JURIS POIESIS
REVISTA DO CURSO DE DIREITO DA UNIVERSIDADE ESTÁCIO DE SÁ

AUDITABILIDADE ALGORÍTMICA E DEVIDO PROCESSO: O *HABEAS CODE* COMO CATEGORIA DOGMÁTICO-PROCEDIMENTAL DE CONTESTAÇÃO DE DECISÕES AUTOMATIZADAS

HABEAS CODE AND ALGORITHMIC AUDITABILITY: DUE PROCESS OF AUTOMATED DECISIONS

Paulo José Pereira Carneiro Torres da Silva[1]

Melhym Pereira Quemel[2]

Data de submissão: 13 de julho de 2026

Data de aceite: 31 de julho de 2026

[1] Doutor em Direito pelo PPGD/UNESA e Mestre em Direito Constitucional pelo PPGDC/UFF, com ênfase em Teoria e História do Direito Constitucional, Direito Constitucional Internacional e Comparado. Professor dos programas de Mestrado e Doutorado da UNESA, onde lidera o Grupo de Pesquisa 'Fundamentos do Processo' e da UCAM, onde lidera o Grupo de Pesquisa 'Tecnologia, Sustentabilidade e Justiça: Novas Gramáticas do Direito ao Desenvolvimento'. Desenvolve pesquisa sobre as interfaces entre Teoria Constitucional e Tecnologia com ênfase nas hipóteses de Colapso Constitucional, Erosão da Soberania e Difusão da Autoridade frente à ascensão das plataformas digitais, propondo uma Nova Gramática Constitucional como resposta contemporânea à este fenômeno. Possui produção qualificada em veículos de excelência internacional e nacional, investigando a regulação de plataformas e a crise das instituições jurídicas aliada a uma intensa atividade de formação de recursos humanos, principalmente nos seguintes temas: Constitucionalismo Digital, Regulação de Plataformas, Crise das Instituições Jurídicas e Nova Gramática Constitucional. Pesquisador do Laboratório de Estudos Interdisciplinares em Constitucionalismo Latino Americano (LEICLA) e do Observatório de Acesso à Justiça em Ibero América (OAJIA).

[2] Pesquisador com perfil interdisciplinar na convergência entre Direito, Tecnologia e Inclusão, unindo a dogmática jurídica à arquitetura de sistemas. Mestre em Direito pela Universidade Estácio de Sá (UNESA - Bolsista CAPES, 2024), com foco em Direitos Fundamentais e Novos Direitos. Graduando em Engenharia de Software, possui formação híbrida que lhe permite investigar a ''caixa-preta'' das tecnologias emergentes sob uma ótica crítica e técnica.Sua agenda de pesquisa atual concentra-se no ''Devido Processo Legal Tecnológico'' e na Governança Algorítmica, com ênfase em três eixos: 1) A integridade da prova digital e a cadeia de custódia frente à Inteligência Artificial; 2) A gestão judiciária de dados (BNMP 3.0) e seus impactos em direitos fundamentais; e 3) A hipervulnerabilidade algorítmica em serviços profissionais (''Shopee-ficação'') e a inclusão digital de pessoas com deficiência.Produção acadêmica recente destaca-se pela aprovação de artigos na Revista do CNMP (2025) sobre a modulação de nulidades em provas digitais e a implementação do BNMP 3.0, além de produção bibliográfica sobre vieses algorítmicos e precarização do trabalho (''Uberização'').Possui sólida formação jurídica com pós-graduações em Advocacia Cível (FMP), Ciências Penais e Segurança Pública (IRG) e Políticas Públicas (IERBB/MPRJ). Concluiu o Programa de Residência Jurídica do Ministério Público do Estado do Rio de Janeiro (2025), atuando com ênfase em tutela coletiva e investigação penal. Presidente da Comissão de Defesa dos Direitos da Pessoa com Deficiência da OAB/RJ (51 Subseção), onde atua na defesa de políticas de inclusão, partindo de seu lugar de fala como pessoa com deficiência visual (CIF H54.0). Busca, na academia, desenvolver marcos regulatórios que compatibilizem inovação tecnológica, eficiência processual e proteção integral da dignidade humana. Atua também na difusão cultural e literária sobre acessibilidade e identidade sensorial.

RESUMO: O artigo examina a insuficiência dos instrumentos jurídico-processuais atualmente disponíveis no direito brasileiro para assegurar a contestabilidade de decisões automatizadas que impactam direitos fundamentais. Parte-se da premissa de que a lesão algorítmica contemporânea nem sempre decorre da existência de dados pessoais incorretos ou ilicitamente armazenados, mas pode resultar da lógica de processamento que transforma dados em classificações, perfis, escores, bloqueios, exclusões ou restrições. A pesquisa adota abordagem jurídico-dogmática e jurídico-propositiva, de natureza qualitativa, com revisão bibliográfica, análise normativa e reconstrução crítica dos limites do habeas data, da Lei Geral de Proteção de Dados, do mandado de segurança e de técnicas probatórias ordinárias. Sustenta-se que decisões automatizadas de impacto relevante somente se compatibilizam com o devido processo quando oferecem condições mínimas de auditabilidade funcional, sem que isso implique transparência absoluta, abertura irrestrita do código-fonte ou supressão do segredo industrial. O artigo propõe compreender o *Habeas Code* não como nova ação constitucional autônoma, mas como categoria dogmático-procedimental destinada a organizar, a partir de instrumentos já existentes, uma tutela mandamental de auditabilidade algorítmica. Conclui-se que essa categoria pode contribuir para estruturar deveres de explicação individualizada, preservação de registros técnicos, acesso controlado à lógica decisória, contraditório técnico, revisão humana substancial e provimentos proporcionais de correção, suspensão ou invalidação de decisões automatizadas opacas.

Palavras-chave: *Habeas Code*; auditabilidade algorítmica; devido processo algorítmico; habeas data; decisões automatizadas.

ABSTRACT: This article examines the insufficiency of the legal and procedural instruments currently available under Brazilian law to ensure the contestability of automated decisions that affect fundamental rights. It starts from the premise that contemporary algorithmic harm does not always arise from inaccurate or unlawfully stored personal data, but may result from the processing logic that transforms data into classifications, profiles, scores, account blocks, exclusions, or restrictions. The research adopts a qualitative legal-dogmatic and legal-propositional approach, based on bibliographic review, normative analysis, and critical reconstruction of the limits of habeas data, the Brazilian General Data Protection Law, mandamus-like remedies, and ordinary evidentiary techniques. It argues that automated decisions with significant impact are compatible with due process only when they provide minimum conditions of functional auditability, without requiring absolute transparency, unrestricted access to source code, or the suppression of trade secrecy. The article proposes to understand Habeas Code not as a new autonomous constitutional action, but as a dogmatic-procedural category aimed at organizing, through existing legal instruments, mandatory relief for algorithmic auditability. It concludes that this category may contribute to structuring duties of individualized explanation, preservation of technical records, controlled access to decision-making logic, technical adversarial procedure, substantive human review, and proportionate remedies for the correction, suspension, or invalidation of opaque automated decisions.

Keywords: Habeas Code; algorithmic auditability; algorithmic due process; habeas data; automated decisions.

INTRODUÇÃO

A crescente incorporação de sistemas automatizados de decisão em atividades públicas e privadas alterou o modo pelo qual direitos são distribuídos, restringidos, condicionados ou negados. Avaliações de crédito, seleção e desligamento de trabalhadores, moderação de conteúdos, concessão de benefícios, decisões judiciais, entre outros processos, passaram a depender, em diferentes graus, de modelos computacionais que classificam indivíduos, inferem perfis, calculam riscos e produzem consequências jurídicas, econômicas ou sociais relevantes.

O problema não reside na automação em si, nem na mera utilização de dados pessoais como insumo decisório. A questão juridicamente mais sensível está na dificuldade de compreender, reconstruir e contestar a lógica pela qual determinados dados são convertidos em decisões que afetam posições subjetivas protegidas. Essa transformação desloca a proteção de dados de uma perspectiva centrada apenas no acesso, correção ou eliminação de registros para uma dimensão procedimental mais complexa: a contestabilidade da decisão automatizada.

Em muitos casos, o indivíduo afetado não desconhece apenas quais dados foram utilizados, mas sobretudo como esses dados foram ponderados, quais variáveis tiveram relevância decisória, que inferências foram extraídas, que proxies eventualmente substituíram categorias sensíveis, que parâmetros técnicos orientaram o resultado e se havia registros mínimos capazes de permitir controle posterior. A opacidade algorítmica, nesse contexto, não é apenas limitação cognitiva decorrente da complexidade técnica. Ela pode operar como assimetria processual estrutural, pois impede que o afetado formule impugnação qualificada contra uma decisão cujo fundamento permanece inacessível.

A literatura sobre regulação por arquitetura técnica já demonstrou que o código não é artefato neutro. Ao organizar possibilidades, restringir condutas e parametrizar escolhas, a arquitetura computacional produz efeitos normativos relevantes, ainda que não se apresente sob a forma clássica da lei (LESSIG, 2006). Essa intuição ganha densidade específica quando sistemas de inteligência artificial e aprendizado de máquina deixam de ser instrumentos auxiliares e passam a influenciar decisões que incidem sobre direitos fundamentais.

Citron (2008) identifica, nesse ponto, uma crise do devido processo diante de sistemas automatizados que combinam funções decisórias individualizadas com regras incorporadas ao software, sem se submeterem integralmente às garantias tradicionais de publicidade, motivação, participação e revisão. Pasquale (2015), por sua vez, descreve a assimetria informacional das

sociedades de caixa-preta, nas quais indivíduos se tornam crescentemente transparentes para instituições públicas e privadas, enquanto os critérios que os classificam permanecem protegidos por segredo, complexidade ou opacidade deliberada.

O direito brasileiro dispõe de instrumentos relevantes para enfrentar parte desse problema, mas sua resposta ainda é fragmentária. O habeas data, previsto no art. 5º, LXXII, da Constituição e disciplinado pela Lei nº 9.507/1997, foi concebido para assegurar o conhecimento e a retificação de informações pessoais constantes de registros ou bancos de dados de entidades governamentais ou de caráter público. Sua importância histórica é incontestável, especialmente no processo de reconstrução democrática e na formação de uma cultura jurídica de proteção informacional.

Contudo, sua estrutura dogmática foi moldada para lidar com o desconhecimento ou a inexatidão de informações pessoais registradas. A decisão automatizada contemporânea pode ser lesiva ainda que o dado de entrada seja formalmente verdadeiro. O vício pode estar no tratamento, na inferência, na modelagem, na ponderação estatística, na ausência de documentação técnica, na inexistência de logs auditáveis ou na revisão humana meramente aparente.

A Lei Geral de Proteção de Dados avançou ao reconhecer, no art. 20, o direito do titular de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive decisões destinadas à definição de perfil pessoal, profissional, de consumo, de crédito ou de aspectos da personalidade. Esse dispositivo tem relevância normativa expressiva, pois desloca a proteção de dados para além do simples controle cadastral e reconhece que a automação decisória pode produzir efeitos juridicamente relevantes.

Ainda assim, o art. 20 não resolve integralmente o problema. Ele não estabelece, por si só, uma arquitetura processual robusta para preservar registros técnicos, delimitar o alcance da explicação, compatibilizar auditabilidade e segredo industrial, estruturar perícia algorítmica, garantir contraditório técnico, permitir acesso controlado à lógica decisória ou definir provimentos jurisdicionais adequados quando a opacidade inviabiliza a defesa.

Nenhum dos instrumentos processuais hoje existentes, isoladamente considerado, oferece gramática procedimental específica para decisões automatizadas de impacto relevante. Em regra, ou se exige prova pré-constituída que o afetado não possui, ou se trata a controvérsia como simples acesso documental, ou se reduz a explicação a informação genérica, ou se admite a

invocação abstrata de segredo empresarial como barreira quase absoluta ao escrutínio. O resultado é um déficit de contestabilidade: há decisão, há impacto e há lesão potencial, mas não há condições materiais mínimas para reconstruir juridicamente a razão decisória.

É nesse ponto que se situa o problema de pesquisa deste artigo: em que medida os instrumentos processuais e informacionais disponíveis no direito brasileiro são suficientes para assegurar a contestabilidade de decisões automatizadas quando a lesão a direitos fundamentais decorre não apenas dos dados utilizados, mas da lógica de processamento, dos critérios inferenciais e dos registros técnicos que estruturam o ato decisório?

A questão exige distinguir três camadas analíticas. A primeira corresponde ao input, isto é, aos dados pessoais e contextuais utilizados pelo sistema. A segunda corresponde ao processing, isto é, à lógica de tratamento, aos pesos, inferências, regras, métricas, parâmetros, correlações e modelos que transformam os dados em resultado. A terceira corresponde ao output, isto é, à decisão comunicada ao afetado. Essa decomposição não é adotada como método autônomo, mas como ferramenta analítica para localizar o ponto de opacidade juridicamente relevante.

A hipótese de trabalho é que decisões automatizadas de impacto relevante somente atendem ao devido processo quando oferecem condições mínimas de contestabilidade algorítmica. Tais condições não exigem transparência absoluta, abertura irrestrita do código-fonte ou eliminação do segredo industrial, mas exigem auditabilidade funcional suficiente para que o afetado, o perito, o regulador ou o magistrado possam verificar, em ambiente juridicamente controlado, se a decisão observou parâmetros mínimos de legalidade, não discriminação, coerência, proporcionalidade, documentação, rastreabilidade e revisão humana substancial.

A contestabilidade algorítmica, portanto, não equivale ao direito de conhecer todos os detalhes técnicos de um sistema proprietário. Corresponde ao direito de obter explicação individualizada e funcionalmente útil, preservação de registros técnicos, acesso controlado aos critérios decisórios relevantes, identificação de variáveis sensíveis ou proxies discriminatórios, possibilidade de perícia sigilosa, contraditório técnico e eventual correção, suspensão ou invalidação do ato automatizado.

Neste artigo, a expressão Habeas Code não designa uma ação constitucional autônoma já positivada, mas uma categoria dogmático-procedimental destinada a organizar a tutela mandamental de auditabilidade algorítmica a partir de garantias e instrumentos já existentes no ordenamento brasileiro. A escolha terminológica preserva a força heurística da expressão, mas

evita a conclusão precipitada de que o sistema constitucional brasileiro já teria incorporado novo remédio constitucional nominado.

O Habeas Code é aqui compreendido como modelo de tutela voltado a fazer comparecer em juízo a lógica decisória relevante, não necessariamente o código-fonte integral. Seu núcleo não é a curiosidade técnica sobre o funcionamento interno de sistemas computacionais, mas a exigência jurídica de que nenhuma decisão automatizada relevante permaneça imune à explicação funcional, à auditoria proporcional e ao contraditório substancial.

O objetivo geral da pesquisa é construir uma proposta dogmático-procedimental de tutela mandamental de auditabilidade algorítmica, denominada Habeas Code, destinada a enfrentar a insuficiência do habeas data e do direito genérico à revisão de decisões automatizadas, mediante um modelo de acesso funcional, proporcional e judicialmente controlado à lógica decisória de sistemas algorítmicos relevantes.

Como objetivos específicos, pretende-se: demonstrar que decisões automatizadas podem gerar déficit de contestabilidade quando sua razão decisória permanece oculta na camada de processamento; examinar os limites do habeas data, do art. 20 da LGPD, do mandado de segurança e dos instrumentos probatórios tradicionais diante da opacidade algorítmica; redefinir o Habeas Code como categoria dogmático-procedimental de tutela mandamental de auditabilidade, e não como novo remédio constitucional autônomo já existente; propor uma arquitetura mínima para sua aplicação; e integrar essa proposta ao devido processo algorítmico, especialmente nos planos da explicabilidade, documentação, logs, supervisão humana, governança de IA e conformidade by design.

Metodologicamente, o artigo adota abordagem jurídico-dogmática e jurídico-propositiva, com pesquisa qualitativa, revisão bibliográfica qualificada e análise normativa. A investigação não pretende demonstrar empiricamente a frequência de erros algorítmicos em determinado setor, nem formular modelo técnico universal de interpretação, mas identificar uma lacuna de tutela, reorganizar instrumentos existentes e propor critérios processuais para decisões automatizadas de impacto relevante.

A matriz teórica articula três blocos. O primeiro bloco discute código, arquitetura e poder algorítmico, com apoio em Lessig (2006), Pasquale (2015), Hildebrandt (2015), Zuboff (2019), O'Neil (2016) e Barocas e Selbst (2016). O segundo examina explicabilidade, accountability, auditabilidade e limites da transparência, dialogando com Citron, Mittelstadt, Floridi e Wachter.

O terceiro reconecta proteção de dados, contraditório substancial e tutela jurisdicional adequada, com atenção ao direito brasileiro e à contribuição de Doneda para a compreensão da proteção de dados como tutela dinâmica da pessoa na sociedade informacional.

1. DECISÕES AUTOMATIZADAS, CÓDIGO NORMATIVO E DÉFICIT DE CONTESTABILIDADE

A expansão das decisões automatizadas desloca o problema jurídico da tecnologia do plano meramente instrumental para o plano institucional. Sistemas algorítmicos não apenas executam comandos previamente definidos por agentes humanos, mas classificam riscos, priorizam condutas e produzem resultados que condicionam o exercício de direitos.

Essa constatação não autoriza afirmar que o algoritmo substitui o Direito, nem que todo sistema automatizado exerça função normativa em sentido estrito. Contudo, quando uma arquitetura técnica passa a estruturar as condições de acesso a bens, serviços ou oportunidades sociais, ela deixa de ser simples meio operacional e passa a integrar o ambiente de produção prática de efeitos jurídicos.

Ao afirmar que o código regula, Lessig (2006) não pretende equiparar software e lei em todos os aspectos, mas demonstrar que a arquitetura digital condiciona comportamentos por meio da própria estrutura técnica do ambiente. A regulação não opera apenas por comandos jurídicos, sanções estatais ou normas sociais, mas também por desenhos técnicos que tornam certas condutas possíveis e outras mais difíceis ou inviáveis.

No espaço digital, portanto, a arquitetura deixa de ser cenário neutro e passa a constituir modalidade de ordenação. Em termos jurídicos, isso significa que a análise das decisões automatizadas não pode se limitar ao exame formal da norma aplicável ou do ato decisório final. Ela precisa compreender a mediação técnica que transforma dados em resultados juridicamente relevantes.

Ainda assim, a afirmação de que code is law não deve ser convertida em fórmula absoluta, sob pena de obscurecer diferenças essenciais entre código computacional e Direito. A lei está submetida a procedimentos de criação, publicidade, validade, interpretação, controle institucional e justificação pública. O código, por sua vez, pode ser produzido por agentes privados, protegido por segredo industrial, incorporado a infraestruturas fechadas e aplicado em escala sem que seus critérios sejam visíveis ao afetado.

Justamente por isso, o problema não é reconhecer ao código uma natureza jurídica autônoma, mas identificar quando sua função prática se torna juridicamente relevante a ponto de exigir controle, explicação e contestabilidade. No campo das decisões automatizadas, a classificação de um indivíduo como candidato incompatível com determinada vaga, por exemplo, pode decorrer de operações técnicas não acessíveis ao sujeito afetado. Nesses casos, a lesão potencial não se encontra apenas no resultado desfavorável, mas na impossibilidade de reconstruir o caminho decisório.

O Direito tradicionalmente admite que decisões restritivas sejam impugnadas porque pressupõe alguma forma de motivação, documentação ou acesso à razão do ato. A decisão automatizada opaca rompe essa racionalidade ao comunicar ao interessado o output, mas não os elementos mínimos para discutir o processamento que o produziu.

A imagem da caixa-preta, trabalhada por Frank Pasquale (2015), descreve uma assimetria na qual indivíduos, consumidores, trabalhadores e usuários tornam-se crescentemente transparentes para sistemas institucionais, enquanto os critérios de classificação empregados por esses sistemas permanecem invisíveis, seja por segredo, complexidade, ofuscação ou desenho deliberadamente inacessível.

A pessoa afetada por uma decisão automatizada não sofre apenas a assimetria comum entre cidadão e administração, consumidor e fornecedor, trabalhador e empresa ou usuário e plataforma. Enfrenta uma assimetria cognitiva qualificada, pois a razão decisória está inscrita em camadas técnicas que não se reduzem ao dado utilizado nem ao resultado comunicado.

A informação juridicamente relevante pode estar no desenho do modelo, na definição da variável-alvo, na seleção de atributos, na base de treinamento, na ponderação de variáveis, nas correlações inferidas, na calibragem de risco, nos limiares de corte, nos registros de execução ou nas políticas internas de revisão humana. A opacidade, assim, não é simples déficit de transparência. É obstáculo à formação de uma pretensão impugnativa minimamente racional.

Danielle Citron (2008) demonstra que sistemas automatizados podem combinar, em uma mesma arquitetura técnica, elementos de adjudicação individual e de formulação normativa, sem se submeterem integralmente às garantias de uma nem de outra. A decisão automatizada aplica critérios a casos concretos, mas esses critérios podem ter sido incorporados ao software sem participação, publicidade, documentação ou controle adequados.

Além disso, a audiência ou revisão posterior tende a perder substância quando o agente humano presume a infalibilidade do sistema ou não possui meios técnicos para compreender sua lógica. O contraditório substancial não se satisfaz com a simples comunicação do resultado, nem com a abertura de um canal formal de reclamação. Ele exige condições materiais de contestação, o que inclui explicação funcionalmente útil, preservação de registros, documentação mínima do sistema, possibilidade de perícia e capacidade de identificar se a decisão resultou de erro factual, regra mal traduzida, inferência discriminatória, proxy indevido, falha de treinamento, inconsistência estatística ou ausência de revisão humana efetiva. Sem esses elementos, a impugnação degenera em ato ritual.

A retórica da neutralidade matemática também não se sustenta. Conforme descreve Cathy O'Neil, modelos matemáticos nocivos são capazes de ampliar desigualdades sob aparência de objetividade. O ponto central não é rejeitar modelos quantitativos, mas recusar o pressuposto de que a mediação estatística elimina juízos de valor. Modelos envolvem escolhas sobre o que medir, quais dados considerar, quais variáveis incluir ou excluir, que margens de erro tolerar e que custos sociais aceitar.

Barocas e Selbst (2016) demonstram esse problema no campo do impacto discriminatório do Big Data. A discriminação algorítmica frequentemente não decorre de intenção discriminatória explícita, mas de propriedades emergentes do uso do sistema, o que torna especialmente difícil provar e explicar o dano em juízo. A ausência de propósito discriminatório não elimina a lesão; apenas desloca a dificuldade probatória para a estrutura técnica e estatística do modelo.

A literatura ética sobre algoritmos reforça essa distinção ao separar problemas epistêmicos e normativos. Um sistema pode produzir evidências inconclusivas, inescrutáveis ou enviesadas, assim como pode gerar resultados injustos, discriminatórios ou transformadores das condições de autonomia. A opacidade compromete controle, monitoramento e correção, mas a transparência também não deve ser tratada como solução universal. A mera disponibilidade de informação não basta. A informação deve ser acessível, compreensível e útil para a finalidade de contestação. Por isso, a resposta jurídica não deve exigir transparência total, mas auditabilidade proporcional, funcional e orientada ao problema decisório concreto.

A distinção entre input, processing e output permite localizar com maior precisão o déficit de contestabilidade. A camada de input corresponde aos dados utilizados: informações pessoais

declaradas, dados observados, registros comportamentais, metadados, dados inferidos ou bases externas agregadas. Essa camada é tradicionalmente mais próxima da proteção de dados pessoais e do habeas data, pois envolve conhecimento, correção, atualização, eliminação ou contextualização de informações.

A camada de output corresponde ao resultado, seja ele uma negativa de crédito, bloqueio de conta, descredenciamento ou qualquer outro efeito individual ou coletivo. Essa camada é a mais visível, pois se manifesta como decisão comunicada ou consequência prática percebida pelo afetado. Muitos litígios se concentram nesse nível, buscando anular o ato, obter indenização, restaurar acesso, suspender bloqueio ou corrigir uma classificação. Todavia, a impugnação centrada apenas no output pode ser insuficiente quando o vício decisório não é aparente no resultado, mas na lógica que o produziu.

A camada decisiva para o Habeas Code é a de processing. Nela se situam regras de transformação, critérios inferenciais, pesos, limiares, correlações, modelos, métricas, parâmetros de otimização, escolhas de treinamento, variáveis proxy e registros de execução. É nessa camada que dados formalmente corretos podem gerar decisões materialmente injustificadas. O processing, portanto, funciona como motivação interna do ato automatizado.

Essa motivação interna não deve ser confundida com a motivação jurídica formal exigida em atos administrativos ou decisões judiciais. Trata-se de categoria analítica destinada a indicar o conjunto de operações técnicas que explica por que determinado input gerou determinado output. Nas decisões humanas, a motivação juridicamente relevante aparece em linguagem natural, ainda que possa ser incompleta, contraditória ou insuficiente. Em decisões automatizadas, a razão decisória pode estar distribuída entre modelo, dados, parâmetros, documentação e logs.

Exigir motivação em ambiente algorítmico não significa exigir que o sistema pense ou fundamente como um juiz. Significa exigir documentação funcional suficiente para permitir controle externo da cadeia decisória. A ausência dessa documentação produz problema de validade procedimental. Se o afetado não consegue saber quais elementos foram decisivos, a decisão automatizada torna-se praticamente incontestável. A forma externa do devido processo pode estar preservada, mas sua substância desaparece quando não se pode discutir a razão do ato.

Esse déficit não se resolve com a exigência abstrata de abertura do algoritmo, que pode ser desnecessária, desproporcional ou tecnicamente insuficiente. Em muitos sistemas, o código não revela sozinho os dados de treinamento, os pesos efetivamente aprendidos, o comportamento

em produção, as atualizações realizadas, os limiares decisórios ou os efeitos agregados sobre grupos vulneráveis.

Além disso, há interesses legítimos relacionados a segredo empresarial, segurança, privacidade de terceiros e prevenção de manipulação do sistema. A resposta juridicamente adequada reside na explicabilidade funcional, compreendida como auditabilidade controlada capaz de possibilitar controle jurisdicional das condições de legalidade e contestabilidade.

A explicabilidade funcional não exige que todo destinatário domine a arquitetura matemática do modelo. Exige, porém, que se possa saber quais categorias de dados foram utilizadas, quais fatores tiveram peso relevante, que tipo de inferência foi realizada, se houve uso de atributos sensíveis ou proxies, qual política de revisão humana foi aplicada, que registros técnicos existem e quais alternativas poderiam modificar o resultado em casos juridicamente pertinentes.

A noção de contestabilidade algorítmica articula três exigências. A primeira, cognitiva, requer que o afetado tenha acesso a informações suficientes para compreender a decisão em termos úteis. A segunda, probatória, exige registros, documentação e meios técnicos que permitam verificar a regularidade do processamento. A terceira, procedimental, demanda instância capaz de revisar, corrigir, suspender ou invalidar a decisão quando a lógica decisória se mostrar inadequada. A ausência de qualquer dessas dimensões compromete o devido processo.

Por isso, o devido processo em ambiente automatizado não pode limitar-se à comunicação do output. Ele exige condições materiais de contestação da lógica decisória.

2. *HABEAS DATA*, LGPD E A INSUFICIÊNCIA DA TUTELA PROCESSUAL ORDINÁRIA

A constatação de que decisões automatizadas podem produzir déficit de contestabilidade não conduz, por si só, à necessidade de criação imediata de novo remédio constitucional autônomo. Antes, impõe a tarefa dogmática de verificar se os instrumentos já disponíveis no ordenamento brasileiro são capazes de oferecer resposta suficiente quando a lesão não decorre apenas do dado utilizado, mas da lógica de processamento que transforma dados em consequência jurídica ou socialmente relevante.

O ponto de partida dessa análise deve ser o habeas data. A Constituição de 1988 prevê sua concessão para assegurar o conhecimento de informações relativas à pessoa do impetrante,

constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, bem como para a retificação de dados quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Essa estrutura, porém, revela limite importante diante das decisões automatizadas contemporâneas. O habeas data foi dogmaticamente desenhado para enfrentar a opacidade do registro, não necessariamente a opacidade da inferência. Seu objeto típico é a informação relativa à pessoa do impetrante. A decisão automatizada, contudo, pode produzir lesão mesmo quando o dado de entrada é verdadeiro, atualizado e licitamente coletado. O habeas data acessa bem o input, mas pouco alcança a etapa de processing.

Longe de ser obsoleto, o habeas data em matéria algorítmica pode cumprir funções relevantes, como permitir o conhecimento de dados pessoais utilizados por sistemas de classificação ou viabilizar a correção de informações inexatas que alimentam modelos. Entretanto, quando a pretensão envolve saber por que determinada combinação de variáveis produziu determinado resultado, sua estrutura tende a mostrar insuficiência.

A doutrina brasileira de proteção de dados, especialmente a partir de Danilo Doneda (2020), contribui para compreender esse deslocamento. A proteção de dados não se confunde com simples atualização do direito à privacidade como reserva ou isolamento. Ela se relaciona ao controle jurídico do tratamento informacional em uma sociedade na qual dados pessoais se tornam infraestrutura de decisões econômicas, administrativas e sociais.

A Lei Geral de Proteção de Dados avança precisamente ao reconhecer que o titular tem direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. Ainda assim, o art. 20 não resolve integralmente o problema descrito. Sua formulação reconhece um direito material-informacional, mas não estrutura, com suficiente densidade, o procedimento de auditabilidade contraditória. Em termos dogmáticos, a LGPD reconhece a necessidade de revisão, mas não entrega, por si só, uma arquitetura jurisdicional completa de contestação.

A insuficiência é agravada pela ambiguidade prática do que significa revisar uma decisão automatizada. Em leitura minimalista, bastaria ao controlador reexaminar o resultado e confirmar sua correção, fornecendo explicação genérica sobre categorias de dados utilizadas. Essa leitura esvaziaria a garantia. A revisão juridicamente relevante deve permitir verificar se a decisão foi

produzida por tratamento lícito, adequado, necessário, não discriminatório, documentado e compatível com a finalidade informada.

Por isso, a revisão não pode ser apenas ato interno de confirmação. Ela deve ser tecnicamente informada, capaz de reconstruir a relação entre dados, critérios, inferências e resultado, e deve admitir controle externo quando a resposta administrativa for insuficiente.

A literatura europeia sobre direito à explicação alerta contra leituras excessivamente fortes ou fracas da transparência algorítmica. Wachter, Mittelstadt e Russell (2018) sustentam que explicações úteis podem, em certos contextos, ser oferecidas sem abertura integral da caixa-preta, por meio de informações capazes de ajudar o titular a compreender, contestar ou alterar decisões futuras.

Essa contribuição é relevante para o direito brasileiro porque evita reduzir a discussão a uma alternativa binária entre segredo absoluto e abertura total do código-fonte. O que se deve exigir é explicabilidade funcional suficiente para a finalidade jurídica em questão. Em alguns casos, bastará indicar fatores decisivos e fontes dos dados. Em outros, será necessário preservar logs, permitir auditoria independente, realizar testes de vieses ou franquear acesso pericial controlado a documentos técnicos.

O mandado de segurança também apresenta utilidade limitada. Em situações nas quais uma decisão automatizada administrativa produz efeito imediato sobre direito individual e a ilegalidade é demonstrável por prova documental pré-constituída, ele pode ser adequado. O problema é que a opacidade algorítmica frequentemente impede a própria constituição da prova prévia. A exigência de direito líquido e certo torna-se, nesse contexto, paradoxal: a pessoa precisa de acesso à lógica decisória para demonstrar a ilegalidade, mas não consegue obter esse acesso porque ainda não demonstrou suficientemente a ilegalidade.

Esse limite não torna o mandado de segurança irrelevante para o Habeas Code. Isoladamente, porém, ele não oferece solução suficiente para a camada de processamento quando a liquidez do direito depende de prova técnica ainda inacessível.

Outros instrumentos processuais, como a produção antecipada de prova e a exibição documental, também não esgotam a tutela necessária. São meios probatórios, não uma gramática completa de auditabilidade. Podem permitir a obtenção de informação, mas não necessariamente impõem explicação funcional, revisão substancial ou correção do ato automatizado. Por isso, a objeção de que o Habeas Code seria apenas uma produção antecipada de prova é inadequada. A

prova pode ser um de seus instrumentos, mas a categoria proposta é mais ampla, pois articula informação, preservação, explicação, perícia, revisão e provimento mandamental em torno da contestabilidade algorítmica.

A ausência de instrumento que componha essa gramática compreensiva de auditabilidade compromete a efetividade de respostas jurídicas já existentes. A Súmula 550 do STJ, por exemplo, reconhece a licitude do escore de crédito como método estatístico de avaliação de risco que não constitui banco de dados e dispensa consentimento do consumidor, mas assegura o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no cálculo.

Esse enunciado é importante porque demonstra que o problema não é apenas a existência de informações pessoais, mas sua valoração em método estatístico. No entanto, sua própria formulação revela o limite da resposta tradicional: esclarecer informações pessoais valoradas e fontes de dados é necessário, mas pode não ser suficiente para compreender pesos, inferências, proxies, limiares, segmentações e critérios de calibragem que determinam o resultado.

Outro limite dos instrumentos atuais está na proteção do segredo industrial. Controladores e fornecedores de tecnologia frequentemente invocam confidencialidade, propriedade intelectual, segurança do sistema e risco de manipulação como razões para não fornecer detalhes sobre modelos algorítmicos. Essa sustentação é plausível, mas deve ser ponderada. A abertura irrestrita de sistemas pode expor segredos legítimos, dados de terceiros, vulnerabilidades de segurança ou permitir manipulação estratégica dos critérios decisórios. Todavia, a proteção do segredo não pode funcionar como imunidade contra controle jurídico.

A questão dogmática não é escolher entre segredo e auditabilidade, mas construir mecanismos que permitam auditabilidade sob sigilo. Essa compatibilização exige instrumentos processuais mais refinados: segredo de justiça, delimitação do objeto pericial, termos de confidencialidade, acesso restrito a peritos, apresentação de documentação técnica em camadas, testes em ambiente controlado, anonimização de dados de terceiros, preservação de logs e eventual sandbox judicial.

Nessa arquitetura, o juiz não precisa tornar público o código-fonte nem expor integralmente tecnologia proprietária. Pode, porém, determinar que a parte responsável demonstre, perante o juízo e sob controle técnico, que a decisão observou requisitos mínimos de

legalidade, não discriminação, documentação e coerência. O segredo industrial limita a forma de acesso, mas não elimina o dever de justificação funcional.

Também é necessário reconhecer que a explicabilidade técnica nem sempre será plenamente possível. Sistemas complexos de aprendizado de máquina podem ser difíceis de interpretar, especialmente quando envolvem modelos de alta dimensionalidade, atualização contínua, dados massivos e interações não lineares. Essa limitação deve ser incorporada ao Direito, não ignorada. O objetivo jurídico não deve ser exigir transparência impossível, mas estabelecer graus mínimos de explicabilidade funcional proporcionais ao impacto da decisão e ao risco de lesão.

Aqui se revela diferença central entre explicação técnica e explicação jurídica. A explicação técnica busca tornar compreensível o funcionamento de um modelo em termos computacionais, estatísticos ou matemáticos. A explicação jurídica busca fornecer razões suficientes para avaliar se uma decisão que afeta direitos é lícita, proporcional, não discriminatória, coerente e contestável.

Em certos casos, a explicação jurídica pode prescindir da compreensão integral do modelo, desde que existam informações suficientes sobre fatores relevantes, dados utilizados, critérios de decisão, revisão humana e testes de impacto. Em outros, especialmente quando houver suspeita de discriminação, erro sistêmico ou violação massiva, a explicação jurídica exigirá auditoria técnica mais intensa.

Por fim, é preciso notar que, em litígios tradicionais, a parte autora deve narrar fatos, indicar fundamentos e produzir prova mínima de sua pretensão. Em decisões automatizadas opacas, porém, os elementos centrais da prova estão sob controle do réu ou de terceiro fornecedor tecnológico. Exigir da vítima prova detalhada da ilegalidade algorítmica antes de permitir acesso a documentação técnica significa impor ônus impossível ou excessivo.

Assim, a dogmática processual deve reconhecer situações de assimetria informacional qualificada, nas quais a parte que controla o sistema assume deveres reforçados de documentação, preservação e explicação. A resposta jurídica contemporânea não pode permanecer presa às formas procedimentais clássicas. É necessário reconstruir garantias processuais em chave técnica (CITRON, 2008).

Não se trata de ausência completa de normas, mas de ausência de coordenação dogmática entre normas existentes. Os instrumentos jurídico-processuais disponíveis operam de modo

fragmentado. Falta uma categoria que organize sua incidência quando o núcleo da lesão está na camada de processamento algorítmico.

A noção de Habeas Code surge precisamente para preencher essa lacuna. Não como ação constitucional autônoma já positivada, mas como categoria de organização da tutela mandamental de auditabilidade algorítmica. Seu papel é reunir, sob uma gramática comum, deveres de explicação funcional, preservação de registros, acesso controlado à lógica decisória, perícia técnica, sigilo processual, contraditório substancial, revisão humana efetiva e provimentos corretivos.

Em vez de substituir as ferramentas clássicas, o Habeas Code opera como racionalidade procedimental capaz de orientar sua utilização coordenada diante da opacidade algorítmica. O direito brasileiro possui instrumentos relevantes, mas ainda carece de uma gramática dogmática específica para organizar a tutela de auditabilidade. Daí a necessidade de formular o Habeas Code como categoria dogmático-procedimental voltada à contestabilidade de decisões automatizadas relevantes.

3. *HABEAS CODE* COMO TUTELA MANDAMENTAL DE AUDITABILIDADE ALGORÍTMICA

Habeas Code designa, neste artigo, uma categoria dogmático-procedimental de tutela mandamental destinada a assegurar auditabilidade funcional de decisões automatizadas relevantes. Não se trata de afirmar a existência de nova ação constitucional autônoma, mas de sistematizar, a partir de garantias já existentes, um modelo de acesso controlado à lógica decisória algorítmica, com o objetivo de tornar contestáveis decisões automatizadas cuja razão decisória se encontre oculta na camada de processamento.

A escolha por uma categoria dogmático-procedimental, e não por um novo remédio constitucional imediatamente autônomo, é decisiva para preservar a consistência do argumento. O constitucionalismo brasileiro já dispõe de garantias voltadas à liberdade, à informação, à legalidade, ao contraditório, à ampla defesa, à proteção de dados pessoais e ao acesso à jurisdição. O problema não é a ausência absoluta de instrumentos, mas a falta de uma racionalidade procedimental capaz de coordená-los diante da opacidade algorítmica.

Seu pressuposto material é a existência de decisão automatizada relevante. Não basta a presença de tecnologia no processo decisório, nem a utilização ordinária de softwares

administrativos, sistemas de gestão ou ferramentas estatísticas auxiliares. A categoria se justifica quando há impacto concreto ou potencialmente relevante sobre direitos, interesses juridicamente protegidos, posições sociais sensíveis ou exposição a tratamento discriminatório. A intensidade do controle deve variar conforme o grau de impacto, a vulnerabilidade do afetado, a assimetria informacional e o risco de lesão coletiva.

O objeto do Habeas Code não é, necessariamente, o código-fonte integral. Em alguns casos, o código-fonte pode ser insuficiente para explicar a decisão; em outros, sua abertura integral pode ser desproporcional, expor segredo empresarial legítimo, comprometer a segurança do sistema ou afetar dados de terceiros. A tutela de auditabilidade deve incidir sobre a lógica decisória relevante, compreendida como o conjunto de elementos técnicos, documentais e procedimentais necessários para reconstruir por que determinado input gerou determinado output.

Não se exige, portanto, transparência total. Exige-se rastreabilidade cognitiva suficiente, isto é, a possibilidade de reconstruir, em grau adequado de precisão, a cadeia técnica e institucional que produziu a decisão. Essa rastreabilidade deve ser compreendida como requisito procedimental, não como metáfora retórica. Ela envolve três planos: o informacional, relativo aos dados e variáveis considerados; o técnico, relativo ao modelo, aos critérios e aos registros de processamento; e o institucional, relativo à governança, à revisão humana e à responsabilidade pelo resultado.

Sem esses três planos, a explicação tende a ser insuficiente. Um controlador pode informar quais dados foram utilizados, mas ocultar pesos e limiares. Pode descrever genericamente o modelo, mas não preservar logs. Pode afirmar que houve revisão humana, mas não demonstrar que essa revisão teve poder real de modificação. O Habeas Code serve precisamente para impedir que a contestação seja neutralizada por explicações formais ou incompletas.

A legitimidade ativa deve ser compreendida de modo funcional. No plano individual, cabe ao sujeito diretamente afetado por decisão automatizada relevante buscar a tutela de auditabilidade. No plano coletivo, devem poder atuar os legitimados coletivos quando a opacidade atingir grupos, categorias de usuários, consumidores, trabalhadores, beneficiários de políticas públicas ou segmentos vulneráveis. Essa dimensão é necessária porque danos algorítmicos podem não se apresentar como violações isoladas, mas como padrões sistêmicos de

classificação, exclusão ou discriminação. A tutela individual revela a lesão situada; a tutela coletiva permite examinar a arquitetura decisória em escala.

A legitimidade passiva deve alcançar quem controla a decisão, ainda que não tenha desenvolvido tecnicamente o sistema. Em ambientes algorítmicos, é comum a fragmentação entre desenvolvedor, fornecedor, integrador, contratante, operador e instituição que aplica o resultado. Essa fragmentação não pode servir como mecanismo de evasão de responsabilidade informacional. A entidade que utiliza a decisão automatizada para produzir efeitos sobre terceiros deve demonstrar sua auditabilidade mínima ou, ao menos, viabilizar o acesso judicial aos elementos necessários junto ao fornecedor. A terceirização tecnológica não pode gerar terceirização do devido processo.

No plano da admissibilidade, o pedido deve demonstrar quatro elementos mínimos: existência de decisão automatizada ou substancialmente automatizada; impacto relevante sobre direito ou interesse juridicamente protegido; insuficiência da explicação previamente fornecida, quando houver; e plausibilidade de que a opacidade da camada de processamento impede a contestação adequada.

Não se deve exigir prova plena da ilegalidade algorítmica no momento inicial, pois essa prova muitas vezes depende justamente da auditabilidade requerida. O ônus inicial do requerente é indicar a opacidade relevante e o impacto decisório. O ônus subsequente recai sobre o controlador, que deverá demonstrar, de forma documentada, a regularidade funcional do processo decisório.

Essa distribuição do ônus informacional evita o paradoxo da prova impossível. Em decisões automatizadas opacas, exigir que o afetado demonstre previamente a ilegalidade do algoritmo antes de obter acesso à documentação técnica equivale a negar a tutela. Por isso, a dogmática do Habeas Code deve operar com deveres reforçados de documentação e cooperação processual. O controlador não precisa revelar tudo publicamente, mas deve demonstrar ao juízo, sob regime adequado de sigilo, que a decisão pode ser auditada e contestada.

O segredo industrial constitui interesse juridicamente relevante para a proteção da inovação, da segurança, da competitividade e da integridade dos sistemas. Todavia, não pode ser convertido em barreira absoluta contra direitos fundamentais, devido processo, proteção de dados e não discriminação. A solução não é negar o segredo, mas processualizá-lo.

Sigilo judicial, confidencialidade pericial, delimitação do escopo de acesso, termos de responsabilidade, segregação de dados de terceiros, relatórios técnicos em camadas e ambientes controlados de análise permitem compatibilizar auditabilidade e proteção de informação sensível. Wachter, Mittelstadt e Russell (2018) observam que explicações úteis podem servir à compreensão, à contestação e à alteração de decisões sem exigir, necessariamente, abertura integral da caixa-preta. Essa compreensão reforça a ideia de explicabilidade funcional e finalisticamente delimitada.

É nesse ponto que se justifica a ideia de sandbox judicial. A expressão é empregada como referência a um ambiente processual controlado no qual elementos técnicos do sistema podem ser examinados por peritos, assistentes técnicos, magistrado ou órgão regulador cooperante, sob regras de confidencialidade e delimitação de finalidade. O sandbox judicial não é laboratório de inovação regulatória, nem autorização para o juiz redesenhar sistemas algorítmicos. Trata-se de técnica processual de contenção de risco informacional.

Esse ambiente permite que documentos, bases, logs, modelos, parâmetros ou simulações sejam submetidos a verificação controlada, sem exposição pública desnecessária e sem transformar segredo industrial em zona de imunidade. A perícia algorítmica, por sua vez, não deve ser concebida como simples perícia de informática. Seu objeto não é apenas verificar integridade de arquivos ou funcionamento de software, mas reconstruir a cadeia decisória de um sistema automatizado em relação a determinado caso ou padrão de casos.

Essa perícia precisa ser juridicamente orientada. O perito não substitui o juiz na qualificação da ilicitude, nem o juiz substitui o perito na compreensão técnica. A função pericial é oferecer inteligibilidade técnica suficiente para a decisão jurídica. Isso exige quesitos adequados, delimitação do objeto, preservação da cadeia de custódia informacional, documentação das versões do modelo, indicação das limitações técnicas da análise e explicitação do grau de confiabilidade das conclusões. A perícia algorítmica não deve prometer certeza incontestável, mas reduzir a opacidade a nível compatível com decisão jurisdicional motivada.

O contraditório técnico é outro elemento essencial. Não basta que o juiz receba relatório técnico unilateral produzido pelo controlador ou por auditoria privada contratada pela própria plataforma. A parte afetada deve poder formular quesitos, impugnar premissas, indicar assistente técnico, discutir a suficiência da documentação, questionar a metodologia de teste e requerer complementação quando a explicação permanecer inconclusiva. O contraditório, nesse campo,

não se limita à manifestação jurídica sobre documentos; envolve capacidade efetiva de disputar a interpretação técnica da decisão automatizada. Sem contraditório técnico, a auditabilidade pode converter-se em validação pericial unilateral da opacidade.

A revisão humana substancial deve integrar a arquitetura do Habeas Code. A existência formal de intervenção humana não basta para afastar a incidência da tutela. Se o agente humano não compreende a lógica do sistema, não possui acesso aos elementos relevantes, não tem poder para alterar o resultado ou apenas confirma automaticamente a saída algorítmica, há revisão meramente aparente. A revisão substancial exige competência decisória real, acesso a informações suficientes, consideração das circunstâncias individuais do caso e possibilidade de afastar ou corrigir o resultado automatizado.

Hildebrandt (2020) observa que decisões baseadas em inferências de machine learning tensionam a explicabilidade do processo decisório, a justificação da decisão e sua contestabilidade, especialmente quando a participação humana é incapaz de explicar ou controlar o resultado. No modelo proposto, a tutela mandamental de auditabilidade pode produzir diferentes provimentos, graduados conforme a necessidade do caso.

Entre os provimentos cautelares, admite-se tutela de explicação, consistente na apresentação de relato individualizado, funcional e inteligível sobre os fatores decisivos da decisão, e tutela de conservação, destinada à preservação de logs, versões do modelo, registros de execução, documentos técnicos e demais elementos necessários à futura perícia.

Entre os provimentos instrutórios, é possível determinar a exibição controlada de documentos ou elementos técnicos em juízo, sob sigilo, ou a realização de auditoria, perícia, inspeção técnica, teste de viés ou avaliação independente. Entre os provimentos finais, podem ser deferidas ordem de revisão humana substancial, com fundamentação adequada; medidas corretivas, como retificação, reclassificação, restauração de acesso, reprocessamento ou exclusão de critério ilegal; e medidas inibitórias ou suspensivas, quando persistir opacidade incompatível com direitos fundamentais.

A categoria também incorpora lógica de governança ex ante. O Habeas Code não é apenas remédio reativo para decisões já tomadas. Sua incidência incentiva documentação prévia, preservação de logs, avaliações de impacto, explicações padronizadas, trilhas de auditoria, políticas de revisão humana e desenho de sistemas com conformidade incorporada. Nesse

sentido, dialoga com a ideia de legal protection by design, segundo a qual sistemas técnicos devem ser estruturados de modo a não tornar ilusória a proteção de direitos.

Hildebrandt (2020) distingue a pretensão problemática de tornar sistemas legais por design da exigência mais adequada de incorporar proteção jurídica no desenho técnico, especialmente quando a infraestrutura informacional pode afetar direitos e remédios jurídicos. O Código de Processo Civil de 2015 já fornece instrumentos importantes para essa arquitetura, especialmente tutela provisória, exibição de documentos, produção antecipada de prova, prova pericial, cooperação processual, distribuição dinâmica do ônus da prova e segredo de justiça em hipóteses legalmente admitidas.

O Habeas Code utiliza essas técnicas para lidar com a contestabilidade da camada de processamento. A originalidade da proposta não está em inventar todos os meios processuais, mas em coordená-los sob uma finalidade nova e tecnicamente delimitada.

A proposta também deve enfrentar a objeção de que a explicabilidade nem sempre é tecnicamente possível. Essa objeção é correta, mas não elimina a tutela, apenas exige modulação. Quando a explicação interna completa for inviável, podem ser admitidas explicações contrafactuais, relatórios de fatores relevantes, testes de sensibilidade, auditoria de resultados, documentação do desenho do sistema, demonstração de governança e análise de impacto.

Explicabilidade funcional não significa tradução integral do modelo em linguagem comum. Significa prestação de razões suficientes para compreender, contestar e controlar juridicamente a decisão. A impossibilidade de explicação plena pode reduzir o tipo de informação exigível, mas, em sistemas de alto impacto, pode também revelar inadequação do próprio modelo para determinadas finalidades decisórias.

Esse ponto tem consequência normativa relevante. Em determinados contextos, como sistemas que participem da atividade jurisdicional, modelos tecnicamente opacos podem ser juridicamente inadequados. Se uma decisão exige motivação qualificada, controle individualizado, identificação de critérios e possibilidade de revisão efetiva, o uso de sistema incapaz de oferecer auditabilidade mínima pode ser incompatível com o devido processo.

Não se trata de declarar ilícita toda tecnologia complexa, mas de reconhecer que certas funções públicas ou privadas de alto impacto não podem ser exercidas com instrumentos que inviabilizem a contestação. O grau admissível de opacidade depende da natureza da decisão.

O Habeas Code, portanto, atua em dois níveis. No nível individual, protege a pessoa contra decisões que não consegue compreender nem impugnar. No nível institucional, incentiva a construção de sistemas decisórios documentados, auditáveis e juridicamente governáveis. Essa dupla função aproxima a proposta da noção de devido processo tecnológico.

Citron (2008) sustenta que a automação pode esvaziar garantias de aviso, audiência, participação e revisão, exigindo mecanismos capazes de restaurar transparência, accountability e precisão em decisões baseadas em regras incorporadas ao código. O Habeas Code traduz essa preocupação para o ambiente brasileiro, combinando proteção de dados, tutela processual e controle constitucional de decisões automatizadas.

A categoria também permite superar a falsa oposição entre inovação e direitos fundamentais. A auditabilidade não impede a inovação, apenas impõe que sistemas decisórios relevantes sejam juridicamente governáveis. Um modelo que não preserva logs, não documenta versões, não permite revisão humana real, não identifica fatores relevantes e não admite auditoria mínima transfere ao afetado todo o custo da opacidade. A inovação, nesse caso, opera por externalização do risco processual. O Habeas Code recoloca esse custo sobre quem projeta, controla ou utiliza a arquitetura decisória.

O Habeas Code deve ser compreendido como tutela de contestabilidade, não como tutela de curiosidade técnica. O interessado não tem direito irrestrito de conhecer toda tecnologia empregada por empresa ou pelo Estado. Tem direito, porém, a obter os elementos necessários para contestar decisão automatizada que o afete de modo relevante.

Essa distinção é o núcleo dogmático da proposta. Ela preserva o segredo industrial, evita pedidos abusivos, reduz o risco de exposição desnecessária de sistemas e, ao mesmo tempo, impede que decisões opacas se tornem imunes ao Direito.

CONSIDERAÇÕES FINAIS

A incorporação de sistemas automatizados de decisão em relações públicas e privadas desloca o centro de gravidade das garantias informacionais. O problema jurídico contemporâneo já não se limita ao acesso a dados pessoais armazenados em registros ou bancos de dados, nem à correção de informações inexatas.

Em decisões algorítmicas relevantes, a lesão pode decorrer da camada menos visível do processamento. Nesses casos, o sujeito afetado pode conhecer o resultado e, ainda assim,

permanecer incapaz de compreender os critérios, inferências, pesos, proxies, limiares ou registros técnicos que o produziram. A opacidade deixa de ser mero problema técnico e converte-se em déficit de contestabilidade.

A hipótese formulada no artigo confirma-se de modo qualificado. Decisões automatizadas de impacto relevante somente se compatibilizam com o devido processo quando oferecem condições mínimas de contestação. Essas condições não exigem transparência absoluta, abertura irrestrita do código-fonte ou supressão integral do segredo industrial. Exigem, porém, auditabilidade funcional suficiente para que a pessoa afetada, o juízo, o perito ou o órgão de controle possam reconstruir, em grau proporcional ao impacto da decisão, a cadeia decisória relevante.

Sem explicação individualizada, preservação de registros técnicos, documentação mínima, acesso controlado a critérios decisórios, possibilidade de perícia, revisão humana substancial e contraditório técnico, a impugnação da decisão automatizada tende a converter-se em formalidade vazia.

O habeas data permanece instrumento constitucional relevante, assim como a LGPD, que avançou ao reconhecer o direito à revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais. Contudo, nenhum desses instrumentos resolve integralmente o problema. Em síntese, falta no ordenamento brasileiro uma gramática dogmática específica para articular as medidas existentes diante da opacidade da camada de processamento.

É nesse espaço que se justifica a categoria do Habeas Code. Ele não deve ser compreendido como nova ação constitucional extraída diretamente do texto constitucional, mas como gramática processual de auditabilidade algorítmica, capaz de articular instrumentos já existentes em torno de uma finalidade comum: tornar contestáveis decisões automatizadas que impactam direitos fundamentais.

Sua função é mandamental porque busca impor deveres positivos de explicação, preservação, exibição controlada, auditoria, revisão e correção. Sua natureza é dogmático-procedimental porque não depende da criação imediata de novo remédio autônomo, mas da reorganização racional de garantias constitucionais, direitos informacionais e técnicas processuais já disponíveis. Isso não afasta a conveniência futura de disciplina legislativa própria, especialmente para conferir maior segurança jurídica ao procedimento, aos critérios de admissibilidade, aos regimes de sigilo e aos provimentos possíveis.

A consequência dogmática mais relevante é que a opacidade passa a ser tratada como problema de validade procedimental. Uma decisão automatizada relevante não se torna ilícita apenas por ser automatizada, nem válida apenas por decorrer de modelo matemático ou sistema proprietário. Sua legitimidade depende da possibilidade de explicação, contestação e controle.

Conclui-se, portanto, que o Habeas Code não é solução retórica para todos os conflitos da sociedade algorítmica. Trata-se de categoria destinada a organizar, no plano processual, a exigência de que decisões automatizadas relevantes permaneçam submetidas à Constituição, à legalidade e à justificação do poder. Nesse sentido, a tutela mandamental de auditabilidade algorítmica representa atualização necessária das garantias processuais diante de decisões que, embora produzidas por arquiteturas técnicas, continuam juridicamente contestáveis.

REFERÊNCIAS

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. *California Law Review*, Berkeley, v. 104, n. 3, p. 671-732, 2016. DOI: http://dx.doi.org/10.15779/Z38BG31.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 jun. 2026.

BRASIL. *Lei nº 9.507, de 12 de novembro de 1997*. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Brasília, DF: Presidência da República, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 1 jun. 2026.

BRASIL. *Lei nº 13.105, de 16 de março de 2015*. Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 1 jun. 2026.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 jun. 2026.

BRASIL. Superior Tribunal de Justiça. *Súmula n. 550*. A utilização de escore de crédito dispensa consentimento do consumidor, mas assegura o direito de solicitar esclarecimentos sobre informações pessoais valoradas e fontes dos dados considerados no cálculo. Brasília, DF: STJ, 2015. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2015/2015-10-16_09-09_Segunda-Secao-aprova-cinco-novas-sumulas.aspx. Acesso em: 1 jun. 2026.

CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, St. Louis, v. 85, n. 6, p. 1249-1313, 2008.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DOSHI-VELEZ, Finale; KIM, Been. *Towards a rigorous science of interpretable machine learning*. arXiv preprint arXiv:1702.08608, 2017. DOI: https://doi.org/10.48550/arXiv.1702.08608 . Acesso em: 1 jun. 2026.

FLORIDI, Luciano. *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*. Oxford: Oxford University Press, 2023. DOI: https://doi.org/10.1093/oso/9780198883098.001.0001.

HILDEBRANDT, Mireille. *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*. Cheltenham: Edward Elgar Publishing, 2015.

HILDEBRANDT, Mireille. *Law for Computer Scientists and Other Folk*. Oxford: Oxford University Press, 2020.

LESSIG, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: Mapping the debate. *Big Data & Society*, Thousand Oaks, v. 3, n. 2, p. 1-21, 2016. DOI: https://doi.org/10.1177/2053951716679679.

O'NEIL, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown, 2016.

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

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, Oxford, v. 7, n. 2, p. 76-99, 2017. DOI: https://doi.org/10.1093/idpl/ipx005.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, Cambridge, v. 31, n. 2, p. 841-887, 2018.

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