**UNIVERSIDADE FEDERAL DE UBERLÂNDIA - UFU FACULDADE DE DIREITO "PROFESSOR JACY DE ASSIS" - FADIR GRADUAÇÃO EM DIREITO**

AGNALDO ALVES DA CRUZ NETO

12121DIR032

# LGPD, INTELIGÊNCIA ARTIFICIAL E COMPLIANCE: O DEVER DA TRANSPARÊNCIA ALGORÍTMICA

UBERLÂNDIA - MG

2026

AGNALDO ALVES DA CRUZ NETO

# LGPD, inteligência artificial e compliance: o dever da transparência algorítmica

Trabalho de Conclusão de Curso componente ao TCC-2 apresentado à Faculdade de Direito Prof. Jacy de Assis da Universidade Federal de Uberlândia como requisito parcial para obtenção do título de Bacharel em Direito

Orientadora: Prof.ª Dra. Keila Pacheco Ferreira

UBERLÂNDIA - MG

2026

**LGPD, inteligência artificial e compliance: o dever de transparência algorítmica**

Trabalho de conclusão de curso orientado pela Prof.ª Dra. Keila Pacheco Ferreira, apresentado à Faculdade de Direito da Universidade Federal de Uberlândia (UFU), como requisito para obtenção do grau de bacharel em Direito, aprovado pela banca examinadora formada por:

Uberlândia/MG, 07 de julho de 2026.

---

Prof.ª Dra. Keila Pacheco Ferreira

Orientadora – Professora Doutora na UFU

---

Prof. Dr. Fernando Martins

Professor Doutor da UFU

---

Jeová Marques de Oliveira

Mestrando da Faculdade de Direito da UFU

*A Deus, que iluminou meu caminho durante essa jornada.*

*À minha mãe, sinônimo de força e ternura, cujo colo e palavras sempre foram alento nos dias difíceis.*

*Ao meu pai, que sob muito sol, me proporcionou as condições para chegar aqui.*

*Ao meu irmão, que esteve presente e me apoiou, desde seu nascimento.*

*À minha família, que sempre acreditou no meu potencial.*

*Aos meus amigos e amigas, que me apoiaram ao longo de toda a trajetória.*

## RESUMO

A crescente delegação de decisões a sistemas de inteligência artificial, alimentados por grandes volumes de dados pessoais, instaurou uma tensão estrutural entre a opacidade dessas tecnologias, o fenômeno da "caixa-preta" e a efetividade dos direitos dos titulares. Diante desse cenário, o presente trabalho investiga como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) pode orientar e exigir práticas de compliance voltadas à transparência algorítmica, conciliando a proteção de direitos fundamentais com a preservação da competitividade e da inovação empresarial. Adotou-se abordagem qualitativa, mediante revisão bibliográfica e análise documental, orientada pelo método jurídico-dogmático. A pesquisa demonstra que a opacidade dos algoritmos compromete direitos como a privacidade, a igualdade, a não discriminação e a autodeterminação informativa, e que a LGPD oferece os fundamentos normativos da transparência algorítmica ao consagrar os princípios da transparência e da responsabilização, garantir o direito à explicação e à revisão de decisões automatizadas e instituir o relatório de impacto à proteção de dados. Reconhece-se, contudo, que a transparência absoluta é inalcançável diante de limites técnicos, jurídicos e práticos, razão pela qual se defende uma transparência proporcional, calibrada conforme o risco e o impacto de cada sistema. Conclui-se que a transparência algorítmica e o compliance são faces complementares de uma mesma exigência, pois a lei fornece o fundamento normativo e o compliance os meios de sua realização prática, institucionalizando a inteligibilidade, a auditabilidade e a prestação de contas.



**Palavras-chave:** Lei Geral de Proteção de Dados; compliance; inteligência artificial; transparência algorítmica; direitos fundamentais.

## ABSTRACT

The growing delegation of decision-making to artificial intelligence systems, fueled by large volumes of personal data, has established a structural tension between the opacity of these Technologies, the so-called "black box" phenomenon, and the effectiveness of data subjects rights. Against this backdrop, this study investigates how the Brazilian General Data Protection Law (Law No. 13,709/2018) may guide and require compliance practices aimed at algorithmic transparency, reconciling the protection of fundamental rights with the preservation of business competitiveness and innovation. A qualitative approach was adopted, based on bibliographic review and documentary analysis, guided by the legal-dogmatic method. The research demonstrates that algorithmic opacity undermines rights such as privacy, equality, non-discrimination, and informational self-determination, and that the LGPD provides the normative foundations for algorithmic transparency by enshrining the principles of transparency and accountability, guaranteeing the right to explanation and to the review of automated decisions, and establishing the data protection impact assessment. It is acknowledged, however, that absolute transparency is unattainable in light of technical, legal, and practical constraints, which is why this study advocates for proportional transparency, calibrated according to the risk and impact of each system. It is concluded that algorithmic transparency and compliance are complementary facets of a single requirement, as the law provides the normative foundation and compliance provides the means for its practical implementation, institutionalizing intelligibility, auditability, and accountability.



**Keywords:** Brazilian General Data Protection Law; compliance; artificial intelligence; algorithmic transparency; fundamental rights.

**SUMÁRIO**

# 1. INTRODUÇÃO

Nas últimas décadas, a inteligência artificial deixou de ser um tema restrito à ficção científica e passou a fazer parte do cotidiano da sociedade digital. Esse avanço está diretamente ligado à chamada Quarta Revolução Industrial, marcada pela integração entre tecnologias digitais, conectividade e o processamento de grandes quantidades de dados. Com computadores cada vez mais potentes e com acesso a um volume enorme de informações, os sistemas baseados em algoritmos passaram a realizar tarefas que antes dependiam do raciocínio humano, como identificar padrões, fazer previsões e tomar decisões. Hoje, a inteligência artificial está presente em inúmeras atividades do dia a dia e vem transformando a forma como empresas e órgãos públicos funcionam.

Essa presença é especialmente marcante em áreas que afetam de perto a vida das pessoas. No setor de crédito, por exemplo, algoritmos avaliam o risco de cada cliente e ajudam a decidir quem terá ou não um empréstimo aprovado. Na área de recursos humanos, sistemas automatizados selecionam currículos e auxiliam em processos de contratação. Na saúde, apoiam diagnósticos e a definição de tratamentos. Na segurança pública, orientam ações de policiamento e avaliações de risco. E, no compliance corporativo, ajudam a monitorar condutas, identificar irregularidades e antecipar riscos. Em todos esses casos, a decisão tomada pela máquina não é apenas uma sugestão técnica, ela produz efeitos concretos sobre direitos importantes, como o acesso ao crédito, ao emprego, à saúde e, em algumas situações, à própria liberdade.

O que todas essas aplicações têm em comum é a forte dependência do tratamento de grandes quantidades de dados pessoais. Os sistemas de inteligência artificial não funcionam sozinhos, eles aprendem a partir de conjuntos enormes de informações sobre hábitos, preferências e características dos indivíduos. Quanto mais dados recebem, maior costuma ser sua capacidade de prever comportamentos. Por isso, a coleta e o cruzamento de dados pessoais não são um detalhe secundário, mas a própria base de funcionamento dessas tecnologias, o que coloca o tema no centro do direito à proteção de dados.

Esse modo de funcionar, porém, traz um problema importante: a opacidade dos algoritmos. À medida que os sistemas ficam mais complexos e passam a se ajustar sozinhos, torna-se cada vez mais difícil entender como eles chegaram a determinado resultado e, muitas vezes, nem mesmo quem criou o sistema consegue explicá-lo com clareza. Esse fenômeno costuma ser chamado de caixa-preta, ou *black box*, devido à falta de explicabilidade, decisões

que afetam direitos são tomadas sem que se possa compreender a lógica por trás delas. A opacidade, nesse caso, não é um simples erro a ser corrigido, mas uma característica das tecnologias mais avançadas, o que torna o problema ainda mais desafiador para o Direito.

A falta de transparência sobre essas decisões acaba afetando uma série de direitos fundamentais. A privacidade é colocada em risco quando o cruzamento de dados permite revelar aspectos íntimos da pessoa sem que ela saiba. A igualdade e a não discriminação ficam ameaçadas quando preconceitos presentes nos dados ou no próprio sistema se transformam em tratamentos injustos, muitas vezes escondidos sob a aparência de neutralidade da tecnologia. E a autodeterminação informativa, ou seja, o direito de cada pessoa controlar o uso das suas próprias informações, perde o sentido quando o titular sequer sabe quais dados estão sendo usados, com quais critérios e para quais finalidades. A opacidade, portanto, deixa de ser uma questão apenas técnica e passa a ser um obstáculo real ao exercício de direitos.

É diante desse cenário que ganha importância a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), principal marco regulatório da proteção de dados no Brasil. Organizada em torno de princípios e de um conjunto de direitos do titular, a lei estabelece regras para o tratamento de dados pessoais, tanto por empresas quanto por órgãos públicos, prevendo deveres, garantias e formas de responsabilização. Com isso, ela oferece a base normativa necessária para enfrentar juridicamente os desafios trazidos pela inteligência artificial, levando a discussão para além do campo ético.

Entre os princípios da LGPD, merece destaque o da transparência, previsto no art. 6º, VI, que garante aos titulares informações claras, precisas e de fácil acesso sobre como seus dados são tratados e por quem, respeitados os segredos comercial e industrial. A transparência não é apenas uma formalidade, é ela que torna possível controlar as decisões automatizadas, já que, sem saber o que é feito com seus dados, o titular dificilmente conseguirá exercer os demais direitos previstos na lei e na Constituição Federal. É justamente essa importância, somada à tensão que a transparência cria com a opacidade técnica e com a limitação pela proteção do segredo das empresas, que motivou a realização deste estudo.

A partir dessas considerações, o presente trabalho parte do seguinte problema de pesquisa: como a Lei Geral de Proteção de Dados pode orientar e exigir práticas de compliance voltadas à transparência algorítmica em sistemas de inteligência artificial, conciliando a proteção de direitos fundamentais com a preservação da competitividade e da inovação empresarial?

O objetivo geral da pesquisa é analisar de que forma a LGPD pode servir de fundamento para exigir práticas de compliance voltadas à transparência algorítmica, mostrando como um programa de conformidade é capaz de transformar o dever jurídico de transparência em uma prática efetiva dentro das organizações, sem deixar de lado interesses legítimos como o segredo empresarial, a competitividade e a inovação. A ideia central é demonstrar que proteger os direitos do titular e estimular o desenvolvimento tecnológico não precisam ser objetivos opostos, podendo caminhar juntos por meio de uma transparência proporcional.

Quanto à metodologia, a pesquisa adota a abordagem qualitativa, voltada à compreensão e à interpretação do fenômeno jurídico em sua complexidade, em detrimento de mensurações quantitativas. O estudo desenvolve-se mediante revisão bibliográfica, com exame de obras sobre proteção de dados, inteligência artificial, governança e compliance, promovendo o diálogo entre os autores. Recorre-se, ainda, à análise documental, com foco na legislação pertinente, em especial a Lei n° 13.709/2018 e de documentos normativos correlatos. O trabalho orienta-se pelo método jurídico-dogmático, que toma o ordenamento positivo como ponto de partida para a construção interpretativa, sistematizando princípios e regras com vistas à solução do problema proposto.

Para alcançar esse objetivo, o trabalho está organizado, além desta introdução, em três partes principais e nas considerações finais. A primeira trata da inteligência artificial, do tratamento de dados pessoais e dos riscos jurídicos que surgem desse uso, destacando a opacidade como origem dos principais desafios e seus reflexos sobre os direitos fundamentais. A segunda discute o dever de transparência na LGPD e seus limites, abordando o direito à informação nas decisões automatizadas, o problema da explicabilidade e o conflito entre transparência e segredo empresarial. A terceira analisa a relação entre transparência algorítmica e compliance, tratando da responsabilização, da governança algorítmica, das ferramentas práticas de transparência, da gestão de riscos e das boas práticas nas empresas. Por fim, as considerações finais retomam o problema e reúnem as principais conclusões. Compreendido o panorama geral do problema, seus contornos teóricos e sua delimitação metodológica, cumpre aprofundar o primeiro eixo de análise.

## 2. INTELIGÊNCIA ARTIFICIAL, DADOS PESSOAIS E RISCOS JURÍDICOS

A crescente delegação de decisões a sistemas computacionais transformou a maneira como dados pessoais são coletados, processados e utilizados, deslocando para máquinas

escolhas que antes pertenciam, com exclusividade, ao domínio humano. Esse movimento, embora prometa eficiência e objetividade, traz consigo um conjunto de riscos jurídicos que desafiam tanto o ordenamento posto quanto os instrumentos de governança de dados. Para compreender esses riscos, convém percorrer quatro pontos: o funcionamento da inteligência artificial, sua imbricação com o tratamento de dados pessoais, a problemática das decisões automatizadas e os principais riscos jurídicos que delas decorrem. Ao final, ficará claro porque a transparência algorítmica é o pressuposto do controle jurídico dessas tecnologias.

### 2.1. Funcionamento da inteligência artificial

O ponto de partida para compreender a inteligência artificial (IA) é a própria noção de algoritmo. Trata-se de uma sequência lógica e finita de instruções voltada à resolução de um problema ou à execução de uma tarefa, contudo, como ressaltam Pinheiro e Brega (2021, p. 166), "sem material sobre o qual atuar, os algoritmos possuem limitada funcionalidade". O termo inteligência artificial, cunhado em 1956 por John McCarthy, designa, segundo os autores, os algoritmos capazes de desempenhar atividade normalmente atribuída à inteligência humana. Na mesma direção, Dias e Ferreira (2023, p. 222) definem a IA como área da Ciência da Computação que desenvolve máquinas que buscam imitar a inteligência humana, apropriando-se de atividades como raciocinar, planejar, aprender e decidir com autonomia.

Essa capacidade de imitação não decorre de instruções fixas, mas de processos de aprendizagem. O *machine learning*, ou aprendizado de máquina, é descrito por Dias e Ferreira (2023, p. 221) como a vertente da IA "baseada em algoritmos que utilizam um grande número de exemplos para o treinamento de modelos computacionais". Pinheiro e Brega (2021) detalham o mecanismo e sua forma mais avançada, o *deep learning*:

> [...] essa capacidade de realizar aquilo que, tradicionalmente, é considerado como fruto da inteligência humana é possibilitada, sobretudo, a partir do processo de machine learning, pelo qual os algoritmos aprendem e se desenvolvem com base em suas experiências anteriores, de modo que os próprios códigos estariam em constante mutação. A forma de *machine learning* de maior eminência hoje é o *deep learning*, que consiste na alimentação da máquina com vasta quantidade de dados, que serão por ela classificados sucessivamente, através de redes neurais não lineares, com base nos outputs de camadas antecedentes. (PINHEIRO; BREGA, 2021, p. 167)

O excerto evidencia a centralidade das redes neurais e, sobretudo, a dependência estrutural da IA em relação às bases de dados que a alimentam. Sem dados, o sistema é inerte. Doneda e Almeida (2018) sintetizam essa relação ao recordarem a lição de Gillespie, para quem "os algoritmos são inertes, máquinas sem sentido, enquanto não estiverem ligados a bases de dados sobre as quais venham a funcionar" (GILLESPIE, 2014 apud DONEDA; ALMEIDA,

2018, p. 144). É justamente o treinamento sobre grandes volumes de dados, e a contínua reorganização interna do modelo, que confere à IA seu poder, mas também o que a torna imprevisível e dependente da qualidade daquilo que recebe como insumo.

## 2.2. Inteligência artificial e o tratamento de dados pessoais

Se os dados são a matéria-prima da IA, o tratamento de dados pessoais torna-se o ponto de contato inevitável entre a tecnologia e o Direito. Pinheiro e Brega (2021, p. 174) observam que o tratamento de dados a que se refere a Lei Geral de Proteção de Dados (Lei n° 13.709/2018) é, muitas das vezes, realizado por algoritmos, de modo que as provisões dessa legislação se aplicam diretamente à inteligência artificial. Nesse escopo, o dado pessoal é definido, conforme o artigo 5°, I da LGPD, como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).

Ainda, a mesma legislação traz a definição de dados pessoais sensíveis no art. 5°, II:

> dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018)

A categoria dos dados pessoais sensíveis ganha contornos próprios nesse cenário de tratamento. A clássica decisão da Corte Constitucional alemã de 1983, marco da proteção de dados, já advertia, conforme registra Kischelewski (2025, p. 72), que "não mais existiriam dados insignificantes nas circunstâncias modernas do processamento eletrônico de dados", pois "o risco do processamento de dados residiria mais na finalidade do processamento [...] do que no tipo dos dados mesmos (ou no fato de quão sensíveis ou íntimos são)" (MENDES, 2021, p. 188-189 apud KISCHELEWSKI, 2025, p. 72). A lição é decisiva, na lógica algorítmica, dados aparentemente triviais podem, uma vez cruzados, revelar informações tão íntimas quanto aquelas formalmente classificadas como sensíveis.

Daí emerge a perfilização. Precedentes alemães do século XX reconheciam que, da coleta de dados, "poderia ser realizado um perfil completo da personalidade" (KISCHELEWSKI, 2025, p. 72). No direito brasileiro, o art. 20 da LGPD endereça expressamente as decisões "destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito" (BRASIL, 2018), abrangendo, inclusive, os perfis comportamentais construídos a partir de dados anonimizados (PINHEIRO; BREGA, 2021, p. 186). A perfilização articula-se, ainda, às inferências automatizadas, descritas por Frazão (2018, p. 2) em termos contundentes: "os algoritmos estão adquirindo o poder de decodificar as pegadas digitais das pessoas,

inferindo e predizendo até mesmo aquilo que ninguém revela e que muitas vezes não tem nem mesmo consciência".

O substrato de tudo isso é o *big data*. Para Frazão (2018, p. 1), ele constitui "a matéria-prima utilizada pelos algoritmos", isto é, a enorme quantidade de dados que, processada, se converte em informações economicamente úteis. Doneda e Almeida (2018) caracterizam o paradigma pelos chamados três Vs (volume, variedade e velocidade) alimentado pelos rastros que nossas atividades deixam, quase sempre de modo monitorado. É a confluência entre *big data*, perfilização e inferência que permite à IA decidir sobre pessoas, e é nesse exato ponto que os riscos jurídicos se adensam.

### 2.3. Decisões automatizadas

A automatização das decisões marca uma mudança qualitativa na relação entre tecnologia e ser humano. Como sintetiza Harari (2024, p. 19), "a IA não é uma ferramenta, é um agente", no sentido de que não se limita a executar comandos, mas decide e atua com margem própria de autonomia.

Por decisão automatizada compreende-se, justamente, aquela tomada unicamente com base em tratamento automatizado de dados pessoais, sem intervenção humana significativa. O art. 20 da LGPD a reconhece ao assegurar ao titular o direito de solicitar a revisão de decisões "tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses". A definição é jurídica, mas o fenômeno é cotidiano: contratações, concessões de crédito, avaliações de risco e até decisões judiciais passam a ser subsidiadas por máquinas.

Os exemplos práticos são abundantes. Frazão (2018) lembra que algoritmos já decidem contratações de empresas, celebrações de contratos, probabilidade de reincidência de criminosos e, no caso extremo dos carros autônomos, quem será ou não atropelado. Lovatto (2024) acrescenta os domínios do recrutamento e do crédito, ilustrados pelos casos da Amazon[1]

[1] Em outubro de 2018, a agência Reuters revelou que a Amazon havia descontinuado, no ano anterior, um sistema experimental de inteligência artificial voltado à triagem de currículos para vagas técnicas. Treinado a partir do histórico de currículos recebidos pela empresa na década anterior, majoritariamente masculino, o algoritmo passou a atribuir notas mais baixas a candidaturas que continham a expressão "women's" e a currículos de egressas de faculdades exclusivamente femininas, penalizando sistematicamente candidatas mulheres a cargos de desenvolvimento de software. O episódio tornou-se referência recorrente na literatura sobre governança algorítmica como exemplo de viés discriminatório originado não da intenção do desenvolvedor, mas da composição enviesada da base de dados de treinamento.

e do Apple Card[2]. Dias e Ferreira (2023, p. 233) recorrem a Harari para descrever, de modo eloquente, o impacto sobre o indivíduo submetido a uma negativa de empréstimo:

> [...] o banco responderá: 'O algoritmo disse que não'. Você pergunta: 'Por que o algoritmo disse não? O que há de errado comigo?', e o banco responde: 'Não sabemos. Nenhum ser humano entende esse algoritmo, porque é baseado num aprendizado de máquina avançado. Mas confiamos em nosso algoritmo, por isso não lhe daremos um empréstimo'. (HARARI, 2018, p. 77 apud DIAS; FERREIRA, 2023, p. 233)

O exemplo expõe o cerne do problema: a decisão afeta diretamente a esfera jurídica da pessoa, mas escapa a qualquer justificação inteligível. O impacto não é apenas individual. Pinheiro e Brega (2021, p. 187) recordam o episódio do *chatbot* Tay, da Microsoft, que em poucas horas passou a emitir comentários machistas, racistas e antissemitas, prova de que sistemas automatizados podem incorporar e amplificar os piores padrões presentes nos dados. Por isso, Laux (2023 apud MENDES, 2025, p. 48) sustenta que, "em contextos sensíveis como saúde, finanças e direito penal, as fragilidades associadas às decisões automatizadas tornam-se particularmente críticas", exigindo supervisão humana efetiva, e não meramente simbólica.

### 2.4. Principais riscos jurídicos

O primeiro e mais estrutural dos riscos é a opacidade algorítmica. Doneda e Almeida (2018, p. 142) advertem que "os algoritmos acrescentam um elemento novo à cadeia de informação, a sua opacidade, que costuma estar associado à dificuldade de decodificar o seu resultado". Pinheiro e Brega (2021, p. 172) levam a constatação ao limite ao afirmar que os sistemas de IA "tornam-se verdadeiras caixas-pretas (*black boxes*), materializadas em milhões de linhas de códigos que, após uma série de mutações autorrealizadas, mostram-se incompreensíveis e inescrutáveis inclusive por seus desenvolvedores". Em registro convergente, Harari (2024) observa que muitos sistemas se tornaram complexos a ponto de superar a capacidade de compreensão de qualquer indivíduo e relata, com base em Suleyman, que as redes neurais em rota de autonomia "não são explicáveis" (SULEYMAN apud HARARI, 2024, p. 335). A opacidade, porém, não é apenas técnica: ela resulta também "de aspectos não

[2] Em novembro de 2019, o desenvolvedor David Heinemeier Hansson denunciou publicamente que o algoritmo de concessão de crédito do Apple Card, cartão lançado pela Apple em parceria com o Goldman Sachs, havia lhe atribuído limite vinte vezes superior ao oferecido à sua esposa, não obstante o casal declarar impostos em conjunto e possuírem bens comuns; relato semelhante foi feito pelo cofundador da Apple, Steve Wozniak. A repercussão do episódio levou o Departamento de Serviços Financeiros do Estado de Nova York (NYDFS) a instaurar investigação. Ao final da apuração, concluída em 2021, o órgão não constatou impacto discriminatório intencional nas decisões de crédito, mas identificou falhas de transparência e de atendimento ao consumidor por parte do Goldman Sachs, aptas a gerar a percepção de discriminação de gênero. O caso permanece, ainda assim, como ilustração paradigmática da opacidade dos critérios empregados em decisões automatizadas de crédito e da dificuldade do titular em obter explicação inteligível sobre elas.

técnicos, relacionados à concorrência", pois os códigos são propriedade intelectual cuja exposição geraria desvantagem competitiva (PINHEIRO; BREGA, 2021, p. 194).

A esse risco somam-se os vieses algorítmicos. Dias e Ferreira (2023, p. 233) são diretas: "os algoritmos podem ser tendenciosos, refletindo preconceitos e discriminações que existem na sociedade". A origem do viés está nos próprios dados de treinamento, coletados com seletividade, baixa qualidade ou extemporaneidade, de modo que "o algoritmo aprenderá a manter aquele viés, que pode também lhe ser imperceptível" (DIAS; FERREIRA, 2023, p. 233). O viés conduz à discriminação automatizada, fenômeno que Doneda e Almeida (2018, p. 145) inscrevem na longa tradição da discriminação estatística, já questionada há quatro décadas, mas hoje potencializada pela escala algorítmica. O caso do Apple Card, citado por Lovatto (2024) em que limites de crédito mais baixos foram atribuídos a mulheres, ilustra a discriminação de gênero produzida por decisões automatizadas. A LGPD reage a esse risco ao consagrar, no art. 6º, IX, o princípio da não discriminação, segundo o qual os dados não podem ser manuseados "para fins discriminatórios ilícitos ou abusivos" (BRASIL, 2018).

Decorre da opacidade um terceiro risco: a falta de auditabilidade. Pinheiro e Brega (2021, p. 172) observam que, com a incorporação de técnicas avançadas de IA, "a possibilidade de auditagem e controle sobre seus *inputs* e *outputs* estaria ainda mais prejudicada". Lovatto (2024) reforça que a ausência de explicabilidade impede auditorias adequadas e compromete a supervisão regulatória.

Por fim, configura-se uma profunda assimetria informacional. É paradoxal que a IA seja adotada, segundo Pinheiro e Brega (2021, p. 168), para a "mitigação de assimetrias informacionais", quando, na prática, a opacidade engendra uma assimetria nova e mais grave: aquela entre quem controla o algoritmo e quem a ele se submete. O próprio direito à explicação, previsto no art. 20 da LGPD, é restringido pela ressalva expressa aos "segredos comercial e industrial", o que, nas palavras dos autores, "pode prejudicar seriamente o escrutínio desses processos decisórios automatizados" (PINHEIRO; BREGA, 2021, p. 186).

Esses riscos representam desafios reais para o Direito e para a governança de dados por uma razão fundamental: eles desorganizam o pressuposto da responsabilidade. Doneda e Almeida (2018, p. 146) formulam a pergunta que o ordenamento ainda não respondeu satisfatoriamente: "quem fica responsável pelo seu uso?"; quando o criador, o operador e a máquina partilham a autoria de uma decisão lesiva? Pinheiro e Brega (2021, p. 193) concluem que o simples cumprimento das normas de proteção de dados "não se mostra suficiente para

dirimir os efeitos perniciosos que a automatização pode gerar", justamente porque a inescrutabilidade e a imprevisibilidade dos sistemas escapam às molduras jurídicas tradicionais, fundadas na previsibilidade e na imputação.

### 2.5. Direitos fundamentais afetados

Os riscos descritos não são abstratos, eles convertem-se em ameaças concretas a direitos fundamentais. A privacidade é o primeiro deles. Quando Frazão (2021, p. 1), valendo-se de Pasquale, descreve uma sociedade em que algoritmos decidem "quem somos, o que pensamos e o que queremos", anuncia a erosão da vida privada pela perfilização. A advertência alemã sobre a perfilização (KISCHELEWSKI, 2025) demonstra que a privacidade deixa de ser apenas o direito a ocultar fatos íntimos para tornar-se o direito a não ser reconstruído, sem consentimento, pela máquina.

A proteção de dados pessoais, embora conexa à privacidade, afirmou-se como direito fundamental autônomo. Kischelewski (2025, p. 76-77) registra que o Supremo Tribunal Federal, ao julgar a ADI nº 6.387-MC-REF/DF, e, posteriormente, a Emenda Constitucional nº 115/2022[3], ao inserir o inciso LXXIX no art. 5º da Constituição, consolidaram esse direito no ordenamento brasileiro, elevando-o à estatura constitucional e blindando-o contra eventuais fragilidades da legislação infraconstitucional.

A jurisprudência constitucional não se limitou, porém, ao reconhecimento abstrato do direito. Ao julgar conjuntamente a ADI n° 6.649/DF e a ADPF n° 695/DF, que impugnavam o Decreto n° 10.046/2019, instituidor do Cadastro Base do Cidadão e do compartilhamento massivo de dados entre órgãos da administração federal, o Supremo Tribunal Federal conferiu ao ato interpretação conforme a Constituição, fixando que o compartilhamento de dados pessoais entre entes públicos pressupõe finalidades legítimas, específicas e explícitas, tratamento limitado ao mínimo necessário e observância dos deveres de motivação, publicidade e proporcionalidade (BRASIL, 2022). A decisão aplicou, em escala estatal, exatamente a advertência que remonta aos precedentes alemães examinados anteriormente, de que a agregação de dados dispersos permite a reconstrução de um perfil completo da personalidade,

[3] A Emenda Constitucional nº 115, promulgada em 10 de fevereiro de 2022 e originada da PEC nº 17/2019, alterou a Constituição Federal de 1988 em três dispositivos: acrescentou o inciso LXXIX ao art. 5º, assegurando "nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"; incluiu o inciso XXVI ao art. 21; e o inciso XXX ao art. 22, fixando a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Ao inserir a proteção de dados pessoais no rol do art. 5º, a Emenda elevou-a à condição de direito fundamental autônomo e de cláusula pétrea (art. 60, § 4º, IV, da CF/88), insuscetível de abolição ou de restrição por emenda constitucional superveniente, ainda que passível de ampliação.

razão pela qual a autodeterminação informativa impõe limites mesmo, e sobretudo, ao tratamento realizado pelo poder público.

A igualdade e a não discriminação são igualmente atingidas. A discriminação automatizada, examinada acima, viola frontalmente a vedação do art. 6º, IX, da LGPD, e reproduz, sob o manto da pretensa objetividade estatística, as desigualdades estruturais que o Direito busca combater. O risco é mais insidioso porque, ao revestir a discriminação de neutralidade técnica, dificulta sua identificação e correção.

No núcleo de todos esses direitos situa-se a autodeterminação informativa. Bioni, citado por Kischelewski (2025), recorda que "historicamente, a proteção dos dados pessoais tem sido compreendida como o direito de o indivíduo autodeterminar as suas informações pessoais: autodeterminação informacional" (BIONI, 2019 apud KISCHELEWSKI, 2025, p. 72). Quando o sistema infere e decide sem que o titular possa controlar a utilização de seus dados, é precisamente essa autodeterminação que se esvazia.

Acima de tudo, é a dignidade da pessoa humana que se vê comprometida. No julgamento do STF, o Ministro Luiz Fux assentou que "a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana" (FUX apud KISCHELEWSKI, 2025, p. 76). Na mesma linha, Mendes (2025) destaca, com apoio em Laux, que a supervisão humana visa a mitigação de riscos e a consolidação de preceitos fundamentais para o exercício da autodeterminação digital, sendo a supervisão humana "indispensável para garantir a legitimidade e a ética no uso desses sistemas em áreas de alto impacto" (MENDES, 2025, p. 48). Frazão (2021), ao evocar o *dataísmo* de Harari, alerta para o risco último: a subjugação do próprio homem aos dados, o que reduz a pessoa a objeto de cálculo e nega-lhe a condição de sujeito.

### 2.6. A necessidade da transparência algorítmica

O percurso até aqui revela que a opacidade é a raiz comum dos riscos jurídicos e da lesão a direitos fundamentais. Vieses não detectados, discriminação invisível, ausência de auditoria e assimetria informacional são, todos, manifestações de um mesmo problema: a impossibilidade de compreender, explicar e controlar as decisões algorítmicas. Disso decorre que nenhum dos direitos analisados (privacidade, proteção de dados, igualdade, autodeterminação informativa e dignidade) pode ser efetivamente tutelado enquanto a decisão

permanecer inescrutável. A transparência algorítmica deixa de ser um valor acessório para constituir-se em condição de possibilidade do controle jurídico da IA.

Coerentemente, a doutrina converge para a transparência como eixo de qualquer modelo de governança. Doneda e Almeida (2018, p. 145-147) propõem uma governança dos algoritmos centrada na responsabilização, na transparência e nas garantias técnicas, reconhecendo que a transparência "não é natural a muitos dos algoritmos que estão em uso", devendo ser estimulada por instrumentos próprios. Lovatto (2024) propõe a explicabilidade, as auditorias internas e os relatórios de conformidade como ferramentas concretas para realizá-la.

Há, contudo, um tensionamento que não pode ser ignorado. Frazão (2021, p. 2) demonstra que a busca pela transparência esbarra em um dos mais difíceis *tradeoffs* da LGPD: o conflito entre os princípios da transparência e da prestação de contas, de um lado, e a proteção do segredo comercial e industrial, de outro, limite que a própria lei reconhece ao conformar o princípio da transparência "observados os segredos comercial e industrial" (art. 6º, VI da LGPD). A autora alerta para o pior cenário: o de permitir que o segredo de negócios opere como escudo absoluto, transformando os algoritmos, já vistos por muitos como armas, também em instrumentos de blindagem contra o escrutínio. Equilibrar inovação e responsabilidade, sem chancelar a irresponsabilidade organizada, é o desafio que se coloca ao Direito.

A transparência algorítmica é, portanto, a base de toda a estrutura de proteção. Ela não elimina, por si só, os vieses ou a discriminação, mas é o pressuposto sem o qual estes não podem sequer ser identificados, atribuídos e corrigidos. Como sintetizam Pinheiro e Brega (2021, p. 193-194), o marco regulatório vigente, embora relevante, mostra-se insuficiente diante da complexidade da IA, reclamando sua complementação por formas adicionais de governança. Entre elas, a exigência de transparência ocupa posição central, é por meio dela que os direitos fundamentais afetados readquirem efetividade e que a decisão automatizada se torna, enfim, passível de controle humano e jurídico. Sem transparência, a tutela é meramente nominal, com ela, abre-se a via para uma inteligência artificial compatível com a dignidade da pessoa humana e com o Estado Democrático de Direito.

## 3. O DEVER DE TRANSPARÊNCIA NA LGPD E SEUS LIMITES

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) elegeu a transparência como um dos eixos estruturantes da disciplina do tratamento de dados pessoais. Mais do que uma

exigência formal, o dever de transparência traduz a pretensão de que o titular compreenda o que se faz com suas informações e possa, a partir daí, exercer seus direitos. Quando o tratamento passa a ser conduzido por sistemas de inteligência artificial, contudo, esse dever depara-se com obstáculos técnicos e jurídicos que põem à prova sua efetividade. Este tópico percorre o princípio da transparência e suas conexões, o direito à informação diante das decisões automatizadas, o problema da explicabilidade e a tensão entre transparência e segredo empresarial. Ao final, discute-se se a transparência absoluta é alcançável e defende-se um modelo de transparência proporcional, compatível com a inovação.

### 3.1. O princípio da transparência

O princípio da transparência encontra assento expresso no art. 6º, VI, da LGPD, que o define nos seguintes termos:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. (BRASIL, 2018)

Dois elementos do dispositivo merecem realce desde logo. O primeiro é que a transparência não é princípio isolado: o caput do art. 6º subordina todo o tratamento à boa-fé. A transparência é, portanto, projeção da boa-fé objetiva no tratamento de dados, impondo aos agentes deveres de lealdade, cooperação e informação para com o titular. Não basta tratar licitamente, é preciso fazê-lo de modo compreensível, sem que o titular seja surpreendido por usos que não poderia antever. O segundo elemento é que a própria definição legal já traz, em sua parte final, um limite, "observados os segredos comercial e industrial", de sorte que a transparência nasce, no texto da lei, conformada por uma ressalva que será o centro nevrálgico de toda a discussão posterior.

A transparência articula-se, ainda, com a *accountability*. O art. 6º, X da LGPD consagra a responsabilização e prestação de contas como "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (BRASIL, 2018). Há uma relação de mútua dependência entre os dois princípios: sem transparência não há como prestar contas, e a prestação de contas é o mecanismo pelo qual a transparência se torna verificável. Nessa direção, Machado (2018) registra que Doneda e Almeida sugerem que "as empresas criem mecanismos de revisão interna em regime de autorregulação, adotando padrões de transparência e accountability dos algoritmos" (DONEDA; ALMEIDA, 2016 apud

MACHADO, 2018, p. 53), de modo que ambos os deveres caminham juntos como instrumentos de governança.

Por fim, a transparência se concretiza, na prática, como dever de informação. Ele se manifesta tanto no já citado art. 6º, VI da LGPD, que exige informações "claras, precisas e facilmente acessíveis", quanto no art. 6º, IV, que assegura o livre acesso, isto é, a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento" (BRASIL, 2018). O dever de informação é, assim, a face ativa da transparência, pois não se limita a permitir o acesso, mas obriga o agente a comunicar, de forma compreensível, as circunstâncias relevantes do tratamento. O desafio jurídico surge precisamente quando o tratamento é automatizado, pois informar "de forma clara" aquilo que nem mesmo o controlador compreende plenamente revela-se tarefa de difícil cumprimento.

### 3.2. Direito à informação e decisões automatizadas

É no art. 20 da LGPD que o dever de transparência se especializa para o universo das decisões automatizadas. O dispositivo assegura ao titular um feixe de direitos diante de decisões tomadas exclusivamente por máquinas:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
>
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. (BRASIL, 2018)

Da leitura do dispositivo extraem-se os direitos do titular: o direito à revisão da decisão automatizada que afete seus interesses e o direito à explicação, entendido, segundo Pinheiro e Brega (2021, p. 185), como o direito de "receber informações suficientes e inteligíveis que permita ao titular dos dados entender a lógica e os critérios utilizados" no tratamento. Trata-se de prerrogativa decorrente do próprio princípio da transparência (art. 6º, VI da LGPD), que, conforme os autores, "assegura aos titulares dos dados o direito de saber que tipos de dados pessoais seus são utilizados pelos algoritmos em suas decisões automatizadas, bem como os critérios utilizados no processo" (PINHEIRO; BREGA, 2021, p. 186), alcançando inclusive os perfis comportamentais construídos a partir de dados anonimizados.

A questão da revisão de decisões automatizadas, contudo, comporta importante controvérsia. Em sua redação original, o art. 20 previa um § 3º que assegurava ao titular o direito de ter a decisão revisada "por pessoa natural", tal previsão, porém, foi vetada por ocasião

da Lei nº 13.853/2019, de modo que o texto vigente não exige, expressamente, que a revisão seja humana. O ponto é decisivo, pois uma revisão meramente automatizada, em que outra máquina reaprecia a decisão da primeira, esvaziaria a garantia, perpetuando a opacidade que o dispositivo pretendia combater. A supressão da exigência de revisão humana é, por isso, medida que enfraquece o controle sobre o resultado da decisão.

As interpretações doutrinárias convergem, todavia, no sentido de extrair do conjunto da LGPD um dever mínimo de inteligibilidade. Frazão (2021, p. 3) sustenta que, "em que pese a proteção do segredo de negócios", a própria lei ampara o entendimento de que "decisões algorítmicas que afetem terceiros precisam ser, no mínimo, inteligíveis e explicáveis, de forma que o segredo de negócios não pode ser utilizado para a ausência de explicações", sendo essa a razão de ser do direito à explicação e à revisão previsto no art. 20 da LGPD. Pinheiro e Brega (2021, p. 186) acrescentam que o direito à explicação na LGPD é "mais amplo do que aquele previsto no General Data Protection Regulation" europeu, embora reconheçam que a ressalva aos segredos comercial e industrial "pode prejudicar seriamente o escrutínio desses processos decisórios automatizados", limitação que conduz diretamente ao problema da explicabilidade.

### 3.3. O problema da explicabilidade

O direito à explicação pressupõe que a decisão seja explicável, ocorre que essa premissa nem sempre se verifica. O obstáculo central é a chamada *black box*. Lovatto (2024) descreve que a

> maioria dos modelos de IA é formada por redes neurais profundas (*deep learning*), e geram as chamadas 'caixas-pretas' (*black box*), ou seja, embora possam produzir resultados precisos, é praticamente impossível entender e explicar como os resultados foram alcançados, se tornando um sistema impenetrável e por consequência que não pode ser auditado (LOVATTO, 2024, p. 5)

A constatação é antiga na literatura, Machado (2018) recorda que Pasquale evoca a noção de "caixa preta" para se referir "à extrema opacidade dos mecanismos decisórios de certos algoritmos" (PASQUALE, 2015 apud MACHADO, 2018, p. 43), e Pinheiro e Brega (2021, p. 194) chegam a afirmar que tais sistemas se tornam "incompreensíveis inclusive para seus desenvolvedores".

Como reação a esse problema, desenvolveu-se o campo da inteligência artificial explicável (*Explainable AI*), voltado a produzir modelos cujos resultados possam ser justificados. Lovatto (2024, p. 4) apresenta a explicabilidade como "capacidade de justificar como e por que um modelo de IA produziu determinados resultados", situando-a entre os pilares de uma boa governança, ao lado da rastreabilidade das origens dos modelos e dos dados que os

treinaram. A explicabilidade não é apenas exigência técnica, mas também jurídica e reputacional, como destacado por Lovatto, “a transparência de algoritmos contribui diretamente para a confiança do consumidor e para a credibilidade das empresas que utilizam IA” (SANCHES VILALTA, 2024 apud LOVATTO, 2024, p. 4).

Entre a opacidade total e a abertura completa do código, a doutrina situa o critério da inteligibilidade. Para Frazão (2021, p. 3), o que se exige é que “pelo menos os aspectos principais e a lógica da decisão algorítmica, e especialmente os critérios de decisão, precisam ser esclarecidos”, de modo que seria possível preservar o segredo de empresa, “já que não se revelaria inteiramente o código, mas sim os aspectos mais relevantes da decisão algorítmica, os quais seriam convertidos da linguagem matemática para a linguagem natural”. A inteligibilidade desloca, portanto, o foco do código-fonte para a justificação compreensível da decisão.

Subsistem, no entanto, limitações técnicas da explicação algorítmica que não podem ser ignoradas. Machado (2018) adverte que “há algoritmos que são opacos por natureza, tais como vários algoritmos de inteligência artificial e aprendizado de máquina, devido ao caráter extremamente não-linear e não-determinista de sua matemática” (TUTT, 2017 apud MACHADO, 2018, p. 43). Soma-se a isso o problema da confiabilidade, como observa Frazão (2021, p. 3), que é “limitada a confiabilidade de uma explicação que, por ser oferecida pelo controlador de dados, é interessada e não está sujeita a qualquer tipo de controle”, razão pela qual a autora defende a importância de auditorias externas independentes. A explicabilidade, assim, é necessária, mas insuficiente quando isolada de mecanismos de verificação.

### 3.4. Transparência *versus* segredo empresarial

A ressalva legal aos segredos comercial e industrial, repetida no art. 6º, VI, e no art. 20, § 1º, da LGPD, instala um dos mais difíceis tensionamentos do regime de proteção de dados. De um lado, a transparência e a accountability, de outro, a livre iniciativa e a proteção do segredo empresarial. Frazão (2021) qualifica esse conflito como um dos mais relevantes *tradeoffs* da LGPD, agravado pelo fato de o próprio princípio da transparência ser conformado expressamente pelo segredo comercial e industrial.

Os fundamentos invocados em favor do segredo são consistentes. Pinheiro e Brega (2021, p. 194) lembram que a opacidade resulta “também de aspectos não técnicos, relacionados à concorrência”, pois “os códigos são propriedades intelectuais, de modo que sua exposição poderia levar a desvantagens competitivas em relação a outras sociedades”. No mesmo sentido,

Doneda e Almeida (2018, p. 143) reconhecem que “um algoritmo aberto pode colocar a empresa por ele responsável em desvantagem diante da concorrência”. A livre iniciativa, a propriedade intelectual e a competitividade empresarial são, portanto, interesses legítimos que o ordenamento protege e que a abertura indiscriminada dos algoritmos poderia comprometer.

Esses interesses, contudo, não são absolutos. Frazão (2021, p. 4) sustenta que “nem mesmo a propriedade intelectual, seja a propriedade industrial, seja o direito autoral, é considerada absoluta”, havendo relevante discussão sobre a função social da propriedade nesse campo. A autora vai além ao recordar, com apoio em Taylor Moore, que os segredos de negócio, embora apelidados de “propriedade intelectual”, não estão sujeitos a qualquer mecanismo de equilíbrio entre os interesses do titular e os da sociedade, diferentemente das patentes, sujeitas a requisitos legais, o que constitui argumento adicional para não compreendê-los como direitos absolutos quando afetam diretamente terceiros (MOORE, 2017 apud FRAZÃO, 2021).

A crítica adensa-se quando o segredo é oposto não apenas ao titular, mas ao próprio regulador. Frazão (2021, p. 4) indaga “se e em que medida o segredo de negócios pode ser oposto ao regulador, considerando que este não tem como regular algo que não compreende”. Machado (2018), ao resenhar Wagner, registra que “as autoridades não têm nem mesmo o acesso necessário aos algoritmos que lhes permitiriam averiguar a efetividade de normas legais ou regulatórias” (WAGNER, 2016 apud MACHADO, 2018, p. 53). O risco extremo, sintetizado por Frazão (2021, p. 5) a partir do caso Compas[4], em que Pasquale denunciou que “algoritmos secretos ameaçam a rule of law”, é o de permitir que o segredo se converta em defesa absoluta, transformando os algoritmos, de armas em diversos contextos, também em escudos contra o escrutínio. O mesmo caso é registrado por Harari (2024, p. 332), que destaca ter a empresa responsável pelo Compas se recusado a revelar a metodologia do algoritmo sob a justificativa de tratar-se de “segredo comercial”, ilustração prática de como a proteção do sigilo pode ser oposta até mesmo ao controle judicial.

[4] O Correctional Offender Management Profiling for Alternative Sanctions (Compas) é um sistema proprietário de avaliação de risco, desenvolvido pela empresa Northpointe, empregado por tribunais estadunidenses para estimar a probabilidade de reincidência de réus e subsidiar decisões sobre fiança, condicional e dosimetria da pena. O caso tornou-se paradigmático a partir de State v. Loomis (Wisconsin, 2016), em que a defesa de Eric Loomis alegou violação ao devido processo legal pelo fato de a metodologia do algoritmo, protegida como segredo comercial, ser inacessível ao réu; a Suprema Corte de Wisconsin, todavia, manteve a sentença. Pouco antes, reportagem da organização de jornalismo investigativo ProPublica, já apontara que o sistema atribuía, proporcionalmente, escores de risco mais elevados a réus negros do que a réus brancos com perfis de reincidência assemelhados. O episódio é referido na literatura como emblema da tensão entre o segredo de negócios e o controle jurisdicional de decisões automatizadas em matéria penal.

É contra esse desfecho que a LGPD reage ao prever, no art. 20, § 2º, que, diante da recusa de informações fundada em segredo comercial e industrial, "a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais" (BRASIL, 2018).

### 3.5. É possível a transparência absoluta?

Diante do exposto, impõe-se a pergunta: é possível alcançar a transparência absoluta dos sistemas de inteligência artificial? A resposta, à luz das fontes examinadas, é negativa, por três ordens de razões convergentes. Em primeiro lugar, há um limite técnico, como visto, certos algoritmos são "opacos por natureza" (TUTT, 2017 apud MACHADO, 2018, p. 43), e a explicação plena de modelos de *deep learning* é, segundo Lovatto (2024), praticamente inalcançável. Em segundo lugar, há um limite jurídico, pois a própria LGPD conforma a transparência aos segredos comercial e industrial (art. 6º, VI; art. 20, § 1º), tutelando a livre iniciativa e a propriedade intelectual. Em terceiro lugar, há um limite prático, haja vista que a explicação fornecida pelo controlador é interessada e de confiabilidade limitada (FRAZÃO, 2021). A transparência absoluta é, pois, ao mesmo tempo tecnicamente inatingível, juridicamente indesejável e praticamente insuficiente.

A inviabilidade da transparência total não conduz, porém, à resignação diante da opacidade. Conduz, antes, à construção de um modelo de transparência proporcional. Frazão (2021, p. 5-6) o formula com precisão ao propor uma "transparência qualificada", intermediária "entre o segredo algorítmico e a transparência completa", que possibilite que "determinados experts possam atestar a qualidade, a validade e a confiabilidade dos sistemas algorítmicos, mantendo o segredo de negócios". Esse modelo combina três instrumentos: a inteligibilidade, esclarecimento da lógica e dos critérios da decisão, convertidos para a linguagem natural (FRAZÃO, 2021); a auditabilidade, verificação por experts independentes e pela ANPD (art. 20, § 2º da LGPD); e a *accountability*, prestação de contas demonstrável (art. 6º, X da LGPD). Nesse sentido, Doneda e Almeida (2018, p. 145) propõem uma governança centrada na responsabilização, na transparência e nas garantias técnicas, advertindo que "não existe uma solução única para todos os casos", o que reforça o caráter gradual e proporcional da transparência exigível, calibrada conforme o risco e o impacto da decisão.

Esse modelo proporcional é, ademais, plenamente compatível com a inovação. Longe de ser entrave ao desenvolvimento tecnológico, a transparência bem calibrada o favorece, como destacam Correia e Água, "a transparência e a governança proativa em IA ajudam as empresas

a inovar com segurança, criando um ambiente competitivo e alinhado às melhores práticas de mercado" (CORREIA; ÁGUA, 2023 apud LOVATTO, 2024, p. 4). A explicabilidade reduz riscos legais, vieses e crises reputacionais, conferindo credibilidade às empresas que dela se valem (LOVATTO, 2024). A transparência deixa de ser percebida como sacrifício da competitividade para revelar-se condição de uma inovação sustentável e confiável.

O dever de transparência da LGPD não reclama, portanto, a utopia da abertura integral dos códigos, mas a efetividade de uma transparência proporcional, inteligível, auditável e responsável, capaz de conciliar a tutela dos direitos do titular com a proteção legítima do segredo empresarial e o estímulo à inovação. É nesse equilíbrio, e não na falsa alternativa entre opacidade absoluta e transparência total, que reside a resposta adequada do Direito ao desafio da inteligência artificial.

## 4. TRANSPARÊNCIA ALGORÍTMICA E COMPLIANCE

Se o dever de transparência previsto na LGPD é, em si, um comando principiológico e abstrato, sua efetividade depende de instrumentos capazes de traduzi-lo em práticas concretas no interior das organizações. É nesse ponto que o compliance assume papel decisivo: longe de ser mero cumprimento formal de normas, ele constitui a estrutura por meio da qual a transparência algorítmica deixa de ser promessa e passa a ser demonstrável, auditável e responsável. Cabe agora examinar o papel do compliance na governança da inteligência artificial, sua relação com a *accountability* e a governança algorítmica, as ferramentas práticas de transparência, a integração com a gestão de riscos e as boas práticas corporativas. O objetivo é demonstrar como o compliance operacionaliza o dever de transparência da LGPD, encerrando-se com o exame do Projeto de Lei n° 2.338/2023, que projeta para o marco legal da inteligência artificial as conclusões aqui alcançadas.

### 4.1. O papel do compliance na governança de IA

O termo *compliance* deriva do verbo inglês *to comply*, que significa cumprir, e refere-se, segundo Campos e Carreiro (2024, p. 4), "à conformidade com normas, regulamentos internos, ou decisões de líderes". Originado das preocupações de empresas norte-americanas no início do século XX e impulsionado por marcos como o *Foreign Corrupt Practices Act* (1977), o instituto ganhou densidade no Brasil com a Lei nº 12.846/2013 (Lei Anticorrupção),

que difundiu a noção de Programa de Integridade como sistema de gestão da conformidade (CAMPOS; CARREIRO, 2024, p. 4).

A evolução do compliance é o traço mais marcante do instituto. As autoras descrevem uma trajetória que avança das "abordagens mais holísticas, que incorporam forte gerenciamento de riscos, avaliando não somente considerações éticas, culturais e de governança corporativa, como a busca pela eficiência" (CAMPOS; CARREIRO, 2024, p. 3). O compliance deixa de ser série de atividades isoladas para integrar-se aos objetivos estratégicos da empresa, evoluindo "para além da esfera jurídica" e tornando-se ferramenta crucial de governança corporativa (CAMPOS; CARREIRO, 2024, p. 5).

Nesse movimento surge o compliance digital, voltado às novas tecnologias e à proteção de dados. Campos e Carreiro (2024, p. 5) identificam a LGPD como base "para implementação de uma Governança que permita mitigação dos riscos nas atividades que realizam tratamento de Dados Pessoais, revendo processos, políticas internas, avaliação de impacto e riscos, mecanismos de supervisão de controles internos e monitoramento contínuo". O compliance assume, assim, feição tecnológica: as ferramentas de análise de dados, a inteligência artificial e a automação de processos passam a ser empregadas pela própria função de conformidade (CAMPOS; CARREIRO, 2024, p. 7-8).

É o que se pode denominar compliance orientado por dados. Mendes (2025, p. 44), apoiada em Dias e Ferreira, observa que, a partir do cruzamento de dados internos, a IA "é capaz de verificar a aderência dos comportamentos organizacionais às normas vigentes, identificando desvios e falhas", fortalecendo os controles internos e reduzindo os riscos jurídicos e financeiros. Mais do que identificar irregularidades passadas, a IA "possibilita a antecipação de riscos, ao mapear padrões comportamentais" (MENDES, 2025, p. 44). O compliance torna-se, desse modo, o lugar institucional em que a governança da IA é exercida, tanto governando a IA quanto valendo-se dela.

### 4.2. *Accountability* e governança algorítmica

O fundamento jurídico que liga compliance e transparência é a *accountability*. O art. 6º, X, da LGPD consagra a "responsabilização e prestação de contas" como o dever de "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (BRASIL, 2018). A prestação de contas não se contenta com a mera adoção

de medidas, ela exige a sua comprovação, e é justamente o compliance que produz a documentação, os registros e as evidências capazes de sustentar essa demonstração.

A *accountability* insere-se no marco mais amplo da governança algorítmica. Doneda e Almeida (2018, p. 145) propõem uma governança dos algoritmos que "costuma priorizar a responsabilização, a transparência e as garantias técnicas", ressalvando que a abordagem pode variar conforme a natureza do algoritmo e a análise de risco. Machado (2018) registra, na mesma linha, que a governança algorítmica "conclama uma necessidade de pensar mecanismos mais eficazes de controle e transparência sobre algoritmos" (MUELLER-BIRN, 2013 apud MACHADO, 2018, p. 52). No plano corporativo, Pinheiro e Brega (2021, p. 192) defendem a expansão das medidas de compliance já realizadas pelas sociedades empresárias, "a fim de lidar também com problemas afetos especificamente ao paradigma dos algoritmos".

A governança algorítmica é, em essência, gestão de riscos. Campos e Carreiro (2024, p. 6) lembram que padrões como a ISO 31000:2018, o COSO ERM e o NIST 800-37 estruturam ciclos de "estratégia, identificação, análise, registro, tratamento e monitoramento de riscos", aos quais se soma, especificamente para a inteligência artificial, a ISO 42001:2023, voltada ao Sistema de Gestão de Inteligência Artificial (CAMPOS; CARREIRO, 2024, p. 7). A gestão de riscos algorítmicos torna-se, portanto, disciplina própria dentro do compliance.

Por fim, a governança algorítmica reclama supervisão humana. Mendes (2025, p. 48), com apoio em Laux, sustenta que a supervisão humana "configura-se como um dos principais mecanismos de governança da IA", salvaguardando "valores fundamentais como autonomia, dignidade, legitimidade e responsabilização", diretriz reforçada pelo art. 14 do *Ato de Inteligência Artificial* da União Europeia para sistemas de alto risco. A autora adverte, porém, que a supervisão só é eficaz quando os supervisores têm "formação adequada, recursos, autonomia"; do contrário, será "meramente simbólica" (MENDES, 2025, p. 48). A conferência humana funciona, assim, como "contrapeso à autonomia das máquinas" (MENDES, 2025, p. 49).

### 4.3. Ferramentas práticas de transparência

A transparência algorítmica materializa-se por meio de ferramentas concretas. A primeira delas é a auditoria algorítmica. Doneda e Almeida (2018, p. 146) apontam o desenvolvimento de "técnicas de auditoria que podem ser úteis para determinar se o algoritmo adere às normas técnicas exigidas". Frazão (2021, p. 3) reforça a importância de "auditorias externas independentes" para atestar a idoneidade do sistema, ante a confiabilidade limitada da

explicação fornecida pelo próprio controlador, competência que a LGPD, em seu art. 20, §2°, também atribui à ANPD, autorizada a "realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais" (BRASIL, 2018). Lovatto (2024) acrescenta que auditorias regulares, internas e externas, já são praticadas por empresas como IBM e Google para assegurar conformidade ética e regulatória.

A segunda ferramenta é a inteligência artificial explicável (*Explainable AI*). Lovatto (2024, p. 9) descreve a explicabilidade como aquilo que "permite que desenvolvedores, auditores e usuários finais compreendam cada uma das lógicas por trás das decisões algorítmicas", constituindo a contrapartida da *black box* e o instrumento técnico que confere transparência à operacionalização da tecnologia.

A terceira ferramenta, de assento legal expresso, é o relatório de impacto à proteção de dados (RIPD). A LGPD o define no art. 5º, XVII:

> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. (BRASIL, 2018)

O art. 38 da LGPD autoriza a autoridade nacional a determinar a elaboração desse relatório, que deverá conter, no mínimo, "a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" (BRASIL, 2018). O RIPD é, por excelência, o documento em que a transparência se converte em prestação de contas verificável.

A essas ferramentas soma-se, na fronteira regulatória, a avaliação de impacto algorítmico (*AI Impact Assessment*). Lovatto (2024, p. 10) registra que o *AI Act* da União Europeia adota "uma abordagem baseada em risco", classificando os sistemas em risco mínimo, limitado, alto e inaceitável, e impondo "obrigações mais rigorosas" aos de alto risco, inclusive avaliações de conformidade pré-lançamento e monitoramento contínuo após a implementação. A avaliação de impacto algorítmico funciona, assim, como uma evolução do RIPD especificamente vocacionada para os riscos da inteligência artificial.

### 4.4. Integração com gestão de riscos

As ferramentas de transparência só produzem efeito quando integradas a um ciclo de gestão de riscos. A identificação de riscos é o ponto de partida, Campos e Carreiro (2024, p. 8) destacam que a adoção de tecnologias avançadas "possibilita uma abordagem mais proativa na

identificação de riscos e na implementação de controles preventivos", reduzindo a probabilidade de incidentes e violações regulatórias.

Segue-se o mapeamento de riscos algorítmicos, que adapta esse ciclo às especificidades da IA. Trata-se de catalogar os riscos próprios dos algoritmos, como manipulação, vieses, discriminação, violação da privacidade, opacidade, e de avaliar seu impacto sobre os titulares. Pinheiro e Brega (2021, p. 192) propõem precisamente a expansão do compliance para abarcar esses riscos, ao passo que a IA, conforme Mendes (2025, p. 44-45), pode auxiliar no próprio mapeamento ao identificar padrões comportamentais e sinais antecipatórios de desvios de conduta.

A mitigação de vieses é a etapa em que o risco identificado é tratado. Lovatto (2024, p. 7-9) sugere a criação de políticas de governança que tratem da "prevenção de discriminação" e da "mitigação de vieses", lembrando que o caso Amazon evidenciou a necessidade de "monitoramento e auditorias contínuas" dos algoritmos de recrutamento. Como os vieses decorrem sobretudo da qualidade dos dados de treinamento, como constatado por Dias e Ferreira (2023), sua mitigação exige controle sobre a origem, a representatividade e a atualização das bases utilizadas.

Por fim, o monitoramento contínuo encerra o ciclo e o reabre. Campos e Carreiro (2024, p. 5) inserem o "monitoramento contínuo" entre os mecanismos próprios do compliance digital, e Lovatto (2024, p. 9) reforça que "o monitoramento constante dos sistemas e a realização de auditorias regulares são práticas fundamentais para verificar a conformidade dos algoritmos com as diretrizes éticas e regulatórias". Por serem sistemas que aprendem e se modificam, os algoritmos exigem acompanhamento permanente, uma transparência que não se esgota no momento da implementação, mas se renova continuamente.

### 4.5. Boas práticas corporativas

No plano das boas práticas corporativas, destacam-se, em primeiro lugar, os comitês de ética. Pinheiro e Brega (2021, p. 192) mencionam a implementação, pelo Google, de um "conselho de ética (*ethics board*) destinado à resolução de questões ligadas à inteligência artificial", e Doneda e Almeida (2018) referem a possibilidade de órgãos internos e comitês multissetoriais voltados a garantir a integridade dos códigos e sua conformidade com o interesse público. Tais comitês institucionalizam o juízo ético que a decisão automatizada, por si, não realiza.

A governança de dados é a segunda boa prática. Lovatto (2024, p. 9) recomenda a criação de “políticas e diretrizes para o uso ético da tecnologia” e de um “código de conduta claro” que defina limites e compromissos da empresa quanto à ética, à transparência e à mitigação de vieses. A governança de dados estabelece os papéis, as responsabilidades e os fluxos que asseguram o tratamento conforme, sem a qual as demais ferramentas operam no vazio.

Os treinamentos constituem a terceira prática. A Estratégia Brasileira de Inteligência Artificial, conforme Pinheiro e Brega (2021, p. 193), propõe “medidas para aumentar a conscientização interna sobre a necessidade dessa conformidade, inclusive por treinamentos”. Mendes (2025, p. 44) acrescenta que a IA pode, ela própria, apoiar o “desenvolvimento de treinamentos e testes de aprendizado”, mapeando vulnerabilidades de compreensão dos colaboradores. A cultura de conformidade depende, em última análise, da formação contínua das pessoas.

Os controles internos completam o quadro. Campos e Carreiro (2024, p. 6) recordam que a própria Lei Anticorrupção exige “mecanismos internos de integridade”, e que a gestão de riscos pressupõe “supervisão de controles internos” (CAMPOS; CARREIRO, 2024, p. 5). É por meio dos controles internos, políticas, procedimentos, canais de denúncia, segregação de funções e auditorias, que as boas práticas se tornam operacionais e verificáveis no cotidiano da organização.

### 4.6. O compliance como operacionalização do dever de transparência

A análise empreendida permite concluir que o compliance é o instrumento por excelência de operacionalização do dever de transparência previsto na LGPD. A lei estabelece os comandos transparência (art. 6º, VI), responsabilização e prestação de contas (art. 6º, X), direito à explicação e à revisão de decisões automatizadas (art. 20) e relatório de impacto (arts. 5º, XVII, e 38), mas esses dispositivos, por si, permaneceriam abstratos. É o programa de compliance que os converte em práticas concretas: políticas de governança, auditorias algorítmicas, explicabilidade e avaliações de impacto, mapeamento e mitigação de riscos, monitoramento contínuo, comitês de ética, treinamentos e controles internos.

Como já assinalado, Pinheiro e Brega (2021, p. 193-194), advertem que o simples cumprimento das normas de proteção de dados não é suficiente para dirimir a complexidade dos riscos algorítmicos, reclamando sua complementação por outras formas de governança. O compliance é, precisamente, essa complementação: o que converte o dever legal de

transparência em realização prática, traduzindo o princípio em evidência demonstrável, em conformidade com a exigência de *accountability*, e calibrando o grau de abertura conforme o risco de cada sistema.

Demonstra-se, assim, que transparência algorítmica e compliance são faces da mesma moeda. A transparência fornece a finalidade; o compliance, os meios. Ao institucionalizar a inteligibilidade, a auditabilidade e a prestação de contas, o compliance permite que a transparência proporcional defendida pela LGPD seja efetivamente alcançada, conciliando a proteção dos direitos do titular com a preservação legítima do segredo empresarial e com o estímulo a uma inovação responsável e sustentável.

### 4.7. O Projeto de Lei n° 2.338/2023 e a consolidação legislativa da transparência algorítmica

A análise desenvolvida até aqui tomou por eixo normativo a Lei Geral de Proteção de Dados, mas o cenário regulatório brasileiro encontra-se em plena transformação. O Projeto de Lei nº 2.338/2023, elaborado a partir dos trabalhos de comissão de juristas e apresentado pelo então Presidente do Senado, Rodrigo Pacheco, foi aprovado pelo Senado Federal em dezembro de 2024 e tramita atualmente na Câmara dos Deputados, propondo-se a instituir o marco legal da inteligência artificial no país. Seu exame interessa a este trabalho por uma razão precisa, visto que o projeto constitui a resposta legislativa aos mesmos problemas aqui percorridos, a opacidade, os vieses, a discriminação automatizada e a assimetria informacional, e, como se demonstrará, confirma e projeta para o futuro as duas teses centrais desta pesquisa, a transparência proporcional e o compliance como seu instrumento de realização.

Desde o seu início, o projeto assume como premissa a conciliação que orienta o problema de pesquisa deste trabalho. O art. 1º declara como objetivos simultâneos "proteger os direitos fundamentais" e "estimular a inovação responsável e a competitividade" (BRASIL, 2023), recusando, portanto, a falsa alternativa entre tutela do titular e desenvolvimento tecnológico. Os fundamentos e princípios do projeto respondem, um a um, aos riscos examinados no segundo capítulo, pois consagram-se, como fundamentos, a privacidade, a proteção de dados pessoais e a autodeterminação informativa (art. 2º, IX), exatamente os direitos cujo desgaste pela perfilização e pela inferência algorítmica se demonstrou; e, como princípios, a supervisão e determinação humana efetiva e adequada no ciclo de vida da IA (art. 3º, III), a não discriminação ilícita ou abusiva (art. 3º, IV), a transparência e explicabilidade (art. 3º, VI), a diligência devida e auditabilidade ao longo de todo o ciclo de vida do sistema

(art. 3º, VII) e a prestação de contas e responsabilização (art. 3º, X) (BRASIL, 2023). Merece destaque, ainda, a incorporação dos aportes do direito antidiscriminatório: o projeto define a discriminação abusiva ou ilícita (art. 4º, XI) e a discriminação indireta abusiva ou ilícita, configurada quando normativa, prática ou critério aparentemente neutro tem a capacidade de acarretar desvantagem para pessoa ou grupos afetados (art. 4º, XII), capturando, no plano legislativo, precisamente o traço mais insidioso da discriminação algorítmica identificado neste trabalho: sua ocultação sob a aparência de neutralidade técnica.

No campo das decisões automatizadas, o projeto funciona como verdadeira resposta ao enfraquecimento produzido pelo veto ao § 3º do art. 20 da LGPD, examinado no terceiro capítulo. Além dos direitos assegurados a toda pessoa ou grupo afetado, independentemente do grau de risco do sistema, informação, privacidade e não discriminação, com o correlato direito à correção de vieses (art. 5º, I a III), o texto aprovado garante, aos afetados por sistemas de alto risco, um feixe de direitos que restaura e amplia a garantia suprimida:

> Art. 6º A pessoa ou grupo afetado por sistema de IA de alto risco tem os seguintes direitos:
>
> I – direito à explicação sobre a decisão, a recomendação ou a previsão feitas pelo sistema;
>
> II – direito de contestar e de solicitar a revisão de decisões, recomendações ou previsões de sistema de IA;
>
> III – direito à revisão humana das decisões, levando-se em conta o contexto, o risco e o estado da arte do desenvolvimento tecnológico. (BRASIL, 2023)

A disciplina do direito à explicação, por sua vez, positiva o critério da inteligibilidade defendido por Frazão (2021): a explicação incluirá informações "suficientes, adequadas e inteligíveis", respeitado o segredo comercial e industrial (art. 6º, § 1º), e será fornecida por processo gratuito, em linguagem simples, acessível e adequada que facilite à pessoa compreender o resultado da decisão (art. 7º), sem que se exija, portanto, a abertura do código-fonte, mas a conversão da lógica decisória para a linguagem natural. No âmbito do poder público, garante-se de forma facilitada e efetiva ao cidadão o direito à explicação e à revisão humanas de decisões que gerem efeitos jurídicos relevantes (art. 23, II). Anote-se, contudo, que a revisão humana do art. 6º, III, é assegurada apenas aos afetados por sistemas de alto risco.

O tensionamento entre transparência e segredo empresarial, identificado como o mais difícil *tradeoff* da LGPD, reproduz-se no projeto sem solução de continuidade, o que confirma seu caráter estrutural. O texto arrola entre seus próprios fundamentos a proteção do segredo

comercial e industrial (art. 2º, XVII), e o princípio da transparência e explicabilidade já nasce, tal como na LGPD, conformado pela ressalva expressa a esse sigilo (art. 3º, VI). A solução projetada, todavia, coincide em essência com a transparência qualificada proposta por Frazão (2021): as conclusões da avaliação de impacto algorítmico serão públicas, observados os segredos industrial e comercial (art. 28); a autoridade competente poderá realizar ou determinar auditorias de sistemas de alto risco ou que produzam efeitos jurídicos relevantes, garantido o tratamento confidencial das informações (art. 49, VII); e será mantida base de dados pública de IA de alto risco, com os documentos das avaliações de impacto, igualmente resguardado o sigilo empresarial (art. 44). Dá-se publicidade às conclusões e viabiliza-se o escrutínio por experts e pela autoridade, sem exposição integral do código, impedindo-se que o segredo se converta naquele escudo absoluto contra o qual adverte a doutrina.

A construção do projeto corresponde, ademais, à transparência proporcional defendida no terceiro capítulo. Todo o sistema estrutura-se sobre uma abordagem baseada em risco: prevê-se a avaliação preliminar para classificação do grau de risco (art. 12), vedam-se os sistemas de risco excessivo (art. 13) e impõem-se obrigações reforçadas de governança aos de alto risco (art. 14), graduando-se inclusive os próprios princípios conforme o risco envolvido, como se dá com a supervisão humana, exigida "considerando o grau de risco" (art. 3º, III), e com a auditabilidade, devida "de acordo com o risco envolvido e o estado da arte" (art. 3º, VII). A calibragem da transparência conforme o risco e o impacto de cada sistema, sustentada neste trabalho com apoio em Frazão (2021) e em Doneda e Almeida (2018), corresponde, assim, à própria espinha dorsal do marco legal em construção.

É, porém, no plano das ferramentas de governança que o projeto mais claramente confirma a tese da complementaridade entre transparência e compliance. A avaliação de impacto algorítmico (art. 4º, XVI) torna-se obrigatória para os sistemas de alto risco (art. 25) e consistirá em processo contínuo, executado ao longo de todo o ciclo de vida do sistema (art. 26), em sintonia com o monitoramento permanente examinado no tópico 4.4, podendo, ainda, ser realizada em conjunto com o RIPD da LGPD (art. 27), o que positiva a continuidade entre os dois instrumentos. A mitigação e prevenção de vieses discriminatórios converte-se em dever legal do desenvolvedor e do aplicador (art. 18, I, "e", e II, "e"), e a supervisão humana deverá viabilizar que os responsáveis possam compreender, interpretar, decidir e intervir nos sistemas (art. 8º), embora sua dispensa, quando comprovadamente impossível ou desproporcional (parágrafo único), possa reconduzi-la àquela supervisão meramente simbólica contra a qual adverte Mendes (2025).

O projeto institucionaliza, por fim, o próprio compliance como categoria jurídica do regime sancionatório. Além de facultar códigos de boas práticas e programas de governança dotados de controles internos, auditoria, canais de denúncia e códigos de ética (art. 40, § 2º) e a autorregulação setorial (art. 41), o texto determina que a adesão a boas práticas seja considerada indicativo de boa-fé na aplicação de sanções (art. 40, § 3º) e que a dosimetria das penalidades leve em conta a adoção demonstrada de mecanismos internos de minimização de riscos, inclusive a análise de impacto algorítmico, o código de ética e a política de boas práticas e governança (art. 50, § 1º, VIII e IX). Reproduz-se, assim, a lógica inaugurada pela Lei nº 12.846/2013 (CAMPOS; CARREIRO, 2024), o programa de conformidade torna-se critério legal de atenuação da responsabilidade, evidência de que o marco legal da inteligência artificial já nasce estruturalmente dependente do compliance para se tornar efetivo.

A confirmação desse mesmo horizonte regulatório não se limita, contudo, ao projeto de lei específico sobre inteligência artificial. O Decreto nº 12.975, de 20 de maio de 2026, que alterou o Decreto nº 8.771, de 11 de maio de 2016, regulamentador do Marco Civil da Internet (Lei nº 12.965/2014), estende a mesma lógica de transparência proporcional e de compliance como seu instrumento de realização à governança das plataformas digitais como um todo. Entre os deveres gerais impostos aos provedores de aplicações de internet, o decreto exige a prestação, às autoridades competentes, de informações sobre as regras e os procedimentos utilizados para moderação de conteúdo e, de modo particularmente relevante para este trabalho, sobre as regras de perfilamento de usuários, de veiculação de publicidade e de impulsionamento remunerado de conteúdos, além de relatórios periódicos de transparência sobre o monitoramento e a gestão de riscos sistêmicos (art. 16-A e art. 20-A). Exige-se, em outras palavras, a explicitação dos critérios dos sistemas algorítmicos de recomendação, curadoria e moderação, no mesmo sentido de inteligibilidade que, no terceiro capítulo deste trabalho, identificou-se como núcleo do direito à explicação do art. 20 da LGPD. O decreto reproduz, ademais, a lógica de valorização do compliance examinada neste capítulo, ao dispor que a autorregulação será considerada elemento de comprovação de boa-fé na apuração de infrações, desde que voltada à criação de padrões técnicos e de governança que protejam os direitos dos usuários (art. 20-A, § 2º), e amplia expressamente a competência fiscalizatória da Autoridade Nacional de Proteção de Dados, que passa a atuar também na apuração de infrações relativas aos deveres dos provedores de aplicações de internet, com fundamento simultâneo na Lei nº 12.965/2014 e na própria Lei nº 13.709/2018 (art. 19-A). Revela-se, assim, que a ANPD, cuja competência auditora sobre decisões automatizadas discriminatórias já se extraía do art. 20, § 2º, da LGPD, é chamada a

exercer, no âmbito da regulação da internet, o mesmo papel de garantidora da transparência qualificada aqui reconhecido no campo da proteção de dados pessoais, evidenciando que a arquitetura de compliance e transparência defendida neste trabalho transcende o diploma legal que a originou.

O Projeto de Lei nº 2.338/2023 oferece, em síntese, a confirmação legislativa das conclusões deste trabalho: adota a transparência calibrada pelo risco, restaura a revisão humana suprimida da LGPD, equaciona pela via da transparência qualificada o *tradeoff* com o segredo empresarial e converte o compliance em peça central da responsabilização. Trata-se, contudo, de texto ainda em tramitação, cujas concessões já realizadas, como a avaliação preliminar convertida em mera boa prática e a possibilidade de dispensa da supervisão humana, demonstram, em tempo real, que o embate entre direitos fundamentais e interesses econômicos, analisado ao longo deste trabalho, segue disputando cada dispositivo do marco legal em construção.

## 5. CONSIDERAÇÕES FINAIS

O presente trabalho partiu de um problema que se tornou incontornável no cenário contemporâneo: a crescente delegação de decisões a sistemas de inteligência artificial, alimentados por dados pessoais, instaurou uma tensão estrutural entre a opacidade dessas tecnologias e a efetividade dos direitos dos titulares. Foi dessa constatação que emergiu a pergunta orientadora da investigação: como a Lei Geral de Proteção de Dados pode orientar e exigir práticas de compliance voltadas à transparência algorítmica em sistemas de inteligência artificial, conciliando a proteção de direitos fundamentais com a preservação da competitividade e da inovação empresarial? A trajetória percorrida permite, agora, retomar criticamente cada uma das etapas que conduziram à resposta.

Demonstrou-se, inicialmente, que a inteligência artificial depende estruturalmente das bases de dados que a alimentam, sem as quais os algoritmos seriam meros conjuntos de instruções inertes. Por aprender e se reconfigurar continuamente a partir de grandes volumes de dados, esses sistemas tornam-se progressivamente mais complexos, a ponto de se converterem em verdadeiras caixas-pretas, cujo processo decisório escapa à compreensão até mesmo de quem os desenvolveu.

Com efeito, da opacidade decorrem os vieses, a discriminação automatizada, a falta de auditabilidade e a assimetria informacional, riscos que não são abstratos, pois se convertem em ameaças concretas à privacidade, à proteção de dados, à igualdade, à autodeterminação informativa e, em última instância, à dignidade da pessoa humana. O trabalho sustentou, criticamente, que tais riscos desafiam o Direito porque desorganizam o próprio pressuposto da responsabilidade: quando o criador, o operador e a máquina partilham a autoria de uma decisão lesiva, torna-se difícil imputar responsabilidade e oferecer ao titular uma justificação inteligível. Mais do que isso, evidenciou-se que o simples cumprimento formal das normas de proteção de dados não basta para dirimir tamanha complexidade, pois a inescrutabilidade e a imprevisibilidade dos sistemas escapam às molduras jurídicas tradicionais, assentadas na previsibilidade e na imputação.

A análise evidenciou, em seguida, que a própria legislação de proteção de dados oferece os fundamentos normativos para a transparência algorítmica. O dever de transparência projeta-se como desdobramento da boa-fé que deve presidir todo tratamento de dados e articula-se com a responsabilização e a prestação de contas (*accountability*), que exigem do agente não apenas adotar, mas comprovar a eficácia das medidas de conformidade. No campo das decisões automatizadas, assegura-se ao titular o direito de obter informações claras sobre os critérios empregados e de solicitar a revisão das decisões que o afetem, ao passo que o relatório de impacto à proteção de dados institui o documento por excelência da prestação de contas verificável. A lei fornece, portanto, uma base principiológica robusta, da qual a transparência algorítmica se deduz.

Demonstrou-se, contudo, que esses fundamentos convivem com limites intransponíveis, de modo que a transparência absoluta não é alcançável. Há um limite técnico, pois determinados algoritmos são opacos por sua própria natureza, dada a complexidade não linear de seu funcionamento, que resiste à tradução em explicações plenamente compreensíveis. Há um limite jurídico, pois a própria lei conforma a transparência à proteção dos segredos comercial e industrial, tutelando interesses empresariais legítimos. E há um limite prático, pois a explicação fornecida pelo próprio responsável pelo tratamento é interessada e de confiabilidade reduzida quando não submetida a controle externo. A inviabilidade da abertura total não conduz, todavia, à resignação diante da opacidade, mas à defesa de uma transparência proporcional, assentada na inteligibilidade da lógica e dos critérios da decisão, na auditabilidade do sistema e na efetiva prestação de contas.

É nesse ponto que o compliance se revelou o elo decisivo entre o dever jurídico e a prática organizacional. Tendo evoluído de uma simples conformidade regulatória para uma abordagem holística, integrada à estratégia e à governança corporativa, o compliance digital tornou-se a estrutura por meio da qual a transparência deixa de ser comando abstrato e se materializa em instrumentos concretos, como auditorias algorítmicas, mecanismos de explicabilidade, relatórios e avaliações de impacto, mapeamento e mitigação de riscos, monitoramento contínuo, comitês de ética, programas de treinamento e controles internos. A exigência de responsabilização funciona como a ponte que liga o princípio à evidência demonstrável, e o programa de compliance constitui, precisamente, a complementação de governança sem a qual o dever legal de transparência permaneceria nominal.

O trabalho insistiu, por isso, na necessidade de equilíbrio entre transparência, segredo empresarial, competitividade e inovação. De um lado, reconheceu-se que a livre iniciativa, a propriedade intelectual e a competitividade são interesses legítimos, pois a exposição irrestrita dos códigos poderia colocar a empresa em desvantagem concorrencial e desestimular o investimento em novas tecnologias. De outro, sustentou-se que nem a propriedade intelectual nem o segredo de negócios são direitos absolutos, não podendo converter-se em escudo contra o escrutínio quando decisões automatizadas afetam diretamente terceiros. O equilíbrio buscado não é, portanto, um meio-termo resignado, mas uma transparência calibrada conforme o risco e o impacto de cada sistema, capaz, inclusive, de favorecer a inovação, na medida em que a governança proativa e a confiança que dela resulta tornam-se diferenciais competitivos, e não entraves ao desenvolvimento tecnológico.

À luz desse percurso, responde-se explicitamente à pergunta de pesquisa. A legislação de proteção de dados orienta e exige práticas de compliance voltadas à transparência algorítmica ao consagrar a transparência e a responsabilização como princípios vinculantes, ao garantir o direito à explicação e à revisão das decisões automatizadas, ao instituir o relatório de impacto e ao autorizar a auditoria pela autoridade competente diante da recusa de informações fundada em sigilo. Esses comandos, contudo, somente se tornam efetivos quando traduzidos por programas de compliance, que convertem o dever abstrato em rotinas demonstráveis de governança. A conciliação entre a proteção dos direitos fundamentais e a preservação da competitividade e da inovação realiza-se, por fim, mediante um modelo de transparência proporcional: nem a opacidade absoluta, que sacrifica os direitos do titular, nem a abertura integral, que sacrifica o segredo legítimo, mas a inteligibilidade auditável e responsável, ajustada ao risco de cada decisão automatizada.

Reconhecem-se, ainda, as limitações desta pesquisa. Tratou-se de investigação de natureza teórico-doutrinal, conduzida por revisão bibliográfica e documental, sem o levantamento de dados empíricos sobre a efetiva adoção, pelas organizações, das práticas de compliance aqui examinadas. Soma-se a isso o caráter recente e ainda em consolidação do marco normativo: a regulamentação infralegal pela autoridade nacional encontra-se em construção, a jurisprudência sobre decisões automatizadas é incipiente e o ordenamento ainda não dispõe de legislação específica sobre inteligência artificial em vigor, embora o Projeto de Lei n° 2.338/2023, aprovado pelo Senado Federal em dezembro de 2024, tramite atualmente na Câmara dos Deputados, o que torna provisórias algumas das conclusões e dependentes do desfecho do debate regulatório em curso. Tais limites não infirmam os resultados alcançados, mas delimitam seu alcance e convidam ao seu aprofundamento.

Justamente por isso, abrem-se promissoras linhas de investigação futura. No campo da regulação da inteligência artificial, impõe-se acompanhar a tramitação do Projeto de Lei n° 2.338/2023 na Câmara dos Deputados, avaliando as eventuais alterações promovidas pela Casa e seu impacto sobre o modelo de transparência proporcional e sobre o papel do compliance aqui examinados. No campo da governança algorítmica, cabe aprofundar os arranjos institucionais, como comitês, supervisão humana e garantias técnicas, capazes de tornar a governança efetiva, e não meramente simbólica. No campo da responsabilização, mostra-se relevante desenvolver métricas e mecanismos de verificação que permitam aferir, e não apenas afirmar, a conformidade dos sistemas. E, no campo do compliance digital, recomenda-se a realização de estudos empíricos sobre a maturidade das práticas corporativas, de modo a confrontar o dever normativo com a realidade organizacional.

Conclui-se, em síntese, que transparência algorítmica e compliance constituem faces complementares de uma mesma exigência, pois a legislação de proteção de dados fornece o fundamento normativo, e o compliance, os meios de sua realização prática. Ao institucionalizar a inteligibilidade, a auditabilidade e a prestação de contas, o compliance permite que a transparência proporcional preconizada pela lei seja efetivamente alcançada, conciliando a tutela dos direitos fundamentais com a proteção legítima do segredo empresarial e o estímulo a uma inovação responsável.

**REFERÊNCIAS**

BRASIL. Decreto nº 12.975, de 20 de maio de 2026. Altera o Decreto nº 8.771, de 11 de maio de 2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2026.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Texto aprovado pelo Senado Federal em 10 de dezembro de 2024, em tramitação na Câmara dos Deputados. Brasília, DF: Senado Federal, 2023.

BRASIL. Supremo Tribunal Federal (Plenário). Ação Direta de Inconstitucionalidade nº 6.649/DF e Arguição de Descumprimento de Preceito Fundamental nº 695/DF. Relator: Min. Gilmar Mendes, 15 de setembro de 2022. Brasília, DF: STF, 2022.

CAMPOS, Daniella; CARREIRO, Flavia dos Reis. Compliance e gestão de riscos em tempos de inovação e disrupção digital. Revista de Gestão e Secretariado - GeSec, São Paulo, v.15, n.4, p. 1-22, 2024.

DIAS, Cintia Coelho; FERREIRA, Roberta Valiatti. O uso da inteligência artificial na atividade de compliance: riscos e benefícios. Revista Científica do CPJM, Rio de Janeiro, v. 2, n. 8, 2023.

DONEDA, Danilo; ALMEIDA, Virgilio AF. A. O que é governança de algoritmos. In: BRUNO, F. et al. (org.). Tecnopolíticas da vigilância: perspectivas da margem, p. 141 148, 2018.

FRAZÃO, Ana. Algoritmos e inteligência artificial: Repercussões da sua utilização sobre a responsabilidade civil e punitiva das empresas. Jota, São Paulo, v. 15, 2018.

FRAZÃO, Ana. Transparência de algoritmos x segredo de empresa: As controvérsias a respeito das decisões judiciais trabalhistas que determinam a realização de perícia no algoritmo da Uber. v. 9, 2021.

HARARI, Yuval Noah. Nexus: uma breve história das redes de informação, da Idade da Pedra à inteligência artificial. Tradução de Berilo Vargas e Denise Bottmann. 1ª ed. São Paulo: Companhia das Letras, 2024.

KISCHELEWSKI, Flávia Lubieska N. A interseção entre as legislações argentina e brasileira de proteção de dados pessoais. Diálogo Jurídico em torno do Direito Argentino & Brasileiro. 2ª edição. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2025.

LOVATTO, Manuela Betiele Aude. Inteligência Artificial: governança e transparência? Revista IBMEC de Direito, v. 1, n. 1, 2024.

MACHADO, Henrique Felix de Souza. Algoritmos, regulação e governança: uma revisão de literatura. Journal of Law and Regulation, v. 4, n. 1, p. 39-62, 2018.

MENDES, Adrise Lage de Mendonça. A autorregulação da inteligência artificial como instrumento de prevenção de riscos e promoção da integridade empresarial. Diálogo Jurídico em torno do Direito Argentino & Brasileiro. 2ª edição. Brasília: Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2025.

PINHEIRO, Caroline da Rosa; BREGA, Gabriel Ribeiro. Inteligência artificial e compliance: A (in)suficiência dos marcos de proteção de dados. Revista Semestral de Direito Empresarial, n. 28, p. 161-196, 2021.