REVISTA DCS
FUNDADA EN 2000

SOB O PESO DOS DADOS: O DATA DUMPING E OS DESAFIOS DO CONTRADITÓRIO NA ERA DIGITAL

UNDER THE WEIGHT OF DATA: DATA DUMPING AND THE CHALLENGES OF ADVERSARIAL PROCEEDINGS IN THE DIGITAL AGE

BAJO EL PESO DE LOS DATOS: EL DATA DUMPING Y LOS DESAFÍOS DEL CONTRADICTORIO EN LA ERA DIGITAL

Alcian Pereira de Souza[1], Danielle Costa de Souza Simas[2], Jeibson dos Santos Justiniano[3], Albefredo Melo de Souza Junior[4], Vânia Maria do Perpétuo Socorro Marques Marinho[5], Neuton Alves de Lima[6], Alessandro de Souza Bezerra[7]

DOI: 10.54899/dcs.v22i83.3389
Recibido: 17/09/2025 | Aceptado: 18/09/2025 | Publicación en línea: 02/10/2025.

RESUMO

O presente artigo analisa criticamente o fenômeno do *data dumping* no processo penal brasileiro, entendido como a entrega massiva e desorganizada de dados à defesa, sob o pretexto de assegurar transparência e acesso às provas. Argumenta-se que essa prática, cada vez mais comum em investigações complexas envolvendo crimes econômicos, corrupção e lavagem de dinheiro, compromete o exercício efetivo do contraditório e da ampla defesa, configurando violação ao devido processo legal e à paridade de armas. A partir de uma abordagem normativa, doutrinária e comparativa, o estudo evidencia que o acesso formal às provas não basta: é imprescindível que as informações sejam inteligíveis, organizadas e utilizáveis. A doutrina nacional, representada por Aury Lopes Jr., Fernando Capez, Yuri Felix e outros, destaca os limites da atuação estatal e alerta para os riscos da sobrecarga informacional como forma de cerceamento da defesa. No plano internacional, documentos como os *Sedona Principles* e estudos de Jenia Turner e Brian Chen reforçam a necessidade de proporcionalidade e usabilidade na produção de provas digitais, condenando a prática do *document dump*. Diante disso, propõem-se medidas concretas para mitigar o problema, como a exigência de indexação e formatos pesquisáveis, a aplicação da

[1] Doutor em Ciências pela Universidade de São Paulo (USP), Universidade do Estado do Amazonas, Manaus, Amazonas, Brasil. E-mail: alcian@uea.edu.br Orcid: https://orcid.org/0000-0002-1139-5234
[2] Mestre em Direito Ambiental pela Universidade do Estado do Amazonas (UEA), Processamento de Dados Amazonas S.A (PRODAM), Manaus, Amazonas, Brasil. E-mail: dani_souza1403@hotmail.com
Orcid: https://orcid.org/0000-0001-6104-3563
[3] Doutor em Direito pela Universidade Federal de Minas Gerais (UFMG), Universidade do Estado do Amazonas, Manaus, Amazonas, Brasil. E-mail: jeibson.justiniano@gmail.com Orcid: https://orcid.org/0009-0009-4538-0020
[4] Doutorando em Direito pela Universidade Federal de Minas Gerais (UFMG), Universidade do Estado do Amazonas, Manaus, Amazonas, Brasil. E-mail: albefredo@uea.edu.br
Orcid: https://orcid.org/0000-0002-5181-478X
[5] Doutora em Direito pela Universidade Federal de Minas Gerais (UFMG), Universidade do Estado do Amazonas (UEA), Manaus, Amazonas, Brasil. E-mail: vamrinho@uea.edu.br Orcid: https://orcid.org/0000-0002-4872-6703
[6] Doutor em Direito pela Universidade Federal de Minas Gerais (UFMG), Universidade do Estado do Amazonas (UEA), Manaus, Amazonas, Brasil. E-mail: nalima@uea.edu.br Orcid: https://orcid.org/0009-0003-2638-0574
[7] Doutor em Ciências pela Universidade de São Paulo (USP), Universidade do Estado do Amazonas, Manaus, Amazonas, Brasil. E-mail: abezerra@uea.edu.br Orcid: https://orcid.org/0000-0002-6410-7099

proporcionalidade na entrega de dados, a previsão de remédios processuais (prorrogação de prazos, filtragem judicial, exclusão de provas abusivas) e a consolidação de uma cultura de cooperação e lealdade processual. Conclui-se que enfrentar o *data dumping* não é um desafio meramente técnico, mas uma exigência democrática. Preservar a efetividade do contraditório e da ampla defesa na era digital significa reafirmar a centralidade do devido processo legal e da dignidade da pessoa humana como fundamentos do Estado de Direito.

Palavras-chave: Data Dumping. Processo Penal Digital. Contraditório. Ampla Defesa. Paridade de Armas. Devido Processo Legal.

ABSTRACT

This article critically analyzes the phenomenon of data dumping in the Brazilian criminal procedure, understood as the massive and disorganized delivery of data to the defense, under the pretext of ensuring transparency and access to evidence. It is argued that this practice, increasingly common in complex investigations involving economic crimes, corruption, and money laundering, undermines the effective exercise of adversarial proceedings and the right to a full defense, constituting a violation of due process of law and equality of arms. From a normative, doctrinal, and comparative approach, the study shows that mere formal access to evidence is not enough: it is essential that information be intelligible, organized, and usable. National doctrine, represented by Aury Lopes Jr., Fernando Capez, Yuri Felix, among others, highlights the limits of state action and warns against the risks of informational overload as a form of restricting the defense. At the international level, documents such as the Sedona Principles and studies by Jenia Turner and Brian Chen reinforce the need for proportionality and usability in the production of digital evidence, condemning the practice of document dumping. In light of this, concrete measures are proposed to mitigate the problem, such as the requirement of indexing and searchable formats, the application of proportionality in data delivery, the provision of procedural remedies (extension of deadlines, judicial filtering, exclusion of abusive evidence), and the consolidation of a culture of cooperation and procedural loyalty. It is concluded that confronting data dumping is not merely a technical challenge, but a democratic necessity. Preserving the effectiveness of adversarial proceedings and full defense in the digital age means reaffirming the centrality of due process of law and the dignity of the human person as foundations of the Rule of Law.

Keywords: Data Dumping. Digital Criminal Procedure. Adversarial Proceedings. Full Defense. Equality of arms. Due Process of Law.

RESUMEN

El presente artículo analiza críticamente el fenómeno del *data dumping* en el proceso penal brasileño, entendido como la entrega masiva y desorganizada de datos a la defensa, bajo el pretexto de asegurar transparencia y acceso a las pruebas. Se sostiene que esta práctica, cada vez más común en investigaciones complejas que involucran delitos económicos, corrupción y lavado de dinero, compromete el ejercicio efectivo del contradictorio y de la defensa amplia, configurando una violación al debido proceso legal y a la igualdad de armas. Desde un enfoque normativo, doctrinario y comparativo, el estudio evidencia que el acceso formal a las pruebas no basta: es imprescindible que la información sea inteligible, organizada y utilizable. La doctrina nacional, representada por Aury Lopes Jr., Fernando Capez, Yuri Felix y otros, destaca los límites

de la actuación estatal y alerta sobre los riesgos de la sobrecarga informacional como forma de restricción de la defensa. En el plano internacional, documentos como los *Sedona Principles* y estudios de Jenia Turner y Brian Chen refuerzan la necesidad de proporcionalidad y usabilidad en la producción de pruebas digitales, condenando la práctica del *document dump*. Ante ello, se proponen medidas concretas para mitigar el problema, tales como la exigencia de indexación y formatos buscables, la aplicación de la proporcionalidad en la entrega de datos, la previsión de remedios procesales (prórroga de plazos, filtrado judicial, exclusión de pruebas abusivas) y la consolidación de una cultura de cooperación y lealtad procesal. Se concluye que enfrentar el *data dumping* no es un desafío meramente técnico, sino una exigencia democrática. Preservar la efectividad del contradictorio y de la defensa amplia en la era digital significa reafirmar la centralidad del debido proceso legal y de la dignidad de la persona humana como fundamentos del Estado de Derecho.

Palabras clave: Data Dumping. Proceso Penal Digital. Contradictorio. Defensa Amplia. Igualdad de Armas. Debido Proceso Legal.

INTRODUÇÃO

O avanço das tecnologias digitais e o crescimento exponencial da produção de informações impactaram diretamente a forma como provas são obtidas, armazenadas e apresentadas no processo penal. Nesse cenário, emergiu o fenômeno denominado *data dumping*, que consiste na entrega massiva, desorganizada e, em grande parte, irrelevante de documentos, registros e arquivos digitais à defesa, sob o pretexto de assegurar acesso amplo às provas. À primeira vista, tal prática poderia ser interpretada como manifestação de transparência processual; no entanto, na prática, ela tende a inviabilizar o exercício efetivo do contraditório e da ampla defesa, em afronta ao art. 5º, LV, da Constituição Federal.

Esse problema se agrava em investigações complexas, como aquelas envolvendo crimes econômicos, corrupção e lavagem de dinheiro, em que podem ser fornecidos terabytes de dados, extratos bancários, e-mails, conversas em aplicativos, metadados, gravações, sem qualquer forma de indexação ou organização mínima. A defesa, sujeita a prazos processuais restritos, enfrenta sérias dificuldades para identificar informações relevantes, o que representa, em termos práticos, uma barreira intransponível para a elaboração de teses defensivas consistentes. Dessa forma, o que se apresenta formalmente como acesso às provas revela-se, materialmente, um obstáculo que desequilibra a paridade de armas no processo penal.

A doutrina brasileira, representada por autores como Aury Lopes Jr. e Fernando Capez, enfatiza que as garantias constitucionais do contraditório e da ampla defesa não podem ser esvaziadas por expedientes que inviabilizem sua aplicação prática. Mais recentemente, estudos como os de Yuri Felix e Carlos Hélder Mendes têm evidenciado que a coleta e disponibilização de grandes volumes de provas digitais exigem critérios metodológicos claros, sob pena de se transformar o direito de acesso em mero formalismo incapaz de assegurar defesa efetiva. Na mesma linha, a literatura estrangeira, a exemplo das orientações do *Sedona Conference* e dos estudos de Jenia Turner e Brian Chen, aponta que a mera entrega de dados em massa não satisfaz o dever de disclosure, sendo imprescindível que as informações sejam apresentadas em formato inteligível, indexado e pesquisável.

Diante desse contexto, este artigo busca analisar criticamente o fenômeno do *data dumping* no processo penal brasileiro, explorando seus impactos sobre os direitos fundamentais, a partir de referenciais normativos, doutrinários e comparativos. O objetivo é demonstrar que, mais do que um problema de técnica processual, trata-se de uma questão de efetividade de garantias constitucionais, exigindo do Judiciário e dos atores processuais a adoção de critérios de proporcionalidade, razoabilidade e cooperação. Além de problematizar a prática, o trabalho propõe soluções normativas e processuais capazes de mitigar seus efeitos, reforçando a centralidade do devido processo legal na era digital.

O FENÔMENO DO *DATA DUMPING* NO PROCESSO PENAL

O termo *data dumping*, ainda pouco difundido na doutrina nacional, vem sendo empregado para designar a prática de disponibilizar à defesa um volume massivo e desorganizado de informações, em geral relacionadas a interceptações telefônicas, registros bancários, metadados, arquivos digitais ou comunicações eletrônicas (CNN Brasil, 2025). Sob o discurso da transparência e da ampla publicidade, essa entrega indiscriminada de dados não cumpre, em essência, a finalidade de garantir o efetivo exercício do contraditório, mas, ao contrário, gera entraves quase intransponíveis à atuação defensiva. Trata-se de uma forma de sobrecarga informacional que, em vez de democratizar o acesso às provas, pode configurar verdadeiro cerceamento de defesa.

No plano jurídico, o problema se traduz na aparente dissociação entre forma e substância: há, formalmente, cumprimento da obrigação de fornecer acesso às provas, mas, materialmente,

esse acesso se revela inócuo. Como assinala Aury Lopes Jr. (2019), não basta assegurar o direito de acesso em tese; é necessário que esse acesso seja exercido em condições que possibilitem à defesa a compreensão e utilização dos elementos probatórios. O excesso desorganizado de informações acaba por distorcer o equilíbrio entre acusação e defesa, violando princípios como a paridade de armas, a razoabilidade e a cooperação processual.

O impacto do *data dumping* é ainda mais visível em investigações complexas de natureza econômica ou financeira, em que podem ser entregues terabytes de documentos sem qualquer indexação ou separação por relevância. Nessas situações, os prazos processuais fixados pela legislação processual penal tornam-se manifestamente incompatíveis com a análise da massa documental. Como resultado, a defesa se vê diante de uma barreira prática insuperável, comprometendo a elaboração de teses defensivas adequadas. Essa prática, portanto, não representa uma ampliação do devido processo legal, mas uma subversão de sua lógica, criando um ambiente de assimetria processual.

O Superior Tribunal de Justiça tem sido claro ao defender que a produção de provas digitais deve obedecer a critérios específicos, nos quais se inclui a proporcionalidade, organização e usabilidade, de modo a evitar a sobrecarga artificial da parte adversa e falta de confiabilidade na prova.

Conforme se extrai do acórdão expedido no bojo do HC 828.054- STJ:

> (...) Diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material.
> A auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade são quatro aspectos essenciais das evidências digitais, os quais buscam ser garantidos pela utilização de metodologias e procedimentos certificados, como, e.g., os recomendados pela ABNT.
> A observação do princípio da mesmidade visa a assegurar a confiabilidade da prova, a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital. Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo hash, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital. De relevo trazer à baila o entendimento majoritário desta Quinta Turma no sentido de que "é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia" (AgRg no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, DJe de 2/3/2023) (...). (STJ, 2024).

Deste modo, a mera entrega de dados brutos não satisfaz o dever estatal: o material deve ser entregue em condições utilizáveis, indexadas e compreensíveis.

Assim, o *data dumping* no processo penal brasileiro deve ser compreendido não apenas como um problema de técnica probatória, mas como uma prática que atinge o núcleo das garantias constitucionais do acusado. Ele não apenas dificulta o trabalho da defesa, mas compromete a própria legitimidade do processo penal acusatório, ao criar uma fachada de transparência que oculta a desigualdade material entre as partes.

FUNDAMENTOS NORMATIVOS E DOUTRINÁRIOS

A análise do *data dumping* no processo penal brasileiro demanda, inicialmente, a recuperação dos fundamentos constitucionais que asseguram a efetividade das garantias processuais. O art. 5º, incisos LIV e LV, da Constituição Federal consagra o devido processo legal, o contraditório e a ampla defesa como direitos fundamentais, assegurando ao acusado meios efetivos de responder à acusação em igualdade de condições. Não se trata de meros enunciados formais, mas de princípios estruturantes do Estado de Direito, que exigem concretização material no âmbito processual. Nesse sentido, a entrega massiva e desorganizada de dados contraria tais garantias, pois esvazia a possibilidade de exercício real da defesa.

A doutrina brasileira tem enfatizado a centralidade desses princípios. Aury Lopes Jr. (2019) sustenta que o contraditório não pode ser reduzido a um simples “direito de ser ouvido”, mas deve se traduzir em um direito de influência real sobre a formação da prova e sobre a decisão judicial. Fernando Capez (2020), ao abordar os limites da atuação estatal na investigação, destaca que a defesa não pode ser colocada em situação de desvantagem material frente ao aparato acusatório. Já Luiz Flávio Gomes (2003), embora focado na discussão sobre provas ilícitas, contribui ao sublinhar que a legitimidade da prova depende de sua acessibilidade e da possibilidade de impugnação efetiva, elementos igualmente comprometidos pelo *data dumping*.

Autores contemporâneos têm aprofundado a reflexão sobre a especificidade das provas digitais. Yuri Felix e Carlos Hélder Carvalho Furtado Mendes (2024), ao analisar a aquisição de provas informáticas, apontam que a coleta de grandes volumes de dados requer método, transparência e possibilidade de contraprova, sob pena de o contraditório se tornar inviável. André Machado Maya (2017), por sua vez, discute o acesso a dados públicos e privados à luz da jurisprudência europeia, enfatizando a necessidade de compatibilização entre a produção

probatória e as garantias fundamentais. Pedro de Oliveira Alves e Felipe Gustavo Oliveira Filho (2023) aproximam a prática do *data dumping* da figura do *fishing expedition*, em que a autoridade busca dados de forma ampla e inespecífica, produzindo acervos de difícil ou impossível manejo pela defesa. Já Marcelo Mendes Arigony, Letícia Thomasi Jahnke Botton e Ana Luiza Ortiz Arigony (2025) analisam a persecução penal digital e os riscos da massificação probatória, ressaltando que a defesa tende a ser sufocada diante do volume de informações.

No plano internacional, o debate encontra paralelo em documentos e análises amplamente citados. O *Sedona Conference (2017)* defende, em seus relatórios e princípios, que a produção de provas eletrônicas deve ser organizada, pesquisável e proporcional, vedando a prática do chamado *document dump*. Jenia I. Turner (2018), em estudo sobre o *e-discovery* criminal, alerta que a sobrecarga de informações compromete prazos e garantias constitucionais, propondo que técnicas civis de organização sejam adaptadas ao processo penal. Brian Chen (2024) mostra que o *big data* pode diluir provas exculpatórias em meio a vastos conjuntos de informações, violando obrigações de disclosure. Por fim, a National Association of Criminal Defense Lawyers (NACDL) reconhece expressamente o *data dump* como prática antiética, que pode ensejar sanções e ordens judiciais corretivas.

Esses aportes normativos e doutrinários convergem para uma mesma conclusão: o *data dumping* não é apenas um problema técnico ou logístico, mas um expediente que compromete a essência do contraditório, da ampla defesa e da paridade de armas. Ao invés de garantir acesso pleno às provas, transforma o processo penal em um espaço de desigualdade estrutural, onde a acusação se beneficia da complexidade informacional e a defesa se vê impossibilitada de exercer plenamente suas funções constitucionais.

IMPACTOS E DESAFIOS NO PROCESSO PENAL DIGITAL

A consolidação do processo penal digital, marcada pelo uso intensivo de tecnologias de vigilância e coleta de dados, potencializou tanto as possibilidades investigativas quanto os riscos de violação às garantias fundamentais. Nesse contexto, o *data dumping* se insere como uma prática que amplia sobremaneira as dificuldades da defesa, criando obstáculos práticos e éticos à efetividade do contraditório e da ampla defesa. O impacto imediato consiste na impossibilidade de examinar, em prazos processuais exíguos, grandes volumes de informações sem qualquer organização ou filtragem mínima, comprometendo a elaboração de teses defensivas consistentes.

Além da sobrecarga quantitativa, há o risco qualitativo de diluição de provas exculpatórias em meio a um oceano de dados. Brian Chen (2024) observa, em estudo recente, que a entrega indiscriminada de bases massivas pode ocultar ou tornar inacessíveis elementos favoráveis ao acusado, esvaziando o dever de disclosure da acusação. Esse fenômeno produz uma falsa impressão de transparência: o acesso é formalmente garantido, mas, na prática, a defesa não consegue identificar os pontos cruciais para contestar a narrativa acusatória. Trata-se, portanto, de um desequilíbrio estrutural que fragiliza a paridade de armas no processo penal.

A dimensão ética do problema também merece destaque. Na literatura de *e-discovery*, a prática de *document dump* é frequentemente associada a expedientes de má-fé, pois transfere ao adversário o ônus de organizar e filtrar informações que deveriam ser entregues em formato utilizável. No Brasil, o termo *data dumping* foi expressamente utilizado de forma bastante recente pelo Ministro Luiz Fux, por ocasião do julgado do caso conhecido como golpe do 8 de janeiro[8], extraindo-se a ideia de que os princípios constitucionais da razoabilidade, cooperação processual e lealdade oferecem fundamentos suficientes para a censura dessa prática (CNN Brasil, 2025).

Outro desafio relevante relaciona-se aos chamados *fishing expeditions*. Mandados de busca e apreensão amplos e genéricos, especialmente no âmbito digital, resultam em apreensões indiscriminadas de dados pessoais e profissionais, que, ao serem produzidos sem delimitação adequada, aumentam o risco de *data dumping*. Como apontam Pedro de Oliveira Alves e Felipe Gustavo Oliveira Filho (2023), a coleta massiva sem critério viola tanto o direito fundamental à proteção de dados quanto a lógica do devido processo legal. A massificação da prova digital, longe de servir à verdade processual, pode converter-se em obstáculo intransponível à defesa, configurando verdadeiro excesso estatal.

Deste modo, os impactos do *data dumping* se projetam em múltiplas dimensões: prática (impossibilidade de análise em tempo hábil), qualitativa (diluição de elementos exculpatórios), ética (uso de expedientes protelatórios ou abusivos) e estrutural (desequilíbrio processual). Os desafios postos ao processo penal digital, portanto, não dizem respeito apenas à gestão de informações, mas à própria preservação da legitimidade democrática do processo penal.

[8] No dia 8 de janeiro de 2023 o Brasil foi surpreendido por um ataque, quando autonomeados patriotas invadiram e vandalizaram o Congresso Nacional, o Palácio do Planalto e o Supremo Tribunal Federal (STF) (Ricupero, 2024).

PROPOSTAS E CAMINHOS PARA SUPERAR O *DATA DUMPING*

Superar os riscos do *data dumping* demanda não apenas a crítica doutrinária à prática, mas também a formulação de parâmetros normativos e processuais que assegurem a efetividade do contraditório e da ampla defesa no processo penal digital. O ponto de partida deve ser a compreensão de que o dever de disponibilizar provas não se esgota na entrega formal dos dados, mas requer que o acesso seja inteligível, organizado e proporcional às necessidades do caso concreto.

Uma primeira medida consiste na exigência de organização mínima das informações disponibilizadas. Dados devem ser entregues com indexação, metadados preservados e em formatos pesquisáveis, de modo que a defesa possa efetivamente manuseá-los. Essa diretriz encontra respaldo em documentos internacionais, como os *Sedona Principles*, que repudiam a prática de *document dump* e estabelecem a usabilidade como requisito essencial da produção probatória. A adoção desses critérios no Brasil pode servir como guia de boas práticas, ainda que em caráter infralegal, reforçando a cooperação processual entre as partes.

Outra proposta é a aplicação do princípio da proporcionalidade na entrega de provas digitais. Assim como ocorre em sistemas estrangeiros, a acusação não deve ser autorizada a repassar indiscriminadamente grandes massas de dados sem relevância direta para o objeto da acusação. Cabe ao Judiciário intervir para delimitar a produção probatória, filtrando informações e impondo parâmetros de pertinência, de modo a equilibrar o acesso e evitar sobrecargas artificiais. Essa prática pode ser complementada por medidas de mitigação, como a entrega de *key-document sets* e a definição de critérios de seleção previamente discutidos em audiência com as partes.

Também se mostra imprescindível prever remédios processuais contra o *data dumping*. Entre eles, destacam-se: a prorrogação de prazos processuais quando a defesa receber volumes massivos de informações; a possibilidade de requerer ordem judicial para reorganização ou filtragem dos dados; e, em situações extremas, a exclusão de provas entregues de forma abusiva ou ininteligível. Essas medidas não apenas preservam a integridade do processo, mas desincentivam condutas de má-fé por parte da acusação.

Por fim, a consolidação de uma cultura de cooperação e lealdade processual é fundamental para enfrentar o problema. Doutrina e jurisprudência devem avançar no sentido de reconhecer expressamente o *data dumping* como forma de abuso processual, capaz de comprometer a

legitimidade do processo penal. Nesse cenário, a defesa, o Ministério Público e o Judiciário compartilham a responsabilidade de adotar boas práticas que garantam a paridade de armas, preservando a substância das garantias constitucionais diante dos desafios impostos pela era digital.

METODOLOGIA

A presente pesquisa adota uma abordagem qualitativa, de caráter exploratório e explicativo, voltada à análise crítica do fenômeno do *data dumping* no processo penal brasileiro, entendido como a entrega massiva e desorganizada de dados à defesa sob o pretexto de assegurar transparência e acesso às provas. O enfoque qualitativo permite compreender esse fenômeno em sua complexidade jurídica, técnica e política, considerando tanto os fundamentos normativos quanto os efeitos práticos sobre as garantias constitucionais do contraditório e da ampla defesa.

Do ponto de vista da natureza, trata-se de uma pesquisa básica, na medida em que busca aprofundar o conhecimento sobre a relação entre processo penal digital, sobrecarga informacional e efetividade de direitos fundamentais, fornecendo subsídios teóricos e práticos para o aprimoramento da justiça criminal na era digital.

A escolha metodológica se ancora em revisão bibliográfica e documental, incluindo legislações nacionais pertinentes como a Constituição Federal; Jurisprudência recente do Superior Tribunal de Justiça e do Supremo Tribunal Federal, com destaque para acórdãos sobre cadeia de custódia e validade da prova digital; Documentos internacionais, como os *Sedona Principles*, bem como relatórios e pareceres de entidades como a NACDL; Literatura científica especializada (Aury Lopes Jr., Fernando Capez, Yuri Felix, Brian Chen, Jenia Turner, entre outros).

A metodologia adotada, portanto, busca articular fundamentos normativos, dados empíricos (jurisprudenciais e institucionais) e análises doutrinárias em uma perspectiva dialética, evidenciando como práticas processuais de sobrecarga probatória afetam a substância das garantias constitucionais. Assim, a pesquisa não se limita a descrever o fenômeno, mas propõe-se a problematizá-lo criticamente e a sugerir parâmetros para sua mitigação, contribuindo para o debate acadêmico e para a formulação de práticas judiciais e legislativas que reforcem a centralidade do devido processo legal no contexto digital.

CONCLUSÃO

A investigação do fenômeno do *data dumping* no processo penal brasileiro permitiu identificar que se trata de uma prática que desafia diretamente os pilares constitucionais da ampla defesa, do contraditório e da paridade de armas. A entrega indiscriminada de volumes massivos e desorganizados de dados, muitas vezes sem qualquer indexação ou separação por relevância, cria uma aparência de legalidade e transparência, mas, em termos materiais, converte-se em um obstáculo quase intransponível à atuação defensiva. Esse cenário evidencia a tensão entre forma e substância no processo penal: cumpre-se, formalmente, a obrigação de disponibilizar as provas, mas inviabiliza-se, na prática, a sua utilização adequada pela defesa.

A literatura nacional e internacional é enfática ao demonstrar que o contraditório só se realiza plenamente quando o acesso à prova é efetivo e utilizável. Aury Lopes Jr. e Fernando Capez destacam que as garantias constitucionais não podem ser esvaziadas por expedientes que criem desvantagem material à defesa, enquanto Yuri Felix e Carlos Hélder Mendes apontam para a necessidade de critérios técnicos na coleta e disponibilização de provas digitais. No direito comparado, os documentos produzidos pelo *Sedona Conference*, os estudos de Jenia Turner e a análise de Brian Chen demonstram que a mera entrega de grandes bases de dados não satisfaz o dever de disclosure, pois dilui a informação relevante em um volume incontrolável de irrelevâncias. Trata-se, portanto, de um fenômeno global, cujos riscos já vêm sendo debatidos em sistemas jurídicos mais maduros no enfrentamento de provas digitais.

O impacto do *data dumping* manifesta-se em diferentes dimensões. Do ponto de vista prático, a defesa se vê impossibilitada de analisar, em tempo hábil, os elementos necessários para a construção de sua tese. Sob o prisma qualitativo, a diluição de provas exculpatórias em meio a dados irrelevantes compromete a busca da verdade processual. Em termos éticos, a prática aproxima-se da má-fé processual, pois transfere à parte adversa o ônus de organizar informações que deveriam ser fornecidas de forma inteligível. Finalmente, no aspecto estrutural, o desequilíbrio criado fragiliza a legitimidade do processo penal acusatório, transformando-o em um procedimento assimétrico e contrário aos ideais de justiça e cooperação processual.

Nesse contexto, as propostas apresentadas neste trabalho ganham relevo. A exigência de organização mínima dos dados (indexação, metadados, formatos pesquisáveis), a aplicação do princípio da proporcionalidade na entrega das provas digitais e a previsão de remédios processuais (como prorrogação de prazos, filtragem judicial e exclusão de provas entregues de

forma abusiva) representam caminhos viáveis para restaurar a equidade processual. A consolidação de uma cultura de cooperação e lealdade entre acusação e defesa, inspirada nas melhores práticas internacionais, também se revela indispensável para evitar que o processo se torne refém de expedientes abusivos.

O combate ao *data dumping* não é, portanto, um mero debate técnico sobre gestão de informações, mas uma exigência democrática que toca a essência do Estado de Direito. A preservação do devido processo legal na era digital requer não apenas a adaptação de regras formais, mas a afirmação de uma postura judicial ativa, capaz de impor limites ao excesso estatal e de proteger a integridade da defesa. Nesse sentido, a crítica ao *data dumping* transcende o plano acadêmico, constituindo também uma agenda prática para operadores do direito, tribunais e legisladores.

Em última análise, reconhecer e enfrentar o *data dumping* é reafirmar que a justiça penal não pode se contentar com aparências formais de legalidade. A legitimidade do processo depende de que cada acusado tenha condições reais e materiais de exercer sua defesa, influir na decisão judicial e garantir que o peso do aparato estatal não se converta em barreira intransponível. Preservar tais garantias é condição imprescindível para que o processo penal, mesmo diante das complexidades da sociedade digital, continue sendo expressão da dignidade da pessoa humana e instrumento de proteção dos direitos fundamentais.

REFERÊNCIAS

ARIGONY, Marcelo Mendes; BOTTON, Letícia Thomasi Jahnke; ARIGONY, Ana Luiza Ortiz. ***Persecução penal digital**: a prova na era da informação*. Revista de Direito, Ética e Tecnologia da Informação, v. 1, n. 20, 2025. Disponível em < https://direitoeti.com.br/direitoeti/article/view/268> Acesso em 11 Set. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em < https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 16 set. 2025.

BRASIL. Superior Tribunal de Justiça. **AgRg no Habeas Corpus n. 828.054/RN**. Relator Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 23 abr. 2024, Diário da Justiça eletrônico, Brasília, DF, 24 abr. 2024. Disponível em < https://www.jusbrasil.com.br/jurisprudencia/busca?q=hc+828054>. Acesso em: 16 set. 2025.

CAPEZ, Fernando. ***Curso de processo penal***. 27. ed. São Paulo: Saraiva, 2020.

CHEN, Brian. ***Big Data and Brady Disclosures***. New York University Law Review, v. 99, n. 2, 2024. Disponível em < https://nyulawreview.org/issues/volume-99-number-5/big-data-and-brady-disclosures/> Acesso em 10 Set. 2025.

CNN Brasil. **Entenda o que é a expressão "data dump", citada por Fux no Julgamento**. Artigo publicado em 10 Set. 2025. Disponível em < https://www.cnnbrasil.com.br/politica/entenda-o-que-e-a-expressao-data-dump-citada-por-fux-no-julgamento/ > Acesso em 16 Set. 2025.

FELIX, Yuri; MENDES, Carlos Hélder Carvalho Furtado. **Aquisição das fontes de prova penal digital**: reflexões a partir do informativo de jurisprudência nº 763 do STJ. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 197, n. 197, p. 215–247, 2024. Disponível em < https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/504> Acesso em 10 Set. 2025.

GOMES, Luiz Flávio. **Prova ilícita:** direito à exclusão dos autos do processo (exclusionary rule). Revista dos Tribunais São Paulo v.92, n.809, p. 471-484, mar. 2003. Disponível em: https://dspace.almg.gov.br/handle/11037/35501. Acesso em: 12 Set. 2025.

LOPES JR., Aury. ***Direito processual penal***. 16. ed. São Paulo: Saraiva, 2019.

MAYA, André Machado. **Conservação e acesso a dados públicos e privados para fins penais:** a normativa legal brasileira examinada desde a perspectiva da jurisprudência do Tribunal de Justiça da Comunidade Europeia. *Revista CEJ*, v. 26, n. 92, 2022. Disponível em < https://dialnet.unirioja.es/servlet/articulo?codigo=6339757> Acesso em 08 Set. 2025.

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS (NACDL). ***Commentary on prosecutorial data dumps and document dump discovery practices***. Washington, DC: NACDL, 2021.

OLIVEIRA ALVES, Pedro de; OLIVEIRA FILHO, Felipe Gustavo Ramos de. **O direito fundamental de proteção de dados no processo penal brasileiro**: a ilicitude dos mandados de busca e apreensão como práticas de *fishing expedition*. *Revista Acadêmica da Faculdade de Direito do Recife*, v. 95, n. 1, 2023.

RICUPERO, Bernardo. **O que foi o 8 de janeiro?** Artigo publicado em 8 jan.2024. Disponível em < https://jornal.usp.br/artigos/o-que-foi-o-8-de-janeiro/> Acesso em 14 Set. 2025.

THE SEDONA CONFERENCE. ***Commentary on Proportionality in Electronic Discovery***. 2017. Disponível em < https://www.thesedonaconference.org/download-publication?fid=3003> Acesso em 16 Set. 2025.

TURNER, Jenia I. **Managing Digital Discovery in Criminal Cases**.109 J. CRIMINOLOGY. L. & CRIMINOLOGY 237, 2019. Disponível em < https://scholarlycommons.law.northwestern.edu/jclc/vol109/iss2/3/> Acesso em 15 Set. 2025.