, por serem porto, afeto silencioso e companhia que cura.

À minha psicóloga, Dra. Andreza, por ajudar a reorganizar o que por vezes desmoronou dentro de mim e por me oferecer novas formas de existir no mundo.

Ao NAJUP, Vestibular Cidadão e a LIGADDOS, por me mostrarem que universidade pública se faz na prática.

Ao IP.rec, minha segunda casa, onde aprendi a ser pesquisadora e encontrei um espaço que acolhe curiosidade, rigor e afeto em igual medida. Em especial a Raquel Saraiva, André Fernandes, Mariana Canto e Clarissa Mendes, que foram faróis nesse percurso acadêmico e humano.

E, finalmente, à minha orientadora, Antonella Galindo, cuja generosidade intelectual e sensibilidade moldaram este trabalho. Obrigada por inspirar, guiar e acreditar.

“Apesar da batalha, o pente cheio

As tecnologias ancestrais nós temos

Pra induzir o sonho dentro de um pesadelo

Entre um traçante e outro

Dilatar o tempo e imaginar um mundo novo.”

— DON L, Primavera.

RESUMO

A incorporação de sistemas de inteligência artificial pela administração pública brasileira tem intensificado formas de tratamento de dados baseadas em inferências opacas que dificultam transparência e contestação. Este trabalho investiga se o habeas data e a Lei Geral de Proteção de Dados asseguram, de modo efetivo, os direitos de acesso, revisão e controle informacional, especialmente no que se refere à autodeterminação informativa, quando decisões estatais passam a ser mediadas por IA. A análise normativa, articulada a três estudos de caso, demonstra que o ordenamento jurídico já contém princípios e garantias suficientes em tese para disciplinar o uso de tecnologias inferenciais. Contudo, a opacidade algorítmica, a ausência de documentação técnica, a dependência tecnológica e a colonialidade informacional impedem que tais instrumentos produzam efeitos práticos. O cidadão conhece os dados brutos que o representam, mas não as inferências que moldam decisões administrativas, jurisdicionais e de segurança pública. Nesse cenário, o constitucionalismo digital emerge como chave hermenêutica que exige ampliar a publicidade, a motivação e o devido processo para abranger também as operações analíticas que produzem efeitos jurídicos. Conclui-se que a efetividade da proteção constitucional de dados depende menos de novos dispositivos normativos e mais de condições institucionais e epistêmicas capazes de tornar inteligíveis as decisões automatizadas e de preservar, na prática, a autodeterminação informativa.

Palavras-chave: inteligência artificial; habeas data; lgpd; constitucionalismo digital; opacidade algorítmica

ABSTRACT

The incorporation of artificial intelligence systems by the Brazilian public administration has intensified forms of data processing based on opaque inferences that hinder transparency and contestation. This study examines whether habeas data and the General Data Protection Law effectively secure the rights of access, review, and informational control, particularly with respect to informational self-determination, when state decisions become mediated by AI. The regulatory analysis, combined with three case studies, shows that the legal framework already contains principles and safeguards that are, in principle, sufficient to govern the use of inferential technologies. However, algorithmic opacity, the absence of technical documentation, technological dependence, and informational coloniality prevent these instruments from producing practical effects. Citizens may know the raw data that represent them, but not the inferences that shape administrative, judicial, and public security decisions. In this context, digital constitutionalism emerges as a hermeneutic key that requires expanding publicity, reasoning, and due process to encompass the analytical operations that produce legal effects. The study concludes that the effectiveness of constitutional data protection depends less on new normative provisions and more on institutional and epistemic conditions capable of rendering automated decisions intelligible and of preserving, in practice, informational self-determination.

Keywords: artificial intelligence; habeas data; gdpr; digital constitutionalism; algorithmic opacity.

SUMÁRIO

1 INTRODUÇÃO

O uso crescente de sistemas de inteligência artificial pelo Estado brasileiro tem transformado profundamente a forma como informações pessoais são coletadas, organizadas e mobilizadas na formulação de políticas públicas, na gestão administrativa, na prestação jurisdicional e na segurança pública. Modelos de classificação, ranqueamento, predição e identificação biométrica tornam-se cada vez mais centrais na atuação estatal, deslocando o eixo decisório de agentes públicos para sistemas computacionais que frequentemente operam de modo opaco e tecnicamente complexo. Nesse cenário, a transparência, a justificabilidade das decisões estatais e o controle pelo cidadão passam a depender de condições epistêmicas e informacionais distintas daquelas consideradas nos modelos jurídicos concebidos para ambientes analógicos.

A digitalização estatal no Brasil ocorre em ambiente marcado por forte dependência de soluções tecnológicas desenvolvidas por empresas privadas estrangeiras e por um arcabouço normativo que ainda não consegue acompanhar plenamente a complexidade dos sistemas utilizados. Nesse cenário, ganha centralidade a noção de opacidade algorítmica, expressão que busca traduzir a dificuldade estrutural de compreender como algoritmos chegam aos resultados que produzem (BURRELL, 2016). Em termos simples, trata-se de situação na qual é possível observar o ponto de partida e o ponto de chegada de uma decisão, mas não o caminho interno percorrido pelo sistema para transformar dados em classificações, recomendações ou ações estatais.

Essa lacuna de inteligibilidade não é acidental nem limitada à complexidade matemática dos modelos. Burrell (2016) demonstra que a opacidade algorítmica possui múltiplas camadas, que incluem não apenas dificuldades técnicas inerentes a determinadas arquiteturas de aprendizado de máquina, mas também formas de opacidade intencional e institucional decorrentes de decisões humanas, econômicas e jurídicas. Para o autor, a opacidade pode surgir tanto de estruturas matemáticas difíceis de interpretar quanto de barreiras derivadas de segredos industriais, ausência de documentação, assimetrias de especialização ou restrições contratuais impostas pelos fornecedores dos sistemas. Ao reunir essas dimensões, Burrell evidencia que a falta de explicabilidade não é mero efeito colateral, mas característica estrutural de grande parte das tecnologias contemporâneas.

As consequências práticas dessa multiplicidade de opacidades são profundas. A impossibilidade de compreender como dados são transformados em inferências produz assimetrias informacionais que fragilizam pilares centrais da atuação estatal, como a publicidade dos atos, a motivação das decisões e a possibilidade de controle pelos cidadãos. Quando os processos inferenciais permanecem inacessíveis, o fundamento técnico das

decisões deixa de integrar o espaço público de justificação e escapa às ferramentas jurídicas tradicionais de transparência, revisão e responsabilização. Assim, mesmo quando as decisões aparentam estar motivadas, parte relevante de sua racionalidade permanece fora do alcance do titular, comprometendo a própria lógica constitucional de controle do poder público.

Nesse contexto, a tensão entre proficiência tecnológica e controle democrático se aprofunda, tornando imprescindível examinar se os instrumentos jurídicos existentes conseguem alcançar o atual locus decisório, que deixou de ser o documento e passou a ser o processo algorítmico. Diante desse cenário, ganha relevo a necessidade de examinar a compatibilidade entre tais tecnologias e as garantias constitucionais destinadas a assegurar o acesso, a transparência e o controle sobre informações pessoais.

Entre essas garantias, destacam-se o habeas data, previsto no artigo 5º, LXXII da Constituição de 1988, e a Lei Geral de Proteção de Dados, que estabelece princípios e direitos voltados à proteção da esfera informacional do indivíduo. Ambos os instrumentos foram concebidos com o propósito de limitar o poder informacional do Estado e assegurar que cidadãos possam conhecer e contestar dados armazenados sobre si. Entretanto, o modo como a inteligência artificial é incorporada às práticas estatais suscita dúvidas quanto à capacidade desses mecanismos de assegurar transparência efetiva em ambientes decisórios mediados por inferências estatísticas e mecanismos automatizados de predição. O contraste entre a finalidade protetiva desses instrumentos e o ambiente técnico no qual hoje devem operar revela possível descompasso entre o desenho normativo e a realidade informacional contemporânea. A literatura nacional, especialmente Doneda (2019) e Schertel Mendes (2019), já advertiu que direitos informacionais só podem ser exercidos quando as condições epistêmicas mínimas de compreensão e contestabilidade estão asseguradas. Nesse sentido, a autodeterminação informativa, tal como formulada pela doutrina constitucional contemporânea, é entendida neste trabalho como o poder do indivíduo de compreender, interferir e contestar não apenas os dados que o Estado armazena, mas também os efeitos inferenciais produzidos a partir desses dados.

É nessa conjuntura que se insere a pergunta orientadora desta pesquisa: até que ponto o habeas data e a Lei Geral de Proteção de Dados são capazes de assegurar transparência, acesso e controle sobre informações pessoais quando o Estado emprega sistemas de inteligência artificial cujos mecanismos de funcionamento permanecem opacos ou inacessíveis ao cidadão? Parte-se da hipótese de que esses instrumentos jurídicos, embora fundamentais, não são suficientes para responder às condições tecnológicas atuais, o que torna necessário o desenvolvimento de normas adicionais capazes de lidar com modelos decisórios baseados em inferências algorítmicas. A investigação busca verificar empiricamente se essa insuficiência decorre primordialmente de lacunas normativas ou se é

agravada por fatores estruturais ligados ao modo como tecnologias de inteligência artificial operam e reorganizam a atuação estatal. Sustenta-se, portanto, que existe um descompasso estrutural entre instrumentos concebidos para bancos de dados estáticos e práticas decisórias produzidas por sistemas dinâmicos de inferência, reforçando a necessidade de aperfeiçoamento legislativo.

A relevância do tema decorre de quatro fatores centrais. No plano jurídico, envolve direitos fundamentais que integram o núcleo do Estado Democrático de Direito, como privacidade, acesso à informação, autodeterminação informativa, igualdade e devido processo legal. No plano institucional, diz respeito à capacidade do Estado de justificar decisões em conformidade com os princípios constitucionais de motivação e publicidade. No plano político, a expansão de tecnologias automatizadas de vigilância e classificação ocorre em um país marcado por desigualdades raciais, territoriais e socioeconômicas que podem ser reproduzidas e amplificadas por sistemas algorítmicos. No plano acadêmico, há lacunas relevantes na literatura jurídica sobre a aplicação concreta do habeas data e da LGPD frente à automatização das decisões estatais, especialmente em contextos de opacidade algorítmica. Assim, a pesquisa se insere no esforço contemporâneo de compreender como direitos fundamentais concebidos em um contexto analógico podem, ou não podem, ser reinterpretados para enfrentar a racionalidade tecnológica que estrutura decisões públicas na era digital.

A metodologia adotada é qualitativa e baseia-se em análise documental e hermenêutica constitucional. Examina-se a Constituição de 1988, o habeas data, a LGPD, decisões judiciais, documentos públicos relativos ao uso de sistemas de inteligência artificial pelo Estado, e relatórios de estudos de caso publicados por organizações da sociedade civil. A abordagem hermenêutica busca compreender como garantias constitucionais projetadas para bancos de dados estáticos devem ser interpretadas em ambiente decisório estruturado por inferências dinâmicas e técnicas de aprendizado de máquina. O método aplicado combina interpretação normativa e análise das condições epistêmicas e institucionais que condicionam a efetividade dos direitos, partindo da premissa de que a proteção constitucional depende não apenas de previsão normativa, mas também de sua possibilidade material de exercício.

A análise empírica organiza-se em três estudos de caso: o Sistema Nacional de Emprego, a adoção da ferramenta MAIA Justiça pelo Tribunal de Justiça de Pernambuco e o reconhecimento facial aplicado à segurança pública. A escolha desses casos permite observar a atuação estatal em três dimensões distintas: políticas públicas distributivas, jurisdição e vigilância policial. A seleção dessas experiências decorre da diversidade de funções estatais envolvidas e da capacidade de cada uma de revelar dimensões específicas do problema investigado. Adota-se, assim, metodologia que combina densidade dogmática com

observação empírica qualificada, permitindo testar a hipótese teórica em situações concretas de uso de IA pelo Estado.

A pesquisa não examina o funcionamento interno dos algoritmos, tampouco propõe alterações legislativas ou avalia projetos normativos em tramitação. O foco recai sobre a interpretação constitucional das garantias existentes e sobre sua eficácia atual diante da automatização de decisões. Assume-se que a proteção de dados exige análise que ultrapassa o texto normativo e alcança a estrutura informacional que condiciona a possibilidade efetiva de exercício de direitos. Trata-se de investigação voltada não à engenharia dos algoritmos, mas à engenharia constitucional necessária para que direitos fundamentais permaneçam operativos em ambientes governados por técnicas opacas. Esse recorte metodológico permite evitar reducionismos tecnicistas e sustentar a análise no diálogo entre teoria constitucional, estudos críticos de tecnologia e evidências empíricas.

Com essa moldura, a investigação busca avaliar se o habeas data e a LGPD oferecem instrumentos suficientes para garantir transparência e controle em decisões estatais mediadas por inteligência artificial, ou se as próprias características técnicas, institucionais e epistêmicas dessas tecnologias impõem desafios que demandam reinterpretação das categorias constitucionais vigentes. A pesquisa não parte de conclusões prévias, mas de uma hipótese inicial sujeita à verificação ao longo do trabalho, conforme as evidências documentais, teóricas e empíricas analisadas. O objetivo último consiste em compreender se o déficit de transparência e controle informacional decorre daquilo que a Constituição dispõe ou daquilo que a tecnologia transforma.

2 HABEAS DATA: FUNDAMENTOS, EVOLUÇÃO E FUNÇÃO CONSTITUCIONAL NA ERA DIGITAL

2.1 Evolução histórica

A necessidade de adaptação do Direito a novas realidades é inquestionável, especialmente diante das rápidas transformações sociais e tecnológicas. Ao lidar com desafios contemporâneos, é imperativo refletir sobre como o ordenamento jurídico se ajusta a essas mudanças, preservando valores e garantias individuais. Nesse contexto, a compreensão da intenção do legislador e o contexto da criação da norma emergem como elementos-chave na interpretação das leis, sendo vitais para atribuir valores objetivos à legislação e reconstruir sua função constitucional ao longo do tempo.

De acordo com MACCORMICK:

> [a atribuição de uma intenção "objetiva" ao Parlamento] deriva de uma leitura da legislação como um todo, orientada pela assunção da racionalidade parlamentar na consecução de uma tarefa teleológica guiada por alguma concepção de justiça e do bem comum – concepção essa que talvez seja contestável, talvez até contestada. Não se trata, portanto, de uma "intenção" descoberta como um fato histórico a partir de elementos externos aos materiais colocados à interpretação e às suposições comuns que a comunidade de intérpretes pode fazer sobre o processo racional de produção do Direito. Trata-se de um instrumento heurístico interno à interpretação jurídica, não um dado novo acrescentado de fora. (MACCORMICK, 2008 *apud* NASCIMENTO, 2021)

Nesse sentido, a compreensão do contexto legislativo não se resume a uma mera busca por intenções históricas isoladas, mas sim a uma abordagem holística que considera a racionalidade parlamentar subjacente à legislação. Isso permite a adaptação do ordenamento jurídico às exigências contemporâneas, garantindo sua relevância e eficácia. Em consonância com as ideias de Maccormick, a interpretação do Direito deve ser encarada como um processo dinâmico, guiado pela compreensão profunda das intenções do legislador. Essa racionalidade teleológica serve, portanto, como critério de reconstrução da norma, especialmente em matéria de direitos fundamentais cuja efetividade depende da capacidade de responder a desafios tecnológicos imprevistos pelo constituinte. Essa abordagem não apenas fortalece a legitimidade do sistema jurídico, mas também proporciona uma base sólida para a adaptação a novos desafios, como os apresentados pela evolução tecnológica.

A *occasio legis,* torna-se, portanto, crucial para a argumentação deste trabalho, pois tal investigação é fundamental não apenas para analisar criticamente a atual incorporação da inteligência artificial pelo Estado brasileiro, mas principalmente para compreender qual bem jurídico deveria estar sendo protegido nesse processo. A identificação dessa finalidade original funciona como parâmetro interpretativo indispensável para aferir se a proteção constitucional permanece adequada diante de um novo ambiente informacional. À vista disso,

torna-se imperativo investigarmos a evolução histórica do habeas data, a fim de ampliar nossa compreensão sobre as bases e fundamentos desse instrumento jurídico no contexto das transformações sociais e tecnológicas.

Em uma primeira análise, é válido ressaltar que o habeas data, enquanto instrumento legal, desempenha um papel essencial na salvaguarda do bem jurídico da privacidade e integridade das informações pessoais dos cidadãos. Ao resguardar a individualidade e dignidade das pessoas, a garantia busca não apenas assegurar o acesso do titular a essas informações, mas também corrigir eventuais imprecisões nos dados registrados e impedir que representações estatais distorcidas produzam efeitos jurídicos indevidos.

De acordo com Alexandre de Moraes (2016), podemos conceituar tal instrumento como um "direito que assiste a todas as pessoas de solicitar judicialmente a exibição dos registros públicos ou privados nos quais estejam incluídos seus dados pessoais para que deles se tome conhecimento e se necessário for, sejam retificados os dados inexatos ou obsoletos ou que impliquem em discriminação."

Tal surgimento significou uma resposta direta às transformações sociais e tecnológicas na Europa da década de 1970. Seu embrião legislativo encontra-se na Lei do Land de Hesse, Alemanha Ocidental, datada de 7 de outubro de 1970, e na lei francesa de proteção à intimidade, promulgada em 17 de julho de 1970. Essas legislações pioneiras marcaram o reconhecimento da necessidade premente de proteger os cidadãos diante do crescente advento dos registros de dados informáticos e da percepção de que a informatização ampliava os riscos de vigilância e de manipulação invisível das informações pessoais.

A expansão dos registros digitais e a universalização do acesso à informação impulsionaram a concepção do habeas data. Na esteira desses avanços, a legislação sueca, representada pela Datalug sueca, e o Reino Unido, por meio do Data Protection Act de 1974, bem como a Itália, com sua lei nº 98 de 1974, consolidaram a proteção à privacidade e à precisão dos dados registrados. No cenário constitucional, Portugal, em sua Constituição de 1976, e a Espanha, na Constituição de 1978, incorporaram o direito ao acesso à informação de dados, instituindo o habeas data como uma garantia constitucional. Nos Estados Unidos, a permissão ao acesso de particulares às informações de registros e bancos de dados foi consagrada pelo Freedom of Information Act de 1974, posteriormente alterado pelo Freedom of Information Reform Act de 1978 (MOREIRA, 1997). Esses marcos revelam que a proteção de dados emergiu como resposta institucional à centralização informacional e aos riscos associados ao tratamento massivo de informações pessoais pelo Estado e por grandes organizações.

A origem do habeas data no contexto brasileiro está profundamente ligada aos

eventos políticos que se desenrolaram durante o golpe militar de 1964. Nesse período, o país enfrentou a imposição de governos militares à margem da ordem constitucional, marcados por violações de direitos, uso de informações sigilosas e construção de registros falsos. O golpe estabeleceu um regime autoritário que perdurou por anos, resultando em um sistema de informações sigilosas amplamente utilizado, liderado pelo Serviço Nacional de Informações (SNI). Tortura, escuta telefônica, corrupção e falsificação de dados foram alguns dos meios imorais e ilegais empregados para sustentar o regime e consolidar um aparato informacional voltado ao controle político e à repressão.

Durante esse período, dados muitas vezes falsos foram utilizados para divulgação pela imprensa ou como base para processos administrativos e judiciais. O acesso a esses bancos de dados, considerados sigilosos "por motivo de segurança nacional", era restrito, privando as pessoas registradas e seus defensores legais, bem como juízes e tribunais, do conhecimento dessas informações. Essa prática de manipulação de dados e restrição de acesso serviu como base para a criação do habeas data no Brasil como instrumento de ruptura com a lógica autoritária de produção e utilização de informações pelo Estado.

Ao emergir como resposta às injustiças e abusos ocorridos durante o regime militar, o habeas data brasileiro se distingue claramente do simples acesso à informação. Tal instrumento foi concebido como uma resposta específica à utilização maliciosa de dados durante o regime ditatorial (MOREIRA, 1997), destacando-se como uma ferramenta crucial para quebrar o sigilo de informações em posse das autoridades de segurança e corrigir erros e falsidades em registros públicos ou bancos de dados. É fundamental reconhecer que, mesmo que o direito à informação, em um sentido amplo, já estivesse reconhecido no Direito brasileiro, a criação do habeas data representou uma abordagem única e necessária diante das circunstâncias particulares da época. Ele não apenas assegura a privacidade e a integridade dos dados, mas também têm propósitos distintos, que permitem que o interessado acione a jurisdição para garantir não apenas o acesso, mas a correção das informações. Sua natureza jurídica é dual, desempenhando o papel de garantia constitucional e ação mandamental:

> O 'habeas data' configura remédio jurídico-processual, de natureza constitucional, que se destina a garantir em favor da pessoa interessada, o exercício de pretensão jurídica discernível em seu tríplice aspecto: a) direito de acesso aos registros existentes; b) direito de retificação dos registros errôneos e c) direito de complementação dos registros insuficientes ou incompletos. Trata-se de relevante instrumento de ativação da jurisdição constitucional das liberdades, que representa, no plano institucional, a mais expressiva reação jurídica do Estado às situações que lesem, efetiva ou potencialmente, os direitos da pessoa, quaisquer que sejam as dimensões em que estes se projetem" (STF, HD 75/DF, Rel. Min. Celso de Mello, DJU de 19-10-2006).

A dimensão histórica do habeas data no Brasil se estende desde sua proposta pelo jurista José Afonso da Silva perante a Comissão Provisória de Estudos Constitucionais, durante os debates constitucionais brasileiros de 1978 (MOREIRA, 1997). Essa proposta foi

incorporada no Anteprojeto dos Notáveis da Constituição de 1988, consagrando-se no artigo 5º, inciso LXXII:

> LXXII - conceder-se-á "habeas-data":
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
>
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Apesar de sua inclusão na Carta Magna, um amplo período transcorreu sem regulamentação legislativa específica, o que resultou na predominância da jurisprudência para sua aplicação. Foi somente em 1997 que a Lei nº 9.507 veio a regulamentar o habeas data, conferindo-lhe procedimento próprio.

O habeas data, ao assegurar o conhecimento e retificação de informações junto a entidades governamentais, preenche uma lacuna essencial na defesa dos cidadãos contra o mau uso de dados e a possibilidade de construções equivocadas acerca de suas vidas. Assim, ele não apenas reflete a evolução histórica desse instrumento em outros países, mas também carrega consigo a marca da resistência contra o autoritarismo e a luta pela restauração democrática. Sua inclusão na Constituição de 1988 foi uma resposta concreta à necessidade de proteger os cidadãos contra o uso indevido de dados durante um período sombrio da história do Brasil.

O bem jurídico protegido pelo habeas data transcende o mero acesso a registros e bancos de dados; ele resguarda a própria dignidade e autonomia dos indivíduos. A privacidade, nesse contexto, não é apenas uma esfera restrita de informações, mas um pilar fundamental da identidade e liberdade de cada pessoa. Assim, fundamentado no princípio da intimidade e vida privada, ao garantir o direito de retificação e conhecimento, promove a defesa da integridade subjetiva, permitindo que os cidadãos controlem a narrativa de sua própria existência diante das instituições públicas e previnam distorções que possam gerar estigmatização ou restrições indevidas de direitos.

Não obstante, a Súmula 2 do Superior Tribunal de Justiça (STJ) destaca que o direito de ação relativo ao habeas data nasce da negativa no fornecimento de informações, evidenciando a necessidade de um ato gerador de conflito para acionar o provimento judicial. Isso sublinha a importância de uma provocação específica para que a Justiça intervenha e resolva questões relacionadas à privacidade e acesso a dados:

> EMENTA
>
> Habeas data. Ausência de postulação administrativa.
>
> I -Ante a ausência de pleito administrativo, suficiente a configurar relutância da

> Administração a atender o pedido, sofre o habeas data de "ausência de interesse de agir".
>
> II - Pedido não conhecido.

Portanto, se apresenta como uma peça fundamental no xadrez jurídico, cujo movimento busca proteger não apenas a privacidade individual, mas também preservar as relações jurídicas e sociais em um mundo cada vez mais interconectado. A incorporação desse instrumento no ordenamento jurídico brasileiro, inspirada por experiências europeias, reflete a busca constante por um equilíbrio entre a informatização e a proteção dos direitos individuais. Tal equilíbrio assume uma relevância ainda maior nos tempos atuais, em que a inteligência artificial se integra às estruturas estatais, demandando uma interpretação jurídica adaptativa e uma proteção robusta diante da opacidade dos dados.

2.2 Finalidade constitucional e limitações enfrentadas

A finalidade constitucional do habeas data deve ser compreendida à luz do projeto normativo da Constituição de 1988, que consagra um modelo de Estado orientado pela supremacia da dignidade da pessoa humana, pela centralidade dos direitos fundamentais e pela limitação do poder estatal mediante instrumentos de transparência e controle democrático. Sua razão de existir está associada à necessidade de impedir a formação de espaços informacionais impenetráveis, capazes de produzir efeitos jurídicos sobre a esfera individual sem possibilidade de escrutínio pelo próprio interessado e sem aderência ao princípio republicano da publicidade das razões públicas.

Enquanto garantia constitucional, o habeas data protege um bem jurídico complexo, que ultrapassa o mero acesso material a documentos e se projeta sobre a integridade da identidade informacional do indivíduo. A informação pessoal, na ordem constitucional vigente, não é elemento neutro: ela compõe o modo como o Estado enxerga o cidadão, orienta decisões administrativas e judiciais e influencia a maneira pela qual direitos e deveres são atribuídos. A finalidade do habeas data, portanto, consiste em conferir ao titular o poder de verificar a exatidão, atualidade e licitude das informações que o representam no âmbito institucional, preservando a coerência entre sua identidade real e sua identidade registrada. Essa dimensão ativa transforma a privacidade em faculdade de controle e reconstrução narrativa, integrando o titular ao processo de conformação de sua própria representação estatal.

Essa compreensão aproxima o instituto da ideia de autodeterminação informativa desenvolvida pelo Tribunal Constitucional Alemão (ALEXY, 2008), segundo a qual cabe ao indivíduo decidir, dentro de limites constitucionalmente legítimos, sobre a produção, circulação e utilização de dados que lhe digam respeito. Embora o constituinte brasileiro não

tenha utilizado expressamente essa terminologia, a Constituição de 1988 atribuiu, por meio do habeas data, uma dimensão ativa ao direito à privacidade. Não se trata apenas de impedir que o Estado invada a esfera íntima do indivíduo, mas também de garantir que informações pessoais, uma vez registradas, possam ser conhecidas, compreendidas e corrigidas.

A doutrina destaca que o habeas data possui caráter mandamental, impondo ao ente detentor de registros o dever de prestar informações ou de realizar retificações quando demonstrada a inadequação, incompletude ou desatualização dos dados (BARROSO, 1993). A natureza desse dever revela que o bem jurídico tutelado não se restringe ao conteúdo informacional, mas abrange também a regularidade procedimental do tratamento de dados pelo Estado. Ao viabilizar o controle individual sobre bancos de dados públicos, o habeas data reforça o dever estatal de obedecer a critérios de finalidade, necessidade e precisão, antecipando conceitos que a Lei Geral de Proteção de Dados positivaria décadas depois.

A jurisprudência constitucional corrobora essa leitura. O Supremo Tribunal Federal, em precedentes como o Habeas Data 75 do Distrito Federal, reconheceu que o instituto constitui instrumento de proteção das liberdades, destinado a evitar que dados imprecisos ou inacessíveis produzam efeitos negativos na esfera jurídica do titular. Segundo o Tribunal, o remédio cumpre papel essencial na garantia de transparência administrativa, funcionando como mecanismo de contenção de possíveis abusos informacionais.

No cenário contemporâneo, marcado pela presença de sistemas automatizados e por técnicas sofisticadas de tratamento de dados, a finalidade constitucional do habeas data adquire novo significado. A expansão de bases de dados interconectadas e a utilização de algoritmos para classificação, previsão e tomada de decisão intensificam o risco de que informações pessoais sejam processadas de maneira opaca, incorreta ou discriminatória. A função constitucional do instituto, nesse contexto, requer interpretação capaz de abranger não apenas dados estáticos, mas também resultados inferidos, perfis preditivos e registros gerados por técnicas de aprendizado de máquina. A proteção efetiva do bem jurídico pressupõe, assim, a possibilidade de compreender os critérios mínimos que orientam o tratamento automatizado de dados, sob pena de tornar o acesso e a retificação direitos meramente formais.

Sob essa perspectiva, a finalidade do habeas data é indissociável da exigência de transparência sobre processos informacionais que impactam a esfera jurídica do indivíduo. Essa transparência não se confunde com abertura irrestrita de códigos ou modelos computacionais, mas envolve a disponibilização de informações suficientes para permitir controle, questionamento e correção. O bem jurídico protegido, portanto, abrange não apenas

a integridade dos dados propriamente ditos, mas também a inteligibilidade mínima das práticas que envolvem seu tratamento pelo Estado.

A leitura sistemática da Constituição permite afirmar que o habeas data cumpre papel estruturante no regime jurídico da proteção de dados pessoais, atuando como garantia fundamental que preserva a confiança do indivíduo no Estado e assegura as condições necessárias para o exercício de liberdades públicas. Sua finalidade constitucional deriva de uma concepção de cidadania informada e capaz de exercer controle sobre representações estatais que lhe digam respeito. Ao resguardar a integridade informacional e a autodeterminação do sujeito, o instituto constitui instrumento indispensável para evitar que o poder informacional estatal se converta em mecanismo de exclusão, discriminação ou violação de direitos fundamentais.

A conformação constitucional do habeas data, embora inovadora à época de sua positivação, foi projetada para um ambiente informacional substancialmente distinto daquele que caracteriza a sociedade digital contemporânea. O avanço acelerado das tecnologias de informação, aliado à crescente delegação de decisões a sistemas automatizados e modelos algorítmicos, evidencia limites estruturais do instituto que não decorrem de insuficiência normativa, mas da transformação profunda das condições materiais de produção, circulação e uso de dados. O problema não reside no texto constitucional, mas na mutação do próprio objeto sobre o qual o habeas data deve incidir.

Um primeiro desafio emerge da assimetria informacional que caracteriza a relação entre titular e controlador. O exercício do habeas data depende, conforme reiterado pela Súmula 2 do Superior Tribunal de Justiça, do prévio conhecimento da existência do dado e da negativa explícita ou implícita de acesso ou retificação. Tal requisito se harmonizava com um ambiente de registros estáveis e identificáveis, nos quais a violação era perceptível e a iniciativa do titular correspondia a um ato de vigilância ativa sobre sua própria informação. No ecossistema contemporâneo, marcado por big data, inferências, perfis preditivos e decisões automatizadas, essa premissa simplesmente não se sustenta. O titular não sabe que está sendo classificado, ranqueado ou predito, tampouco tem condições materiais de identificar que determinada decisão deriva de um tratamento de dados que lhe diz respeito.

Nesse cenário, o brocardo *dormientibus non succurrit ius* adquire releitura inevitável. A ausência de provocação não decorre de inércia voluntária, mas de ignorância estrutural produzida pela arquitetura informacional. Quando o cidadão desconhece que seus dados são coletados, correlacionados, inferidos ou utilizados para decisões automatizadas, não lhe é possível deflagrar a tutela constitucional. O pressuposto fático de acionamento do habeas data desaparece. A garantia permanece juridicamente intacta, mas perde condições

epistêmicas de exercício. Trata-se de deslocamento que limita o instituto em sua própria origem procedimental.

A opacidade algorítmica constitui obstáculo ainda mais profundo. Modelos de aprendizado de máquina operam com estruturas matemáticas complexas, de difícil interpretabilidade, frequentemente inacessíveis até mesmo a seus desenvolvedores. Em tais casos, ainda que o titular tenha acesso a dados brutos, permanece incapaz de compreender como aqueles dados foram processados, ponderados ou combinados para produzir determinado resultado. É exatamente esse conjunto de barreiras que fragiliza o habeas data e a LGPD em sua aplicação a modelos de inteligência artificial. Não se trata de insuficiência normativa, mas de transformação material das condições que tornavam tais garantias efetivamente exercíveis.

Essa conceituação reforça a hipótese deste trabalho: a distância entre titularidade formal e capacidade real de exercício dos direitos decorre da opacidade algorítmica como fenômeno estrutural da era digital. O habeas data assegura o acesso documental, mas não alcança a dimensão hermenêutica do tratamento. O que produz efeitos jurídicos não é o dado isolado, mas a inferência dele derivada, invisível ao titular e protegida, muitas vezes, por sigilo técnico, segredo industrial ou ausência de documentação. Assim, o remédio constitucional chega ao núcleo externo do problema, sem tocar sua racionalidade decisória.

Parte da insuficiência decorre da própria mudança no locus do poder informacional. No paradigma analógico, o risco estava associado ao acúmulo estatal de registros errôneos ou desatualizados. No paradigma algorítmico, o risco decorre do modo como bases de dados são articuladas para produzir classificações, probabilidades e perfis. A lógica de funcionamento do algoritmo - e não o registro bruto - é o elemento determinante da lesão. Entretanto, o habeas data não possui desenho procedimental capaz de exigir do Estado a explicitação dos critérios que orientam o processamento e a inferência. O controle jurisdicional torna-se inviável quando nem mesmo o controlador dispõe de documentação adequada sobre o funcionamento de sistemas adquiridos de empresas privadas. A consequência é a criação de zonas de imunidade técnica, em que a racionalidade administrativa permanece inacessível ao cidadão e ao próprio Poder Judiciário.

Outro limite relevante decorre da coexistência entre o habeas data e a Lei Geral de Proteção de Dados Pessoais. A LGPD amplia o catálogo de direitos e impõe deveres de transparência, prevenção e responsabilização, mas contém exceções significativas, sobretudo no campo da segurança pública, persecução penal e defesa nacional. Nessas áreas, o habeas data seria, em tese, o mecanismo residual de proteção. Contudo, tais setores concentram exatamente os sistemas mais opacos, como reconhecimento facial, análise preditiva ou

cruzamento massivo de bases. A fragmentação normativa aprofunda a lacuna: onde a LGPD não alcança integralmente e onde a IA opera de modo mais invasivo, o habeas data não possui instrumentação suficiente para romper a opacidade. O instituto foi concebido para registros, não para arquiteturas algorítmicas dinâmicas.

Há, ainda, limitações intrínsecas decorrentes da autolimitação. A exposição voluntária de dados em redes sociais, aplicativos e plataformas dilui a fronteira entre dado público e privado, produzindo novos vetores de acesso e circulação que dificultam a identificação de responsabilidades. Contudo, mesmo esse fenômeno reforça a insuficiência do habeas data, pois a lesão em sistemas algorítmicos não decorre do dado fornecido voluntariamente, mas das inferências derivadas, sobre as quais o titular não exerce controle e que o instituto não consegue alcançar.

O conjunto desses elementos evidencia que o habeas data permanece normativamente relevante, mas enfrenta limites substanciais diante do ambiente tecnológico contemporâneo. Sua eficácia depende de reconstrução hermenêutica capaz de integrar princípios constitucionais tradicionais com exigências próprias do cenário digital, em que a proteção da pessoa humana demanda instrumentos aptos a lidar com processos decisórios automatizados, inferências dinâmicas e riscos difusos. Enquanto garantia histórica de resistência ao arbítrio informacional, o habeas data mantém função simbólica e normativa significativa, mas já não basta, por si só, para assegurar controle efetivo sobre tecnologias que operam além da cognoscibilidade individual e institucional.

3 A LEI GERAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO DE CONCRETIZAÇÃO DA PROTEÇÃO CONSTITUCIONAL

3.1 Estrutura normativa da LGPD e seu papel constitucional

A Lei Geral de Proteção de Dados Pessoais deve ser compreendida como marco de consolidação de um projeto constitucional previamente inaugurado pelo habeas data. Ambos os instrumentos, embora distintos em sistemática e alcance, integram uma mesma arquitetura de limitação do poder informacional, cujo núcleo consiste na afirmação da autodeterminação informativa e na garantia de que o cidadão possa conhecer, controlar e contestar as informações que o Estado e agentes privados produzem sobre si.

O habeas data inaugurou, em 1988, a primeira formulação normativa expressa dessa pretensão de controle; a LGPD representou sua expansão sistemática e sua readequação às condições tecnológicas contemporâneas, preservando o fundamento constitucional que lhe dá sentido. Nesse ponto, a formulação de Laura Schertel Mendes (2019) revela-se especialmente elucidativa ao afirmar que:

> "a proteção de dados pessoais somente alcança densidade constitucional efetiva quando o titular dispõe de instrumentos que lhe permitam intervir sobre a totalidade dos dados que o representam, e não apenas sobre aqueles que fornece diretamente, razão pela qual habeas data e legislação infraconstitucional não podem ser compreendidos de forma dissociada".

A interpretação conjunta desses mecanismos reafirma que a Constituição de 1988 não concebeu o indivíduo como objeto passivo de registros estatais, mas como sujeito ativo na construção de sua identidade informacional.

A formação histórica da LGPD confirma essa vocação constitucional. Desde as primeiras discussões conduzidas pelo Ministério da Justiça entre 2010 e 2015, já se reconhecia que o ordenamento brasileiro convivia com crescente expansão de bases de dados governamentais, forte dependência tecnológica de empresas estrangeiras e ausência de parâmetros normativos para práticas de tratamento intensivo de dados.

A promulgação do Marco Civil da Internet, em 2014, sinalizou a transição para um modelo de regulação voltado à proteção de direitos fundamentais no ambiente digital, mas não ofereceu respostas suficientes para a complexidade dos fluxos informacionais estruturados por big data e técnicas de aprendizado de máquina. A aprovação da LGPD em 2018 surgiu, portanto, como resposta necessária à assimetria crescente entre titulares e controladores, assimetria que a lógica tradicional do habeas data já não conseguia mitigar. Ao estruturar princípios, direitos e deveres aplicáveis ao tratamento de dados em todos os setores, a LGPD não apenas atualizou a proteção constitucional, mas também consolidou um regime

jurídico coerente com a ideia de que a esfera informacional constitui dimensão essencial da personalidade.

A arquitetura normativa da LGPD é marcada por forte densidade principiológica, que orienta a interpretação de todas as suas disposições. Os princípios de finalidade, adequação e necessidade funcionam como critérios de proporcionalidade do tratamento de dados, exigindo que cada operação informacional seja justificada não apenas de forma abstrata, mas de modo concreto e vinculado a um propósito legítimo.

Na atividade estatal, esses princípios impedem que dados coletados para finalidades administrativas sejam ampliados de maneira indiscriminada ou convertidos em instrumentos de vigilância incompatíveis com a Constituição. A transparência e o livre acesso impõem deveres de inteligibilidade e completude das informações fornecidas ao titular, o que vincula diretamente o regime da LGPD ao habeas data, pois ambos têm por objetivo impedir zonas opacas de poder informacional. A prevenção, a não discriminação e a responsabilização completam o núcleo normativo da lei, inserindo no ordenamento a exigência de governança algorítmica adequada, auditoria contínua e demonstração ativa de conformidade, o que responde aos riscos que emergem quando decisões públicas passam a incorporar, parcial ou integralmente, inferências automatizadas.

Esse regime principiológico sustenta a estrutura normativa das bases legais. A LGPD afastou a ideia de que o consentimento seria fundamento único ou predominante de licitude do tratamento e adotou modelo plural que reconhece situações nas quais o consentimento é inviável ou inadequado, como no caso de execução de políticas públicas.

Essa pluralidade, contudo, não afrouxa a tutela da pessoa, pois cada base legal é condicionada ao respeito aos princípios constitucionais e legais que regem o tratamento. No âmbito estatal, a base do artigo 7º, III, que autoriza o tratamento para execução de políticas públicas, não constitui autorização irrestrita, mas pressupõe justificativa adequada, proporcionalidade, documentação técnica, avaliação de riscos e mecanismos de publicidade que assegurem condições mínimas de controle democrático. A criação da Autoridade Nacional de Proteção de Dados, posteriormente convertida em agência reguladora, integra esse arranjo institucional, garantindo função regulatória e fiscalizatória permanente, essencial para um regime de direitos que depende de supervisão contínua e especializada.

A análise dos direitos do titular permite observar a profundidade da convergência entre LGPD e habeas data e ao mesmo tempo explicitar o ponto central da hipótese deste trabalho. O direito de acesso, núcleo histórico do habeas data, foi expandido pela LGPD em extensão e profundidade. Não basta fornecer ao titular os dados brutos que constam em registros administrativos; é necessário indicar finalidades, critérios de tratamento, agentes com quem

os dados foram compartilhados e informações que permitam compreender minimamente os processos decisórios que deles derivam. Essa exigência dialoga diretamente com a hipótese deste TCC, segundo a qual tais direitos, concebidos para garantir transparência e controle, tornam-se materialmente insuficientes quando aplicados a sistemas que operam em lógica opaca, probabilística e de difícil interpretabilidade.

A correção, a eliminação, a anonimização, a portabilidade e a informação sobre compartilhamento completam o conjunto de direitos que estruturam a cidadania informacional. Todavia, o mais relevante para a análise da incompatibilidade entre o desenho normativo da LGPD e a lógica da inteligência artificial aplicada pelo Estado é o direito de revisão de decisões automatizadas.

À primeira vista, esse dispositivo representa verdadeiro avanço normativo, pois confere ao titular prerrogativa de contestar decisões tomadas exclusivamente por meios automatizados. Entretanto, como demonstram os estudos de caso analisados nos capítulos seguintes, a eficácia desse direito depende de condições epistêmicas que frequentemente não se verificam na prática. A revisão somente pode ser efetiva se acompanhada de explicabilidade mínima, isto é, se o titular puder compreender, ao menos em nível descritivo, como a decisão foi produzida e quais critérios orientaram a classificação ou o ranqueamento que lhe afetou. Quando algoritmos operam como caixas pretas epistêmicas, tal como afirmam Pasquale (2015), Wachter, Mittelstadt e Floridi (2017), a possibilidade de revisão se dissolve, e o próprio núcleo da autodeterminação informativa é esvaziado.

A partir dessa análise, compreender a estrutura normativa da LGPD e seus direitos do titular constitui etapa indispensável para analisar os estudos de caso do capítulo seguinte, nos quais as promessas normativas de acesso, correção, transparência e revisão se mostram incompatíveis com as práticas estatais de classificação automatizada, ranqueamento estatístico e vigilância algorítmica. O exame detido da LGPD revela não apenas sua importância constitucional, mas também os limites materiais de sua eficácia em contextos de opacidade algorítmica, preparando o terreno para demonstrar, empiricamente, como a inteligência artificial desafia a própria estrutura dogmática do direito fundamental à proteção de dados no Brasil.

3.2 Lacunas e limites estruturais da LGPD

Embora a Lei Geral de Proteção de Dados Pessoais constitua o marco normativo mais avançado já produzido no Brasil sobre tutela da esfera informacional, sua eficácia enfrenta limites estruturais que não derivam de defeitos redacionais, mas da natureza das tecnologias às quais deve se aplicar. A LGPD foi concebida para produzir transparência,

garantir autodeterminação informativa e limitar o poder informacional estatal e privado. No entanto, quando transposta para ambientes decisórios mediados por inferências automatizadas, modelos preditivos e sistemas opacos de inteligência artificial, sua capacidade de assegurar controle efetivo se reduz drasticamente. A hipótese central deste trabalho - a distância entre titularidade formal e capacidade real de exercício de direitos em contextos de opacidade algorítmica - manifesta-se de forma evidente quando se analisam as exceções legislativas, as limitações institucionais e a complexidade técnica que envolvem a aplicação da LGPD.

Um primeiro limite emerge do próprio desenho legislativo. O artigo 4º da LGPD exclui de seu âmbito as atividades de segurança pública, defesa nacional e investigação penal, remetendo seu tratamento a legislação específica ainda inexistente. Essa remissão cria um vácuo normativo que permite que estruturas estatais historicamente marcadas por opacidade continuem operando sem parâmetros proporcionais de necessidade, adequação e transparência. Danilo Doneda (2019) observa que "as zonas de exceção tendem a reproduzir lógicas informacionais pré-constitucionais, baseadas na coleta indiscriminada e na ausência de justificativa pública". Essa advertência é central porque demonstra que o problema não está apenas na inexistência da legislação setorial, mas na fragilidade estrutural do Estado em controlar práticas informacionais que operam com alto potencial lesivo, especialmente quando associadas a sistemas de inteligência artificial.

A inexistência de legislação específica para regular o tratamento de dados em segurança pública e persecução penal não produz apenas incerteza jurídica, mas efeitos concretos sobre direitos fundamentais, uma vez que permite a adoção de tecnologias altamente invasivas sem parâmetros mínimos de proporcionalidade, verificação ou auditoria. Essa lacuna normativa tem resultado, em diferentes estados brasileiros, na utilização de sistemas de reconhecimento facial e soluções algorítmicas de baixa acurácia, ocasionando prisões indevidas de pessoas absolutamente inocentes. Esse dado ilustra que a ausência de disciplina jurídica específica não é um problema meramente abstrato, mas uma fonte direta de violações ao devido processo, à presunção de inocência e à própria integridade da proteção de dados. Assim, a discussão sobre uma eventual LGPD penal surge menos como iniciativa de sofisticação normativa e mais como resposta à urgência concreta de impedir que decisões automatizadas continuem a produzir danos irreversíveis em contextos marcados por seletividade estrutural.

O segundo limite estrutural da LGPD decorre da assimetria epistêmica que caracteriza os sistemas de decisão automatizada utilizados pelo Estado. A lei pressupõe possibilidade de reconstrução do processo decisório por meio de princípios como transparência, responsabilização e prevenção, além do direito à revisão de decisões

automatizadas. Entretanto, tais instrumentos perdem efetividade quando o tratamento de dados envolve modelos matemáticos não interpretáveis, técnicas de aprendizado de máquina autoajustáveis e operações de inferência realizadas sobre bases massivas e heterogêneas. A LGPD opera com a premissa de que aquilo que produz efeitos jurídicos pode ser auditado, explicado e eventualmente corrigido. Em sistemas de inteligência artificial que funcionam como caixas pretas, essa premissa deixa de ser verdadeira. Esse descompasso entre as capacidades técnicas do sistema e as exigências normativas do direito produz exatamente o tipo de cenário no qual a titularidade formal dos direitos não se converte em possibilidade real de exercício, confirmando a hipótese deste TCC.

A precariedade institucional da Autoridade Nacional de Proteção de Dados reforça essa fragilidade. A ANPD foi concebida como órgão capaz de produzir governança regulatória contínua, harmonizar interpretações, fiscalizar práticas e impor sanções. No entanto, enfrenta limitações orçamentárias, restrições técnicas e, sobretudo, desequilíbrios de poder frente aos atores que deveria regular. A dependência estatal de plataformas tecnológicas privadas, frequentemente estrangeiras, intensifica esse cenário, pois coloca a autoridade reguladora diante de agentes com poder econômico, técnico e político muito superior. A literatura denomina esse fenômeno captura regulatória, entendida como a interferência de interesses privados na atuação de autoridades públicas encarregadas de fiscalizá-los. As mobilizações que resultaram no enfraquecimento político do PL 2630, com participação ativa das grandes plataformas digitais, ilustram esse ambiente de pressão permanente que limita a capacidade estatal de impor governança algorítmica robusta. O déficit institucional da ANPD compromete diretamente a eficácia da LGPD, pois os direitos previstos na lei dependem de enforcement consistente para se converterem em proteção material.

Esse quadro de lacuna normativa tem sido enfrentado pelo Supremo Tribunal Federal em decisões estruturantes que delimitam o núcleo constitucional da proteção de dados frente ao avanço tecnológico estatal. No julgamento conjunto das ADIs 6387, 6388 e 6389, que discutiam o compartilhamento massivo de dados de telecomunicações com o IBGE durante a pandemia, o Tribunal fixou balizas que incidem diretamente sobre o problema aqui tratado.

O STF afirmou que “nenhuma atividade estatal de tratamento de dados, ainda que voltada ao interesse público, pode afastar-se dos critérios constitucionais de necessidade, adequação e proporcionalidade”, reconhecendo expressamente a existência de um devido processo informacional que vincula toda a Administração, mesmo nos domínios excepcionados pelo art. 4º da LGPD. Em outro trecho, o ministro relator advertiu que “a ausência de legislação específica não gera espaços de anomia, pois a Constituição mesma estabelece limites materiais ao tratamento de dados”, reforçando que nem mesmo razões de

governança, emergência ou segurança pública autorizam práticas de coleta e integração de bases que escapem ao crivo constitucional.

Ao suspender a norma impugnada, o Tribunal afirmou que “o Estado não pode exigir dos cidadãos confiança irrestrita em estruturas informacionais que não oferecem garantias mínimas de transparência e controle”, reconhecendo que a legitimidade democrática do tratamento de dados depende de condições epistêmicas que permitam ao titular compreender os efeitos que esses dados produzem sobre sua esfera jurídica. Essa orientação jurisprudencial tem impacto direto sobre o debate da LGPD penal e sobre o uso de tecnologias opacas pela Administração Pública. Se nem o compartilhamento manual de bases de dados pode ocorrer sem satisfazer critérios constitucionais estritos, com muito mais razão o emprego de sistemas algorítmicos, capazes de produzir classificações automáticas e erros graves como prisões indevidas de inocentes, deve se submeter a mecanismos reforçados de justificação pública. A jurisprudência constitucional, portanto, não apenas revelam a insuficiência normativa do regime atual, mas demonstram que o problema não está na ausência de comandos normativos, mas na dificuldade de sua aplicação em ambientes marcados pela opacidade técnica e pela assimetria de poder entre cidadãos e máquinas decisórias.

O avanço de tecnologias como reconhecimento facial, sistemas de ranqueamento automatizado e modelos preditivos amplifica esses desafios. Tais sistemas operam em lógicas estatísticas que frequentemente reproduzem desigualdades estruturais, reforçam vieses históricos e impactam de forma desproporcional grupos vulnerabilizados. A LGPD dispõe do princípio da não discriminação, mas sua eficácia depende da capacidade de detectar padrões discriminatórios inseridos em modelos algorítmicos complexos. A ausência de auditorias sistemáticas, avaliações de impacto e documentação técnica torna esse controle praticamente inviável. Com isso, o titular perde sua posição de sujeito de direitos e se converte em objeto de classificações invisíveis que estruturam seu acesso a bens públicos, oportunidades e garantias processuais.

A lei oferece princípios densos, deveres rigorosos e direitos robustos, mas sua aplicação depende de condições de transparência, governança e fiscalização que, nos casos analisados, não se concretizam. Assim como o habeas data, a LGPD permanece formalmente adequada, porém enfrenta limite material decorrente da impossibilidade de traduzir a racionalidade algorítmica em termos acessíveis ao titular. A insuficiência não decorre de falha normativa, mas de transformação epistêmica: decisões que antes se baseavam em registros estáticos passam a ser estruturadas por inferências complexas, que escapam ao âmbito de controle previsto pela legislação.

Essa constatação prepara o terreno para os estudos de caso dos capítulos seguintes, que demonstram empiricamente como práticas de inteligência artificial utilizadas pelo Estado - seja na gestão do trabalho, na atividade jurisdicional ou na segurança pública - desafiam os parâmetros normativos da LGPD e revelam a distância entre a promessa constitucional de autodeterminação informativa e sua concretização material. A análise desses casos permitirá evidenciar que, diante de estruturas decisórias mediadas por opacidade algorítmica, o problema não é de ausência normativa, mas de incompatibilidade entre os instrumentos existentes e as condições epistêmicas da era digital.

4 ESTUDOS DE CASO SOBRE O USO DE IA PELO ESTADO E SEUS IMPACTOS SOBRE GARANTIAS FUNDAMENTAIS

4.1 IA na gestão pública: Caso SINE

O estudo de caso do Sistema Nacional de Emprego baseia-se no relatório Sistema Nacional de Emprego e a gestão automatizada do desemprego, publicado em 2021 por Fernanda Bruno, Paula Cardoso e Paulo Faltay, no âmbito do projeto Inteligencia Artificial e Inclusión en América Latina. O documento foi selecionado porque constitui uma investigação empírica completa sobre a introdução de sistemas algorítmicos em políticas públicas de emprego no Brasil, descrevendo em detalhe a reestruturação institucional do SINE, a parceria com a Microsoft e a adoção de modelos de perfilização capazes de reorganizar silenciosamente o acesso a oportunidades de trabalho. Trata-se de política pública cuja finalidade histórica sempre foi promover a inclusão de trabalhadores marginalizados, o que torna particularmente relevante analisar como a automação altera o exercício de direitos fundamentais e como se relaciona com os instrumentos jurídicos existentes para assegurar transparência, acesso e controle sobre informações pessoais.

O relatório reconstrói a transformação do SINE a partir de 2019, quando o governo federal implementou o chamado “Novo SINE”, abriu sua base de dados a empresas privadas e firmou um Acordo de Cooperação Técnica com a Microsoft para introduzir ferramentas de machine learning no Emprega Brasil e no SINE Aberto. A pesquisa demonstra que essas ferramentas executam duas funções centrais. A primeira é o pareamento automatizado entre perfis de trabalhadores e vagas; a segunda é a perfilização, que segmenta usuários segundo sua capacidade estatística de reinserção no mercado. Esse processo envolve a criação de scores de empregabilidade baseados em variáveis como idade, escolaridade, localização, vínculos anteriores e tempo de desemprego.

A classificação opera de maneira opaca, sem que os trabalhadores tenham conhecimento das variáveis utilizadas, dos pesos atribuídos ou das razões pelas quais recebem ou deixam de receber determinadas vagas. É justamente aqui que o estudo dialoga diretamente com a pergunta deste trabalho, pois mostra que a lógica decisória relevante não está contida nos dados brutos acessíveis ao titular, mas nas inferências produzidas pelo modelo. A ausência de transparência impede que o indivíduo compreenda ou controle a forma como suas informações são transformadas em decisões administrativas, revelando um obstáculo estrutural ao exercício de direitos que, em tese, deveriam garantir acesso e revisão.

A pesquisa inclui entrevistas com representantes da bancada dos trabalhadores no CODEFAT, que expressaram preocupação formal com a falta de clareza sobre o uso e a proteção dos dados. O relatório registra ipsi litteris o depoimento:

> "Nós somos muito favoráveis ao uso de tecnologias para melhorar o sistema, como o Portal Emprega Brasil, o aplicativo Sine Fácil, por exemplo. A preocupação da bancada dos trabalhadores foi em relação à possível privatização do sistema, à falta de clareza sobre a proteção de sigilo dos dados das pessoas e dos possíveis usos dessas informações, como também da falta de garantias sobre mecanismos de equidade e igualdade de oportunidades. Veja, não está evidente para mim o interesse dessas empresas em ter acesso a esse banco de dados. Falo isso porque o perfil que elas atendem é, em média, mais escolarizado e qualificado - pessoas que inclusive podem pagar pelo serviço - do que as pessoas que procuram o SINE. Especulo o porquê desse interesse e se esta medida terá alguma efetividade. Outra razão (do voto contrário) foi no sentido de que essa abertura de dados não tenha como consequência o estabelecimento de um sistema que limite o acesso a algumas pessoas, especialmente aquelas que mais precisam, e que atenda apenas a uma pequena parcela da sociedade. Estamos falando, por exemplo, do acesso das pessoas à banda larga. Será que a procura por vagas do trabalhador mais humilde vai ter o mesmo tratamento, as mesmas condições, que a busca de alguém que pode pagar neste sistema? Os votos contrários e as abstenções se devem a não termos clareza em relação à proteção do sistema público de emprego, ao uso dos dados e, especialmente, sobre a igualdade de condições".

A fala dos representantes sindicais é relevante porque confirma empiricamente o que a pergunta orientadora busca investigar: a utilização de modelos de decisão que não permitem ao cidadão compreender como são produzidos os resultados que impactam diretamente sua trajetória laboral. O estudo demonstra que o trabalhador não sabe que é perfilizado, não conhece o critério de sua segmentação e não dispõe de qualquer meio para contestar ou influenciar as inferências que determinam sua visibilidade diante das vagas oferecidas. A opacidade, portanto, não decorre de lacuna normativa, mas de arquitetura institucional incapaz de cumprir o que a legislação já prevê.

Outro ponto central do relatório é a constatação de que o SINE, criado justamente para incluir trabalhadores vulneráveis, passa a reforçar desigualdades estruturais por meio de suas ferramentas algorítmicas. Os modelos aprendem padrões do mercado de trabalho e tendem a reproduzir a exclusão histórica de mulheres, jovens, pessoas negras e trabalhadores de baixa escolaridade, que passam a ser classificados como menos empregáveis. Como consequência, recebem menos encaminhamentos, tornam-se menos visíveis no sistema e têm sua trajetória condicionada por parâmetros estatísticos que refletem desigualdades acumuladas. O relatório denomina esse processo de "regulação do campo de oportunidades", indicando que a automação deixa de ser apenas um mecanismo administrativo para se tornar uma tecnologia que reorganiza estruturalmente quem terá ou não acesso a direitos. Este achado é diretamente relacionado à hipótese analisada neste trabalho. Embora a LGPD proíba discriminação algorítmica, imponha deveres de explicação e assegure o direito de revisão, o estudo mostra que tais garantias permanecem sem efetividade prática. O titular não consegue exercer seu direito de revisão porque não compreende a decisão; não consegue contestar a

lógica discriminatória porque a lógica não é disponibilizada; e não consegue se autodeterminar informacionalmente porque desconhece como suas características produzem efeitos administrativos. Há aqui um descompasso claro entre norma e prática, mas não uma insuficiência normativa.

O relatório também evidencia que a parceria firmada entre o governo federal e a Microsoft ultrapassa a automação do pareamento de vagas, alcançando a própria concepção das políticas de qualificação profissional por meio da Escola do Trabalhador 4.0. A pesquisa mostra que a plataforma, anteriormente estruturada com cursos de múltiplas áreas e formações diversificadas, foi progressivamente remodelada para oferecer conteúdos fortemente alinhados às trilhas tecnológicas definidas pela Microsoft, com foco em computação em nuvem, desenvolvimento de software, administração de ambientes Azure e competências digitais diretamente relacionadas às demandas de mão de obra da empresa. Essa convergência não é acidental. A presidência da Microsoft Brasil declarou publicamente que o país enfrenta "um déficit de profissionais qualificados em tecnologia" e que a empresa necessita "formar rapidamente trabalhadores para suprir a demanda crescente do setor", o que reforça o alinhamento entre a política pública de capacitação e os interesses privados da corporação.

A justificativa institucional inicialmente apresentada pelo governo para a cooperação de que a parceria teria sido motivada pela urgência educacional imposta pela pandemia de Covid-19, não se sustenta diante da cronologia reconstruída pelo relatório, que demonstra negociações e desenho de cursos anteriores a 2020. A discrepância temporal revela que a reconfiguração da Escola do Trabalhador não é resposta emergencial, mas parte de um processo mais amplo de dependência tecnológica em que corporações transnacionais passam a definir conteúdos, metodologias e prioridades de qualificação profissional no interior de uma política pública estatal. Esse movimento desloca o centro decisório da formulação de políticas de emprego e insere o Estado brasileiro em um arranjo no qual parâmetros pedagógicos, competências valorizadas e trajetórias formativas são moldados por interesses empresariais globais, não por diagnósticos públicos de necessidades nacionais de qualificação.

Embora o relatório não utilize esse vocabulário, o fenômeno se aproxima do que a literatura recente descreve como neocolonialismo digital, caracterizado pela transferência de capacidades estratégicas, infraestruturas críticas e agendas de formação profissional para atores privados transnacionais. A relação entre Microsoft e Estado brasileiro, tal como documentada, sugere um modelo no qual a automação pública e a qualificação de trabalhadores passam a ser estruturadas por epistemologias e infraestruturas externas ao controle soberano, produzindo assimetrias epistêmicas que limitam o exercício concreto das

garantias constitucionais associadas à autodeterminação informativa e ao controle democrático das decisões estatais. A discussão detalhada sobre essa dimensão será aprofundada posteriormente neste trabalho, mas o estudo de caso já oferece indícios suficientes de que a reconfiguração do SINE envolve não apenas questões técnicas, mas arranjos de poder que condicionam a efetividade real dos instrumentos jurídicos existentes.

A partir da análise do relatório, percebe-se que cada achado relevante se conecta diretamente à pergunta orientadora desta pesquisa. A pergunta busca investigar se instrumentos como habeas data e LGPD são capazes de garantir transparência, acesso e controle sobre informações pessoais em contextos de IA. O estudo do SINE demonstra que o titular até pode acessar seus dados cadastrais, mas não alcança as inferências decisórias que condicionam seu acesso a direitos. Mostra também que a LGPD já contém princípios e direitos que, se aplicados em sua inteireza, seriam suficientes para impedir práticas discriminatórias, exigir explicabilidade, impor mecanismos de revisão e garantir auditoria do processo decisório. No entanto, a prática administrativa revela uma incapacidade institucional de aplicar tais normas a sistemas complexos. Em outras palavras, o estudo não aponta para ausência de legislação, mas para ausência de condições de efetividade. A insuficiência é operacional, hermenêutica e estrutural, não normativa.

Assim, sem antecipar a conclusão da hipótese, o estudo demonstra que o problema central não é a falta de dispositivos jurídicos, mas a dificuldade de interpretar e fazer cumprir as garantias já existentes diante de tecnologias que operam por inferências opacas. A situação revela a necessidade de uma abordagem compatível com o constitucionalismo digital, capaz de reinterpretar e tornar eficazes os direitos à autodeterminação informativa, à motivação administrativa, à revisão de decisões automatizadas e à não discriminação. O SINE exemplifica como tais garantias permanecem formais quando o Estado adota sistemas decisórios que não se deixam traduzir segundo as categorias tradicionais de publicidade, motivação e controle democrático. O estudo de caso, portanto, oferece o material empírico necessário para demonstrar que a legislação não é insuficiente; é sua aplicação que ainda não alcança os centros invisíveis de produção de poder informacional que estruturam as decisões automatizadas do Estado.

4.2 IA no judiciário: Caso MAIA

O segundo estudo de caso examina a implementação da ferramenta de inteligência artificial denominada MAIA Justiça pelo Tribunal de Justiça de Pernambuco, com base na investigação técnica e documental conduzida pelo Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec) e publicada no texto “Tal qual os Incas, Maias e Astecas? O Mecanismo Artificial Inteligente de Apoio à Justiça do TJPE”. A pesquisa, complementada

por pedidos formais de acesso à informação registrados na Nota Metodológica que integra o dossiê documental da investigação, foi escolhida porque oferece uma reconstrução empírica precisa da adoção de IA em atividade-fim jurisdicional, permitindo observar de forma concreta como um tribunal estadual estrutura, governa e utiliza um modelo de linguagem de grande porte no processo de formação de julgamentos.

Isso torna o caso altamente relevante para esta dissertação, pois fornece evidências diretas sobre a possibilidade de transparência, acesso e controle quando o Estado utiliza sistemas algorítmicos cujos processos internos permanecem opacos ao cidadão. Além disso, o Judiciário é o espaço institucional onde o dever de motivação, a publicidade das razões decisórias e a integridade cognitiva do julgador assumem maior densidade constitucional, o que torna o conflito entre IA e garantias fundamentais particularmente nítido.

A investigação do IP.rec mostra que a implementação do MAIA Justiça se insere em um movimento nacional de transformação digital do Judiciário e é apresentada pelo TJPE como mecanismo de apoio destinado a aumentar a eficiência, agilizar a análise processual, estruturar votos, resumir autos e sugerir precedentes relevantes. O tribunal afirma que o sistema não decide, mas apenas auxilia magistrados e assessores. Contudo, o relatório demonstra que a distinção formal entre apoio e decisão não afasta, por si só, o risco de influência cognitiva significativa. Esta constatação é central para a pergunta deste trabalho, pois indica que mesmo sistemas que não tomam decisões autônomas exercem efeitos decisórios substantivos, interferindo na racionalidade humana e modulando a construção dos julgamentos.

O estudo destaca que o MAIA Justiça opera a partir de bases de dados internas como PJe, Códex e Pangea, utilizando um modelo de linguagem treinado com decisões anteriores do tribunal, o que inclui padrões argumentativos, estruturas retóricas e estilos decisórios dos gabinetes. A documentação fornecida pelo TJPE confirma que o sistema é capaz de gerar minutas completas de votos, resumos estruturados e ementas no formato CNJ.

Embora o tribunal afirme que o usuário pode editar qualquer texto, o relatório ressalta que esta afirmativa não resolve o problema da motivação oculta. Se a primeira versão do voto é gerada pelo sistema, ainda que editada posteriormente, a cadeia de raciocínio que influenciou o julgador permanece invisível ao jurisdicionado. Isso se relaciona diretamente com a pergunta orientadora desta pesquisa, pois demonstra uma situação em que o cidadão não consegue acessar nem controlar a lógica que influenciou a atividade estatal, uma vez que o processo inferencial do modelo não é disponibilizado. A jurisprudência constitucional sobre o dever de motivação exige que o cidadão possa reconstruir as razões públicas da decisão,

algo inviável quando parte da racionalidade permanece alojada em um sistema algorítmico não transparente.

Durante a análise do funcionamento do MAIA Justiça, o relatório do IP.rec chama atenção para a distinção, reiterada pelo tribunal, entre decisão humana e sugestão algorítmica. Ainda que formalmente a decisão permaneça atribuída ao magistrado, o estudo mostra que o sistema é capaz de produzir minutas estruturadas, resumos e ementas completos, organizando previamente o arcabouço argumentativo que servirá de base ao julgamento. Embora essa constatação derive dos documentos obtidos por meio dos pedidos de informação, a literatura especializada evidencia que tal distinção é insuficiente para afastar riscos substanciais de influência cognitiva.

Pesquisas publicadas nos últimos anos (VICENTE e MATUTE, 2023), demonstram que operadores humanos tendem a absorver vieses e padrões sugeridos por sistemas de IA, mesmo quando advertidos sobre sua possível existência. O efeito de ancoragem cognitiva, bem documentado em ambientes de alta pressão e sobrecarga de trabalho, sugere que a primeira versão de argumento apresentada ao julgador tende a orientar, ainda que de forma implícita, o raciocínio subsequente. Esses achados teóricos, ainda que não integrem o corpus empírico analisado pelo IP.rec, dialogam diretamente com a realidade documentada no TJPE, reforçando a conclusão de que o apoio algorítmico produz uma camada invisível de racionalidade que influencia a motivação final da decisão judicial.

Essa relação entre evidências documentais e literatura científica é central para esta pesquisa, pois conecta diretamente o caso do MAIA Justiça à pergunta orientadora sobre transparência, acesso e controle. O estudo revela que, mesmo quando o titular teoricamente pode acessar os autos do processo e, portanto, exercer o habeas data em seu sentido tradicional, ele não tem condições de reconstruir a influência algorítmica que moldou a estrutura argumentativa do julgamento. O sistema opera uma transformação silenciosa na racionalidade judicial, e essa transformação não é capturada pelos instrumentos jurídicos tradicionais.

Da mesma forma, embora a LGPD assegure direitos de revisão, explicação e não discriminação, a prática observada no TJPE não oferece os meios materiais para seu exercício, pois o tribunal não disponibiliza documentação técnica sobre critérios de treinamento, detecção de vieses ou parâmetros utilizados pelo modelo. O fenômeno descrito pela literatura, segundo o qual humanos incorporam vieses algorítmicos sem perceber, agrava a dificuldade jurídica de identificar quando e de que modo a IA influenciou o julgamento, criando uma zona de opacidade incompatível com o devido processo legal, mas não prevista pela legislação existente, que pressupõe transparência mínima das etapas decisórias.

A Nota Metodológica registra que o IP.rec enviou dois pedidos de acesso à informação com base na LAI e na LGPD, solicitando documentos sobre governança, arquitetura técnica, critérios de treinamento, validação, vieses, auditorias, logs, mecanismos de supervisão humana e relatórios de impacto. As respostas do tribunal, embora formalmente detalhadas, não fornecem documentação técnica suficiente para verificar a conformidade do sistema com a legislação.

O TJPE declara que há rastreabilidade e supervisão humana, mas não apresenta testes de viés, métricas de performance, protocolos de auditoria, critérios de curadoria do dataset ou práticas que permitam avaliar se o modelo aprende e reproduz padrões discriminatórios presentes nos próprios bancos processuais. Essa insuficiência documental tem relação direta com a pergunta desta dissertação. A norma garante transparência e acesso, mas o órgão estatal não cria condições materiais para que esses direitos sejam exercidos. Assim, mesmo que o titular ingresse com habeas data, continuará tendo acesso apenas aos dados processuais, mas não às inferências, pesos, correlações ou camadas internas do modelo que estruturam a sugestão decisória. O estudo mostra, portanto, uma lacuna prática da garantia constitucional, e não uma limitação de seu conteúdo.

O relatório do IP.rec também aponta que não há documentação que permita compreender como o MAIA foi treinado, como os dados foram pré-processados, quais padrões decisórios foram priorizados, nem de que forma o tribunal pretende evitar que vieses de gabinetes específicos sejam amplificados de forma sistêmica. Essas lacunas se conectam diretamente com o princípio da qualidade dos dados (art. 6º, V da LGPD) e com o dever de prevenção, que exige avaliação contínua de riscos. O ponto, mais uma vez, não é que a LGPD deixa de prever esses princípios, mas que o tribunal não demonstra mecanismos capazes de cumpri-los. A desconexão entre regra existente e implementação revela, de maneira nítida, que a hipótese inicial desta dissertação - a de que novas normas seriam necessárias - precisa ser examinada com cautela, já que o estudo sugere que o problema está mais na prática institucional do que na estrutura normativa.

Outro elemento relevante é a dupla camada decisória identificada pela investigação. As minutas produzidas pelo sistema, ainda que formalmente atribuídas ao magistrado, contêm estruturas argumentativas geradas por uma racionalidade técnica que o jurisdicionado não consegue acessar. A decisão final visível não revela a influência algorítmica que atuou na sua construção. Esse fenômeno, descrito como motivação parcialmente oculta, coloca o habeas data diante de uma fronteira hermenêutica. A garantia constitucional permite acesso a informações registradas, mas não alcança processos matemáticos de inferência. O estudo demonstra que essa limitação não deriva do texto constitucional, mas do modo como a atividade jurisdicional se reorganiza em torno de

modelos opacos. Aqui, novamente, o caso fornece material empírico extremamente valioso para a hipótese, pois mostra que a dificuldade não está na ausência de direitos, e sim na ausência de condições epistêmicas e institucionais para exercê-los em ambientes algorítmicos.

Por fim, o relatório evidencia que, embora o tribunal declare aderência à LGPD, à LAI e às resoluções do CNJ, não há mecanismos que permitam ao jurisdicionado exercer o direito previsto no artigo 20 da LGPD. A ausência de explicabilidade inviabiliza qualquer contestação substantiva. A alegação de que o juiz mantém o controle cognitivo da decisão não elimina o dever de demonstrar como a IA influenciou a construção argumentativa. Assim, o estudo fornece indícios de que a legislação vigente seria suficiente para exigir maior transparência, revisão humana efetiva, auditoria e governança robusta. O problema reside na falta de cumprimento, não na falta de norma.

Sem resolver a hipótese, mas preparando o terreno para sua análise, o estudo de caso do MAIA Justiça demonstra que o ordenamento jurídico brasileiro já contém instrumentos capazes de garantir transparência, acesso e controle sobre informações pessoais em ambientes algorítmicos. Contudo, tais instrumentos não são implementados pelo tribunal de modo a permitir seu exercício real. A tensão revelada pelo caso não aponta para lacuna legislativa, mas para insuficiência de práticas institucionais alinhadas às exigências do constitucionalismo digital, que será discutido adiante neste trabalho.

4.3 IA na segurança pública: Reconhecimento facial

O terceiro estudo de caso examina a adoção de sistemas de reconhecimento facial na segurança pública brasileira a partir dos relatórios Vigilância por Lentes Opacas, produzido pelo projeto O Panóptico/CESeC, e Mapeando a Vigilância Biométrica, elaborado pelo CESeC e pela Defensoria Pública da União. Esses estudos foram escolhidos porque formam o levantamento empírico mais completo sobre vigilância biométrica no país e porque evidenciam, de modo paradigmatico, a dificuldade de exercer direitos de transparência, acesso e contestação quando decisões estatais passam a ser mediadas por inferências algorítmicas opacas.

O caso é particularmente relevante para esta pesquisa porque opera justamente no espaço normativo de exceção descrito no capítulo anterior, em que a LGPD não se aplica integralmente às atividades de segurança pública, e porque revela, com clareza histórica, como práticas de sigilo decisório reproduzem dinâmicas que o habeas data foi originalmente criado para romper.

Os relatórios demonstram que, a partir da Portaria 793/2019, o reconhecimento facial foi implementado de forma acelerada em todo o país, resultando em 337 projetos ativos e na

vigilância biométrica contínua de cerca de 81 milhões de pessoas. Essa escala, inédita na história das tecnologias de controle no Brasil, opera em ambiente de baixa transparência institucional. Estados contratam empresas estrangeiras, como NEC, Huawei, Cognyte e Quantica, sem divulgar contratos completos, bases de dados utilizadas, métricas de precisão ou critérios de funcionamento dos algoritmos. Esse cenário se conecta diretamente à pergunta orientadora deste trabalho, pois revela que o titular não possui meios para compreender ou contestar as inferências que produzem intervenções policiais potencialmente coercitivas. A LGPD contém direitos de acesso, transparência e revisão, e o habeas data foi concebido como garantia contra sigilo informacional abusivo. No entanto, na prática analisada, nenhum desses instrumentos consegue alcançar o processo inferencial que fundamenta a suspeição algorítmica.

A fragilidade das bases de dados utilizadas pelos sistemas reforça essa constatação. Os relatórios documentam que estados integram fotografias de Detrans, Secretarias de Segurança, institutos de identificação e bancos criminais sem padronização metodológica, atualização adequada ou mecanismos de exclusão de registros indevidos. Fotografias antigas, de má qualidade e registros duplicados alimentam sistemas de identificação em tempo real, produzindo erros previsíveis.

Esses achados empíricos se conectam diretamente à hipótese deste trabalho, pois demonstram a distância entre a titularidade formal dos princípios previstos na LGPD (qualidade, necessidade, adequação e prevenção) e a capacidade real de seu exercício quando o Estado não cria condições institucionais para cumpri-los. A norma existe; o problema está na ausência de sua execução efetiva em contextos de opacidade estrutural.

Os relatórios também identificam um padrão racializado de erros. Em 2019, 90 por cento das pessoas presas por reconhecimento facial eram negras, indicando que a tecnologia reforça desigualdades historicamente produzidas pelo sistema penal brasileiro. Estudos do NIST citados nos relatórios demonstram que sistemas comerciais apresentam taxas de erro significativamente maiores para pessoas racializadas. A ligação com a pergunta do TCC é direta: a LGPD prevê o princípio da não discriminação, mas, na prática, não há mecanismos de auditoria técnica, testes de viés ou prestação de contas capazes de materializá-lo. A limitação, portanto, não está na legislação, mas na incapacidade institucional de exigir e comprovar sua observância.

Os dois estudos documentam casos de prisões indevidas motivadas por reconhecimentos falhos. Esses episódios mostram como classificações estatísticas são convertidas em decisões coercitivas sem motivação adequada ou possibilidade de contestação eficaz. Aqui, o elo com a hipótese é imediato: o habeas data permite acesso a informações

registradas, mas não à lógica inferencial que levou à identificação algorítmica; a LGPD prevê revisão de decisões automatizadas, mas não há meios materiais de exercê-la quando o próprio processo decisório é inacessível. Assim como discutido no capítulo anterior, o reconhecimento facial evidencia a distância entre a existência formal de direitos e a ausência de instrumentos capazes de garantir sua operação substantiva.

Esse quadro contemporâneo de opacidade encontra eco direto na história de criação do habeas data no Brasil. O instituto surgiu como resposta às práticas de vigilância política, falsificação de registros, restrição de acesso a informações e manipulação de dados pelo regime militar instaurado em 1964. Durante esse período, o Serviço Nacional de Informações (SNI) produziu e manteve bancos de dados secretos, muitas vezes falsos, inacessíveis aos próprios interessados, seus defensores e até ao Judiciário. O habeas data foi concebido justamente para romper essa lógica autoritária de produção e circulação de informações, criando instrumento constitucional para obrigar o Estado a revelar, corrigir e justificar o uso de dados sobre o indivíduo. O paralelismo histórico é inevitável. A opacidade dos sistemas contemporâneos de reconhecimento facial reproduz, em ambiente digitalizado, a mesma lógica de assimetria informacional radical que o habeas data buscou desmantelar. Se antes o sigilo era produzido por arquivos físicos e classificações políticas, hoje ele é produzido por redes neurais e classificações algorítmicas. Em ambos os casos, o cidadão permanece incapaz de conhecer e contestar a informação que fundamenta o exercício do poder estatal sobre ele.

Esse vínculo histórico torna ainda mais relevante o entendimento recente do Supremo Tribunal Federal, citado no capítulo anterior, segundo o qual nenhuma atividade estatal de tratamento de dados, mesmo aquelas abrangidas pelo artigo 4º da LGPD, está isenta de observância aos critérios constitucionais de necessidade, adequação e proporcionalidade. O STF enfatiza que a ausência de legislação específica não cria “espaços de anomia”, pois a própria Constituição estabelece limites materiais ao tratamento de dados. Esse entendimento ilumina o estudo de caso: ainda que a segurança pública opere em zona de exceção normativa, não está autorizada a atuar em opacidade absoluta. Os relatórios mostram, contudo, que essa diretriz constitucional permanece sem concretização.

Os dois estudos convergem, por fim, na conclusão de que o reconhecimento facial no Brasil opera em regime de opacidade incompatível com o Estado Democrático de Direito. O titular não acessa a inferência que o classifica como suspeito; não controla o tratamento de seus dados; não compreende como as imagens capturadas são armazenadas, compartilhadas ou descartadas; e não dispõe de vias efetivas de contestação. As garantias previstas na LGPD e no habeas data existem, mas não encontram condições técnicas e institucionais para serem exercidas. O caso responde, portanto, o elemento central da hipótese deste trabalho: o ordenamento jurídico brasileiro não sofre de insuficiência normativa, mas de insuficiência de

cumprimento. A legislação é adequada; o problema está na incapacidade estrutural do Estado de garantir sua efetividade diante de tecnologias de inferência opaca.

4.4 Síntese: como os três estudos de caso demonstram a insuficiência prática do habeas data e da LGPD diante da opacidade algorítmica

Os três estudos de caso convergem para um diagnóstico uniforme: habeas data e LGPD contêm mecanismos normativos capazes de proteger transparência, acesso e controle, mas esses instrumentos perdem eficácia ao serem confrontados com arquiteturas tecnológicas opacas, práticas contratuais de dependência privada e ausência de governança estatal robusta.

No caso do SINE, o relatório evidencia que a decisão relevante não reside apenas nos registros cadastrais acessíveis ao titular, mas nas inferências e scores produzidos por modelos de perfilização treinados sobre grandes bases de dados; essas inferências não são disponibilizadas ao cidadão, não são auditadas e não admitem revisão prática, ainda que o ordenamento preveja direitos de explicação e revisão. Essa limitação exata do alcance do habeas data e de direitos previstos na LGPD fica clara na documentação analisada, que registra a abertura de bases a atores privados e a ausência de relatórios de explicabilidade ou de auditorias independentes, evidenciando um descompasso entre norma e prática.

No caso do MAIA Justiça (TJPE), a investigação documental mostra que o sistema fornece minutas e estruturas argumentativas que orientam o trabalho do magistrado, criando uma camada invisível de racionalidade que o jurisdicionado não consegue acessar. Mesmo quando o processo formalmente permanece sob assinatura humana, a influência cognitiva das sugestões algorítmicas produz efeitos decisórios reais; o habeas data alcança os autos, mas não as relações inferenciais, e a LGPD prevê revisão e não discriminação sem, contudo, detalhar mecanismos processuais que forcem a disponibilização das arquiteturas algorítmicas para fins de controle. A insuficiência prática decorre, portanto, da impossibilidade material de efetivar direitos constitucionais e legais diante de processos inferenciais não documentados, não auditáveis e contratualmente protegidos.

No campo da segurança pública, os relatórios sobre reconhecimento facial mostram em escala ampliada as mesmas fragilidades: integração de bases heterogêneas e frequentemente desatualizadas, contratos pouco transparentes com fornecedores estrangeiros, ausência de avaliações de impacto e falta de protocolos de governança para ciclo de vida das imagens. Esses fatores transformam inferências probabilísticas em decisões coercitivas com alto risco de erro e de reproduzir vieses raciais e sociais; dados empíricos documentam taxas de erro e padrões discriminatórios que recaem sobre grupos racializados. A LGPD e o habeas data garantem, em termos materiais, princípios de qualidade, transparência e não

discriminação, e asseguram vias de acesso e correção de dados; contudo, na prática examinada pelos relatórios, esses mecanismos não são implementados nas rotinas das forças de segurança, o que empurra a proteção legal para um patamar formal sem conteúdo efetivo.

Feitas as observações caso a caso, é possível identificar, trecho por trecho, as correlações entre os achados empíricos e a hipótese central do trabalho. Primeiro trecho, relativo ao acesso: todos os casos demonstram que o titular pode eventualmente acessar dados registrais, mas não as inferências; isso mostra que o campo de incidência do habeas data é insuficiente para desvelar processos inferenciais, não por defeito do instituto, mas por limitação de escopo técnico-constitucional quando confrontado com modelos de aprendizado que não deixam "rastro" explicável ao público. Segundo trecho, relativo à explicabilidade e revisão: a LGPD prevê artifícios (transparência, relatórios de impacto, direito de revisão) que, na teoria, cobrem os riscos identificados; na prática, tribunais, administrações e fornecedores não apresentam documentação, métricas nem protocolos técnicos necessários para que esses direitos sejam exercidos. Terceiro trecho, relativo à não discriminação: os achados sobre perfilização, reprodução de vieses históricos e prisões indevidas indicam que o princípio jurídico existe, mas que sua materialização exige auditoria técnica e processos de remediação que não estão sendo implementados. Em todos esses trechos, portanto, o cerne não é lacuna normativa; é ausência de medidas institucionais, técnicas e contratuais que transformem direitos formais em direitos efetivos.

A síntese prática que emerge dos três casos permite identificar categorias de falha recorrentes que explicam a insuficiência operacional da norma: a) opacidade técnica e contratual que protege modelos e parâmetros; b) governança de dados deficiente, com bases de má qualidade e ausência de protocolos de atualização e exclusão; c) falta de auditorias independentes e de relatórios públicos de impacto; d) dependência tecnológica e transferência de poder decisório para fornecedores privados; e) insuficiência de capacitação e de rotinas estatais para fiscalizar modelos complexos. Cada uma dessas falhas corresponde a requisitos previstos na LGPD e ao alcance proposto pelo habeas data, de modo que a ausência de cumprimento é condição explicativa suficiente do déficit de proteção constatado.

Finalmente, sem antecipar a decisão sobre a hipótese geral, os três estudos, quando lidos em conjunto, demonstram de forma consistente que o ordenamento jurídico brasileiro já contém princípios e instrumentos aptos a exigir transparência, qualidade de dados, auditoria e revisão; o problema empiricamente detectado reside na implementação. A conclusão intermediária que essas evidências sustentam é normativa e prática: para que habeas data e LGPD produzam a proteção prometida é preciso que o Estado implemente procedimentos exequíveis de governança algorítmica, imponha cláusulas contratuais que garantam auditabilidade, estabeleça rotinas de testes de vieses e qualidade de dados, e crie

mecanismos institucionais capazes de traduzir obrigações legais em controles técnicos verificáveis. Em outras palavras, a legislação não é o primeiro obstáculo; o desafio é montar as condições materiais e institucionais para seu cumprimento.

5 CONSTITUCIONALISMO DIGITAL E A INTELIGÊNCIA ARTIFICIAL NO ESTADO BRASILEIRO

5.1 Dependência tecnológica e neocolonialismo digital

A incorporação de sistemas de inteligência artificial pelo Estado brasileiro não pode ser compreendida apenas como fenômeno administrativo ou técnico. Ela se insere em um contexto mais amplo de assimetrias globais de poder, em que infraestruturas digitais, plataformas computacionais e sistemas algorítmicos operam como mecanismos contemporâneos de reorganização da dependência. Autores do Sul Global identificam esse processo como forma de neocolonialismo digital, cujo funcionamento não se dá mais pela ocupação territorial, mas pela circulação desigual de tecnologia, pela captura de dados e pela imposição de racionalidades informacionais externas aos países periféricos.

Milton Santos, ao analisar a globalização informatizada, descreve como o meio técnico-científico-informacional opera segundo lógica que privilegia fluxos globais e subordina Estados periféricos a sistemas concebidos fora de seu horizonte cultural, político e econômico. A importação de soluções algorítmicas sem domínio sobre sua arquitetura, documentação técnica e critérios decisórios aprofunda a heteronomia tecnológica, uma vez que o Estado passa a estruturar políticas públicas sobre bases epistemológicas alheias ao seu contexto. A dependência não é apenas material; é cognitiva e metodológica. Para Santos, essa submissão aos sistemas globais de informação cria formas de hegemonia silenciosa, nas quais técnicas externas moldam comportamentos e decisões internas.

Essa leitura dialoga com Achille Mbembe, cuja análise sobre regimes contemporâneos de vigilância e classificação mostra que tecnologias de captura e predição amplificam assimetrias históricas, sobretudo em sociedades racialmente estratificadas. Para Mbembe, técnicas de visibilização e controle transformam-se em tecnologias de administração da vida e da morte, cujo uso, em países marcados por desigualdades estruturais, tende a reproduzir padrões coloniais. No caso brasileiro, esse fenômeno aparece de forma direta no uso de reconhecimento facial, sistemas de vigilância biométrica e algoritmos de predição que reforçam o sobrepoliciamento de corpos negros e pobres, replicando no campo digital as hierarquias do campo social.

Autores latino-americanos, como Aníbal Quijano (2005), ajudam a compreender por que a dependência tecnológica produz não apenas subordinação operacional, mas colonialidade epistêmica. Quijano demonstra que a ordem mundial é estruturada por hierarquias de produção de conhecimento. Quando o Estado importa modelos de IA treinados em bases euro-americanas, ele importa também categorias analíticas, gramáticas decisórias e

formas de classificação que invisibilizam complexidades locais. A colonialidade do poder, na era algorítmica, manifesta-se na incapacidade de produzir tecnologias próprias e na adoção acrítica de técnicas decisórias estruturadas por racionalidades externas.

Nessa direção, Evgeny Morozov (2021) contribui ao denunciar o que chama de solucionismo tecnológico, ou tecnossolucionismo, que transforma decisões políticas em problemas computacionais administráveis por empresas privadas. O solucionismo reforça dependência estatal, pois desloca a capacidade decisória das instituições públicas para plataformas cuja lógica econômica, jurídica e cognitiva é ditada por interesses corporativos transnacionais. Embora não seja autor do Sul Global, sua contribuição é fundamental para explicar por que Estados periféricos tornam-se usuários passivos de sistemas opacos que moldam políticas públicas sem qualquer participação democrática em seu desenho.

As críticas formuladas por Abeba Birhane (2022) e Nanjala Nyabola (2018), autoras africanas centrais no debate sobre colonialismo digital, aprofundam essa leitura. Birhane demonstra que algoritmos treinados fora do contexto local reproduzem padrões de dominação e racismo estrutural, fenômeno que ela denomina colonialismo computacional. Nyabola evidencia como tecnologias digitais exportadas para países do Sul operam como infraestrutura de controle, vigilância e exclusão, reforçando assimetrias globais na governança informacional. Seus diagnósticos coincidem com os resultados empíricos dos estudos de caso deste trabalho.

A dependência tecnológica produz, portanto, quatro efeitos estruturais que ajudam a compreender os limites dos instrumentos jurídicos analisados neste TCC. O primeiro é a perda de soberania informacional, pois o Estado brasileiro utiliza sistemas cujas bases, modelos e critérios decisórios não controla. O segundo é a transferência de poder normativo, uma vez que racionalidades técnicas externas passam a moldar políticas públicas internas. O terceiro é a vulnerabilização institucional, pois a administração pública não possui capacidade técnica para auditar, validar ou contestar decisões algorítmicas que condicionam direitos fundamentais. O quarto é a intensificação de desigualdades raciais, sociais e territoriais, fenômeno documentado amplamente na literatura crítica do Sul Global.

Esses elementos estruturais se revelam de modo particularmente evidente quando articulados aos três estudos de caso analisados nos capítulos anteriores. No Sistema Nacional de Emprego, a dependência de soluções desenvolvidas por empresas privadas estrangeiras, como Microsoft e BizApp, resulta na adoção de algoritmos cuja arquitetura, critérios de treinamento e bases de dados subjacentes escapam ao domínio cognitivo da administração pública. Os modelos passam a ranquear trabalhadores brasileiros segundo lógicas estatísticas

opacas, definindo perfis e oportunidades com base em inferências que nem o Estado, nem os titulares conseguem reconstruir.

O SINE converte o trabalhador em mero destinatário de decisões cuja racionalidade técnica é importada e inacessível, o que impede o exercício substancial dos direitos de acesso, explicação e revisão previstos na LGPD e no habeas data. O aspecto adicional da Escola do Trabalhador 4.0 reforça essa dinâmica, pois a qualificação profissional ofertada pelo poder público foi reorganizada segundo trilhas formativas concebidas pela Microsoft. Esse arranjo sintetiza a dupla dimensão da dependência tecnológica: o Estado não controla os modelos que classificam trabalhadores nem os currículos que os preparam para se adequar a essas classificações. A relação expressa exatamente o movimento descrito por autores do Sul Global, no qual infraestruturas privadas passam a estruturar políticas públicas e produzir racionalidades administrativas que o Estado apenas internaliza. A heteronomia tecnológica descrita por Santos manifesta-se, aqui, de forma dupla: o indivíduo não compreende as inferências que o classificam e o próprio Estado não dispõe de capacidade para explicá-las ou contestá-las.

No Poder Judiciário de Pernambuco, o uso do MAIA Justiça revela forma ainda mais sofisticada de dependência informacional. O tribunal adota modelo de linguagem treinado sobre bases e arquiteturas técnicas cuja compreensão é parcial e cuja auditabilidade é inexistente. A atividade jurisdicional, que exige motivação racional e transparente, passa a incorporar racionalidade algorítmica cuja origem, lógica interna e vieses não são conhecidos nem mesmo pelos próprios magistrados. Essa situação representa concretamente o que Morozov (2013) identifica como deslocamento da racionalidade pública para sistemas fechados, fenômeno que se agrava quando os próprios operadores do Direito depositam confiança na suposta neutralidade da máquina. O jurisdicionado torna-se objeto de decisões moldadas por ferramentas opacas cuja lógica não integra o espaço democrático de justificação.

No reconhecimento facial aplicado à segurança pública, o fenômeno assume forma explícita de colonialidade computacional, nos termos de Birhane (2021). Empresas estrangeiras fornecem sistemas treinados em bases de dados marcadas por padrões raciais e contextuais alheios ao Brasil. O resultado, como demonstrado pelo CESeC/Panóptico, é a produção de erros seletivos que recaem majoritariamente sobre pessoas negras e pobres, reforçando estigmas coloniais que há séculos estruturam o sistema penal brasileiro. A dependência tecnológica amplifica desigualdades existentes e legitima práticas de vigilância que operam com mínima transparência. Esse caso demonstra de forma paradigmática o que Nyabola (2018) descreve como internalização de tecnologias de controle que consolidam hierarquias raciais importadas.

Ao se observar esses três casos em conjunto, torna-se evidente que a dependência tecnológica funciona como contexto estrutural que explica por que o habeas data e a LGPD tornam-se insuficientes na prática. Não se trata apenas de opacidade algorítmica em sentido técnico, mas de opacidade derivada de relações de poder globais que colocam o Estado brasileiro na posição de operador subordinado de tecnologias que não domina. O habeas data não consegue romper caixas pretas que não pertencem ao Estado. A LGPD não consegue exercer plenamente seus instrumentos de fiscalização sobre empresas e tecnologias que operam segundo parâmetros transnacionais. A insuficiência prática desses instrumentos não decorre do texto normativo, mas da impossibilidade material de controlar sistemas cuja lógica interna está fora do alcance jurídico e técnico nacional.

Dessa forma, a análise crítica da dependência tecnológica revela que a pergunta orientadora deste trabalho não pode ser respondida apenas a partir do exame dos instrumentos normativos, mas deve considerar que a opacidade algorítmica que limita o habeas data e a LGPD está enraizada em condições estruturais de colonialidade digital. Os estudos de caso demonstram que, enquanto o Estado brasileiro depender de tecnologias opacas importadas, não haverá garantia substancial de autodeterminação informativa, transparência administrativa ou controle democrático das decisões automatizadas. É nesse sentido que o neocolonialismo digital não é apenas pano de fundo, mas elemento central para compreender a insuficiência prática das garantias constitucionais analisadas ao longo deste trabalho.

5.2 Opacidade algorítmica como problema estrutural de constitucionalidade

A opacidade algorítmica constitui um dos principais desafios contemporâneos à realização das promessas normativas do Estado Democrático de Direito. Trata-se de fenômeno que não decorre apenas da complexidade intrínseca de modelos de aprendizado de máquina, mas de um conjunto articulado de barreiras técnicas, jurídicas e institucionais que, muitas vezes, são produzidas ou reforçadas por decisões estatais e contratuais. A literatura especializada demonstra que a opacidade dos sistemas de IA não é um fenômeno neutro, tampouco inevitável.

Como argumenta Pasquale (2015), grande parte da caixa-preta algorítmica é resultado de “decisões deliberadas de design, governança e proteção jurídica que limitam a auditabilidade pública”. Wachter, Mittelstadt e Floridi (2017) igualmente enfatizam que segredos industriais, acordos de confidencialidade e restrições contratuais constituem elementos fundamentais do regime de opacidade, indicando que sua persistência deriva menos de obstáculos tecnológicos e mais de escolhas institucionais. Assim, diante da incorporação de IA pelo Estado, a pergunta constitucional relevante não é apenas como

explicar sistemas complexos, mas por que o poder público adota tecnologias cujo funcionamento não pode ser examinado, auditado ou controlado.

Esse ponto ganha densidade adicional quando articulado à discussão anterior sobre dependência tecnológica e neocolonialismo digital. Autores como Quijano (2005), Birhane (2022) e Nyabola (2018) mostram que, no Sul Global, a opacidade algorítmica é frequentemente indissociável de formas de colonialidade epistêmica, nas quais racionalidades decisórias externas se tornam estruturantes de políticas públicas nacionais. A importação de tecnologias opacas não apenas desloca o locus decisório, mas produz ambientes informacionais em que o próprio Estado perde capacidade de compreender, justificar e supervisionar as decisões que toma. Não se trata de acusar intencionalidade arbitrária, mas de reconhecer que a combinação de dependência tecnológica, contratos assimétricos e falta de infraestrutura própria cria condições em que a caixa-preta deixa de ser contingência técnica e passa a constituir efeito institucional e político.

A análise da opacidade algorítmica pode ser sistematizada em quatro dimensões. A primeira é a opacidade técnica. Modelos contemporâneos, especialmente redes neurais profundas, operam com milhões de parâmetros e aprendizado não supervisionado que dificultam a interpretação humana. Wachter, Mittelstadt e Floridi (2017) descrevem essa característica como "caixa-preta epistêmica". Ainda assim, como destaca Barocas e Selbst (2016), a impossibilidade absoluta de explicação não é premissa necessária da IA. O problema emerge quando sistemas complexos são adotados sem contrapartidas de documentação, auditoria interna ou metodologias de interpretabilidade que, embora imperfeitas, poderiam atenuar esse déficit.

A segunda dimensão é a opacidade jurídica. Pasquale (2015) e Hildebrandt (2018) demonstram que a proteção conferida pela propriedade intelectual, somada a cláusulas contratuais que limitam acesso ao modelo, às bases de treinamento e aos parâmetros decisórios, impede o controle democrático e dificulta o cumprimento dos deveres constitucionais de motivação e publicidade. Essa dinâmica é particularmente relevante no contexto brasileiro, em que o Estado, ao contratar soluções proprietárias, frequentemente aceita condições que inviabilizam governança robusta.

A terceira dimensão é a opacidade institucional. Ela decorre de déficits de capacidade técnica, de dependência tecnológica e da ausência de estruturas públicas de auditoria. Como indica Morozov (2013), a transferência de funções decisórias para sistemas opacos tende a reduzir a autonomia estatal e a criar condições em que a administração pública se torna usuária, e não governante, da racionalidade que aplica. Nesses contextos, a própria

autoridade estatal perde as referências necessárias para motivar suas decisões de maneira constitucionalmente adequada.

Por fim, a opacidade epistêmica constitui o efeito final das anteriores. Trata-se da impossibilidade, por parte do titular, de compreender como suas informações foram transformadas em inferências que produzem efeitos jurídicos. Hildebrandt (2018) formula esse fenômeno em termos de ruptura do devido processo informacional: quando as razões decisórias não podem ser reconstruídas, os direitos de contestação, revisão e autodeterminação tornam-se virtualmente não exercitáveis. A opacidade epistêmica não é apenas falta de informação; é ausência estrutural de inteligibilidade.

Essa limitação estrutural da inteligibilidade dos sistemas automatizados tem sido confirmada pela literatura técnica contemporânea. Estudos sobre o ciclo de vida da aprendizagem de máquina demonstram que modelos de IA dependem de intervenção humana em diferentes etapas de seu desenvolvimento, incluindo a seleção e anotação dos dados, a definição das tarefas de treinamento e a avaliação de resultados (WU et al, 2021). Tais pesquisas mostram que arquiteturas de human in the loop tendem a produzir sistemas mais auditáveis, explicáveis e robustos do que modelos totalmente automatizados, justamente porque mitigam parte da opacidade técnica e intrínseca desses sistemas.

Essas dimensões produzem impactos constitucionais diretos. O primeiro é a erosão da motivação pública. A exigência constitucional de motivação não se limita à apresentação formal de razões, mas pressupõe que tais razões sejam verificáveis e contestáveis. Quando decisões incorporam inferências opacas, parte da racionalidade permanece inacessível. O caso do MAIA Justiça exemplifica esse fenômeno: mesmo que o voto final seja redigido e assinado por um magistrado, parcela relevante da estrutura argumentativa pode ter sido moldada por processos inferenciais que não são revelados ao jurisdicionado, criando aquilo que o relatório do IP.rec denomina “motivações parcialmente ocultas”.

O segundo impacto é a fragilização do contraditório substancial. Conforme jurisprudência do Supremo Tribunal Federal, o contraditório implica a possibilidade real de influenciar o resultado. Essa possibilidade desaparece quando o indivíduo não conhece os critérios que moldaram sua classificação. O caso do SINE ilustra esse problema: o trabalhador não acessa o sistema de perfilização que condiciona sua exposição a vagas, não conhece as variáveis utilizadas e não dispõe de meios para contestar a inferência.

O terceiro impacto consiste na quebra da cadeia de responsabilização. A accountability pública exige atribuição clara de responsabilidade. Em sistemas opacos, essa atribuição se dilui entre fornecedores privados, modelos inacessíveis e decisões automatizadas

que o Estado não domina. O caso do reconhecimento facial expõe esse cenário com nitidez. Erros de identificação resultam de processos algorítmicos cujas bases, limiares e métricas não são divulgados. O indivíduo afetado não sabe contra o que dirigir sua contestação e o Estado não possui elementos para reconstruir o processo técnico que fundamentou sua ação.

Esses efeitos convergem para a conclusão de que a opacidade algorítmica constitui problema estrutural de constitucionalidade. A Constituição de 1988 exige inteligibilidade das razões públicas, controle democrático e garantias procedimentais que permitam aos cidadãos compreender e influenciar o exercício do poder. Sistemas algorítmicos opacos desafiam esses fundamentos ao introduzir racionalidades decisórias que escapam ao espaço de justificação pública. Como argumenta Hildebrandt (2011), a transparência das razões do Estado não é requisito ornamental, mas condição de possibilidade do devido processo informacional.

Os estudos de caso analisados anteriormente mostram que esse não é um problema abstrato. No SINE, a lógica opaca de ranqueamento reorganiza oportunidades de trabalho sem justificativa pública. No TJPE, sistemas de apoio à decisão judicial introduzem inferências ocultas na motivação jurisdicional. No reconhecimento facial, decisões policiais coercitivas são mediadas por algoritmos que operam sem documentação técnica, sem auditoria e com padrões de erro que afetam desproporcionalmente grupos racializados. Esses casos mostram que a opacidade não apenas dificulta o exercício de direitos, mas redimensiona o próprio campo de atuação das garantias constitucionais.

A articulação com o subcapítulo anterior permite ver que a opacidade algorítmica, no Brasil, é reforçada pela dependência tecnológica e pela importação de racionalidades externas. Quando o Estado adota soluções proprietárias sem exigir explicabilidade, ele reforça estruturas de colonialidade epistêmica que limitam sua soberania informacional. A opacidade, nesse sentido, é parte de um arranjo global de poder que condiciona a capacidade estatal de aplicar, na prática, os instrumentos jurídicos existentes.

Assim, a opacidade algorítmica apresenta-se como barreira material à efetividade do habeas data, da LGPD e das garantias constitucionais associadas à motivação, publicidade e contraditório. Não porque tais instrumentos sejam insuficientes, mas porque a arquitetura institucional e tecnológica na qual são aplicados desloca as condições epistêmicas que antes permitiam seu exercício. A questão constitucional central, portanto, não diz respeito à ausência de normas, mas à necessidade de reconstruir capacidades públicas compatíveis com o paradigma do constitucionalismo digital.

5.3 O Projeto de Lei 2338/2023

A tramitação do Projeto de Lei 2338/2023 ocorre em um momento de intensa disputa política, institucional e econômica em torno da regulação da inteligência artificial no Brasil. O projeto, originado no Senado Federal e atualmente em análise na Câmara dos Deputados, foi elaborado por uma comissão de juristas e se apresenta como a tentativa mais estruturada de criação de um marco regulatório nacional de IA. Ele surge após a rejeição do PL 21/2020 e em meio à crescente pressão internacional para que países adotem marcos de transparência, governança e responsabilização semelhantes ao AI Act europeu. No Brasil, contudo, o processo legislativo tem enfrentado forte resistência política, divergências setoriais e pressões econômicas de grande intensidade, em especial de empresas de tecnologia estrangeiras e associações empresariais que buscam limitar o alcance das obrigações regulatórias.

O contexto político do PL 2338 é marcado por tensões que não se restringem ao debate técnico. A discussão sobre riscos, transparência e governança algorítmica ocorre em ambiente permeado por um histórico recente de derrotas regulatórias relevantes, como a paralisação do PL 2630, fruto de intensa atuação das grandes plataformas digitais. Há receio, no Congresso, de que uma lei rigorosa de IA imponha custos de conformidade, desestimule investimentos ou gere litígios, o que produz forte lobby para reduzir a densidade normativa do projeto. Ao mesmo tempo, movimentos da sociedade civil, entidades acadêmicas e órgãos de controle defendem que a ausência de intervenção estatal robusta ampliaria o risco de discriminação algorítmica, vigilância em larga escala e decisões automatizadas sem justificabilidade. Esse conflito de forças explica por que o PL tem avançado de forma lenta e negociada, frequentemente com tentativas de diluição de suas exigências centrais.

Do ponto de vista legislativo, o PL 2338 adota estrutura inspirada no AI Act europeu: classifica sistemas de IA por grau de risco, estabelece obrigações de avaliação de impacto, impõe requisitos de documentação técnica, cria parâmetros mínimos de supervisão humana e prevê mecanismos de responsabilização. O projeto também contempla deveres específicos para sistemas de alto risco, como explicabilidade suficiente, registro de logs, auditorias independentes e mitigação de vieses. Em seu desenho normativo, o PL procura responder à constatação, já consolidada no debate internacional, de que a regulação baseada apenas em direitos individuais e em controles reativos é insuficiente para enfrentar tecnologias que operam por inferências estatísticas, aprendizado de máquina e decisões parcialmente autonômicas.

Ainda assim, o PL 2338 não resolve o problema constitucional que estrutura este trabalho. Seu conteúdo normativo avança ao impor obrigações procedimentais e ao qualificar

exigências de transparência, mas permanece condicionado às mesmas limitações estruturais que afetam a LGPD e o habeas data: déficit institucional, forte dependência tecnológica de empresas estrangeiras, assimetria de poder entre Estado e fornecedores privados e fragilidade histórica dos mecanismos de auditoria e fiscalização. Embora proponha instrumentos importantes, como avaliações de impacto algorítmico e registros de rastreabilidade, sua eficácia depende da capacidade de implementação e enforcement, que por sua vez está vinculada à robustez institucional da Administração Pública e da Autoridade Nacional de Proteção de Dados.

Nesse aspecto, o PL ilustra com clareza o argumento central deste TCC: não basta introduzir novos instrumentos normativos se as condições epistêmicas e institucionais que permitem seu exercício permanecem deficitárias. Assim como ocorre com a LGPD, a aplicabilidade prática do PL 2338 dependerá da existência de mecanismos capazes de converter obrigações formais em transparência substantiva. A exigência de supervisão humana qualificada e de explicabilidade mínima, por exemplo, depende não apenas de previsão legal, mas de capacidade técnica de compreender, auditar e controlar sistemas complexos de aprendizado de máquina. Se o Estado não possui domínio sobre a arquitetura dos modelos utilizados, a norma tende a repetir o mesmo descompasso identificado entre a LGPD e a realidade dos sistemas analisados nos estudos de caso.

A razão pela qual o PL 2338 não ocupa posição central neste trabalho é metodológica e substantiva. Metodologicamente, a pesquisa concentra-se na interpretação constitucional de instrumentos já vigentes, especialmente o habeas data e a LGPD, evitando deslocar o eixo argumentativo para debates legislativos futuros. Substantivamente, ainda que indispensável, o PL não enfrenta o núcleo do problema investigado aqui: a opacidade algorítmica como obstáculo estrutural à autodeterminação informativa e à possibilidade material de exercício dos direitos fundamentais. A lei pode reforçar mecanismos de governança, mas não altera, por si só, as condições técnicas que tornam indevassável a racionalidade algorítmica de muitos modelos utilizados pelo Estado.

Além disso, o PL opera predominantemente em chave procedimental e administrativa: estabelece obrigações, cria categorias de risco e impõe etapas de controle. Essas funções são essenciais, mas não substituem a necessidade de reconstrução hermenêutica das garantias constitucionais que condicionam o exercício do poder informacional estatal. Em outras palavras, mesmo um marco de IA sofisticado continua dependendo da interpretação constitucional para ser efetivamente transformador. A Constituição define os limites do poder; a legislação infraconstitucional define os meios. Quando os meios não são suficientes para tornar possíveis os limites constitucionais, não é a Constituição que deve ceder, mas a interpretação das garantias que deve ser atualizada.

O caráter essencial do PL 2338 reside precisamente no fato de que ele oferece instrumentos ausentes no marco normativo atual para lidar com sistemas de inteligência artificial, especialmente no que se refere à rastreabilidade, documentação e supervisão humana. Entretanto, esses instrumentos só serão efetivamente capazes de reduzir a opacidade algorítmica se acompanhados de mecanismos robustos de enforcement e de um reposicionamento hermenêutico das garantias constitucionais. Em outras palavras, o PL é indispensável, mas insuficiente para, isoladamente, assegurar as condições epistêmicas necessárias ao exercício dos direitos informacionais. A norma cria os contornos externos da regulação, mas não resolve o problema central identificado neste estudo: a distância entre titularidade formal e capacidade material de compreender, contestar e controlar decisões automatizadas.

Por essa razão, o PL 2338 aparece aqui como elemento complementar: necessário, mas não resolutivo. Ele oferece ferramentas indispensáveis onde a LGPD e o habeas data não alcançam, mas não supera, por si só, a estrutura de opacidade que impede que esses instrumentos jurídicos se realizem plenamente. Sua eficácia, portanto, dependerá de um constitucionalismo digital capaz de estabelecer critérios substantivos para explicabilidade, revisão, motivação e controle das decisões algorítmicas. Somente nesse enquadramento hermenêutico é que a legislação ordinária se torna, de fato, apta a converter direitos formais em direitos exercíveis.

5.4 Constitucionalismo digital como caminho possível

O constitucionalismo digital constitui uma das respostas teóricas mais sofisticadas à reconfiguração do poder produzida pela digitalização das estruturas estatais e à crescente centralidade dos sistemas algorítmicos na mediação das decisões públicas. Longe de representar mera atualização terminológica, trata-se de um paradigma hermenêutico que reconhece que os direitos fundamentais, tal como concebidos no constitucionalismo moderno, dependem de condições epistêmicas específicas para serem exercidos, e que tais condições foram radicalmente alteradas pela ascensão de tecnologias digitais baseadas em dados, inferências estatísticas e automatização de decisões. Essa vertente não cria novos direitos, mas reivindica a efetividade contemporânea dos direitos existentes, adaptando-os às lógicas sociotécnicas que estruturam o exercício atual do poder.

Autores centrais da teoria constitucional contemporânea, como Jack Balkin (2016), Daniel Solove (2004) e Julie Cohen (2012), têm argumentado que a digitalização do poder cria formas inéditas de assimetria entre indivíduo e Estado, que não podem ser enfrentadas com o arsenal jurídico tradicional. Balkin (2016) sustenta que vivemos em “novos regimes de vigilância estrutural”, nos quais a arquitetura do poder se desloca para plataformas

técnicas que filtram, classificam e influenciam comportamentos de maneira difusa e não percebida. Julie Cohen (2012) afirma que a regulação jurídica só é efetiva se compreender que a infraestrutura digital constitui uma forma de ordenação normativa, reorganizando a autonomia individual e a própria experiência da cidadania. Essas leituras destacam que a tecnologia não é mero instrumento, mas elemento constitutivo da forma de exercício do poder na contemporaneidade, exigindo novos modelos de interpretação constitucional.

Esse movimento teórico encontra ressonância direta no pensamento produzido no Sul Global. Autores como Oscar Vilhena Vieira (2017), Virgílio Afonso da Silva (2010), Danilo Doneda (2019) e Laura Schertel Mendes (2019) identificam que a proteção de dados e a autodeterminação informativa no Brasil são atravessadas por desigualdades históricas e por contextos institucionais frágeis. Para Doneda (2019), a digitalização do Estado introduz "formas invisíveis de exercício de poder" que exigem reconstrução das garantias constitucionais para alcançar a materialidade dos processos decisórios automatizados. Laura Schertel Mendes (2019) argumenta que a opacidade algorítmica cria barreiras epistêmicas que impedem o exercício de direitos fundamentais, porque o titular não tem como compreender nem contestar as inferências que moldam sua posição jurídica. Esses autores convergem no diagnóstico de que o constitucionalismo clássico é insuficiente se não for reinterpretado à luz das condições tecnológicas contemporâneas.

No Brasil, Antonella Galindo desenvolve uma das formulações mais rigorosas sobre a necessidade de repensar o constitucionalismo a partir da estrutura da esfera pública digital (2024). A autora demonstra que a tecnologia altera a própria forma como o cidadão participa da vida pública, influencia o debate democrático e se relaciona com o Estado. A lógica algorítmica, segundo Galindo (2024), introduz filtros invisíveis que modulam a visibilidade e o impacto das informações, reorganizando silenciosamente quem é visto, ouvido e reconhecido. Esse fenômeno atinge o coração do constitucionalismo, pois compromete as condições de possibilidade do debate público, da deliberação racional e da formação da vontade democrática. Aplicado à atuação estatal, o argumento se torna ainda mais contundente: se a digitalização cria mediações opacas no espaço público, cria igualmente mediações opacas no interior da administração pública, afetando diretamente a forma como decisões são tomadas, justificadas e controladas.

O constitucionalismo digital parte da premissa de que o constitucionalismo é inseparável da transparência das razões públicas. O Estado Democrático de Direito exige que o exercício do poder seja justificado por razões acessíveis, compreensíveis e contestáveis. Esse princípio, presente desde o constitucionalismo liberal, assume nova densidade na era da inteligência artificial: não basta a publicidade da decisão final; é necessário que a lógica algorítmica que influenciou ou determinou a decisão seja minimamente inteligível. Como

observa Mireille Hildebrandt (2018), os algoritmos introduzem “normatividades invisíveis” que afetam a autonomia individual sem que o titular possa percebê-las ou contestá-las. Essa invisibilidade rompe a relação entre cidadania e controle do poder, dissolvendo a capacidade do indivíduo de compreender as condições de exercício da autoridade pública.

Esses elementos permitem compreender a centralidade do constitucionalismo digital no argumento desenvolvido ao longo deste TCC. Os estudos de caso do SINE, do Poder Judiciário e do reconhecimento facial demonstram que LGPD e habeas data, embora normativamente densos, não alcançam a opacidade estrutural das tecnologias que o Estado utiliza. A razão dessa insuficiência não reside em falhas normativas, mas na inadequação hermenêutica de instrumentos concebidos para lidar com registros estáticos frente a sistemas que produzem inferências dinâmicas, classificações probabilísticas e decisões parcialmente automatizadas. O constitucionalismo digital revela que, sem ajustamento interpretativo, o titular continuará sendo juridicamente titular de direitos que não consegue exercer materialmente.

Nesse sentido, a autodeterminação informativa deve ser reinterpretada como autodeterminação epistêmica: o direito não apenas de controlar dados brutos, mas de compreender os efeitos informacionais que moldam as escolhas e oportunidades do indivíduo. O devido processo legal precisa abarcar o direito à reconstrução da racionalidade algorítmica que influenciou a decisão administrativa, pois a motivação constitucionalmente exigida não pode ser cumprida quando a decisão incorpora critérios estatísticos indecifráveis. A igualdade exige análise de vieses algorítmicos, pois discriminações automatizadas frequentemente decorrem da replicação de padrões históricos que escapam ao olhar humano, mas que se tornam sistematicamente amplificados pela automação. A segurança jurídica demanda documentação técnica e auditabilidade. A separação de poderes requer que o Judiciário possa revisar decisões algorítmicas, o que é impossível se não houver métodos de explicabilidade. A democracia exige que o cidadão compreenda a estrutura de poder que o governa.

O constitucionalismo digital, portanto, não é uma proposta de adição de novos direitos, mas de releitura das condições de possibilidade dos direitos fundamentais diante de uma transformação material de grande escala. Ele fornece o enquadramento teórico capaz de explicar por que o habeas data não alcança modelos de machine learning; por que o artigo 20 da LGPD se torna letra morta diante da ausência de explicabilidade; por que o devido processo informacional não pode operar quando a Administração Pública terceiriza sua racionalidade para sistemas opacos; por que a igualdade não pode ser protegida sem auditoria de vieses.

Essa abordagem permite retomar a pergunta que orienta este TCC e oferecer uma resposta constitucionalmente robusta: o problema não é que o ordenamento jurídico brasileiro careça de instrumentos; o problema é que a opacidade algorítmica impede que tais instrumentos se realizem materialmente. O constitucionalismo digital se apresenta como caminho possível precisamente porque reconhece essa assimetria entre titularidade formal e capacidade real de exercício de direitos, propondo uma reconstrução hermenêutica que recoloca a Constituição no centro do debate público sobre inteligência artificial. Em síntese, ele oferece uma estrutura de pensamento capaz de assegurar que a inteligência artificial seja compatível com a Constituição, não pela criação de novos direitos, mas pela reafirmação atualizada dos direitos que já compõem o núcleo duro do Estado Democrático de Direito.

A partir desse enquadramento teórico, torna-se possível compreender como a insuficiência prática do habeas data e da LGPD não decorre de uma falha intrínseca, mas de uma inadequação entre o desenho histórico desses instrumentos e o novo ambiente técnico que condiciona o exercício do poder informacional estatal. O habeas data, concebido para enfrentar bancos de dados estáticos, registros administrativos convencionais e situações de opacidade típicas da burocracia analógica, encontra dificuldades estruturais para alcançar modelos probabilísticos que operam por inferências, correlações e aprendizado estatístico. A garantia continua juridicamente válida, mas sua capacidade de incidência depende de reinterpretação compatível com a lógica informacional contemporânea. O constitucionalismo digital exige que o habeas data seja compreendido como instrumento apto a acessar não apenas dados brutos, mas também descrições minimamente inteligíveis dos processos de decisão que utilizam tais dados, sob pena de se tornar mecanismo simbolicamente preservado e materialmente esvaziado.

Nesse sentido, a reinterpretação do habeas data deve enfatizar que o acesso à informação não pode se limitar à obtenção de registros estáticos, mas deve alcançar informações suficientes sobre o funcionamento de sistemas algorítmicos que utilizam esses registros como insumo. Isso não implica revelar códigos-fonte ou modelos proprietários, mas sim garantir que o titular tenha acesso a explicações compreensíveis sobre os critérios essenciais utilizados para classificá-lo, perfilá-lo ou priorizá-lo. Tal reinterpretação amplia o campo de incidência do habeas data, transformando-o em instrumento apto a romper, ainda que parcialmente, a opacidade das técnicas de decisão automatizada.

Essa releitura também deve reconhecer que, em ambientes de inferências automatizadas, o erro não reside necessariamente no dado bruto, mas nos vínculos estatísticos construídos a partir dele. Assim, a retificação prevista no habeas data deve abranger a correção não apenas do conteúdo dos dados, mas das inferências incorretas que impactam a esfera jurídica do titular. Essa ampliação hermenêutica é indispensável para que o instituto

mantenha sua função histórica de proteger a autonomia individual frente ao poder informacional estatal.

Do mesmo modo, a LGPD permanece como referência normativa central do sistema brasileiro de proteção de dados, mas enfrenta barreiras práticas impostas pela complexidade técnica de sistemas de inteligência artificial e por limitações institucionais da Autoridade Nacional de Proteção de Dados. O constitucionalismo digital exige leitura sistemática de seus princípios, de modo que finalidade, necessidade, proporcionalidade, não discriminação, transparência e responsabilização sejam reinterpretados para alcançar o funcionamento interno das arquiteturas algorítmicas.

A finalidade não pode se limitar à descrição genérica do objetivo da política pública; deve incluir a explicitação da lógica inferencial aplicada à classificação de indivíduos. A proporcionalidade não pode se reduzir à análise clássica dos meios e fins; deve incorporar avaliação dos efeitos distributivos e dos riscos estruturais de discriminação algorítmica. A transparência não pode ser cumprida por meio da entrega de dados estáticos ao titular; exige explicabilidade suficiente para permitir controle humano. A responsabilização não pode depender apenas de mecanismos formais de compliance, mas de governança algorítmica capaz de produzir rastreabilidade das decisões.

A reinterpretação da LGPD, nessa chave, demanda compreender que o direito de acesso previsto no artigo 18 inclui não apenas a obtenção de dados pessoais tratados, mas também informações sobre parâmetros mínimos utilizados para decisões automatizadas que afetam direitos dos titulares. Isso significa que o controlador, especialmente quando estatal, deve fornecer explicações estruturadas sobre como variáveis foram combinadas, quais critérios influenciam classificações e quais salvaguardas foram adotadas para mitigar vieses. A transparência substancial, portanto, torna-se elemento essencial para compatibilizar a atuação administrativa com o devido processo informacional.

Ademais, a interpretação constitucionalmente conforme da LGPD implica ampliar o alcance do artigo 20, de modo que o direito de revisão de decisões automatizadas não dependa da existência de uma decisão puramente automatizada, mas alcance também situações em que a decisão humana esteja influenciada por outputs algorítmicos. A revisão deve permitir reconstruir a racionalidade que orientou a decisão, ainda que parcialmente mediada por sistemas opacos. Sem essa releitura, o direito se torna inócuo diante de ferramentas como as utilizadas pelo SINE, pelo TJPE ou por sistemas de reconhecimento facial.

Sob essa perspectiva, o constitucionalismo digital amplia a compreensão jurídica sobre LGPD e habeas data e revela que a efetividade de ambos depende da construção de

condições epistêmicas mínimas para o exercício dos direitos. Não há autodeterminação informativa possível quando o titular não compreende como seu perfil foi gerado. Não há livre acesso quando o conteúdo acessível não traduz a racionalidade da decisão. Não há retificação possível quando o erro não está no dado bruto, mas na inferência construída sobre ele. Não há revisão de decisão automatizada quando a decisão humana é influenciada por critérios opacos produzidos por sistemas de inteligência artificial. Não há controle institucional quando o Judiciário não consegue reconstruir os parâmetros de classificação empregados pelo Estado. Em suma, a insuficiência prática desses instrumentos evidencia a necessidade de interpretar a Constituição em chave digital.

O constitucionalismo digital, portanto, oferece o fundamento conceitual que permite recolocar LGPD e habeas data no centro da proteção de direitos fundamentais em ambiente de decisões automatizadas. Ele não substitui tais instrumentos, mas revela que sua eficácia depende de interpretação capaz de enfrentar a opacidade algorítmica e suas consequências para a cidadania informacional. A partir dessa leitura, a proteção de dados e o habeas data deixam de ser remédios isolados e passam a integrar um projeto constitucional coerente, voltado à reconstrução da inteligibilidade, da contestabilidade e da transparência das práticas estatais em uma sociedade mediada por sistemas de inteligência artificial.

Se o Estado Democrático de Direito depende da capacidade de explicar as razões de suas decisões, o constitucionalismo digital demonstra que essa explicação só pode ser preservada se os instrumentos clássicos forem reinterpretados para alcançar o núcleo invisível das racionalidades algorítmicas. É essa articulação entre tradição constitucional e inovação hermenêutica que permite afirmar que LGPD e habeas data continuam sendo pilares fundamentais do ordenamento brasileiro, mas somente se compreendidos e aplicados à luz das exigências materiais da era digital.

6 CONCLUSÃO

O objetivo deste trabalho foi investigar se o habeas data e a Lei Geral de Proteção de Dados, tomados como instrumentos jurídicos centrais do regime constitucional de proteção informacional, são capazes de assegurar transparência, acesso e controle quando decisões estatais passam a ser mediadas por sistemas de inteligência artificial caracterizados por opacidade técnica, jurídica e institucional. A hipótese inicial sugeria que tais instrumentos talvez fossem estruturalmente insuficientes diante das condições tecnológicas contemporâneas e que, portanto, seria necessário criar novos dispositivos normativos ou reforçar o arcabouço legal existente.

A análise teórica e empírica desenvolvida ao longo do trabalho demonstrou que essa hipótese não se confirma. Não se identificou lacuna normativa estrutural propriamente dita. Tanto o habeas data, concebido historicamente como garantia de ruptura com o sigilo informacional autoritário, quanto a LGPD, positivadora de princípios de necessidade, adequação, proporcionalidade, não discriminação, prevenção e responsabilização, já fornecem critérios materiais capazes de disciplinar o uso estatal de inteligência artificial. A Constituição de 1988, reforçada pela jurisprudência do Supremo Tribunal Federal, estabelece limites claros ao tratamento de dados pelo poder público, inclusive naquelas áreas excepcionalizadas pelo artigo 4º da LGPD. Assim, o ordenamento jurídico dispõe de instrumentos suficientes, ao menos em tese, para exigir explicabilidade, controle e motivação das decisões administrativas e jurisdicionais afetadas por tecnologias de inferência.

Os estudos de caso permitiram verificar, de forma concreta, a distância entre essa suficiência potencial e a insuficiência prática que marca a atuação estatal. No Sistema Nacional de Emprego, as ferramentas de perfilização e ranqueamento reorganizaram silenciosamente o acesso a oportunidades laborais, sem que trabalhadores tivessem condições de compreender ou contestar inferências que lhes afetavam diretamente. No Tribunal de Justiça de Pernambuco, o uso do MAIA Justiça gerou camadas invisíveis de motivação judicial, impedindo que o jurisdicionado pudesse reconstruir a racionalidade que influenciou o julgamento. No reconhecimento facial empregado em segurança pública, erros previsíveis resultaram em prisões indevidas, afetando de maneira desproporcional pessoas negras e reforçando padrões discriminatórios já documentados. Em todos esses cenários, o titular dos dados manteve acesso aos registros formais, mas não às inferências que, na prática, determinam a decisão estatal.

Esses achados convergem para demonstrar que o problema não reside no texto da Constituição ou da LGPD, mas nas condições epistêmicas e institucionais que impedem que tais normas sejam plenamente cumpridas. A opacidade algorítmica não é apenas fenômeno

técnico, mas obstáculo estrutural à realização dos direitos informacionais. Ela impede a motivação pública, esvazia o contraditório substancial e bloqueia a responsabilização estatal, criando esferas decisórias cujo funcionamento permanece inacessível ao cidadão. Quando o Estado incorpora sistemas que não compreende, não controla ou não é capaz de documentar, a publicidade e a racionalidade das decisões deixam de ser realizáveis na prática.

O capítulo cinco permitiu compreender que essa insuficiência prática não decorre apenas de falhas administrativas, mas de fatores estruturais vinculados à dependência tecnológica e à colonialidade informacional. O neocolonialismo digital, tal como analisado a partir de autores do Sul Global, não constitui elemento extrínseco ao problema, mas chave interpretativa que explica por que LGPD e habeas data, apesar de adequados, não conseguem ser efetivos. Quando infraestruturas tecnológicas, modelos de IA e racionalidades decisórias são importados de corporações transnacionais e operam segundo lógicas próprias, o Estado brasileiro perde capacidade de governança e de imposição de parâmetros constitucionais. Nesses casos, a opacidade não é contingência técnica inevitável, mas resultado de arranjos econômicos e políticos que deslocam capacidades decisórias, limitam a soberania informacional e dificultam a aplicação plena das garantias jurídicas já existentes.

Esse cenário ajuda a compreender também o movimento legislativo recente representado pelo PL 2338, que trata da regulação da inteligência artificial no Brasil. Embora o foco desta pesquisa tenha recaído sobre o habeas data e a LGPD, a análise empreendida evidencia que a resposta regulatória brasileira ao fenômeno da inteligência artificial exige instrumentos complementares. O Projeto de Lei 2338/2023 desempenha papel relevante nesse contexto ao enfrentar dimensões que extrapolam o alcance das garantias existentes. O texto legislativo propõe classificação de risco, documentação técnica, rastreabilidade, supervisão humana e mitigação de vieses, além de prever instrumentos específicos para sistemas biométricos e de alto impacto. Trata-se de avanço indispensável, sobretudo porque enfrenta lacunas de governança inexistentes no arcabouço normativo atual.

No entanto, sua eficácia dependerá das mesmas condições que condicionam a aplicação da LGPD: capacidade técnica estatal, autonomia institucional, fiscalização contínua e resistência a pressões econômicas. Por essa razão, o PL é complementar, mas não resolutivo no âmbito da pergunta orientadora deste TCC. Ele atua onde o habeas data e a LGPD não alcançam, mas não reconfigura a exigência de reconstrução hermenêutica das garantias constitucionais.

A resposta à pergunta orientadora desta pesquisa pode, portanto, ser enunciada com precisão: sim, o ordenamento jurídico brasileiro possui instrumentos capazes de assegurar transparência, acesso e controle sobre informações pessoais em contextos de

inteligência artificial. Contudo, tais instrumentos permanecem estruturalmente incapazes de produzir esses efeitos porque os ambientes tecnológicos nos quais as decisões estatais são tomadas ou moldadas se tornaram incompatíveis com as condições tradicionais de cognoscibilidade e justificação exigidas pelo constitucionalismo democrático. É essa desconexão entre a arquitetura das tecnologias adotadas e a arquitetura dos direitos existentes que explica a inefetividade prática das garantias.

O constitucionalismo digital, tal como reconstruído na parte final deste trabalho, surge, assim, não como expansão normativa, mas como transformação hermenêutica. Ele exige que as garantias constitucionais da publicidade, da motivação, do devido processo e da autodeterminação informativa sejam reinterpretadas à luz das condições técnicas atuais, de modo a alcançar não apenas os dados brutos utilizados pelo Estado, mas também as inferências, pesos, correlações e estruturas analíticas que produzem efeitos jurídicos. Ao colocar as inferências no centro da proteção, o constitucionalismo digital permite recuperar a força material de instrumentos que, embora formalmente preservados, têm sido esvaziados pela opacidade algorítmica e pela dependência tecnológica.

A partir desse quadro, algumas proposições normativas se mostram indispensáveis para que o arcabouço existente possa produzir efeitos constitucionais concretos. A primeira envolve a necessidade de compreender o habeas data como garantia que alcança não apenas dados estáticos, mas também inferências, classificações e perfis gerados automaticamente. A proteção da identidade informacional exige que o titular possa conhecer e, quando necessário, contestar as operações inferenciais que moldam decisões estatais, pois são elas que efetivamente delimitam sua posição diante da Administração Pública.

Em complemento, impõe-se a adoção, em harmonia com as diretrizes previstas no PL 2338, de um regime integrado de documentação, explicabilidade e supervisão humana capaz de conferir inteligibilidade mínima às decisões mediadas por IA. Tal regime pressupõe documentação técnica adequada, rastreabilidade, identificação de variáveis relevantes e avaliação sistemática de vieses, além da presença obrigatória de revisão humana qualificada em decisões que produzam efeitos significativos sobre indivíduos. Embora o projeto de lei já avance nessa direção, sua eficácia dependerá da capacidade estatal de implementar e harmonizar essas exigências com as garantias constitucionais existentes.

Também se revela essencial o fortalecimento institucional da Autoridade Nacional de Proteção de Dados, cuja atuação, autonomia e capacidade técnica condicionam a possibilidade real de fiscalização de sistemas de alta complexidade. Em setores hoje

excepcionados da LGPD, a atuação de uma autoridade robusta é ainda mais decisiva para evitar zonas de opacidade incompatíveis com o regime constitucional de proteção de dados.

Por fim, torna-se necessária uma revisão hermenêutica da própria LGPD, de modo que o dever de transparência não seja reduzido ao acesso formal a registros, mas inclua a inteligibilidade mínima das lógicas decisórias que produzem efeitos jurídicos. A publicidade constitucionalmente exigida depende da compreensão das estruturas analíticas que orientam decisões automatizadas, condição sem a qual contraditório, revisão e controle democrático permanecem inviáveis em ambientes modelados por algoritmos.

O desafio que permanece é criar, fortalecer e exigir mecanismos institucionais que tornem possível sua aplicação real, superando não apenas a opacidade técnica dos algoritmos, mas também a opacidade política produzida pela inserção subordinada do Estado brasileiro em fluxos tecnológicos transnacionais. A compatibilidade entre tecnologia e Estado Democrático de Direito depende da transformação da opacidade algorítmica em inteligibilidade suficiente, da reconstrução das condições epistêmicas do exercício dos direitos e da afirmação de que, mesmo em ambiente de automação crescente, a dignidade humana, a igualdade e a liberdade continuam a constituir o núcleo estruturante da ordem constitucional brasileira.

REFERÊNCIAS

ALEXY, Robert. *Teoria dos direitos fundamentais*. São Paulo: Malheiros, 2008.

BALKIN, Jack M. Information fiduciaries and the First Amendment. *UC Davis Law Review*, v. 49, p. 1183–1234, abr. 2016. Disponível em: https://lawreview.law.ucdavis.edu/archives/49/4/information-fiduciaries-and-first-amendment. Acesso em: 02 nov. 2025.

BARLOW, John Perry. A Declaration of the Independence of Cyberspace. Davos, 1996. Disponível em: https://www.eff.org/cyberspace-independence. Acesso em: 15 jul. 2025.

BAROCAS, Solon; SELBST, Andrew D. Big data's disparate impact. *California Law Review*, v. 104, p. 671–732, 2016. Disponível em: http://dx.doi.org/10.2139/ssrn.2477899. Acesso em: 10 jan. 2025.

BARROSO, Luís Roberto. *O direito constitucional e a efetividade de suas normas: limites e possibilidades da Constituição brasileira*. 2. ed. amp. e atual. Rio de Janeiro: Renovar, 1993.

BASTOS, Celso. *Curso de Direito Constitucional*. São Paulo: Saraiva, 1997.

BIRHANE, Abeba. Algorithmic injustice: a relational ethics approach. *Patterns*, v. 2, n. 2, p. 1–14, 2021. Disponível em: https://www.sciencedirect.com/science/article/pii/S2666389921000155. Acesso em: 05 out. 2025.

BIRHANE, Abeba. The unseen Black faces of AI algorithms. *Nature*, v. 610, p. 451–452, 20 Oct. 2022. Disponível em: https://www.nature.com/articles/d41586-022-03050-7. Acesso em: 08 out. 2025.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil de 1988*. Brasília: Senado Federal, 1988.

BRASIL. Congresso Nacional. *Projeto de Lei n. 2.338, de 2023. Dispõe sobre o uso da inteligência artificial no Brasil e estabelece princípios, direitos, deveres e mecanismos de governança*. Brasília, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2363879. Acesso em: 10 ago. 2025.

BRASIL. Jornal do Brasil. Pai do habeas-data briga por ideias. *Jornal do Brasil*, Rio de Janeiro, 11 ago. 1988, p. 5. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/105863/1988_10%20a%2019%20de%2

0Agosto_%20025.pdf?sequence=1&isAllowed=y. Acesso em: 12 jan. 2025.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Marco Civil da Internet. *Diário Oficial da União*, Brasília, 24 abr. 2014.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, 15 ago. 2018.

BRASIL. Senado Federal. *Projeto de Lei n. 2.630, de 2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. Brasília, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 10 ago. 2025.

BRASIL. Senado Federal. *Projeto de Lei n. 21, de 2020. Estabelece princípios, direitos e deveres para o desenvolvimento e a aplicação da inteligência artificial no Brasil*. Brasília, 2020.

BRASIL. Supremo Tribunal Federal. *Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6390 e 6393*. Relatora: Ministra Rosa Weber. Medida Cautelar referendada pelo Plenário. *Diário da Justiça eletrônico*, Brasília, 2020.

BRASIL. Supremo Tribunal Federal. *Habeas Data 75/DF*. Relator: Ministro Celso de Mello. *Diário da Justiça da União*, Brasília, 19 out. 2006.

BRASIL. Superior Tribunal de Justiça. *Súmula n. 2. Não cabe o habeas data (CF, art. 5°, LXXII, letra "a") se não houve recusa de informações por parte da autoridade administrativa*. Primeira Seção, julgado em 08 maio 1990. *Diário da Justiça*, Brasília, 18 maio 1990, p. 4359.

BRUNO, Fernanda; CARDOSO, Paula; FALTAY, Paulo. *Sistema Nacional de Emprego e a gestão automatizada do desemprego*. Derechos Digitales; MediaLab UFRJ; LAVITS, 2021. Disponível em: https://ia.derechosdigitales.org/pt/publicaciones/. Acesso em: 15 abr. 2025.

BURKE-WHITE, William; SLAUGHTER, Anne-Marie. The future of international law. *Harvard International Law Journal*, v. 50, 2009.

BURRELL, Jenna. How the machine "thinks": understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. DOI: https://doi.org/10.1177/2053951715622512. Acesso em: 10 jan. 2025.

CELESTE, E.; DA SILVA SANTARÉM, P. R. Constitucionalismo Digital: Mapeando a resposta constitucional aos desafios da tecnologia digital. *Revista Brasileira de Direitos*

Fundamentais & Justiça, v. 15, n. 45, p. 63–91, 2022. DOI: https://doi.org/10.30899/dfj.v15i45.1219. Acesso em: 10 jan. 2025.

CITRON, Danielle Keats. Technological due process. *Washington University Law Review*, v. 85, 2008.

COHEN, Julie E. *Configuring the networked self: law, code, and the play of everyday practice*. New Haven: Yale University Press, 2012. Disponível em: https://scholarship.law.georgetown.edu/facpub/804. Acesso em: 09 nov. 2025.

CONVENÇÃO 88 da Organização Internacional do Trabalho (OIT). *Serviço público de emprego*. Genebra, 1948.

DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. Seminário *Acción de Amparo y Habeas Data*, Universidad de Talca, 1997; atualizado em 2002.

DE BLASIO, Emiliana et al. *Digital public sphere: rethinking democratic theory in the age of digitalization*. Cambridge: Cambridge University Press, 2020.

DE GREGORIO, Giovanni. From constitutional freedoms to the power of platforms. *European Journal of Legal Studies*, v. 11, n. 2, 2019.

DON L. Primavera (part. Giovani Cidreira e Rael). In: DON L. *Roteiro pra Aïnouz*, Vol. 2. [S.l.]: [s.n.], 2021. 1 arquivo de áudio (4 min). Disponível em: https://open.spotify.com/intl-pt/track/3Dx6Wk14yRdWlQonXjDG0h. Acesso em: 20 nov. 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Revista dos Tribunais, 2019.

FISCHER-LESCANO, Andreas; BOTHE, Michael. *Fragmentation of International Law*. Oxford: Oxford University Press, 2005.

FOUCAULT, Michel. *Vigiar e punir*. Petrópolis: Vozes, 2008.

GALINDO, Antonella Bruna Machado Torres. Constitucionalismo digital, democracia difusa e esfera pública. *ConJur*, 18 set. 2024. Disponível em: https://www.conjur.com.br/2024-set-18/constitucionalismo-digital-democracia-difusa-e-esfera-publica/. Acesso em: 09 dez. 2024.

GILL, Lex; REDEKER, Dennis; GASSER, Urs. *Towards digital constitutionalism*. Berkman Klein Center, 2015.

HABERMAS, Jürgen. *Direito e democracia*. Rio de Janeiro: Tempo Brasileiro, 1997.

HELDT, Amélie. Regulating social media platforms. *Internet Policy Review*, 2020.

HILDEBRANDT, Mireille. Law as computation in the era of artificial legal intelligence: speaking law to the power of statistics. *University of Toronto Law Journal*, v. 68, suppl. 1, p. 12–35, 2018. DOI: https://doi.org/10.3138/utlj.2017-0044. Acesso em: 10 jan. 2025.

HILDEBRANDT, Mireille. Legal Protection by Design: Objections and Refutations. 2011. Disponível em: https://works.bepress.com/mireille_hildebrandt/21/. Acesso em: 09 jan. 2025.

INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.rec. *Nota Técnica PL 2338/2023 (substitutivo da CTIA)*. Recife: IP.rec, 2024. Disponível em: https://ip.rec.br/publicacoes/nota-tecnica-pl-2338-2023-substitutivo-da-ctia/. Acesso em: 10 jul. 2025.

INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.rec. Tal qual os Incas, Maias e Astecas? O Mecanismo Artificial Inteligente de Apoio à Justiça do TJPE. *Blog IP.rec*, 21 out. 2025. Disponível em: https://ip.rec.br/blog/tal-qual-os-incas-maias-e-astecas-o-mecanismo-artificial-inteligente-de-apoio-a-justica-do-tjpe/. Acesso em: 22 out. 2025.

KELLER, Clara Iglesias; PEREIRA, Jane Reis Gonçalves. Constitucionalismo digital: contradições de um conceito impreciso. *Revista Direito e Práxis*, v. 13, n. 4, p. 2648–2689, 2022. Disponível em: https://www.scielo.br/j/rdp/a/5bpy8smKHgXbKqKzDWDCZQm/?format=pdf&lang=pt. Acesso em: 10 jul. 2025.

LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LÉVY, Pierre. *O que é o virtual?* Tradução de Paulo Neves. São Paulo: Editora 34, 1996.

LORDELO, João Paulo. Constitucionalismo digital e devido processo legal. 2022.

LYON, David. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press, 2018.

MENDES, L. S. F. *Privacidade, proteção de dados e defesa do consumidor*. São Paulo: Saraiva, 2014.

MENDES, L. S. F. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. *Revista Brasileira de Direitos Fundamentais & Justiça*, v. 12, n. 39, p. 185–216,

2019. DOI: https://doi.org/10.30899/dfj.v12i39.655. Acesso em: 10 jan. 2025.

MILTON SANTOS. *Por uma outra globalização*. Rio de Janeiro: Record, 2000.

MORAES, Alexandre de. *Direito constitucional*. 32. ed. São Paulo: Atlas, 2016.

MOREIRA, José Carlos Barbosa. O Habeas Data Brasileiro e sua Lei Regulamentadora. *Revista da ABLJ*, n. 13/14, 1996–1997. Disponível em: http://www.ablj.org.br/revistas/revista13e14/revista13e14%20%20JOS%C3%89%20CARLOS%20BARBOSA%20MOREIRA%20%E2%80%93%20O%20Habeas%20Data%20Brasileiro%20e%20sua%20Lei%20regulamentadora.pdf. Acesso em: 05 jan. 2025.

MOROZOV, Evgeny. *Big Tech: A ascensão dos dados e a morte da política*. São Paulo: Ubu Editora, 2021.

MOROZOV, Evgeny. *To Save Everything, Click Here*. New York: PublicAffairs, 2013.

NASCIMENTO, Roberta Simões. O argumento da intenção do legislador: anotações teóricas sobre uso e significado. *Revista de Informação Legislativa*, Brasília, v. 58, n. 232, p. 167–193, out./dez. 2021. Disponível em: https://www12.senado.leg.br/ril/edicoes/58/232/ril_v58_n232_p167.pdf. Acesso em: 08 mai. 2025.

NYABOLA, Nanjala. *Digital Democracy, Analogue Politics: How the Internet Era is Transforming Kenya*. London: Zed Books, 2018.

PASQUALE, Frank. *The Black Box Society*. Cambridge: Harvard University Press, 2015.

PEREIRA, Jane Reis; KELLER, Clara. Constitucionalismo digital: contradições. *Revista Direito e Práxis*, 2022.

QUIJANO, Aníbal. *A colonialidade do saber: eurocentrismo e ciências sociais, perspectivas latino-americanas*. Buenos Aires: CLACSO, 2005.

REED, Chris; MURRAY, Andrew. *Rethinking the rule of law in cyberspace*. Hart, 2018.

RISCH, Michael. *The rule of law in the digital age*. 2018.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 39. ed. São Paulo: Malheiros, 2022.

SILVA, Virgílio Afonso da. *Direitos Fundamentais: Conteúdo Essencial, Restrições e Eficácia*. São Paulo: Malheiros, 2010.

SLAUGHTER, Anne-Marie; BURKE-WHITE, William. The future of international law. *Harvard International Law Journal*, v. 50, 2009.

SOLOVE, Daniel J. *The digital person: technology and privacy in the information age*. New York: New York University Press, 2004. Disponível em: https://ssrn.com/abstract=2899131. Acesso em: 09 nov. 2025.

SUNSTEIN, Cass. *Republic.com 2.0*. Princeton: Princeton University Press, 2007.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho da União Europeia. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending Regulations and Directives of the Union. *Official Journal of the European Union*, L 168, 12 Jul. 2024.

UNITED STATES. *Freedom of Information Act (FOIA)*. Washington: GPO, 1974.

VICENTE, Lucía; MATUTE, Helena. *Humans inherit artificial intelligence biases.* Scientific Reports, v. 13, n. 15737, p. 1-13, 2023. Disponível em: https://doi.org/10.1038/s41598-023-42384-8. Acesso em: Acesso em: 15 jan. 2025.

VIEIRA, Oscar Vilhena. *Direitos Fundamentais: Duas Interpretações*. São Paulo: Malheiros, 2017.

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, maio 2017. DOI: https://doi.org/10.1093/idpl/ipx005. Acesso em: 10 jan. 2025.

WU, Xingjiao et al. A Survey of Human-in-the-loop for Machine Learning. *arXiv*, 2021. Disponível em: https://arxiv.org/abs/2108.00941. Acesso em: 15 jan. 2025.