v7.n11.2026

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

A PROVA DIGITAL NA PERSECUÇÃO PENAL DOS CRIMES CIBERNÉTICOS

DIGITAL EVIDENCE IN THE CRIMINAL PROSECUTION OF CYBERCRIMES

LA PRUEBA DIGITAL EN LA PERSECUCIÓN PENAL DE LOS DELITOS CIBERNÉTICOS

Emilly Betoldo da Silva[1], Luiz Paulo Busquim Braga[2]

e7119699
https://doi.org/10.47820/recima21.v7i11.9699

PUBLICADO: 11/2026

RESUMO

O artigo investiga os principais obstáculos à obtenção, à preservação e à valoração da prova digital na persecução penal dos crimes cibernéticos no Brasil. Parte-se da hipótese de que esses obstáculos não decorrem apenas da ausência de disciplina legal específica, mas de fatores ligados a cada etapa da prova, que teriam em comum a dificuldade de torná-la auditável pela defesa. A pesquisa adota abordagem qualitativa e método hipotético-dedutivo, com revisão de literatura por busca estruturada nas bases SciELO, Google Acadêmico e Oasisbr, pesquisa documental e exame de julgados selecionados do STF e do STJ. Os resultados indicam que, na obtenção, predominam autorizações genéricas de acesso a dados e a dependência de provedores e da cooperação internacional; na preservação, a cadeia de custódia do Código de Processo Penal não incorpora os padrões técnicos da prova digital; e, na valoração, persiste divergência sobre as consequências da quebra da cadeia e o ônus de demonstrar a integridade da prova. Conclui-se que, no conjunto examinado, a hipótese encontra respaldo e pode ser refinada: a auditabilidade pela defesa é critério para distinguir as falhas que afetam apenas o valor da prova daquelas que impedem sua admissão, cabendo a quem a produz assegurar as condições de sua verificação.

PALAVRAS-CHAVE: Prova Digital. Crimes Cibernéticos. Cadeia de Custódia. Persecução Penal. Processo Penal.

ABSTRACT

This article examines the main obstacles to obtaining, preserving and evaluating digital evidence in the criminal prosecution of cybercrimes in Brazil. Its hypothesis is that these obstacles stem not only from the lack of specific legal rules, but from factors linked to each stage of the evidence that share the difficulty of enabling the defense to independently verify the digital evidence. The research is qualitative and hypothetical-deductive, combining a structured literature search in the SciELO, Google Scholar and Oasisbr databases, documentary research and selected decisions of the Brazilian Supreme Court (STF) and Superior Court of Justice (STJ). Results show that, in obtaining evidence, generic authorizations to access data and dependence on providers and international cooperation prevail; in preservation, the Code of Criminal Procedure's chain of custody rules do not incorporate the technical standards of digital evidence; and, in evaluation, there is disagreement about the consequences of a break in the chain and the burden of demonstrating the integrity of the evidence. Within the material examined, the hypothesis was supported and refined: auditability by the defense is a criterion for distinguishing failures that affect

[1] Graduanda em Direito pela Faculdade Cristo Rei (FACCREI), Cornélio Procópio/PR, com pesquisa na área de prova digital e processo penal.
[2] Bacharel em Direito pela Faculdade Cristo Rei (FACCREI), Cornélio Procópio/PR, advogado e professor do Curso de Direito da Faculdade Cristo Rei (FACCREI).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

only the weight of the evidence from those that prevent its admission, and whoever produces it must ensure it can be verified.

KEYWORDS: *Digital Evidence. Cybercrimes. Chain of Custody. Criminal Prosecution. Criminal Procedure.*

RESUMEN
El artículo investiga los principales obstáculos para la obtención, la preservación y la valoración de la prueba digital en la persecución penal de los delitos cibernéticos en Brasil. Se parte de la hipótesis de que dichos obstáculos no derivan únicamente de la ausencia de una regulación legal específica, sino de factores vinculados a cada etapa de la prueba, que tendrían en común la dificultad de hacerla auditable por la defensa. La investigación adopta un enfoque cualitativo y el método hipotético-deductivo, con revisión de literatura mediante búsqueda estructurada en las bases SciELO, Google Académico y Oasisbr, investigación documental y examen de decisiones seleccionadas del STF y del STJ. Los resultados indican que, en la obtención, predominan las autorizaciones genéricas de acceso a datos y la dependencia de los proveedores y de la cooperación internacional; en la preservación, la cadena de custodia del Código de Proceso Penal no incorpora los estándares técnicos de la prueba digital; y, en la valoración, persiste la divergencia sobre las consecuencias de la ruptura de la cadena y la carga de demostrar la integridad de la prueba. Se concluye que, en el conjunto examinado, la hipótesis encuentra respaldo y puede ser refinada: la auditabilidad por la defensa es un criterio para distinguir las fallas que afectan solo el valor de la prueba de aquellas que impiden su admisión, correspondiendo a quien la produce asegurar las condiciones para su verificación.

PALABRAS CLAVE: *Prueba Digital. Delitos Cibernéticos. Cadena de Custodia. Persecución Penal. Proceso Penal.*

1. INTRODUÇÃO

O estelionato consolidou-se como o principal crime patrimonial no Brasil. Em 2025, foram registradas 2.261.055 ocorrências desse delito, número 429,8% superior ao de 2018 (Fórum Brasileiro de Segurança Pública, 2026, p. 15, 125). Os registros policiais, no entanto, não alcançam todo o fenômeno: segundo pesquisa realizada pelo FBSP em março de 2026 e mencionada no Anuário, 15,8% da população com 16 anos ou mais, o equivalente a 26,3 milhões de pessoas, foi vítima de golpe ou perdeu dinheiro pela internet ou pelo celular no último ano (Fórum Brasileiro de Segurança Pública, 2026, p. 123).

Os dados do FBSP indicam, ainda, que entre 2024 e 2025 os boletins de ocorrência de estelionato passaram de 2.193.122 para 2.261.055, os processos penais de 52.649 para 63.771 e o número de presos por esse crime de 4.112 para 4.819 (Fórum Brasileiro de Segurança Pública, 2026, p. 125). Segundo cálculo próprio, esses números correspondem a aumentos de 3,1%, 21,1% e 17,2%, respectivamente. A comparação entre esses números sugere um descompasso entre registros e processos. A partir dos mesmos dados, calcula-se que o número de processos instaurados correspondeu a 2,4% do número de ocorrências registradas em 2024 e a 2,8% em 2025. Trata-se, porém, de comparação descritiva entre agregados estatísticos

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

distintos, sem correspondência individual ou temporal necessária entre ocorrências e processos: um mesmo processo pode reunir diversas ocorrências, e os processos instaurados em um ano não se referem necessariamente aos registros do mesmo período. Os percentuais não demonstram, portanto, quantas ocorrências deixaram de chegar ao Judiciário, mas indicam uma diferença de escala que sugere um possível déficit de responsabilização. Entre os fatores que podem contribuir para esse descompasso, destacam-se as dificuldades de investigação de delitos praticados em meio digital, em especial as relativas à obtenção, à preservação e à valoração da prova digital, objeto deste estudo.

O crescimento descrito insere-se no campo dos crimes cibernéticos, expressão que a doutrina emprega como sinônima de crimes eletrônicos, virtuais, digitais ou informáticos (Molitor; Velazquez, 2017, p. 83). Esses delitos costumam ser divididos em próprios e impróprios: os primeiros dependem necessariamente do uso de ambiente computacional, como a disseminação de vírus e a invasão e destruição de bancos de dados, ao passo que nos segundos a tecnologia é apenas o meio de execução de condutas que poderiam ser praticadas por outras vias, como os crimes contra a honra e o furto (Molitor; Velazquez, 2017, p. 84). No ordenamento brasileiro, exemplificam essas categorias, respectivamente, a invasão de dispositivo informático (art. 154-A do Código Penal) e a fraude eletrônica (art. 171, § 2º-A, do Código Penal). No campo probatório, nos crimes próprios, os vestígios são, em regra, essencialmente digitais; nos impróprios, a prática a distância e sem contato físico com a vítima faz da prova digital, frequentemente, o principal meio de identificação da autoria. Por isso, este artigo trata do regime da prova digital nesses delitos, e não dos tipos penais.

O ordenamento brasileiro dispõe de marcos normativos e jurisprudenciais relevantes para a matéria. Entre eles, destacam-se o Marco Civil da Internet (Lei nº 12.965/2014), a disciplina da cadeia de custódia inserida no Código de Processo Penal pela Lei nº 13.964/2019, a promulgação da Convenção de Budapeste pelo Decreto nº 11.491/2023 e a tese fixada pelo Supremo Tribunal Federal no Tema 977 da repercussão geral, em 2025, ainda pendente de embargos de declaração. Apesar desses marcos, a doutrina aponta a insuficiência do tratamento legal conferido à prova digital. Saad, Rossi e Partata (2024, p. 18-19) observam que o acesso a dados armazenados em dispositivos apreendidos tem sido regido pelas normas da busca e apreensão, concebidas para o mundo físico, o que equipara coisas materiais a dados, ainda que o acesso a estes seja consideravelmente mais invasivo. Diante da fragilidade e da volatilidade desses elementos, os autores defendem que a lei estabeleça com clareza os procedimentos aplicáveis a cada etapa, da obtenção à valoração (Saad; Rossi; Partata, 2024, p. 24), e concluem que a obtenção de provas digitais demanda disciplina jurídica própria no processo penal

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

brasileiro (Saad; Rossi; Partata, 2024, p. 27). É nesse contexto, marcado pela insuficiência de parâmetros normativos para obter, preservar e valorar a prova digital, que se insere o problema desta pesquisa.

Diante desse quadro, a presente pesquisa busca responder à seguinte pergunta: quais os principais obstáculos à obtenção, à preservação e à valoração da prova digital na persecução penal dos crimes cibernéticos no ordenamento jurídico brasileiro? A hipótese inicial é a de que esses obstáculos não decorrem apenas da ausência de disciplina legal específica, mas de três fatores. Na obtenção, os parâmetros de licitude deixam espaços em que o controle ocorre, em grande medida, apenas após o acesso aos dados, somando-se a isso a dependência da atuação dos provedores e dos mecanismos de cooperação internacional. Na preservação, verifica-se a ausência de uniformidade nos procedimentos técnicos destinados a assegurar a integridade, a autenticidade e a rastreabilidade dos vestígios digitais. Na valoração, por fim, falta uniformidade nos entendimentos judiciais quanto às consequências da violação da cadeia de custódia. Esses fatores teriam em comum a dificuldade de tornar a prova digital auditável pela defesa, hipótese a ser confrontada com a doutrina e a jurisprudência examinadas.

O objetivo geral é analisar os principais obstáculos à obtenção, à preservação e à valoração da prova digital na persecução penal dos crimes cibernéticos no Brasil, considerando as limitações dos instrumentos processuais tradicionais diante das novas tecnologias. Para tanto, busca-se, inicialmente, caracterizar a prova digital e suas peculiaridades em relação à prova tradicional. Em seguida, procura-se identificar, na doutrina e na jurisprudência, os principais obstáculos à obtenção lícita de dados telemáticos, incluindo a guarda de registros prevista no Marco Civil da Internet e a cooperação internacional. Depois, analisa-se o regime da cadeia de custódia previsto nos arts. 158-A a 158-F do Código de Processo Penal e sua aplicação aos vestígios digitais. Por fim, examina-se a valoração da prova digital e as consequências da quebra da cadeia de custódia, à luz da tensão entre a eficiência probatória e a proteção de direitos fundamentais. A pesquisa adota abordagem qualitativa e método hipotético-dedutivo, com revisão de literatura realizada por meio de busca estruturada, pesquisa documental e exame de julgados selecionados do STF e do STJ.

Além desta introdução, o artigo organiza-se em cinco seções. A seção 2 descreve o percurso metodológico adotado. A seção 3 apresenta o conceito e as características da prova digital. A seção 4 examina os obstáculos à sua obtenção, à sua preservação e à sua valoração e os ilustra com o caso Banco Master. A seção 5 discute a auditabilidade pela defesa como elemento comum a esses obstáculos. Por fim, as considerações finais retomam o problema e a hipótese à luz dos resultados obtidos.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

2. METODOLOGIA

A pesquisa adota abordagem qualitativa. Seu propósito não é medir a frequência de um fenômeno, e sim compreender e analisar criticamente os obstáculos jurídicos e técnicos que afetam a obtenção, a preservação e a valoração da prova digital na persecução penal dos crimes cibernéticos. Emprega-se o método hipotético-dedutivo: a hipótese apresentada na introdução é confrontada com a legislação, a doutrina e a jurisprudência examinadas, e pode ser confirmada, ajustada ou refutada ao final do estudo. Quanto aos procedimentos, a pesquisa é bibliográfica e documental, complementada pelo exame de decisões dos tribunais superiores.

A pesquisa bibliográfica foi feita por meio de busca estruturada em três bases de dados. A primeira é a Scientific Electronic Library Online (SciELO), que indexa periódicos submetidos a critérios de qualidade editorial. A segunda é o Google Acadêmico, cuja cobertura ampla alcança livros, dissertações e periódicos não indexados em bases seletivas. A terceira é o Portal Brasileiro de Publicações e Dados Científicos em Acesso Aberto (Oasisbr), mantido pelo Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), que reúne a produção depositada em repositórios institucionais brasileiros. O Portal de Periódicos da CAPES estava inicialmente previsto, mas foi substituído pelo Oasisbr porque o acesso esteve indisponível durante o período de coleta.

As buscas foram realizadas em 14 de outubro de 2026 na SciELO e em 15 de outubro de 2026 no Google Acadêmico e no Oasisbr. Foram usadas quatro combinações de descritores, cada uma voltada a um eixo do problema de pesquisa:

1. (“prova digital” OR “evidência digital”) AND (“processo penal” OR “persecução penal”);
2. (“cadeia de custódia”) AND (“prova digital” OR “prova eletrônica”);
3. (“crimes cibernéticos” OR “cibercrime”) AND (“investigação criminal” OR “prova”);
4. (“dados telemáticos”) AND (“reserva de jurisdição” OR “Marco Civil da Internet”).

O Google Acadêmico não admite a mesma sintaxe booleana das demais bases. Por isso, nele as combinações foram adaptadas para pares de expressões exatas, como “prova digital” “processo penal”. Em todas as bases, o período foi limitado a 2015–2025. Na SciELO, aplicaram-se também os filtros de país de publicação (Brasil) e de tipo de literatura (artigo). No Oasisbr, aplicou-se o filtro de tipo de documento (artigo). No Google Acadêmico, foram excluídas patentes e citações, e os resultados foram ordenados por relevância.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

O Google Acadêmico retornou aproximadamente 2.091 registros nas quatro buscas. Diante desse volume, foram examinados os 20 primeiros resultados de cada busca, segundo a ordenação por relevância da própria plataforma. No Oasisbr, foram examinados os 10 primeiros resultados de cada busca, ou todos, quando havia menos de 10. Na SciELO, todos os resultados foram examinados. Esse recorte, validado com o orientador, torna a análise exequível no prazo da pesquisa. Ele implica, porém, que a seleção não esgota a produção sobre o tema, limitação que se reconhece neste trabalho.

Foram incluídos trabalhos publicados entre 2015 e 2025 que tratassem da prova digital, da cadeia de custódia ou da investigação de crimes cibernéticos no processo penal brasileiro, na forma de artigos em periódicos científicos, livros, capítulos de livros, dissertações ou teses. Foram excluídos:

a) trabalhos de conclusão de curso e monografias de graduação;

b) trabalhos publicados em anais de eventos, editoriais, pareceres e textos de divulgação sem avaliação por pares;

c) estudos voltados a outros ramos do direito, como o civil, o trabalhista e o administrativo;

d) estudos restritos a ordenamento jurídico estrangeiro, sem análise do direito brasileiro;

e) trabalhos sem relação direta com o problema de pesquisa;

f) registros duplicados.

A seleção ocorreu em duas etapas. Na primeira, os registros examinados foram organizados em planilha, as duplicatas foram identificadas e os critérios foram aplicados com base no título, na fonte e no tipo de documento, recorrendo-se ao resumo nos casos duvidosos. Quando necessário, o tipo de documento foi confirmado nos metadados dos repositórios. Na segunda etapa, os 48 trabalhos considerados pertinentes foram classificados quanto à prioridade de leitura. Dezesseis foram classificados como de prioridade secundária, por terem sido considerados pertinentes apenas a partir do título e da fonte, e não seguiram para a seleção final. Dentre os 32 trabalhos de prioridade alta, foram selecionados 10 para compor o corpus de análise, número definido em razão da extensão do artigo e em conjunto com o professor orientador. A seleção foi intencional e aplicou, em sequência, três critérios: (i) preferência por artigos submetidos à avaliação por pares, dissertações e obras de autores de referência na área; (ii) disponibilidade do texto integral; e (iii) cobertura equilibrada dos três eixos do problema (obtenção, preservação e valoração), evitando-se trabalhos de abordagem sobreposta à de outros já selecionados. A relação dos 48 trabalhos, com a indicação da etapa em que cada um

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

deixou de ser selecionado, consta do material suplementar. Os textos integrais do corpus foram lidos, e seus argumentos foram organizados por eixo, com a identificação das convergências e divergências entre os autores, que estruturam a seção 4. Utilizou-se ferramenta de inteligência artificial generativa na organização da planilha de triagem. As decisões de inclusão e exclusão, a conferência das passagens citadas e a análise crítica são de responsabilidade da autora.

As buscas resultaram em aproximadamente 2.157 registros, dos quais 115 foram examinados. Excluídas 25 duplicatas, restaram 90 trabalhos únicos. Na triagem, 42 trabalhos foram excluídos e 48 foram considerados pertinentes, dos quais 10 compuseram o corpus final. O Quadro 1 sintetiza o processo, e o Quadro 2 apresenta os trabalhos analisados. Como mostra o Quadro 1, nenhum dos oito trabalhos considerados pertinentes no Oasisbr integrou o corpus final. Em parte, isso decorre do critério de contagem: cada trabalho recuperado em mais de uma base foi atribuído apenas à primeira em que apareceu, e o Oasisbr também recuperou trabalhos já localizados nas outras bases, como a versão em inglês do texto de Badaró, que integra o corpus. Quanto aos demais, na segunda etapa da seleção prevaleceram outros trabalhos que cobriam os mesmos eixos.

Quadro 1. Resultados das buscas e da seleção por base de dados

Base	Data da busca	Resultados	Examinados	Duplicatas	Únicos	Excluídos	Pertinentes	Corpus final
SciELO	14/10/2026	4	4	1	3	1	2	2
Google Acadêmico	15/10/2026	≈ 2.091	80	11	69	31	38	8
Oasisbr	15/10/2026	62	31	13	18	10	8	0
Total	**–**	**≈ 2.157**	**115**	**25**	**90**	**42**	**48**	**10**

Fonte: elaborado pelos autores (2026).

Quadro 2. Trabalhos que compõem o corpus de análise

Eixo	Autor(es) e ano	Título	Tipo
Obtenção	Saad; Rossi; Partata (2024)	A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais	Artigo
Obtenção	Queiroz (2024)	Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios	Artigo

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Eixo	Autor(es) e ano	Título	Tipo
Obtenção	Costa Júnior (2018)	A busca por um marco processual da internet: requisitos para colheita dos dados armazenados em compartimentos eletrônicos	Dissertação
Preservação	Furlaneto Neto; Santos (2020)	Apontamentos sobre a cadeia de custódia da prova digital no Brasil	Artigo
Preservação	Badaró (2021)	Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia	Artigo
Preservação	Fisberg (2025)	Função "*hash*" e a integridade da prova digital	Artigo
Valoração	Vaz, M. F. (2023)	A preservação da cadeia de custódia como pressuposto de admissibilidade da prova digital	Artigo
Valoração	Quemel (2025)	A integridade da prova digital como vetor da modulação da nulidade: repercussões da quebra da cadeia de custódia	Artigo
Valoração	Sarkis; Giacomolli (2025)	A regra de *disclosure* no processo penal e sua relevância para a prova digital	Artigo
Valoração	Vecchio; Beck (2025)	A prova digital e a sua cadeia de custódia no processo penal: uma análise doutrinária, normativa e jurisprudencial	Artigo

Fonte: elaborado pelos autores (2026).

Os trabalhos do corpus foram lidos e fichados; no caso da dissertação, a leitura concentrou-se nos capítulos diretamente relacionados ao problema. Seus argumentos foram organizados segundo os três eixos do problema, de modo a identificar os obstáculos apontados pela doutrina, os pontos de convergência e as divergências entre os autores. Além do corpus, utilizaram-se de forma complementar outras obras doutrinárias, localizadas nas buscas ou nas referências dos textos analisados. Essas obras não se submetem ao recorte temporal de 2015 a 2025 aplicado à busca estruturada, pois foram consultadas para fundamentar pontos específicos da análise, e não como resultado da revisão. É o caso, por exemplo, de Avolio, Borri e Saad Netto (2026), publicado após o período da busca.

A pesquisa documental abrangeu a legislação pertinente, consultada em sua redação vigente no Portal da Legislação do Planalto. Destacam-se a Constituição Federal; o Código de Processo Penal, com as alterações da Lei nº 13.964/2019 sobre a cadeia de custódia; a Lei nº 9.296/1996, que disciplina a interceptação de comunicações; a Lei nº 12.965/2014 (Marco Civil da Internet); as Leis nº 12.737/2012 e nº 14.155/2021, que inseriram no Código Penal os tipos de invasão de dispositivo informático e de fraude eletrônica; o Decreto nº 11.491/2023, que promulgou a Convenção sobre o Crime Cibernético; e a Lei nº 15.487/2026, que disciplinou a

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

requisição direta de dados a provedores em crimes sexuais contra crianças e adolescentes. A pesquisa documental incluiu também os dados estatísticos do Anuário Brasileiro de Segurança Pública 2026, do Fórum Brasileiro de Segurança Pública.

No exame jurisprudencial, foram selecionadas intencionalmente decisões do Supremo Tribunal Federal e do Superior Tribunal de Justiça que enfrentam questões diretamente ligadas aos obstáculos investigados, como o acesso a dados de aparelhos celulares, a preservação da cadeia de custódia de vestígios digitais e a valoração de elementos digitais. Essas decisões foram localizadas nos portais oficiais de jurisprudência e nos informativos dos tribunais. Como a seleção é intencional, os julgados não são apresentados como representativos do conjunto da jurisprudência, e sim como exemplos qualificados dos entendimentos adotados. Por fim, o caso Banco Master é mencionado na seção 4.4 apenas a título ilustrativo e sem pretensão de analisar o mérito, com base em reportagens da Agência Brasil, da Agência Pública, do Poder360 e da Gazeta Digital, uma vez que o processo tramita sob sigilo.

3. A PROVA DIGITAL E SUAS PARTICULARIDADES

Os crimes cibernéticos, sejam próprios ou impróprios, deixam vestígios que raramente assumem forma física. Na persecução desses delitos, registros de acesso, mensagens, arquivos e metadados passam a ocupar o lugar antes reservado aos objetos apreendidos e às testemunhas presenciais. Antes de examinar os obstáculos à obtenção, à preservação e à valoração desses elementos, é preciso delimitar o que se entende por prova digital e identificar as características que a distinguem da prova tradicional. São justamente essas características que explicam as dificuldades analisadas nas seções seguintes.

Na doutrina brasileira, uma definição recorrente é a de Denise Provasi Vaz, para quem a prova digital consiste nos “dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias” (Vaz, D. P., 2012, p. 63 *apud* Saad; Rossi; Partata, 2024, p. 4). Como observam Saad, Rossi e Partata (2024, p. 4), essa definição designa, em rigor, uma fonte de prova, isto é, aquilo de que se pode extrair o elemento de prova. A expressão, contudo, também é empregada com frequência para designar o próprio elemento que confirma ou nega uma afirmação sobre os fatos. A distinção não é apenas terminológica: o aparelho celular apreendido, os dados nele armazenados e o relatório de extração produzido pela perícia são realidades diferentes, submetidas a etapas distintas da persecução penal.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Os mesmos autores advertem que o atributo “digital” não decorre da simples utilização de um dispositivo informático para produzir ou transmitir um documento. Se assim fosse, praticamente qualquer documento poderia ser classificado como prova digital. A qualificação diz respeito ao próprio arquivo informático, cujo conteúdo só se torna compreensível depois da interpretação de uma linguagem não natural, a sequência numérica que o compõe (Saad; Rossi; Partata, 2024, p. 5). Assim, um contrato digitado em computador e depois impresso não se confunde com o arquivo que o originou. O arquivo digital pode conter metadados e outros elementos técnicos relevantes para a investigação de sua origem, criação e eventuais modificações, cuja interpretação depende de procedimentos adequados de análise forense.

Dessa natureza decorrem as características que a doutrina costuma atribuir à prova digital:

a) a imaterialidade: os dados nada mais são do que impulsos elétricos aos quais se atribui sentido informacional;

b) a volatilidade: podem ser modificados, de forma proposital ou involuntária, pela simples alteração da sequência numérica;

c) o desprendimento do suporte físico: podem ser transferidos para outros dispositivos sem perder sua essência;

d) a suscetibilidade de clonagem: admitem cópias idênticas e ilimitadas;

e) a necessidade de intermediação: dependem de equipamentos para se tornarem inteligíveis ao ser humano (Saad; Rossi; Partata, 2024, p. 5-6).

Vaz, M. F. (2023, p. 333) acrescenta a efemeridade, pois a prova digital tem caráter temporário e pode não subsistir sem as devidas precauções; a complexidade, por exigir conhecimentos e técnicas específicas na sua coleta; e a dispersão, relacionada à possibilidade de os dados estarem distribuídos por diferentes locais físicos, geográficos ou virtuais. Badaró (2021, p. 8) sintetiza esse conjunto na ideia de uma “congênita mutabilidade” da prova digital.

Badaró (2021, p. 7) sustenta ainda que a prova digital se diferencia da tradicional em dois planos. No plano ontológico, porque não se expressa em linguagem natural nem possui materialidade imediatamente perceptível. No plano metodológico, porque sua produção deve observar os princípios da ciência da computação. Por essa razão, o valor epistêmico desse tipo de prova depende do respeito aos padrões da computação forense na identificação, coleta, preservação, análise e apresentação dos dados, com documentação integral de cada etapa (Badaró, 2021, p. 7-8). No mesmo sentido, Saad, Rossi e Partata (2024, p. 6) concluem que as características da prova digital exigem cuidados procedimentais destinados a assegurar sua confiabilidade e autenticidade. Queiroz (2024, p. 418), por sua vez, destaca que “a prova digital

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

é volátil e, na maioria das vezes, irrepetível", de modo que uma coleta inadequada pode inviabilizá-la definitivamente.

Esse quadro revela uma ambivalência que orienta a análise desenvolvida neste artigo. As mesmas propriedades que tornam a prova digital valiosa para a investigação dos crimes cibernéticos também a tornam vulnerável. Entre essas propriedades estão a capacidade de registrar com precisão acessos, comunicações e transações e a possibilidade de produzir cópias idênticas para exame. Ao mesmo tempo, um dado pode ser alterado sem deixar vestígio aparente, e a cópia só é confiável se for possível demonstrar que corresponde ao original. Por isso a prova digital não se ajusta plenamente ao tratamento dado aos documentos comuns ou aos objetos apreendidos em geral. Suas particularidades repercutem em cada etapa da persecução penal, desde o modo como os dados são obtidos até o valor que o juiz pode atribuir a eles. São essas repercussões que a seção seguinte examina.

Essas características exigem distinguir conceitos que costumam ser empregados como sinônimos. A integridade diz respeito à inalteração dos dados desde determinado momento, e é o que o código *hash* permite demonstrar (Fisberg, 2025, p. 11-12). A autenticidade refere-se à correspondência entre o dado e a origem que lhe é atribuída; um arquivo pode estar íntegro e, ainda assim, não ser autêntico, já que o *hash* não revela quem o produziu nem se seu conteúdo é verdadeiro (Fisberg, 2025, p. 11-12). A rastreabilidade é atributo do procedimento, e não do dado: consiste na possibilidade de reconstituir o percurso do vestígio, finalidade que o art. 158-A do Código de Processo Penal atribui à cadeia de custódia ao exigir a documentação que permita "rastrear sua posse e manuseio". A confiabilidade, por sua vez, é o juízo sobre o valor epistêmico da prova, que depende do respeito aos padrões da computação forense (Badaró, 2021, p. 7-8). Por fim, a auditabilidade, um dos critérios de confiabilidade indicados pelo Superior Tribunal de Justiça no AgRg no HC 828.054/RN (Brasil, 2024a), é aqui entendida como a possibilidade de que alguém que não produziu a prova verifique, de forma independente, sua integridade, sua autenticidade e seu percurso. Assim, os quatro primeiros conceitos descrevem atributos da prova ou do procedimento, enquanto a auditabilidade descreve a condição para que esses atributos possam ser verificados pela defesa, e é nessa acepção que o termo é empregado nas seções seguintes.

4. OS OBSTÁCULOS À PROVA DIGITAL NA PERSECUÇÃO PENAL

As particularidades descritas na seção anterior repercutem em três momentos da persecução penal: na obtenção dos dados, na sua preservação até o julgamento e na valoração

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

que deles faz o juiz. Esta seção examina os obstáculos próprios de cada um desses momentos e, ao final, os ilustra com um caso concreto.

4.1. Obstáculos à obtenção

A prova digital pode chegar ao processo penal por diferentes caminhos. Saad, Rossi e Partata (2024, p. 16) identificam quatro principais: a interceptação telemática, a coleta de dados após a apreensão do dispositivo eletrônico, a requisição a terceiros, em geral provedores de conexão e de aplicações de internet, e a instalação oculta de programas de acesso remoto. Na investigação dos crimes cibernéticos, ganham relevo especial os dois caminhos mais frequentes: o acesso a aparelhos apreendidos e a requisição de dados a provedores. Cada um apresenta obstáculos próprios.

No primeiro caso, a dificuldade central está no controle do acesso ao conteúdo dos aparelhos. Os autores observam que, como os dados não são percebidos a olho nu, a autorização para apreender um dispositivo não basta para que os dados nele contidos sejam acessados (Saad; Rossi; Partata, 2024, p. 17). O acesso exige decisão fundamentada em elementos concretos de que os vestígios do crime se encontram naquele sistema e de que serão úteis à investigação. A ausência de parâmetros legais claros, contudo, tem resultado em autorizações genéricas para o acesso a todo e qualquer conteúdo armazenado (Saad; Rossi; Partata, 2024, p. 18). Os autores apontam ainda uma inversão da lógica da busca e apreensão: no mundo físico, procura-se e depois se apreende o que interessa; no mundo digital, coleta-se tudo o que o aparelho contém e só depois se seleciona o que é relevante (Saad; Rossi; Partata, 2024, p. 19). Costa Júnior (2018, p. 181) já identificava efeitos práticos dessa falta de regras: autorizações redigidas "em poucas letras" e ordens judiciais que só alcançavam seu destinatário depois da perícia nos aparelhos, quando o sigilo já havia sido afastado. O autor registrava também a oscilação dos tribunais quanto à necessidade de ordem judicial para acessar celulares apreendidos em situação de flagrante (Costa Júnior, 2018, p. 130-131).

Parte dessa oscilação foi enfrentada pelo Supremo Tribunal Federal no julgamento do Tema 977 da repercussão geral (ARE 1.042.075/RJ), concluído em 25 de junho de 2025[3]. A tese fixada distingue a apreensão do aparelho, que não depende de ordem judicial, do acesso aos dados nele contidos. Quando o celular é encontrado fortuitamente, o acesso destinado a esclarecer a autoria ou a identificar o proprietário dispensa consentimento ou decisão prévia,

[3] Em consulta ao portal do Supremo Tribunal Federal em 27 de outubro de 2026, verificou-se que o acórdão, publicado em 24 de setembro de 2025, ainda não havia transitado em julgado. Foram opostos embargos de declaração em 26 de setembro de 2025, nos quais se alegam omissão e contradição, tendo o relator registrado a possibilidade de efeitos infringentes. Após manifestação da Procuradoria-Geral da República, o recurso foi incluído em sessão virtual do Plenário prevista para 6 a 13 de novembro de 2026. A tese, portanto, ainda pode ser modificada.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

desde que justificado posteriormente. Quando o aparelho é apreendido na forma do art. 6º do Código de Processo Penal ou em flagrante, “o acesso aos respectivos dados será condicionado ao consentimento expresso e livre do titular dos dados ou de prévia decisão judicial”, que deve justificar, com base em elementos concretos, a proporcionalidade da medida e delimitar sua abrangência (Brasil, 2025a). A tese responde, em parte, à crítica de Saad, Rossi e Partata, ao exigir que a decisão delimite o alcance do acesso. Não fixa, porém, critérios objetivos para essa delimitação, como os tipos de dados e o período alcançados, que continuam a depender de cada decisão. Além disso, admite que a autoridade policial adote providências para preservar os dados antes da autorização judicial, com justificação posterior, e produz apenas efeitos prospectivos (Brasil, 2025a). O controle sobre o acesso continua, assim, em parte posterior à medida.

No segundo caminho, a obtenção depende da atuação de terceiros. O Marco Civil da Internet obriga os provedores de conexão a guardar os registros de conexão por um ano (art. 13) e os provedores de aplicações a guardar os registros de acesso por seis meses (art. 15). A disponibilização desses registros e do conteúdo das comunicações depende de ordem judicial (art. 10, § 1º, e art. 22), ressalvados os dados cadastrais, que podem ser requisitados pelas autoridades com competência legal (art. 10, § 3º). Queiroz (2024, p. 437-441) destaca a diferença entre preservação e fornecimento. A autoridade pode pedir diretamente ao provedor que preserve os registros além do prazo legal (art. 13, § 2º, e art. 15, § 2º), mas o acesso a eles exige decisão judicial. Essa distinção tem grande importância prática, porque os prazos de guarda são curtos diante do tempo da investigação e, como observa a autora, uma vez apagado o dado das plataformas dos provedores, não há como recuperá-lo (Queiroz, 2024, p. 423). Mais recentemente, a Lei nº 15.487/2026, voltada à repressão da violência sexual contra crianças e adolescentes também no ambiente digital, alterou essa lógica em hipóteses específicas. Em casos de flagrante ou de risco à vida ou à integridade física de criança ou adolescente identificados em ronda virtual, a autoridade policial ou o Ministério Público podem requisitar diretamente aos provedores, sem ordem judicial prévia, registros de conexão ou dados cadastrais, com comunicação ao juiz em até 48 horas (Estatuto da Criança e do Adolescente, art. 190-F, §§ 2º e 3º). A solução reforça a tendência de deslocar o controle judicial para depois do acesso.

Mesmo quando preservados e fornecidos, os registros nem sempre identificam o autor: o compartilhamento de endereços IP e a técnica conhecida como CGNAT fazem com que um mesmo endereço seja usado por vários usuários, e a individualização passa a depender da porta lógica de origem, que nem todos os provedores armazenam (Queiroz, 2024, p. 428-432).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Somam-se a isso as ferramentas de anonimização e a possibilidade de o titular da conta não ser o autor da conduta (Queiroz, 2024, p. 419, 428).

O caráter transnacional dos crimes cibernéticos acrescenta outro obstáculo: os dados frequentemente estão armazenados no exterior, sob controle de empresas estrangeiras. Os mecanismos tradicionais de cooperação jurídica internacional, como os acordos de assistência mútua, são lentos diante da volatilidade dos dados (Queiroz, 2024, p. 444). A promulgação da Convenção de Budapeste pelo Decreto nº 11.491/2023 trouxe instrumentos mais ágeis, como a ordem de apresentação de dados aos provedores e a rede de contato permanente entre os Estados (Queiroz, 2024, p. 432-437). O relatório explicativo da Convenção justifica esses instrumentos pela volatilidade dos dados eletrônicos, que podem ser alterados, transferidos ou apagados em segundos (Council of Europe, 2001, par. 133), e esclarece que a ordem de apresentação do art. 18 alcança o provedor que ofereça serviços no território da Parte, quanto aos dados cadastrais (Council of Europe, 2001, par. 170). A União Europeia foi além: o Regulamento (UE) 2023/1543, aplicável desde agosto de 2026, permite que a autoridade de um Estado-Membro requisite dados diretamente a provedores estabelecidos em outro, que devem entregá-los em dez dias ou, em caso de urgência, em oito horas (União Europeia, 2023, art. 10). No julgamento da ADC 51, o Supremo Tribunal Federal declarou a constitucionalidade dos mecanismos de cooperação jurídica internacional, sem prejuízo do uso dos acordos de assistência mútua. Reconheceu, porém, a possibilidade de requisição direta de dados a empresas com representação no Brasil, nas hipóteses do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste, então já aprovada pelo Congresso Nacional e ratificada pelo Brasil, embora ainda não vigente nem promulgada (Brasil, 2023a; Queiroz, 2024, p. 443-444). Costa Júnior (2018, p. 181-182), por sua vez, alertava para o risco inverso: a coleta de dados no exterior sem observância dos mecanismos de cooperação, o que pode comprometer a licitude da prova.

Os obstáculos à obtenção corroboram, assim, o primeiro fator da hipótese. O controle sobre o acesso aos dados ainda ocorre, em parte, depois de efetuado, seja pela justificação posterior admitida pelo Tema 977, seja pela amplitude das autorizações judiciais. Além disso, a obtenção depende de agentes que o Estado não controla: provedores que nem sempre guardam os dados necessários e jurisdições estrangeiras com tempos próprios. Não é por acaso que tanto Costa Júnior (2018, p. 132-133) quanto Saad, Rossi e Partata (2024, p. 27), com seis anos de intervalo, concluem pela necessidade de uma disciplina legal própria para a obtenção da prova digital. A permanência dessa conclusão indica que o problema não foi superado pelas reformas

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

posteriores. Uma vez obtidos, porém, os dados precisam ser preservados de forma íntegra até o julgamento, que é o objeto da próxima subseção.

4.2. Obstáculos à preservação

Obtidos os dados, é preciso assegurar que aquilo que chega ao juiz corresponde exatamente ao que foi coletado. Esse é o papel da cadeia de custódia, disciplinada nos arts. 158-A a 158-F do Código de Processo Penal, introduzidos pela Lei nº 13.964/2019. O art. 158-A define a cadeia de custódia como "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte". O art. 158-B, por sua vez, descreve dez etapas, que vão do reconhecimento e do isolamento do vestígio até seu armazenamento e descarte. Como observa Badaró (2021, p. 8), o que a lei protege não é a sucessão de pessoas que tiveram contato com o vestígio, mas a documentação que atesta esse percurso: é ela que permite verificar, depois, se o elemento apresentado em juízo é o mesmo que foi recolhido.

A disciplina legal, contudo, foi concebida a partir do vestígio material. Como resume Neves (2025, p. 155), “não há no Brasil qualquer dispositivo legal que trate da prova digital”. Vaz, M. F. (2023, p. 335) registra que as etapas do art. 158-B têm em vista a evidência física e não tratam da prova digital. No mesmo sentido, Furlaneto Neto e Santos (2020) apontam que as regras do Código são genéricas e não contemplam os métodos próprios da recuperação de dados em dispositivos informáticos. A lei não menciona a cópia forense, a função *hash* nem o espelhamento de aparelhos. Também não trata das situações em que o dado não está em um suporte físico apreendido, mas em servidores de terceiros. Queiroz (2024, p. 423-427) observa que os arts. 158-A e 158-B não alcançam os dados mantidos por provedores e propõe sua aplicação por interpretação teleológica. Quemel (2025, p. 242-243), por sua vez, ressalta que os dispositivos deixam em aberto questões como a coleta em nuvem e a preservação de registros eletrônicos.

A insuficiência dessa disciplina fica mais nítida à luz da formulação de Geraldo Prado, referência no estudo da cadeia de custódia no Brasil. Antes mesmo da Lei nº 13.964/2019, o autor inseria a cadeia de custódia no sistema de controles epistêmicos do processo penal. Como o filtro contra as provas ilícitas depende do rastreio de cada prova até sua fonte, a defesa precisa conhecer o conjunto dos elementos colhidos, e a quebra da cadeia conduz à ilicitude da prova (Prado, 2014, p. 41, 57, 82 *apud* Menezes; Borri; Soares, 2018, p. 291, 293). O autor reafirma essa posição em relação à prova digital: violada a sua cadeia de custódia, "incide imperiosa

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

proibição de valoração da prova assim obtida" (Prado, 2021, p. 24). Transposta para a prova digital, essa formulação mostra o alcance da lacuna legal: se a lei não disciplina as etapas próprias dos vestígios digitais, o rastreio da prova até sua fonte passa a depender de práticas não uniformes, definidas por quem coleta e preserva os dados.

Essa lacuna tem sido preenchida por normas técnicas, como a ABNT NBR ISO/IEC 27037, que orienta a identificação, a coleta, a aquisição e a preservação de evidências digitais, e por procedimentos operacionais padronizados da Secretaria Nacional de Segurança Pública (Furlaneto Neto; Santos, 2020; Vaz, M. F., 2023, p. 335-337). Essas normas, porém, não têm força obrigatória, porque nenhuma lei as incorpora expressamente (Vaz, M. F., 2023, p. 335-336; Vecchio; Beck, 2025, p. 7). Segundo relatam Vecchio e Beck (2025, p. 10-11), o próprio Superior Tribunal de Justiça, no AgRg no HC 828.054/RN, tratou a ISO 27037 como guia relevante, mas não vinculante.

Entre as técnicas recomendadas, a mais conhecida é a combinação entre a cópia forense bit a bit e a função *hash*. A perícia trabalha sobre uma cópia integral do suporte e calcula, para o original e para a cópia, um código alfanumérico que se altera diante de qualquer modificação nos dados. Se os códigos coincidem, a cópia é idêntica ao original (Badaró, 2021, p. 8; Vaz, M. F., 2023, p. 337). Fisberg (2025) adverte, porém, que essa ferramenta tem limites que nem sempre são considerados. O *hash* demonstra que um conjunto de dados não foi alterado desde o momento em que o código foi calculado, mas não demonstra quem produziu o arquivo nem se seu conteúdo é verdadeiro (Fisberg, 2025, p. 11-12). Também não se aplica bem a conteúdos dinâmicos, como páginas da internet e registros que se modificam continuamente, nem a capturas de tela, que não reproduzem os dados originais (Fisberg, 2025, p. 11-13). Além disso, algoritmos antes considerados seguros, como o MD5, tornaram-se vulneráveis a colisões (Fisberg, 2025, p. 8-10). Por essas razões, o autor sustenta que o *hash* gera apenas uma presunção relativa de integridade, que não dispensa a documentação de cada etapa (Fisberg, 2025, p. 28).

Há ainda um obstáculo menos visível: em muitos casos, a cadeia de custódia começa antes da intervenção estatal. Quemel (2025, p. 244-249) analisa um caso em que o material foi identificado pela inteligência artificial de uma empresa de tecnologia, comunicado a uma organização estrangeira e só depois encaminhado à polícia brasileira. Nesse percurso, intermediários privados e estrangeiros manusearam os dados antes de qualquer documentação oficial, e a ausência de *hash* calculado na origem tornou-se ponto central da impugnação defensiva (Quemel, 2025, p. 249). Neves (2025, p. 152, 157) aponta problema semelhante nas investigações corporativas internas, em que a prova digital é colhida por particulares, sem regras

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

específicas, e depois compartilhada com as autoridades. A situação é comum nos crimes cibernéticos, em que os primeiros registros costumam estar nas mãos de provedores, plataformas e das próprias vítimas.

Por fim, discute-se quem deve controlar a preservação. Vecchio e Beck (2025, p. 7) sustentam que a custódia e a validação da autenticidade da prova digital devem caber a peritos oficiais, e não à autoridade que investiga ou acusa, e Furlaneto Neto e Santos (2020) defendem a centralização da custódia nos institutos de criminalística, com investimento em equipamentos e capacitação.

Também aqui a hipótese encontra respaldo, com uma precisão: a falta de uniformidade não decorre da inexistência de regras técnicas, que existem e são conhecidas. Decorre do fato de que a lei processual, pensada para vestígios materiais, não as incorpora, e as normas técnicas, sem força obrigatória, são aplicadas de modo desigual. Em consequência, a mesma falha de preservação pode ocorrer em um caso e não em outro, e a decisão sobre seus efeitos fica inteiramente a cargo do juiz. É essa questão, a das consequências da quebra da cadeia de custódia, que a próxima subseção examina.

4.3. Obstáculos à valoração

Os arts. 158-A a 158-F do Código de Processo Penal disciplinam a cadeia de custódia, mas não dizem o que acontece quando ela é descumprida. Badaró (2021, p. 8) observa que o legislador não fixou consequências para a quebra da cadeia, seja no plano da admissibilidade, seja no da valoração da prova. Vecchio e Beck (2025, p. 8) chegam à mesma constatação. Esse silêncio transfere à doutrina e aos tribunais a tarefa de definir os efeitos de uma falha de preservação, e é nesse ponto que se concentra a principal divergência sobre a prova digital no processo penal brasileiro.

Na doutrina examinada, é possível identificar três posições. A primeira sustenta que a quebra da cadeia de custódia torna a prova ilícita e, portanto, inadmissível. Para Vaz, M. F. (2023, p. 340-341), uma vez rompida a cadeia, a prova deve ser excluída do processo, juntamente com as que dela derivarem, independentemente da boa ou má-fé de quem a manuseou. Menezes, Borri e Soares (2018, p. 284, 294-295) fundamentam essa posição nos princípios da mesmidade e da desconfiança: se não é possível demonstrar que a prova apresentada é a mesma que foi colhida, ela se torna ilícita, e a consequência é a proibição de sua valoração, com exclusão dela e das provas derivadas. Costa Júnior (2018, p. 177) segue a mesma linha, ao afirmar que a quebra da cadeia atinge o contraditório e atrai a vedação constitucional às provas ilícitas. A segunda posição trata a quebra como nulidade relativa, que depende da demonstração de

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

prejuízo concreto. Quemel (2025, p. 237, 255-258) sustenta essa leitura com base no art. 563 do Código de Processo Penal, sobretudo quando a integridade do material pode ser confirmada por outros meios, como a perícia e a comparação de códigos *hash*. Furlaneto Neto e Santos (2020) também mencionam a orientação doutrinária que trata as violações procedimentais como nulidades relativas. A terceira posição é intermediária. Fisberg (2025, p. 28, 31-32) exige uma documentação mínima como filtro de admissibilidade, mas defende que as demais falhas em relação às boas práticas técnicas sejam consideradas na valoração, salvo violação de procedimento expressamente previsto em lei. Badaró (2021, p. 9), embora admita que irregularidades da prova em geral se resolvam na valoração, defende solução mais rigorosa para a prova digital: se a cadeia de custódia não pode ser verificada, a prova não tem valor epistêmico e não serve para demonstrar fato algum.

A jurisprudência do Superior Tribunal de Justiça reflete essa divergência. No AgRg no RHC 143.169/RJ, a Quinta Turma reconheceu a inadmissibilidade de provas extraídas de computadores apreendidos. Os dados haviam sido examinados por perito contratado por um banco e pela polícia, sem qualquer documentação dos procedimentos adotados. O acórdão afirmou que "É ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas" (Brasil, 2023b). Ao mesmo tempo, o voto condutor ressalvou que o descumprimento dos arts. 158-A a 158-F não leva, por si só, à exclusão da prova. O que se mostrou decisivo foi a ausência completa de documentação e de qualquer outro elemento capaz de assegurar a integridade do material. No AgRg no HC 828.054/RN, a mesma Turma considerou imprestável um relatório baseado em capturas de tela de conversas de WhatsApp, produzido por consulta direta ao aparelho, sem ferramenta forense de extração. Segundo o Informativo 811, o acórdão afirmou que a falta de procedimentos para garantir a idoneidade e a integridade dos dados extraídos de um celular apreendido "resulta na quebra da cadeia de custódia e na inadmissibilidade da prova digital" (Brasil, 2024a). O julgado indicou ainda quatro critérios de confiabilidade: auditabilidade, repetibilidade, reprodutibilidade e justificabilidade. No AgRg no HC 902.195/RS, a mesma Turma reconheceu a quebra da cadeia de custódia de prova extraída de celular apreendido antes da vigência da Lei nº 13.964/2019. O laudo não recuperou arquivos nem indicou se o aparelho fora adulterado, o que levou ao desentranhamento das evidências digitais. O acórdão assentou que, embora as regras dos arts. 158-A a 158-F não retroajam, “a cadeia de custódia deve ser preservada, mesmo para fatos anteriores à Lei n. 13.964/2019” (Brasil, 2024c). Mais recentemente, no AREsp 2.967.413/RS, a Quinta Turma anulou acórdão que mantivera condenação apoiada em capturas de tela de conversas, sem registro técnico da extração e da preservação, porque o tribunal de origem havia exigido da defesa a prova do

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

prejuízo. A Turma afirmou que cabe ao Estado demonstrar a integridade dos dados e determinou novo julgamento (Brasil, 2025c).

Em sentido diverso, no AgRg no RHC 182.310/RJ, a Sexta Turma recusou o desentranhamento de arquivos digitais apresentados por colaboradores premiados. Entendeu que a defesa não apontou indício algum de adulteração e que a questão da cadeia de custódia não se resolve como nulidade processual, mas no plano da eficácia da prova, a ser vista em cada caso (Brasil, 2024b). A própria Quinta Turma, no AgRg no RHC 208.857/BA, assentou que a alegação de quebra da cadeia de custódia "exige demonstração concreta de adulteração ou prejuízo, não sendo suficiente a mera ausência de documentação" (Brasil, 2025b). Nesses julgados, o ônus se inverte: cabe à defesa demonstrar que a prova foi alterada.

A divergência, portanto, não se limita à consequência da quebra. Ela envolve também a questão de quem deve provar a integridade da prova digital, e essa segunda questão parece ser a mais relevante. Vecchio e Beck (2025, p. 9) observam que exigir da defesa a demonstração de que o dado foi adulterado equivale a impor-lhe uma prova diabólica, já que, sem documentação, nenhuma das partes consegue verificar o que aconteceu com os dados. A discussão não é exclusiva do Brasil. Na Inglaterra, as condenações baseadas em registros do sistema informático Horizon, depois reconhecido como não confiável, levaram Marshall *et al.* (2021, p. 19-21) a criticar a presunção de que computadores funcionam corretamente. Os autores propõem que, contestada a confiabilidade, caiba a quem se apoia na prova revelar os registros de erros, de alterações e de controles de acesso do sistema e demonstrar que essas falhas não a afetaram (Marshall *et al.*, 2021, p. 24-25). Fisberg (2025, p. 19-27, 32), ao analisar decisões do mesmo tribunal sobre fatos semelhantes, aponta soluções diferentes e conclui que essa variação gera insegurança jurídica. Avolio, Borri e Saad Netto (2026) registram oscilações semelhantes, inclusive quanto à aceitação de capturas de tela de conversas sem a apreensão do aparelho, e defendem a uniformização da jurisprudência com a atribuição ao Estado do ônus de demonstrar a integridade da prova, pois "as fontes de prova não se tornam idôneas porque o acusado deixou de questionar alguma adulteração" (Avolio; Borri; Saad Netto, 2026, p. 20). É preciso registrar, além disso, que os julgados examinados são decisões colegiadas de turmas, e não precedentes qualificados. O tema ainda não foi objeto de tese firmada pela Terceira Seção nem pelo Supremo Tribunal Federal.

Apesar da divergência, as decisões e a doutrina examinadas permitem identificar um critério em formação. Vecchio e Beck (2025, p. 9, 13) distinguem a ausência total de documentação, que impede qualquer verificação da integridade e conduz à inadmissibilidade, das irregularidades formais menores, sem indício concreto de alteração, que devem ser

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

consideradas na valoração. É também o que sugere o AgRg no RHC 143.169/RJ, ao condicionar a exclusão da prova à inexistência de qualquer elemento que assegure sua integridade. Esse critério evita os dois extremos: a exclusão automática de provas íntegras por falhas formais e a admissão de provas cuja integridade ninguém consegue verificar. Ainda assim, ele depende da possibilidade de a defesa examinar os dados, questão retomada na seção 5. O mesmo vale para o terceiro fator: falta uniformidade quanto às consequências da quebra da cadeia de custódia e, sobretudo, quanto à distribuição do ônus de demonstrar a integridade da prova.

4.4. Uma ilustração: o caso Banco Master

Os obstáculos examinados podem ser observados na investigação sobre fraudes envolvendo o Banco Master, em curso no Supremo Tribunal Federal. Como o processo tramita sob sigilo, a análise baseia-se em informações divulgadas pela imprensa e limita-se à prova digital, sem juízo sobre o mérito. Na segunda fase da Operação Compliance Zero, em janeiro de 2026, foram apreendidos aparelhos celulares e outros dispositivos eletrônicos. O então relator determinou que o material fosse encaminhado à Procuradoria-Geral da República antes de qualquer exame pela Polícia Federal e que a perícia fosse realizada por quatro peritos nominalmente designados, medida criticada por associações de delegados e de peritos federais (Freitas, 2026). Em fevereiro, após a mudança de relatoria (Richter, 2026), a perícia de cerca de cem dispositivos passou à Polícia Federal, com custódia integral do material em suas instalações (Mendonça..., 2026), e a defesa de um dos investigados requereu acesso aos laudos e aos dados brutos, para permitir a análise independente por assistente técnico (Defesa..., 2026). Os episódios descritos correspondem ao que foi noticiado pela imprensa e às manifestações das partes e de entidades de classe, e não a fatos ou conclusões documentados no processo.

Tomados apenas como ilustração, os episódios noticiados permitem visualizar, em escala ampliada, os três obstáculos. O volume de dispositivos ilustra a coleta de dados muito superior ao que interessa à investigação (Saad; Rossi; Partata, 2024, p. 19). As sucessivas transferências do material e a redistribuição dos peritos precisam estar documentadas para que a cadeia de custódia permaneça verificável, como exige o art. 158-A do Código de Processo Penal. O pedido da defesa, por fim, revela sua dependência em relação ao que a acusação extraiu e selecionou (Sarkis; Giacomolli, 2025, p. 239). Sem avaliar se houve falha na preservação da prova, o episódio mostra que, mesmo sob supervisão direta do Supremo Tribunal Federal, a custódia, a perícia e o acesso da defesa dependeram de decisões caso a caso, por falta de parâmetros legais prévios. Essa constatação conduz à questão examinada na seção seguinte: a auditabilidade da prova digital pela defesa.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

5. A AUDITABILIDADE COMO ELO COMUM

Os obstáculos examinados na seção anterior foram tratados separadamente, mas não são independentes. Em cada um deles, o que está em jogo é a possibilidade de alguém, além de quem produziu a prova, verificar como os dados foram obtidos, preservados e interpretados. Na obtenção, a autorização genérica e a coleta integral seguida de seleção impedem saber, depois, o que foi buscado e por quê. Na preservação, a falta de procedimento uniforme e de documentação impede reconstituir o percurso dos dados. Na valoração, a divergência sobre o ônus da prova decide quem arca com a impossibilidade de fazer essa verificação. O elo comum entre os três obstáculos é, portanto, a auditabilidade da prova digital.

O termo não é estranho à jurisprudência. No AgRg no HC 828.054/RN, o Superior Tribunal de Justiça indicou a auditabilidade, ao lado da repetibilidade, da reprodutibilidade e da justificabilidade, como aspecto essencial da confiabilidade da prova digital (Brasil, 2024a). Em sentido técnico, uma prova é auditável quando um terceiro, com acesso ao material e à documentação, consegue refazer o percurso da coleta e da análise e chegar ao mesmo resultado. No processo penal, esse terceiro é, antes de tudo, a defesa. A auditabilidade é a forma que o contraditório assume diante da prova digital: sem ela, o direito de contestar a prova (CF, art. 5º, LV) reduz-se à possibilidade de discordar de um resultado que não se pode examinar.

É justamente essa possibilidade que a prática atual limita. Sarkis e Giacomolli (2025, p. 239) observam que a defesa nunca tem acesso ao material original, mas apenas a cópias. Os relatórios de extração costumam apresentar somente o resultado da filtragem feita pelos investigadores, sem revelar os critérios de seleção utilizados (Sarkis; Giacomolli, 2025, p. 243-244). Os programas de leitura disponibilizados restringem a defesa ao conteúdo previamente escolhido pela autoridade (Sarkis; Giacomolli, 2025, p. 244-245). Além disso, as ferramentas de extração exigem licenças de alto custo, e o assistente técnico previsto no art. 159, § 3º, do Código de Processo Penal deve ser custeado pelo próprio acusado (Sarkis; Giacomolli, 2025, p. 241-242). Os autores concluem que a defesa se encontra em situação de dependência em relação ao trabalho da investigação (Sarkis; Giacomolli, 2025, p. 242). Costa Júnior (2018, p. 182-183) já sustentava que a defesa deveria poder acompanhar o momento de acesso ao conteúdo dos aparelhos apreendidos e ter acesso a todas as fontes de prova, e não apenas às selecionadas pela acusação.

A auditabilidade oferece, ainda, um critério para enfrentar a divergência descrita na subseção 4.3. Em vez de perguntar, em abstrato, se a quebra da cadeia de custódia gera inadmissibilidade ou apenas afeta o valor da prova, pode-se perguntar se, apesar da falha, a defesa ainda consegue verificar a integridade do material. Quando a documentação disponível,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

a cópia forense e os códigos *hash* permitem essa verificação independente, a irregularidade pode ser tratada na valoração, como sugerem Fisberg (2025, p. 31-32) e Vecchio e Beck (2025, p. 9, 13). Quando a falha impede qualquer verificação, a prova não deve ser admitida, porque não há como submetê-la ao contraditório. É preciso, contudo, distinguir as consequências envolvidas. A ilicitude, prevista no art. 5º, LVI, da Constituição e no art. 157 do Código de Processo Penal, refere-se à prova obtida com violação de normas constitucionais ou legais e conduz ao desentranhamento. A nulidade, regida pelos arts. 563 e seguintes do mesmo Código, atinge atos processuais praticados em desconformidade com a forma prescrita e, em regra, depende da demonstração de prejuízo. A redução do valor probatório, por fim, não exclui a prova, mas diminui o peso que o juiz lhe atribui na formação do convencimento (art. 155 do CPP). A falta de auditabilidade não se confunde necessariamente com a ilicitude da obtenção: uma prova licitamente obtida pode tornar-se inverificável por falhas posteriores de preservação. Nesses casos, o fundamento para não admiti-la não é a violação de uma regra de obtenção, mas a impossibilidade de exercer o contraditório sobre a própria fonte de prova (art. 5º, LV, da Constituição), o que a aproxima da inadmissibilidade, e não da simples nulidade. A proposta não afirma, portanto, que toda falha gera ilicitude, mas que a ausência de qualquer meio de verificação impede que a prova seja validamente valorada. É o que se extrai do AgRg no RHC 143.169/RJ, em que a exclusão decorreu da ausência completa de documentação e de qualquer outro elemento capaz de assegurar a integridade (Brasil, 2023b). Esse critério também resolve a questão do ônus. Se a auditabilidade é condição do contraditório, cabe a quem produz a prova assegurar as condições para que ela seja verificada. Exigir da defesa a demonstração da adulteração, sem que ela tenha acesso aos meios para isso, equivale à prova diabólica apontada por Vecchio e Beck (2025, p. 9), solução incompatível com a posição de Badaró (2021, p. 9) de que o ônus recai sobre a acusação.

Essa conclusão decorre da função que o contraditório exerce no processo penal. Mais do que uma oportunidade de manifestação, ele é o meio pelo qual as afirmações sobre os fatos são testadas pela parte contrária antes de servirem de base à decisão, o que lhe confere uma função epistêmica. Diante da prova digital, essa função só se realiza se a defesa tiver acesso às fontes e aos procedimentos que produziram o resultado apresentado, e não apenas ao resultado. É nesse sentido que Prado, como visto na subseção 4.2, vincula a cadeia de custódia ao rastreio da prova até sua fonte (Prado, 2014, p. 57 *apud* Menezes; Borri; Soares, 2018, p. 293), e que Costa Júnior (2018, p. 182) identifica um elo indissociável entre o contraditório, mesmo antecipado à etapa investigatória, e a preservação do material colhido. O mesmo fundamento alcança o direito à prova. O art. 159, § 3º, do Código de Processo Penal faculta ao acusado

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

formular quesitos e indicar assistente técnico, mas essa faculdade perde sentido se o assistente não puder examinar a cópia dos dados e a documentação da extração, acesso que a regra de *disclosure* defendida por Sarkis e Giacomolli (2025) procura assegurar. A auditabilidade, portanto, não é uma exigência técnica externa ao processo, mas a condição para que o contraditório e o direito à prova tenham objeto. Por isso, como sustenta Badaró (2021, p. 9), a prova digital cuja cadeia de custódia não pode ser verificada não tem valor epistêmico.

Desse critério decorrem exigências práticas, extraídas das fontes examinadas. A primeira é a documentação de cada etapa, que Fisberg (2025, p. 28, 34) considera requisito mínimo, qualquer que seja a tecnologia empregada. A segunda é a disponibilização à defesa de cópia forense integral, acompanhada dos códigos *hash*, e não apenas do relatório final. A terceira é a revelação dos critérios de filtragem e seleção dos dados e das ferramentas utilizadas, nos moldes do modelo alemão mencionado por Sarkis e Giacomolli (2025, p. 245). A quarta é a atribuição da custódia e da perícia a órgãos técnicos oficiais, e não à autoridade que investiga ou acusa (Vecchio; Beck, 2025, p. 7). O que lhes falta é previsão legal que as torne obrigatórias.

Duas ressalvas são necessárias. A primeira: a auditabilidade não resolve todos os obstáculos identificados. A dependência de provedores, a guarda limitada de registros e a lentidão da cooperação internacional, descritas na subseção 4.1, são problemas de acesso aos dados, e não de verificação. A segunda: a exigência de auditabilidade não se opõe à eficiência da investigação. Uma prova cuja integridade pode ser demonstrada é mais resistente à impugnação e serve melhor à própria acusação do que uma prova que depende da presunção de que foi corretamente manuseada. O equilíbrio entre a eficiência da persecução penal e as garantias do acusado, nesse ponto, não depende de concessões de um lado ou de outro, mas de procedimentos que permitam a ambos verificar a mesma prova.

6. CONSIDERAÇÕES FINAIS

Este artigo partiu da seguinte pergunta: quais os principais obstáculos à obtenção, à preservação e à valoração da prova digital na persecução penal dos crimes cibernéticos no ordenamento jurídico brasileiro? A pesquisa permite identificar um obstáculo central em cada momento e o elemento que os une.

Na obtenção, o principal obstáculo é a falta de parâmetros legais para o acesso aos dados. As autorizações judiciais tendem a ser genéricas e permitem a coleta integral do conteúdo dos dispositivos, com seleção posterior do que interessa. O Tema 977 do Supremo Tribunal Federal, ainda pendente de embargos de declaração, trouxe maior segurança quanto à necessidade de autorização judicial ou consentimento nos casos de prisão em flagrante, e exigiu

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

que a decisão delimite a abrangência do acesso. Não fixou, porém, critérios objetivos para essa delimitação e admitiu medidas de preservação com justificação apenas posterior. Somam-se a isso a dependência de provedores, com prazos de guarda curtos e registros nem sempre suficientes para identificar a autoria, e a lentidão da cooperação internacional diante da volatilidade dos dados.

Na preservação, o obstáculo central é a inadequação da disciplina legal da cadeia de custódia à prova digital. Os arts. 158-A a 158-F do Código de Processo Penal foram pensados para vestígios materiais e não tratam de cópia forense, códigos *hash*, dados em nuvem ou registros mantidos por terceiros. As normas técnicas que preenchem essa lacuna não têm força obrigatória e são aplicadas de modo desigual. O próprio *hash*, frequentemente tratado como garantia suficiente, assegura apenas a integridade dos dados a partir do momento em que foi calculado, e não sua autenticidade.

Na valoração, o obstáculo central é a divergência sobre as consequências da quebra da cadeia de custódia e, sobretudo, sobre quem deve demonstrar a integridade da prova. A doutrina se divide entre a inadmissibilidade, a nulidade relativa e soluções intermediárias. Nos julgados examinados, o Superior Tribunal de Justiça ora atribui ao Estado o ônus de comprovar a integridade, ora exige da defesa indícios concretos de adulteração, sem que haja, até o momento, precedente qualificado sobre o tema.

No conjunto documental examinado, de caráter qualitativo e não exaustivo, a hipótese inicial encontrou respaldo. Os obstáculos não decorrem apenas da ausência de disciplina legal específica, mas dos três fatores descritos acima. A pesquisa permitiu, porém, refinar a hipótese em dois pontos. Primeiro, no plano da preservação, o problema não é a inexistência de regras técnicas, mas a falta de sua incorporação pela lei processual. Segundo, a auditabilidade pela defesa não é apenas um traço comum aos três fatores, mas pode funcionar como critério para resolver a divergência sobre a valoração. Quando, apesar de uma falha, a defesa ainda consegue verificar a integridade do material, a irregularidade deve ser considerada na valoração da prova. Quando a falha impede qualquer verificação, a prova não deve ser admitida, porque não pode ser submetida ao contraditório. Desse critério decorre que o ônus de assegurar as condições de verificação cabe a quem produz a prova.

A pesquisa tem limitações. A revisão de literatura examinou um corpus de dez trabalhos, o que não esgota a produção sobre o tema. A análise jurisprudencial baseou-se em seleção intencional de julgados, que não representa o conjunto das decisões dos tribunais. O caso Banco Master foi examinado apenas a partir de informações divulgadas pela imprensa, uma vez que o processo tramita sob sigilo.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Essas limitações indicam caminhos para pesquisas futuras, como o levantamento sistemático das decisões do Superior Tribunal de Justiça sobre a quebra da cadeia de custódia da prova digital e o exame das práticas efetivamente adotadas pelos órgãos periciais. No plano normativo, os resultados apontam para a necessidade de uma disciplina legal própria para a prova digital. Essa disciplina deveria definir o conteúdo mínimo das autorizações de acesso a dados, incorporar padrões técnicos de preservação e assegurar à defesa o acesso à cópia integral dos dados e aos critérios utilizados em sua análise. Enquanto essa disciplina não existir, a auditabilidade oferece um parâmetro já compatível com o ordenamento vigente, porque decorre diretamente da garantia constitucional do contraditório. A prova digital pode contribuir de forma relevante para a responsabilização penal nos crimes cibernéticos, e essa contribuição será tanto mais segura quanto maior for a possibilidade de verificá-la por todos os que participam do processo.

DECLARAÇÕES

Conflito de interesses: os autores declaram não haver conflito de interesses.

Financiamento: a pesquisa não recebeu financiamento.

Uso de inteligência artificial: utilizou-se ferramenta de inteligência artificial generativa na organização da planilha de triagem. As decisões de inclusão e exclusão, a conferência das passagens citadas e a análise crítica são de responsabilidade da autora.

Contribuição dos autores: Emilly Betoldo da Silva — concepção, metodologia, pesquisa, análise e redação; Luiz Paulo Busquim Braga — orientação, supervisão e revisão crítica.

REFERÊNCIAS

AVOLIO, Luiz Francisco Torquato; BORRI, Luiz Antonio; SAAD NETTO, Cláudio. A cadeia de custódia da prova digital: dissensos e consensos entre teoria e práxis. *Boletim IBCCRIM*, São Paulo, ano 34, n. 403, p. 18-21, jun. 2026. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/download/2761/1637/16298. Acesso em: 26 out. 2026.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, ano 29, n. 343, p. 7-9, jun. 2021. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 19 out. 2026.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 26 out. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

BRASIL. *Decreto nº 11.491, de 12 de abril de 2023*. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 26 out. 2026.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 26 out. 2026.

BRASIL. *Decreto-Lei nº 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 26 out. 2026.

BRASIL. *Lei nº 8.069, de 13 de julho de 1990*. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 27 out. 2026.

BRASIL. *Lei nº 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, DF: Presidência da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 26 out. 2026.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 26 out. 2026.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 26 out. 2026.

BRASIL. *Lei nº 13.964, de 24 de dezembro de 2019*. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 26 out. 2026.

BRASIL. *Lei nº 14.155, de 27 de maio de 2021*. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 26 out. 2026.

BRASIL. *Lei nº 15.487, de 6 de agosto de 2026*. Institui medidas de enfrentamento e repressão ao crime de violência sexual contra criança ou adolescente, inclusive no ambiente digital e com uso de inteligência artificial [...]. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15487.htm. Acesso em: 26 out. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

BRASIL. Supremo Tribunal Federal (Plenário). *Ação Declaratória de Constitucionalidade 51/DF*. Relator: Min. Gilmar Mendes, 23 fev. 2023a. Disponível em: https://www.stf.jus.br/arquivo/cms/publicacaoBOInternet/anexo/link_download/casos_relevantes/pt/ADC_51.pdf. Acesso em: 27 out. 2026.

BRASIL. Supremo Tribunal Federal (Plenário). *Recurso Extraordinário com Agravo 1.042.075/RJ*. Tema 977 da repercussão geral. Relator: Min. Dias Toffoli, 25 jun. 2025a. *Informativo STF*, Brasília, DF, n. 1184, 4 ago. 2025. Disponível em: https://www.stf.jus.br/arquivo/informativo/documento/informativo1184.htm. Acesso em: 26 out. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). *Agravo Regimental no Recurso em Habeas Corpus 143.169/RJ*. Relator para o acórdão: Min. Ribeiro Dantas, 7 fev. 2023b. *Diário da Justiça Eletrônico*, Brasília, DF, 2 mar. 2023. Disponível em: https://scon.stj.jus.br. Acesso em: 20 out. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). *Agravo Regimental no Habeas Corpus 828.054/RN*. Relator: Min. Joel Ilan Paciornik, 23 abr. 2024a. *Diário da Justiça Eletrônico*, Brasília, DF, 29 abr. 2024. Informativo de Jurisprudência n. 811. Disponível em: https://scon.stj.jus.br. Acesso em: 20 out. 2026.

BRASIL. Superior Tribunal de Justiça (6. Turma). *Agravo Regimental no Recurso em Habeas Corpus 182.310/RJ*. Relator: Min. Jesuíno Rissato (Desembargador convocado do TJDFT), 14 maio 2024b. *Diário da Justiça Eletrônico*, Brasília, DF, 17 maio 2024. Disponível em: https://scon.stj.jus.br. Acesso em: 26 out. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). *Agravo Regimental no Habeas Corpus 902.195/RS*. Relator: Min. Joel Ilan Paciornik, 3 dez. 2024c. *Diário de Justiça Eletrônico Nacional, Brasília, DF, 9 dez*. 2024. Disponível em: https://scon.stj.jus.br. Acesso em: 26 out. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). *Agravo Regimental no Recurso em Habeas Corpus 208.857/BA*. Relator: Min. Joel Ilan Paciornik, 30 abr. 2025b. *Diário de Justiça Eletrônico Nacional, Brasília, DF, 7 maio* 2025. Disponível em: https://scon.stj.jus.br. Acesso em: 26 out. 2026.

BRASIL. Superior Tribunal de Justiça (5. Turma). *Agravo em Recurso Especial 2.967.413/RS*. Relator: Min. Ribeiro Dantas, 9 dez. 2025c. *Diário de Justiça Eletrônico Nacional, Brasília, DF, 16 dez*. 2025. Disponível em: https://scon.stj.jus.br. Acesso em: 26 out. 2026.

COSTA JÚNIOR, Ivan Jezler. *A busca por um marco processual da internet*: requisitos para colheita dos dados armazenados em compartimentos eletrônicos. 2018. 198 f. Dissertação (Mestrado em Ciências Criminais) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: http://tede2.pucrs.br/tede2/handle/tede/8209. Acesso em: 19 out. 2026.

COUNCIL OF EUROPE. *Explanatory Report to the Convention on Cybercrime*. Budapest, 23 nov. 2001. (European Treaty Series, n. 185). Disponível em: https://rm.coe.int/16800cce5b. Acesso em: 28 out. 2026.

DEFESA de Vorcaro pede ao STF acesso à perícia de celulares apreendidos. *Gazeta Digital*, Cuiabá, 8 mar. 2026. Disponível em: https://www.gazetadigital.com.br/editorias/brasil/defesa-de-

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

vorcaro-pede-ao-stf-acesso-a-pericia-de-celulares-apreendidos/839327. Acesso em: 19 out. 2026.

FISBERG, Yuri. Função “hash” e a integridade da prova digital. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 11, n. 3, e1227, set./dez. 2025. DOI: https://doi.org/10.22197/rbdpp.v11i3.1227. Acesso em: 19 out. 2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *Anuário Brasileiro de Segurança Pública 2026*. São Paulo: FBSP, 2026. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2026/07/anuario-2026.pdf. Acesso em: 19 out. 2026.

FREITAS, Caio de. Banco Master: decisão de Toffoli pode impedir perícia com tecnologia de ponta em celulares. *Agência Pública*, [S. l.], 22 jan. 2026. Disponível em: https://apublica.org/nota/banco-master-decisao-de-toffoli-pode-impedir-pericia-com-tecnologia-de-ponta-em-celulares/. Acesso em: 19 out. 2026.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. *Revista Em Tempo*, Marília, v. 20, n. 1, nov. 2020. DOI: https://doi.org/10.26729/et.v20i1.3130. Acesso em: 19 out. 2026.

MARSHALL, Paul *et al.* Recommendations for the probity of computer evidence. *Digital Evidence and Electronic Signature Law Review*, London, v. 18, p. 18-26, 2021. DOI: https://doi.org/10.14296/deeslr.v18i0.5240. Acesso em: 28 out. 2026.

MENDONÇA autoriza PF a fazer perícias sem restrição no caso Master. *Poder360*, Brasília, 19 fev. 2026. Disponível em: https://www.poder360.com.br/poder-justica/mendonca-autoriza-pf-a-fazer-pericias-sem-restricao-no-master/. Acesso em: 19 out. 2026.

MENEZES, Isabela Aparecida de; BORRI, Luiz Antonio; SOARES, Rafael Junior. A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 4, n. 1, p. 277-300, jan./abr. 2018. DOI: https://doi.org/10.22197/rbdpp.v4i1.128. Acesso em: 26 out. 2026.

MOLITOR, Heloísa Augusta Vieira; VELAZQUEZ, Victor Hugo Tejerina. Breve panorama sobre a legislação aplicada nos crimes eletrônicos. *Revista de Direito, Governança e Novas Tecnologias*, [S. l.], v. 3, n. 2, p. 81-96, jul./dez. 2017. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/2589. Acesso em: 26 out. 2026.

NEVES, Elisa Ramos Pittaro. Ensaio sobre a cadeia de custódia e a prova digital. *Revista Cientifica do CPJM*, Rio de Janeiro, v. 4, n. 14, p. 151-159, 2025. Disponível em: https://rcpjm.emnuvens.com.br/revista/article/view/355. Acesso em: 19 out. 2026.

PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. *Consultor Jurídico*, São Paulo, 26 jan. 2021. Disponível em: https://conjur.com.br/wp-content/uploads/2021/04/artigo-geraldo-prado.pdf. Acesso em: 28 out. 2026.

QUEIROZ, Liv Ferreira Augusto Severo. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios. *Revista do CNMP*, [Brasília], n. 12, p. 417-448, 2024. DOI: https://doi.org/10.36662/revistadocnmp.i12.707. Acesso em: 19 out. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

QUEMEL, Melhym Pereira. A integridade da prova digital como vetor da modulação da nulidade: repercussões da quebra da cadeia de custódia. *Revista do CNMP*, [Brasília], n. 13, p. 236-259, 2025. DOI: https://doi.org/10.36662/revistadocnmp.i13.845. Acesso em: 19 out. 2026.

RICHTER, André. André Mendonça é o novo relator do inquérito do Master. *Agência Brasil*, Brasília, 12 fev. 2026. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2026-02/andre-mendonca-e-o-novo-relator-do-inquerito-do-master. Acesso em: 19 out. 2026.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 10, n. 3, e1071, set./dez. 2024. DOI: https://doi.org/10.22197/rbdpp.v10i3.1071. Acesso em: 14 out. 2026.

SARKIS, Jamilla Monteiro; GIACOMOLLI, Nereu José. A regra de disclosure no processo penal e sua relevância para a prova digital. *Revista da Faculdade Mineira de Direito*, Belo Horizonte, v. 28, n. 55, p. 221-250, 2025. DOI: https://doi.org/10.5752/P.2318-7999.2025v28n55p221-250. Acesso em: 19 out. 2026.

UNIÃO EUROPEIA. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings [...]. *Official Journal of the European Union*, L 191, p. 118-180, 28 jul. 2023. Disponível em: https://eur-lex.europa.eu/eli/reg/2023/1543/oj. Acesso em: 28 out. 2026.

VAZ, Millena Ferreira. A preservação da cadeia de custódia como pressuposto de admissibilidade da prova digital. *Revista da ESMESC*, Florianópolis, v. 30, n. 36, p. 323-350, 2023. DOI: https://doi.org/10.14295/revistadaesmesc.v30i36.p323. Acesso em: 19 out. 2026.

VECCHIO, Fabrizio Bon; BECK, Francis Rafael. A prova digital e a sua cadeia de custódia no processo penal: uma análise doutrinária, normativa e jurisprudencial. *Journal of Law and Corruption Review*, [Guarulhos], v. 7, e0107, 2025. DOI: https://doi.org/10.37497/CorruptionReview.7.2025.108. Acesso em: 19 out. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.