

Dez anos do CPC na sociedade pós-digital: o SNIPER e a necessidade de um devido processo algorítmico

*10 Years of the Civil Procedure Code in Post-Digital Society: The
SNIPER and the Need for Algorithmic Due Process*

*10 Años del CPC en la Sociedad Posdigital: El SNIPER y la Necesidad
de un Debido Proceso Algorítmico*

Simone Gomes Leal

Universidad Nacional de Lomas de Zamora, Lomas de Zamora, Argentina

<https://orcid.org/0009-0007-2685-8645>

E-mail: simoneg.leal@adv.oabsp.org.br

Doutoranda em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP) e pela Universidad Nacional de Lomas de Zamora (Argentina). Mestre em Direito na Sociedade da Informação pelas Faculdades Metropolitanas Unidas (FMU).

Resumo: O presente artigo analisa os dez anos de vigência do Código de Processo Civil de 2015 sob a ótica analítica da Sociedade Pós-Digital, investigando os complexos desafios dogmáticos impostos pela opacidade algorítmica no âmbito da execução civil contemporânea. Diante do reconhecimento formal, pelo Anteprojeto de Reforma do Código Civil (2024), de uma nova dimensão jurídica denominada meio ambiente digital, bem como da autonomização da categoria dos bens digitais, observa-se uma crescente insuficiência operacional de ferramentas estatais de investigação patrimonial, com especial destaque para o sistema SNIPER. Embora tais mecanismos tenham sido desenvolvidos sob a égide da celeridade e da eficiência executiva, sua aplicação prática tem operado sob o fenômeno da “caixa-preta” tecnológica. A problemática central desta investigação reside na inconstitucionalidade material de decisões judiciais e relatórios automatizados opacos que, ao sonegarem a explicabilidade sobre o rastreo e a constrição de ativos desmaterializados e criptoativos, violam frontalmente o princípio da não surpresa, o contraditório substancial e a dignidade da pessoa humana, servindo de vetor para a perpetuação da violência patrimonial e da fraude. Como resposta procedimental a esse hiato de compreensão e controle humano sobre a técnica, propõe-se a implementação do Incidente de Devido Processo Algorítmico (IDPA). Trata-se de uma via incidental e cognitiva apta a assegurar a transparência, a auditabilidade e a governança necessárias para resguardar a integridade das garantias fundamentais e a eficácia da tutela jurisdicional na era dos algoritmos.

Palavras-chave: CPC/2015; SNIPER; explicabilidade; sociedade pós-digital; incidente do devido processo algorítmico (IDPA).

Abstract: This article analyzes the ten years of enforcement of the 2015 Brazilian Civil Procedure Code through the analytical lens of the Post-Digital Society,



investigating the complex dogmatic challenges imposed by algorithmic opacity within contemporary civil enforcement. In light of the formal recognition by the Civil Code Reform Project (2024) of a new legal dimension termed the digital environment, as well as the autonomization of the category of digital assets, a growing operational insufficiency of state asset investigation tools is observed, with particular emphasis on the SNIPER system. Although such mechanisms were developed under the aegis of celerity and enforcement efficiency, their practical application has operated under the technological "black box" phenomenon. The central problem of this investigation lies in the material unconstitutionality of opaque judicial decisions and automated reports which, by withholding explainability regarding the tracking and constraint of dematerialized assets and crypto-assets, frontally violate the principle of non-surprise, substantial adversarial proceedings, and human dignity, serving as a vector for the perpetuation of asset-based violence and fraud. As a procedural response to this gap in understanding and human control over technique, the implementation of the Algorithmic Due Process Incident (IDPA) is proposed. This is an incidental and cognitive recourse capable of ensuring the transparency, auditability, and governance necessary to safeguard the integrity of fundamental guarantees and the effectiveness of jurisdictional protection in the age of algorithms.

Keywords: CPC/2015; SNIPER; explainability; post-digital society; algorithmic due process incident (IDPA).

Resumen: El presente artículo analiza los diez años de vigencia del Código de Procedimiento Civil de 2015 bajo la óptica analítica de la Sociedad Posdigital, investigando los complejos desafíos dogmáticos impuestos por la opacidad algorítmica en el ámbito de la ejecución civil contemporánea. Ante el reconocimiento formal, por parte del Anteproyecto de Reforma del Código Civil (2024), de una nueva dimensión jurídica denominada medio ambiente digital, así como de la autonomización de la categoría de los bienes digitales, se observa una creciente insuficiencia operacional de las herramientas estatales de investigación patrimonial, con especial énfasis en el sistema SNIPER. Aunque dichos mecanismos hayan sido desarrollados bajo la égida de la celeridad y de la eficiencia ejecutiva, su aplicación práctica ha operado bajo el fenómeno de la "caja negra" tecnológica. La problemática central de esta investigación reside en la inconstitucionalidad material de decisiones judiciales y reportes automatizados opacos que, al omitir la explicabilidad sobre el rastreo y la constricción de activos desmaterializados y criptoactivos, violan frontalmente el principio de no sorpresa, el contradictorio sustancial y la dignidad de la persona humana, sirviendo como vector para la perpetuación de la violencia patrimonial y del fraude. Como respuesta procedimental a esta brecha de comprensión y control humano sobre la técnica, se propone la implementación del Incidente de Debido Proceso Algorítmico (IDPA). Se trata de una vía incidental y cognitiva apta para asegurar la transparencia, la auditabilidad y la gobernanza necesarias para resguardar la integridad de las garantías fundamentales y la eficacia de la tutela jurisdiccional en la era de los algoritmos.

Palabras clave: CPC/2015; SNIPER; explicabilidad; sociedad posdigital; incidente del debido proceso algorítmico (IDPA).

Recebido em: junho de 2026

Aceite em: julho de 2026

Publicado em: agosto de 2026



1. Introdução

A celebração da primeira década de vigência do Código de Processo Civil de 2015 ocorre sob a transição definitiva para a Sociedade Pós-Digital, ambiente em que o meio ambiente digital deixa de ser mera extensão instrumental e assume o papel de *locus* primordial de existência da riqueza. Nessa nova configuração social e em rede, o patrimônio se desmaterializa e se converte em fluxos lógicos e ativos intangíveis (bens digitais), que desafiam as estruturas tradicionais de coerção estatal e as premissas analógicas sobre as quais o direito adjetivo foi edificado.

O objetivo desta análise é investigar em que medida o microssistema processual civil brasileiro possui plasticidade e arcabouço dogmático para absorver, compreender e controlar a governança algorítmica que orienta a investigação patrimonial do devedor. Busca-se verificar se os mecanismos de tecnologia da informação adotados pelo Poder Judiciário harmonizam-se com as garantias constitucionais do processo, como o contraditório substancial e o princípio da cooperação, ou se operam à margem delas na era da soberania das plataformas.

A situação-problema reside na insuficiência operacional e na opacidade de ferramentas públicas de execução, com ênfase no sistema SNIPER, que frequentemente entrega relatórios negativos desprovidos de fundamentação auditável sob o manto da "caixa-preta" tecnológica. Esse cenário de eficiência opaca gera uma vulnerabilidade digital interseccional e um cerceamento executivo, pois o Judiciário passa a proferir decisões genéricas de indeferimento baseadas no anacronismo do “não esgotamento dos meios tradicionais”, ignorando a existência de cryptoativos, milhas aéreas e perfis monetizados já reconhecidos pelo Anteprojeto de Reforma do Código Civil de 2024.

A pesquisa adota a metodologia de base jurídico-teórica, pautada no método dedutivo, com procedimento bibliográfico e análise documental de fontes primárias. O marco normativo ancora-se no Código de Processo Civil de 2015, na Lei Geral de Proteção de Dados (LGPD) e no Anteprojeto de Reforma do Código Civil (2024), investigando a hipótese de inconstitucionalidade da opacidade algorítmica judicial frente aos artigos 10 e 489, § 1º, do CPC, para propor, como resposta procedimental, o Incidente de Devido Processo Algorítmico (IDPA).



1. 2. Ontologia sociológica da evolução tecnológica: do ábaco à sociedade pós-digital algorítmica

A trajetória da sociedade pós-digital deve ser compreendida através de marcos estruturais fundamentais. O primeiro situa-se na década de 1940, quando Alan Turing, operando sob a égide de uma sociedade do ábaco cujas limitações técnicas eram superadas pelo rigor lógico, realizou o salto ontológico da mecânica para a computação simbólica ao decifrar o código Enigma. Esse avanço culminou na provocação científica de 1950 sobre a capacidade de “máquinas pensantes”, lançando as bases da inteligência artificial (Turing, 2019, p. 73, 177).

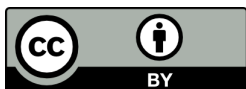
Em paralelo, as teses de Yoneji Masuda descortinaram a arquitetura conceitual da Sociedade da Informação, antecipando a transição do trabalho físico para o processamento mental através de redes de dados. Portanto, Turing e Masuda pavimentaram o caminho material e teórico da sociedade da informação, cujos algoritmos agora estruturam a contemporaneidade (Masuda, 1982 apud Abreu, 1984, p. 172-173).

2.1. A pós-modernidade a fluidez dos fluxos de informação da sociedade da informação

O segundo marco refere-se à sociedade pós-moderna, conceituada por Lyotard, como um “cenário essencialmente cibernético e informacional”, que impulsionou estudos sobre a inteligência artificial. (Lyotard, 2021, p. 10).

No entanto, foi Manuel Castells quem consolidou o conceito de “sociedade em rede”, argumentando que essa reestruturou profundamente a natureza do conhecimento e criou uma nova morfologia social baseada em uma “cultura da virtualidade real”, onde a realidade é capturada por sistemas de mídia eletrônica e fluxos globais de informação. (Castells, 2021, p. 107, apud Leal, 2025, p. 28). É nesse contexto que surge “uma verdadeira revolução tecnológica, na qual as tecnologias da informação e comunicação, materializadas pela internet e computação, dão origem ao ciberespaço. (Leal, 2025, p. 29).

Nesse cenário de virtualização das atividades, o conceito de ciberespaço, difundido por Pierre Lévy (1999, p. 48), passa a ser compreendido pela desterritorialização, visto que “não está vinculado à noção de unidade e de localização. Os vínculos podem se dar entre pontos distantes no espaço físico e em momentos diferentes no



tempo”. Por fim, Zygmunt Bauman traz o contraponto, questionando a fragilidade das relações humanas, a volatilidade e a falta de solidez na modernidade líquida. (Bauman, 2001, p. 7-11).

2.2. Da revolução 4.0 e a sociedade digital e a vulnerabilidade digital interseccional

O terceiro grande marco, que pavimentou a transição para a sociedade pós-digital, materializa-se através da Quarta Revolução. Este período introduz a automação algorítmica e a fusão tecnológica entre os domínios físicos, digitais e biológicos, conforme sedimentado na literatura especializada. (Leal, 2025, p. 34).

Contudo, é imperativo distinguir a Revolução 4.0 da Sociedade Digital: enquanto a primeira representa o conjunto de inovações técnicas e disruptivas que reconfiguraram a produção e a infraestrutura, a Sociedade Digital constitui o desdobramento sociopolítico desse fenômeno, caracterizado pela virtualização das relações e pela onipresença de dados que moldam a subjetividade humana. Dessa forma, a Revolução 4.0 atua como o catalisador técnico que possibilita a emergência de uma Sociedade Digital onde o controle algorítmico passa a mediar a própria democracia e os direitos fundamentais do jurisdicionado.

Esse desdobramento sociológico contemporâneo caminha para diagnosticar a consolidação de uma “Sociedade do Silício” expressão cunhada por André Faustino. para descrever o cenário em que a internet deixa de ser uma autoestrada da informação para se tornar uma autoestrada de conteúdo que dita comportamentos, razão pela qual o reflexo jurídico dessa engrenagem exige um salto teórico imediato. (Faustino, 2023, p. 14).

É preciso ir além da mera constatação social para enfrentar as suas patologias políticas: o nascimento daquilo que se denomina Soberania do Silício.

1.2.1 2.2.1. A nova configuração da vulnerabilidade digital interseccional

É precisamente no ponto de fricção entre a Sociedade do Silício e a Soberania das Plataformas que se estabelece a necessidade de reformulação do conceito de vulnerabilidade. Originalmente cunhada para descortinar a sobreposição de opressões estruturais e tecnológicas no âmbito da violência de gênero onde a assimetria histórica se potencializa pelas propriedades de ubiquidade e



permanência da arquitetura de rede, a vulnerabilidade digital interseccional ressignifica-se no plano processual e executivo contemporâneo como uma patologia de exclusão epistêmica. (Leal, 2026).

No contexto da execução civil pós-digital, a interseccionalidade da vulnerabilidade deixa de ser um fenômeno estritamente biográfico e passa a ser sistêmica, estruturada em três eixos de sobreposição asfíxiante para o jurisdicionado:

1. A Vulnerabilidade Material e de Gênero (Violência Patrimonial Assíncrona):

Manifesta-se de forma aguda nas demandas de Direito de Família e Sucessões, nas quais o ocultamento de ativos desmaterializados (criptoativos, milhas aéreas e perfis monetizados) é instrumentalizado como prolongamento da violência de gênero. A assimetria econômica histórica é renovada pela facilidade técnica de dispersão patrimonial, transformando o ecossistema digital em um campo de fomento ao enriquecimento ilícito do cônjuge opressor.

2. A Vulnerabilidade Técnica Estatal (O Dogma da Eficiência Opaca):

Configura-se pela hipossuficiência técnica do credor diante das próprias ferramentas do aparato judiciário, com especial ênfase no sistema SNIPER. Ao entregar relatórios negativos desprovidos de explicabilidade lógica ou rastreio auditável, o Estado-Juiz transfere ao vulnerável o ônus de decifrar uma “caixa-preta” tecnológica, convertendo a promessa de celeridade em um vetor de cerceamento da execução.

3. A Vulnerabilidade Corporativa (A Cegueira Deliberada das Plataformas):

Consolida-se na disparidade de forças entre o cidadão e os grandes agentes econômicos (instituições financeiras, *exchanges* e Big Techs). Sob o manto de supostas limitações de APIs ou do automatismo de seus códigos, esses entes privados exercem uma ignorância estratégica programada, blindando o patrimônio do devedor e impondo uma barreira de irresponsabilidade que aniquila o princípio da cooperação processual.

Dessa forma, a vulnerabilidade digital interseccional na sociedade pós-digital não representa mera fragilidade econômica, mas sim o completo desarmamento da parte perante a opacidade algorítmica estatal e a soberania técnica privada. Desprovido de controle e compreensão sobre a técnica que dita o resultado de sua pretensão jurídica, o ser humano é reduzido a um dado estatístico desprovido de garantias fundamentais.



2.3. Sociedade pós-digital algorítmica e a vulnerabilidade sistêmica algorítmica

A transição para a sociedade pós-digital algorítmica não constitui apenas um avanço tecnológico, mas também uma ruptura na hierarquia normativa do Estado Democrático de Direito. Nesse contexto, emerge o fenômeno denominado Teoria da Norma Algorítmica, que possui percepção, aprendizado, e especialmente poder decisório, ela percebe quem é vulnerável e dá o veredito sem contraditório, ampla defesa e sem o devido processo legal.¹ Sob a ótica de Hans Kelsen, a norma jurídica consubstancia-se em um sentido objetivo de dever-ser. Contudo, na esfera digital, a sanção transmutou-se em execução direta. O “dever-ser” é substituído pelo “é” do algoritmo, onde o resultado ocorre de forma autônoma e imediata, invertendo essa lógica. (Kelsen, 2019, p. 96-111).

A Sociedade Pós-Digital define-se como o estágio em que a técnica deixa de ser um instrumento externo para se tornar a própria ontologia do habitat social, caracterizando-se pela transversalidade absoluta entre o biológico, o psíquico e o binário. Ela não se funda apenas na conexão, mas na simbiose algorítmica e na automação da vontade, operando como uma estrutura de vigilância panóptica líquida que exige a redefinição do pacto de soberania. Nela, a liberdade não é mais apenas o direito de agir sem interferência, mas a garantia da não-vulnerabilidade neurodigital e da integridade dos fluxos informacionais (Leal, 2026, p. 115).

Nesse contexto, torna-se imperativo distinguir a Era Pós-Digital da Sociedade Pós-Digital. Enquanto a primeira define o estágio cronológico em que a digitalização se tornou uma infraestrutura onipresente e invisível, a Sociedade Pós-Digital caracteriza o fenômeno sociológico da imersão absoluta, onde a fronteira entre o *online* e o *offline* é extinta. É nesta organização social que o “Príncipe Digital” captura o neuroarbitrio, impondo ao Direito o desafio da Soberania de Fluxos frente ao domínio tecnológico das corporações transnacionais (Mazo; Silva; Guimarães, 2026, p. 42).

¹ A “teoria da norma algorítmica”, bem como a tese de que sua senciência preditiva e poder decisório operam uma inversão da pirâmide de Kelsen na sociedade pós-digital, bem como a cegueira deliberada das plataformas, constituem construções dogmáticas inéditas e de autoria exclusiva da autora em sua pesquisa doutoral.



3. Dez anos do Código de Processo Civil: entre a cooperação e o automatismo decisório

Ao completarmos dez anos de vigência da Lei nº 13.105/2015, é imperativo reconhecer que o Código de Processo Civil de 2015 não foi apenas uma atualização legislativa, mas uma verdadeira ruptura com o modelo individualista do Código de 1973. Assim como o Código de Defesa do Consumidor (CDC) revolucionou o Direito Material ao introduzir a boa-fé objetiva e a proteção ao vulnerável, o CPC/2015 transladou esses valores para o plano adjetivo através do Princípio da Cooperação (Art. 6º).

Nesta primeira década, a jurisprudência, especialmente do Superior Tribunal de Justiça (STJ), consolidou institutos que visam a eficiência e a celeridade. Destacam-se o Julgamento Antecipado Parcial do Mérito (Art. 356) e a Improcedência Liminar do Pedido (Art. 332), que permitem que o processo seja um instrumento de resultados, e não um fim em si mesmo. A mudança de paradigma é clara: o foco deslocou-se do rito pelo rito para a Primazia do Julgamento de Mérito, garantindo que o jurisdicionado obtenha uma resposta efetiva do Estado. (Brasil, 2015).

3.1. O princípio da não surpresa e o dever de fundamentação (art. 10 e 489, § 1º)

Um dos “pontos altos” desses dez anos, conforme amplamente debatido em tribunais como o TJDF, é a consagração do Princípio da Não Surpresa. O Artigo 10 do CPC veda decisões baseadas em fundamentos sobre os quais as partes não tiveram oportunidade de se manifestar. Esse dispositivo é o guardião do contraditório substancial, impedindo o arbítrio judicial e garantindo que o processo seja um diálogo ético.

Embora o CPC/2015 tenha trazido inovações procedimentais marcantes, como o remanejamento do ônus de intimação de testemunhas para a própria advocacia (Art. 455) com o escopo de otimizar as pautas de audiências, a realidade atual nos impõe uma análise profundamente crítica sobre a infraestrutura tecnológica que suporta a marcha processual. A Sociedade da Informação, ao mesmo tempo em que oferece



ferramentas de celeridade, introduz os riscos sistêmicos da opacidade algorítmica (Brasil, 2015).

Nesse cenário, a soberania do código privado, quando utilizada por grandes agentes econômicos como barreira de irresponsabilidade, aproxima-se de uma verdadeira ignorância estratégica institucional. A opacidade sistêmica frequentemente invocada por instituições financeiras e intermediários de ativos digitais para justificar a não localização de bens ou o retorno de relatórios negativos em ferramentas de busca denota o que a doutrina civilista contemporânea qualifica como cumplicidade técnica por omissão. No âmbito do inadimplemento obrigacional, a recusa em cooperar efetivamente com o rastro do sistema SNIPER sob o pretexto de “automatismo dos sistemas” ou “limitação técnica de APIs” configura uma evidente e frontal violação aos deveres anexos de conduta decorrentes da boa-fé objetiva, especificamente os deveres de cooperação, informação e transparência (Dellore; Häggström, 2021).

Não se tolera mais que a suposta infalibilidade ou o isolamento dos sistemas bancários sirvam de escusa legal quando tais instituições escolhem a inércia técnica diante de padrões transacionais manifestamente suspeitos de ocultação patrimonial. Trata-se de uma irresponsabilidade corporativa programada, por meio da qual o agente financeiro transfere indevidamente o ônus da prova da dissipação de ativos ao credor. Por conseguinte, a blindagem tecnológica erguida por plataformas de custódia e *exchanges* de criptoativos deve ser superada pela aplicação direta dos regimes de responsabilidade civil e pelo dever de transparência nas relações de crédito, impedindo que o vácuo informacional atue como salvo-conduto para a fraude à execução (Mazo; Silva; Guimarães, 2026, p. 42).

A crítica central, portanto, reside no fato de que, sob o manto dessa pretensa “eficiência”, o próprio Poder Judiciário tem adotado sistemas de Inteligência Artificial para a triagem massiva de recursos e elaboração automatizada de minutas de decisão. Ocorre que, se o fundamento da decisão advém de uma “caixa-preta” tecnológica (um sistema cuja lógica interna e parâmetros de cruzamento permanecem inacessíveis às partes), o Princípio da Não Surpresa é sumariamente aniquilado (Han, 2022, p. 47).

Não há contraditório substancial se não houver explicabilidade técnica. Uma decisão judicial pautada em automatismos opacos carece de fundamentação constitucional



idônea e incorre em manifesta inconstitucionalidade, pois subtrai do jurisdicionado a capacidade elementar de compreender e, por conseguinte, de impugnar analiticamente a razão de decidir. Assim, ao celebrarmos os dez anos de vigência do CPC, o maior desafio contemporâneo deixa de ser a busca cega pela celeridade métrica, transmutando-se na necessidade imperativa de preservação da dignidade humana e do devido processo legal face à soberania dos algoritmos (Leal, 2026, p. 115).

4. A transição da sociedade da informação para a pós-digital

A compreensão da ineficácia das ferramentas de execução contemporâneas passa, necessariamente, pela redefinição ontológica do objeto de busca patrimonial. O Relatório Final do Anteprojeto de Reforma do Código Civil (Brasil, 2024, p. 311), introduz conceitos fundamentais sobre a desmaterialização da riqueza, destacando a necessidade imperativa de alinhar o Direito Privado às novas realidades do ecossistema tecnológico para garantir segurança jurídica às interações em ambiente online.

Nessa perspectiva, o texto reformador conceitua o Meio Ambiente Digital como o espaço dinâmico onde se desenvolvem relações jurídicas complexas por meio de redes de computadores e sistemas de inteligência artificial. Dentro deste ecossistema, surgem normatizados os Bens Digitais, categoria que compreende não apenas ativos financeiros tradicionais em formato eletrônico, mas dados com expressão pecuniária, perfis em redes sociais dotados de valor econômico, criptoativos, tokens e milhas aéreas (Brasil, 2024, p. 310-311).

Portanto, a exemplo dessas inovações de direito material, o Código de Processo Civil deve, urgentemente, regulamentar novas vias procedimentais que viabilizem a penhora e a expropriação de tais posições contratuais intangíveis. A eficácia prática de sistemas de automação e cruzamento de dados, como o SNIPER, depende diretamente de um arcabouço normativo-processual que reconheça a liquidez e a especificidade das novas realidades tecnológicas, sob o risco de as inovações civis se tornarem inócuas se desprovidas de um direito adjetivo igualmente disruptivo.



4.1. O meio ambiente digital como novo *locus* da execução e a vulnerabilidade sistêmica algorítmica

A falha recorrente do sistema SNIPER em localizar ativos em ambiente virtual demonstra que a tecnologia, por si só, não garante a efetividade da prestação jurisdicional se desacompanhada do vetor da explicabilidade. A execução civil não pode se transmutar em um “bilhete de loteria” analógico, no qual a satisfação do crédito dependa exclusivamente da sorte ou da configuração cega de um algoritmo. Diante de uma natureza patrimonial fluida, o processo civil não pode continuar operando com ferramentas de investigação que ignorem os fluxos digitais de riqueza. É justamente nesse vácuo técnico e normativo que o Incidente de Devido Processo Algorítmico (IDPA) projeta sua utilidade: ele serve como ferramenta de controle epistêmico para auditar se o sistema de busca estatal foi programado para alcançar as camadas profundas do ecossistema digital ou se, por falha estrutural, limitou-se à superfície do patrimônio analógico tradicional.

Na prática executiva, a exigência de explicabilidade aplicada ao SNIPER atua como um verdadeiro vetor de eficiência processual. Ao impor que a ferramenta apresente a lógica de seus cruzamentos de dados e as limitações de suas buscas, retira-se do magistrado a possibilidade de proferir decisões genéricas de indeferimento fundamentadas em fórmulas abstratas, como o suposto “não esgotamento de meios ordinários”. Sendo o ciberespaço o novo *locus* da riqueza, a explicabilidade algorítmica qualifica-se como o único mecanismo capaz de garantir ao credor o direito de auditar a ineficácia da execução, permitindo-lhe apontar caminhos investigativos que a máquina, por opacidade ou falha de parametrização, deixou de percorrer (Leal, 2026, p. 155).

4.2. A soberania do silício e a segurança jurídica no ambiente digital

No ecossistema da Sociedade Pós-Digital, presenciamos uma reconfiguração da clássica teoria do poder político. Como advertem Gilmar Mendes e Victor Fernandes (2020), vivemos a transição da soberania estatal para a soberania das plataformas. (Mendes; Fernandes, 2020, p. 5-6).

Nesse cenário, as grandes corporações tecnológicas passam a operar como um “Príncipe” contemporâneo, dominando através da arquitetura de códigos. Essa



realidade descortina uma inédita vulnerabilidade do Estado-Juiz ²que, desprovido de infraestrutura digital própria, torna-se refém técnico de infraestruturas privadas que operam em uma camada imune ao controle democrático. (Beccaria, 2015).

A soberania do algoritmo, ao ser utilizada como barreira de irresponsabilidade, aproxima-se da patologia jurídica da ignorância estratégica. Nesse cenário, a postura das instituições financeiras de se refugiarem na suposta infalibilidade do código para não investigar transações atípicas pode ser confrontada pela Teoria da Cegueira Deliberada. Segundo Pedro Antônio Adorno Bandeira Assumpção, essa doutrina busca impedir que o agente se beneficie da própria torpeza ao criar deliberadamente um vácuo de consciência sobre a ilicitude de seus atos, agindo previa e intencionalmente para se blindar contra uma eventual responsabilização futura. Assim, a “infalibilidade” sistêmica não pode servir de escusa legal quando a instituição escolhe a inércia técnica em face de padrões transacionais manifestamente suspeitos, equiparando-se tal omissão ao dolo eventual por assumir o risco do resultado danoso. (Assumpção, 2017, p. 15).

No ecossistema da Sociedade Pós-Digital, a Segurança Jurídica deve ser compreendida em sentido lato, como o imperativo de previsibilidade e estabilidade normativa que rege o meio ambiente digital. Contudo, essa estabilidade é materialmente impossível sem a Cibersegurança, que atua em sentido estrito como a salvaguarda técnica da integridade e confidencialidade dos dados. Assim, a cibersegurança não é um fim em si mesma, mas o instrumento operacional que viabiliza a segurança jurídica; sem a proteção técnica contra a exploração algorítmica e ataques externos, o ordenamento jurídico torna-se um simulacro incapaz de proteger o neuroarbítrio e a soberania de fluxos. A recente tendência do Superior Tribunal de Justiça em discutir a classificação do aparelho celular como um “produto essencial” (Brasil, 2026).

Evidencia-se uma preocupação com o “mínimo existencial digital”, mas falha ao não enfrentar a insegurança estrutural do ecossistema onde esse bem opera. Na Sociedade Pós-Digital, a verdadeira essencialidade não reside no *hardware*, mas na segurança jurídica das interações, o que exige um modelo de governança baseado em monitoramento constante, capaz de converter princípios de Direitos Humanos

² Trata-se de tese inédita desenvolvida pela autora no âmbito de sua pesquisa de doutoramento, a qual propõe a releitura dos conceitos tradicionais de soberania e jurisdição sob a ótica da “soberania do silício” e da consequente vulnerabilidade do Estado-juiz perante o poder técnico das Big Tech, bem como o conceito das *Big Techs* como o “príncipe contemporâneo”

em recomendações objetivas que preservem a integridade do sistema. (Brasil, 2026). Esta desconexão entre a garantia do bem e a fragilidade do meio funciona como um “irritante legal”, expondo a necessidade de uma reconstrução interna do ordenamento brasileiro que busque a “equivalência funcional” (Dellore; Häggström, 2021).

Em suma, a transição para a soberania do silício redefine a vulnerabilidade, que passa a atingir o próprio Estado e o ordenamento ante a opacidade das grandes plataformas e a inércia técnica bancária. Diante disso, a segurança jurídica no ambiente digital pressupõe superar a mera proteção do *hardware* para exigir uma governança sistêmica baseada na cibersegurança e na explicabilidade algorítmica. Somente através dessa equivalência funcional será possível mitigar os riscos da cegueira deliberada corporativa e resguardar a integridade das relações jurídicas na sociedade pós-digital.

4.3. A inconstitucionalidade da opacidade violência patrimonial e a dignidade da pessoa humana no ambiente digital

A manutenção da opacidade algorítmica em ferramentas como o SNIPER, quando resulta no indeferimento ou na negativa de acesso a bens digitais como cryptoativos, milhas aéreas, perfis monetizados e ativos em *Exchanges*, configura uma evidente inconstitucionalidade por violação ao Princípio da Dignidade da Pessoa Humana (Art. 1º, III, CF/88). No contexto de ações de Direito de Família, como o divórcio, a opacidade das “caixas-pretas” tecnológicas torna-se um instrumento de perpetuação da violência patrimonial. Quando o Judiciário nega a explicabilidade de um relatório negativo ou indefere o acesso a sistemas de busca sob justificativas genéricas, ele chancela a usurpação de bens e o enriquecimento ilícito do cônjuge que oculta patrimônio no Meio Ambiente Digital (Brasil, 1988).

Essa barreira tecnológica impede que a mulher, muitas vezes em situação de extrema vulnerabilidade, acesse o que lhe pertence por direito material, ferindo o Direito Fundamental à Propriedade e o Acesso à Ordem Jurídica Justa (Art. 5º, XXXV e LIV, CF/88). Conforme as diretrizes do Anteprojeto do Código Civil (2024, p. 310), a transparência nas interações digitais é um pilar de segurança; portanto, permitir que algoritmos opacos decidam o destino patrimonial de uma família, sem o

devido controle de explicabilidade, é retirar do jurisdicionado a sua própria humanidade perante o Estado.

A eficácia da execução civil na Sociedade da Informação não pode ser um escudo para a fraude, mas sim um vetor de justiça que, através do Incidente de Devido Processo Algorítmico (IDPA), restabeleça o equilíbrio e a supremacia da Constituição sobre a técnica. Afinal, a centralidade da Dignidade da Pessoa Humana no ordenamento jurídico brasileiro impõe que ela seja o parâmetro último de validade para qualquer interpretação constitucional (Barroso, 2020, p. 290-295).

5. O descompasso operacional do SNIPER diante da desmaterialização patrimonial e da opacidade algorítmica

O Sistema Nacional de Investigação Patrimonial e Recuperação de Ativos (SNIPER) foi inicialmente recepcionado pela comunidade jurídica como a panaceia contra a denominada “blindagem patrimonial”. Conforme diretrizes institucionais do Conselho Nacional de Justiça (CNJ), a ferramenta desenvolvida sob a égide do Programa Justiça 4.0 foi desenhada para agilizar a investigação patrimonial ao centralizar o acesso a sistemas tradicionais como Sisbajud, Renajud, Anacjud e Receitajud, expandindo seu potencial coercitivo em atualizações recentes por meio da integração de bases de dados de registros cartoriais de imóveis em uma interface digital unificada.

Todavia, sob a lente analítica da Sociedade Pós-Digital, a própria arquitetura de expansão celebrada pelo órgão padece de um anacronismo estrutural: seu mapeamento de vínculos, embora centralizado, foca essencialmente em registros de bens tradicionais, lineares e estáticos. Ao priorizar propriedades imobiliárias, veículos automotores, aeronaves e participações societárias formalizadas perante as juntas comerciais, o Estado-Juiz circunscreve sua atuação ao quadrante do mundo físico-burocrático.

Essa ineficácia operacional do SNIPER diante das novas dinâmicas econômicas, premissa que fundamenta e justifica, a necessidade de criação do Incidente de Devido Processo Algorítmico (IDPA) consubstancia-se em três vetores principais:

1. Incompatibilidade Ontológica e de Objeto: Verifica-se um manifesto descompasso entre a ferramenta de busca estatal e a natureza fluida do patrimônio executado. Enquanto o SNIPER opera com base em indexadores analógicos e



registros de propriedade tradicionais, o devedor contemporâneo adota estratégias de dispersão patrimonial pautadas na desmaterialização da riqueza. O patrimônio é vertido para o meio ambiente digital, alocado em ativos intangíveis que transitam à margem das bases de dados estatais convencionais. Exemplos fulcrais dessa assimetria são as *cold wallets* (carteiras frias de criptoativos desconectadas da rede), a tokenização de ativos de valor real, as milhas aéreas e as receitas derivadas da monetização de plataformas digitais, as quais escapam completamente do radar de varredura do SNIPER, gerando relatórios negativos que não refletem a real capacidade financeira do executado.

2. A Opacidade da “Caixa-Preta” e a Inversão do Ônus Epistêmico: O segundo vetor reside na ausência de explicabilidade dos resultados gerados pelo sistema. Quando o SNIPER emite um relatório negativo, ele não fornece ao credor ou ao magistrado as linhas de código, os critérios de cruzamento ou as limitações técnicas que justificaram o insucesso da busca. Instala-se o fenômeno da opacidade algorítmica: o Estado-Juiz assume a infalibilidade da ferramenta e, ato contínuo, indefere os pedidos de cooperação subsequentes sob o argumento genérico de “não esgotamento dos meios tradicionais”. Transfere-se, assim, ao vulnerável digital um ônus epistêmico impossível de ser cumprido, sepultando a eficácia da tutela executiva.

3. A “Caixa-Preta” do Resultado Negativo: A opacidade do sistema gera um grave óbice ao direito de defesa do crédito. Quando o SNIPER retorna uma certidão ou relatório negativo, ele opera sob o fenômeno da “caixa-preta” (*black box*), omitindo quais camadas lógicas ou bases de dados específicas deixaram de ser atingidas ou sequer foram varridas. Sem o acesso à engenharia e à lógica reversa da busca, o credor fica impossibilitado de auditar o procedimento, impedindo-o de identificar e apontar as falhas técnicas da ferramenta ou de sugerir caminhos alternativos para a localização de ativos ocultos.

Embora o Superior Tribunal de Justiça tenha pacificado a legalidade do uso do Sistema Nacional de Investigação Patrimonial e Recuperação de Ativos (SNIPER) nas execuções cíveis, afastando a tese de que sua mera deflagração configuraria quebra automática de sigilo bancário, a validade da medida permanece estritamente vinculada ao princípio da explicabilidade. Isso significa que o provimento jurisdicional não pode se dar por meio de comandos genéricos ou automatizados;



exige-se do magistrado uma fundamentação analítica que justifique a proporcionalidade da invasão patrimonial no caso concreto. Assim, o juiz assume o dever de discriminar detalhadamente quais subsetores lógicos e bases de dados integradas à plataforma serão efetivamente acionados, bem como o escopo exato das informações requisitadas, garantindo o controle humano e a transparência sobre o funcionamento do algoritmo coercitivo. (Castro, 2026).

5.1. A explicabilidade e transparência e a necessidade de novos institutos jurídicos que viabilizem a razão algorítmica

Enquanto as ferramentas atuais de execução, como o SNIPER, operam em um vácuo de regulamentação específica sobre seus critérios algorítmicos, o cenário legislativo brasileiro caminha para a imposição ética da transparência. O Anteprojeto de Reforma do Código Civil, elaborado pela Comissão de Juristas instituída pelo Ato do Presidente do Senado Federal nº 11/2023, introduz de forma pioneira o “Direito Civil Digital”.

O anteprojeto de atualização do Código Civil brasileiro reconhece a urgência de regulamentar as relações jurídicas no ambiente virtual, dedicando um capítulo específico ao Direito Digital para enfrentar os desafios da sociedade da informação. A proposta busca estabelecer diretrizes para a aplicação da inteligência artificial e a proteção de dados, assegurando que a evolução tecnológica seja acompanhada por uma estrita tipicidade normativa que garanta segurança jurídica e proteção aos direitos fundamentais. Conforme destacado no texto, essa modernização é indispensável para que o estatuto civil dialogue com a realidade da comunicação em tempo real e com as novas dinâmicas da Sociedade Pós-Digital, mitigando riscos de disrupção nas relações civis tradicionais (Brasil, 2024, p. 1).

No tocante à interação das pessoas com sistemas de IA, o Livro assegura que as pessoas têm direito à informação sobre como interagem com esses sistemas e como as decisões automatizadas podem influenciar diretamente seus direitos ou interesses econômicos. (Brasil, 2024, p. 310).

Essa previsão legal reforça a tese de que a explicabilidade não é uma faculdade da administração judiciária, mas um direito subjetivo da parte. Ao transpor essa lógica para o processo civil, percebe-se que a utilização de algoritmos na execução

patrimonial (como o SNIPER) deve observar os mesmos princípios de segurança e confiabilidade previstos no Anteprojeto.

A contradição é evidente: enquanto o futuro Direito Civil material já prevê a proteção contra decisões automatizadas opacas, a prática processual contemporânea ainda aceita resultados de sistemas “caixa-preta” sem a devida auditoria. Portanto, o Incidente de Devido Processo Algorítmico (IDPA) surge como o elo necessário para materializar a transparência exigida pelo constitucionalismo digital diante da transição para a sociedade pós-digital algorítmica, a qual não representa apenas um salto tecnológico, mas uma verdadeira ruptura na hierarquia normativa do Estado Democrático de Direito. Nesse cenário, coexiste o fenômeno da Teoria da Norma algorítmica.

Por outro lado, se a evolução das práticas bancárias e mercadológicas globalizadas exigiu da dogmática penal o influxo da Teoria do Domínio do Fato por meio de aparatos organizados de poder conforme a lição de Claus Roxin aplicada à macroadelinquência, o cenário contemporâneo exige idêntica atenção ao “aparato tecnológico estatal”. Ferramentas de inteligência e constrição patrimonial, como o Sniper, operam sob uma estrutura sistêmica automatizada que, se desprovida de explicabilidade, transmuta o julgador em mero agente fungível de uma engrenagem computacional opaca. Mitigar a exigência de inteligibilidade sob o pretexto da complexidade das fraudes financeiras viola o devido processo algorítmico, blindando o real “homem de trás” do código de qualquer controle constitucional. (Roxin, 1963, apud Faria, 2024).

A governança dos sistemas automatizados no setor financeiro deve ser pautada pelo princípio da Accountability, que exige das instituições não apenas a conformidade formal, mas a capacidade de demonstrar a integridade de seus processos. Esse dever de prestação de contas ganha contornos mais rígidos com o *AI Act* (Regulamento de Inteligência Artificial) da União Europeia, que classifica os sistemas de crédito e análise de risco como de alto risco, exigindo transparência absoluta sobre os parâmetros que levam a uma decisão automatizada. (União Europeia, 2023).

Nesse contexto, o *Duty of Care* (Dever de Cuidado) assume uma função preventiva essencial na proteção do correntista contra fraudes sistêmicas. (Reino Unido, 2018).

Inspirado por normas de proteção a ativos digitais, como o MiCA (Markets in Crypto-Assets), esse dever impõe que a instituição financeira zele ativamente pela segurança do fluxo transacional, sendo responsabilizada sempre que a omissão no monitoramento algorítmico permitir a consumação de danos ao patrimônio do vulnerável. (União Europeia, 2024).

Dessa forma, o Incidente de Devido Processo Algorítmico materializa o direito à explicabilidade, combatendo a opacidade que muitas vezes mascara a negligência bancária. Ao exigir a abertura da “caixa-preta”, O Judiciário assegura que a responsabilidade proativa das instituições seja auditável, impedindo que a automação sirva como escudo para o descumprimento de deveres fundamentais de cuidado e transparência.

A transposição metodológica de conceitos como os sistemas de “alto risco” para o rito processual é essencial para balizar a autonomia dos sistemas automatizados. Essa classificação é fundamental porque, segundo a teoria de Robert Alexy, as normas que garantem direitos operam como “mandamentos de otimização”, que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes. Em sistemas classificados como de alto risco, a otimização da segurança jurídica e do controle humano deve ser levada ao grau máximo, pois a medida da satisfação do direito depende das possibilidades normativas colidentes. (Alexy, 2015, p. 90).

A governança global algorítmica deve ser pautada pelo que Ferrajoli caracteriza como o paradigma constitucional: a submissão de qualquer forma de poder aos direitos fundamentais, os quais devem ser entendidos como “fragmentos de soberania popular” que limitam a discricionariedade técnica e política. (Ferrajoli, 2015, p. 85).

Ao adotar uma escala de riscos inspirada no modelo europeu, o sistema de justiça brasileiro define as balizas de atuação da IA discriminando onde a automação pode atuar de forma célere e onde a supervisão humana deve ser mandatária. Essa gradação visa enfrentar a “crise da capacidade regulatória do direito” perante os novos poderes supranacionais, assegurando que a tecnologia não se torne um pretexto para a opacidade ou para a violação de garantias fundamentais. (Ferrajoli, 2015, p. 179).



Em suma, a transição para a Sociedade Pós-Digital exige que a atividade executória seja submetida ao império das garantias constitucionais, impedindo que a busca cega pela celeridade converta o processo em um espaço de opacidade e arbítrio técnico. Portanto, a explicabilidade algorítmica deve ser obrigatoriamente fundamentada nas decisões judiciais para viabilizar a ampla defesa e respeitar o devido processo legal, pois, sob o paradigma do constitucionalismo digital, sem explicabilidade não há constitucionalidade. Desse modo, encerra-se a delimitação teórica dos gargalos estruturais das ferramentas estatais e corporativas para, no capítulo seguinte, inaugurar a análise pragmática e a estruturação procedimental do Incidente de Devido Processo Algorítmico (IDPA) como freio indispensável à soberania das *Big Techs*.

6. O incidente do devido processo algorítmico como freio ao poder da norma algorítmica

A substituição do devido processo legal pela “Eficiência do Score” revela um cenário em que a Constituição exigiria a proteção ao vulnerável, a IA discriminatória identifica a vulnerabilidade para operacionalizar a exclusão, decidindo no lugar do legislador e do magistrado. Dessa forma, o fundamento legal do Incidente do Devido Processo Algorítmico, (IDPA) encontra-se na infringência ao devido processo legal (Art. 5º, LIV, CF), estruturando-se a explicabilidade como um prolongamento do dever de fundamentar as decisões judiciais. (Brasil, 1988).

A necessidade da estruturação do Incidente do Devido Processo Algorítmico emerge como uma resposta imperativa à corrosão das garantias fundamentais e ao lastro de indignidade provocado pela soberania da norma algorítmica. Como bem observa o Prof. Dr. William Santos Ferreira, a efetividade do processo depende de uma cognição que não se deixe seduzir por simplificações técnicas, sob pena de o Judiciário incorrer em uma cegueira deliberada que sacrifica a verdade real no altar da celeridade estatutária. Diante da falência do atual modelo de Processo Civil para lidar com a opacidade das fraudes bancárias (Ferreira, 2026).

o Judiciário permite que a opacidade algorítmica prevaleça sobre provas materiais confessas, resultando na infringência de direitos fundamentais e no esvaziamento de institutos consagrados diante de fraudes bancárias. Propõe-se, assim, que o Devido Processo Algorítmico (IDPA) atue como o mecanismo capaz de sanar esse



hiato de compreensão, transmutando o *fumus boni iuris* e o *periculum in mora* em explicabilidade técnica, impedindo a degradação da dignidade do hipervulnerável. Nessa esteira, a vulnerabilidade do consumidor na era pós-digital transcende a hipossuficiência técnica clássica, alcançando o que Byung-Chul Han denomina de “violência neuronal” na Sociedade do Cansaço (Han, 2017, p. 51).

A Recomendação sobre a Ética da Inteligência Artificial da UNESCO da qual o Brasil é signatário, estabelece que as decisões baseadas em IA devem ser explicáveis, transparentes e sujeitas a controle humano. Ela proíbe expressamente o uso de sistemas de IA que operem em “caixas-pretas” quando afetarem direitos humanos. Enquanto a Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica), em seu Artigo 25, obriga os Estados a oferecer um recurso simples e rápido contra atos que violem direitos fundamentais, bem como, a Resolução 48/4 do Conselho de Direitos Humanos da ONU, foca especificamente no direito à privacidade e como as novas tecnologias e o processamento de dados em larga escala não podem criar um ambiente de exclusão ou decisões opacas que firam a dignidade humana, o que sustenta juridicamente a implementação do Incidente do Devido Processo Algorítmico.

A fundamentação dogmática do Incidente de Devido Processo Algorítmico (IDPA) encontra sólido amparo no microssistema de proteção de dados nacional, especificamente no artigo 20 da Lei Geral de Proteção de Dados (LGPD). O referido diploma confere ao titular o direito de obter a revisão e, fundamentalmente, a transparência acerca dos critérios e procedimentos utilizados em decisões baseadas no tratamento automatizado de dados individuais (Brasil, 2018).

Desse modo, ao transpor tal garantia para o plano processual executório, resta evidente que o devedor, enquanto titular de dados e sujeito passivo da relação processual, possui a prerrogativa jurídica de exigir a auditabilidade e a explicabilidade dos parâmetros lógicos adotados pelas ferramentas públicas de constrição patrimonial eletrônica, obstaculizando o arbítrio decorrente da opacidade algorítmica.

Portanto, a sociedade pós-digital não é apenas informacional; ela é uma sociedade de soberania algorítmica, onde o compliance inconstitucional dita a norma e a dignidade humana torna-se variável de ajuste de um sistema que não admite o erro, exigindo, urgentemente, um Constitucionalismo Digital capaz de restaurar a



supremacia da norma humana sobre a execução do código. (Mendes; Fernandes, 2021, p. 5).

Em suma, a implementação do Incidente de Devido Processo Algorítmico (IDPA) consolida-se como o instrumento processual vocacionado a restabelecer a segurança jurídica em procedimentos executórios que demandam a explicabilidade das decisões e relatórios automatizados. No que tange ao sistema SNIPER, o incidente atua especificamente como um freio cognitivo à opacidade de sua “caixa-preta”, conferindo ao credor o direito público subjetivo de auditar as camadas lógicas não atingidas e as bases de dados ignoradas após a emissão de uma certidão negativa. Portanto, ao converter a consulta tecnológica de um comando cego e insindicável para um rito transparente e passível de controle pelas partes, o IDPA garante que a eficiência da investigação patrimonial não seja alcançada ao custo do atropelo das garantias fundamentais do devido processo legal.

7. Conclusão

A celebração da primeira década de vigência do Código de Processo Civil de 2015 ocorre em um momento de transição paradigmática irreversível. Como reconhecido pelo Anteprojeto de Reforma do Código Civil de 2024, a realidade contemporânea testemunha a consolidação da Sociedade Pós-Digital, abandonando em definitivo as amarras da era analógica para habitar um ecossistema onde as relações jurídicas são profundamente mediadas por algoritmos. O próprio Anteprojeto, em seu Livro Complementar de Direito Digital, estabelece de forma categórica que essa nova configuração social exige proteção, transparência e, fundamentalmente, segurança jurídica nas interações virtuais.

Contudo, a práxis da execução civil brasileira ainda padece de um descompasso estrutural ao tentar capturar esse novo patrimônio desmaterializado. Ferramentas estatais de investigação, como o sistema SNIPER, embora dotadas de inegável potencial tecnológico, tornam-se insuficientes e inócuas quando operam sob o manto da opacidade algorítmica. A atividade executiva que se limita ao rastreamento de bens materiais tradicionais ignora a existência dos bens digitais ativos que o ordenamento material agora conceitua, categoriza e protege. Quando o Judiciário chancela relatórios negativos e profere decisões de indeferimento



baseadas na “caixa-preta” dos sistemas informatizados, instala-se um cenário de flagrante inconstitucionalidade.

Essa opacidade tecnológica fere frontalmente a Dignidade da Pessoa Humana e o devido processo legal. Em contextos de nítida assimetria, como a ocultação de riqueza em lides de Direito de Família e as fraudes bancárias sistêmicas, a falta de explicabilidade dos mecanismos automatizados converte-se em um perigoso instrumento de perpetuação da violência patrimonial contra o vulnerável. Não há contraditório substancial ou ampla defesa onde as partes são impedidas de auditar a lógica interna da prova e da busca. Uma decisão judicial pautada em um relatório tecnológico insindicável carece de fundamentação e esvazia a legitimidade da prestação jurisdicional.

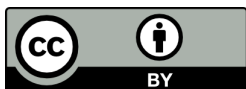
Diante desse cenário, a via premente para garantir que o CPC/2015 sobreviva com integridade constitucional aos seus próximos dez anos é a implementação dogmática do Incidente de Devido Processo Algorítmico (IDPA). Este novo procedimento incidental, integrado à sistemática processual civil, surge como o freio cognitivo necessário para resguardar a segurança jurídica, a explicabilidade e o mandatário controle humano sobre a técnica, especialmente no que tange ao aperfeiçoamento e à auditoria do SNIPER. O IDPA transcende a condição de mera sugestão acadêmica; cuida-se de uma exigência premente do Estado Democrático de Direito para que a busca pela celeridade estatutária não sacrifique os direitos fundamentais no altar da tecnologia. Em suma, a efetividade da execução na era dos algoritmos depende, inexoravelmente, de um processo que se imponha de forma transparente, auditável e essencialmente humano.

Referências

ABREU, A. B. de. A sociedade da informação como sociedade pós-industrial (resenha). **Revista de Administração Pública**, Rio de Janeiro, v. 18, n. 3, p. 171-173, jul./set. 1984. Disponível em: <https://periodicos.fgv.br/rap/article/view/10558>. Acesso em: 12 jul. 2026.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução de Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2015.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo**. 9. ed. São Paulo: Saraiva, 2020.



BAUMAN, Zygmunt. **Modernidade líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001.

BECCARIA, Cesare. **Dos delitos e das penas**. São Paulo: Pilares, 2015.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil**. Brasília, DF: Presidência da República, 2015.

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.

BRASIL. Senado Federal. **Relatório Final dos trabalhos da Comissão de Juristas responsável pela revisão e atualização do Código Civil (CJCODCIVIL)**. Brasília, DF: Senado Federal, 2024. Disponível em: <https://www.senado.leg.br>. Acesso em: 10 maio 2026.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial nº 2.226.610/RJ**. Relatora: Ministra Nancy Andrighi. Julgado em 14 abr. 2026. Diário da Justiça Eletrônico (DJe), Brasília, DF, abr. 2026. Disponível em: <https://www.stj.jus.br>. Acesso em: 10 maio 2026.

CASTELLS, Manuel. **A Sociedade em Rede**. Tradução de Roneide Venancio Majer. 17. ed. São Paulo: Paz e Terra, 2016.

FARIA, Thiago Rodrigues de. **A Teoria do Domínio do Fato de Claus Roxin e sua aplicabilidade ao Direito Penal Econômico**. São Paulo: Dialética, 2024. E-book.

FAUSTINO, André. **A Sociedade do Silício: Inteligência artificial e a proteção da privacidade**. 1. ed. São Paulo: Lura Editorial, 2023.

FERRAJOLI, Luigi. **Direito e Razão: teoria do garantismo penal**. 4. ed. rev. e ampl. São Paulo: Revista dos Tribunais, 2014.

FERRAJOLI, Luigi. **Principia iuris: Teoria do Direito e da Democracia**. São Paulo: Martins Fontes, 2007.

HAN, Byung-Chul. **Infocracia: digitalização e a crise da democracia**. Tradução de Gabriel S. Philipson. Rio de Janeiro: Vozes, 2022.

HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. 2. ed. ampl. Petrópolis: Vozes, 2017.

HART, Herbert L. A. **O Conceito de Direito**. Tradução de A. Ribeiro Mendes. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 1994.

KELSEN, Hans. **Teoria Pura do Direito**. Tradução de João Baptista Machado. 6. ed. São Paulo: Martins Fontes, 1998.



LEAL, Simone Gomes. **Cyberstalking: novas perspectivas de aplicação no âmbito da violência doméstica diante do avanço tecnológico na sociedade da informação**. São Paulo: Dialética, 2025.

LEAL, Simone. Cyberstalking e Violência Doméstica: nova obra da advogada Simone Leal propõe ruptura na interpretação do crime. **Direito News**, 27 fev. 2026. Disponível em: <https://www.direitonews.com.br/2026/02/cyberstalking-violencia-domestica-obra-advogada-simone-leal-ruptura-interpretacao-crime.html>. Acesso em: 10 jun. 2026.

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

LYOTARD, Jean-François. **A Condição Pós-Moderna**. 20. ed. Rio de Janeiro: José Olímpio, 2021.

MAZO, Luisa Baptistella Gatti; SILVA, Maria Eduarda Neves; GUIMARÃES, Antônio Márcio da Cunha. Soberania Estatal, Autonomia Privada e Transformação Digital na Arbitragem Internacional de Investimentos. **Revista de Direito Internacional e Globalização Econômica**, v. 14, p. 35-52, 2026.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Brasileira de Direito**, Passo Fundo, v. 16, n. 1, p. 1-33, 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Conselho de Direitos Humanos. **Resolução 48/4: O direito à privacidade na era digital**. Genebra: ONU, 2021. Disponível em: <https://www.ohchr.org>. Acesso em: 10 maio 2026.

REINO UNIDO. **Data Protection Act 2018**. c. 12. Londres: Parliamentary Digital Services, 2018. Disponível em: <https://www.legislation.gov.uk>. Acesso em: 10 maio 2026.

TURING, Dermond. **A História da Computação Do Ábaco à Inteligência Artificial**. São Paulo: M. Books, 2019.

UNIÃO EUROPEIA. Regulamento (UE) 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023. **Relativo aos mercados de criptoativos e que altera os Regulamentos (UE) n.º 1093/2010 e (UE) n.º 1095/2010 e as Diretivas 2013/36/UE e (UE) 2019/1937 (Regulamento Markets in Crypto-Assets – MiCA)**. Jornal Oficial da União Europeia, Bruxelas, L 150, 9 jun. 2023. Disponível em: <https://eur-lex.europa.eu/>. Acesso em: 10 maio 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. **Cria regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial)**. Jornal Oficial da União Europeia, Bruxelas, L/2024/1689, 12 jul. 2024. Disponível em: <https://eur-lex.europa.eu/>. Acesso em: 10 maio 2026.



