Cadeia de custódia, Prova Digital e código *hash*: uma análise da jurisprudência do STJ à luz do processo penal acusatório

Chain of Custody, Digital Evidence, and Hash Values: An Analysis of STJ Precedents considering the Accusatory Criminal Procedure

Daniele Lovatte Maia[1]

Pesquisadora independente – Niterói, RJ, Brasil

daniele.lovatte@gmail.com

http://lattes.cnpq.br/4430261125725628

https://orcid.org/0000-0002-9756-8828

Resumo: O artigo tem como objetivo a análise da jurisprudência do Superior Tribunal de Justiça (STJ) sobre provas digitais, mapeando a forma como são fundamentados os precedentes em que a defesa requer a nulidade da prova por falta de integridade na cadeia de custódia, dada a ausência de código *hash* nos arquivos digitais. A pesquisa se justifica pela atualidade do tema, em especial considerando que no último ano foram proferidas cinco vezes mais decisões sobre a matéria do que nos dez anos anteriores. Para tanto, utilizou-se uma revisão bibliográfica em matéria de processo penal e prova digital, bem como de metodologia empírica, por meio da análise sistemática dos julgados do STJ, cuja ementa continha a palavra *hash*. O mapeamento descritivo e crítico dos acórdãos teve seus resultados apresentados por meio da combinação de métodos quantitativos e qualitativos. Como consequência, verifica-se

[1] Doutora em Direito e Sociologia pela Universidade Federal Fluminense (UFF), com período de pesquisa (doutorado sanduíche) na Universidade *degli Studi di Macerata* (Itália). Mestre em Direito pela Universidade Federal do Rio de Janeiro. Graduada em Direito pela UFRJ. Advogada e Sócia do *T.F'A&M* – Tristão Farme d'Amoed Maia Advogados. Professora substituta de direito penal, direitos humanos e direito administrativo da Universidade Federal do Rio de Janeiro (2024-2026). Professora substituta de Direito Penal, Prática Penal e Metodologia da UFF/Macaé (2019-2021).

que a maior parte dos precedentes possui um déficit de justificação, retirando do Estado acusador o ônus probatório sobre a validade da prova digital e colocando na defesa a tarefa de comprovar o prejuízo no caso concreto, em ofensa ao sistema acusatório.

Palavras-Chave: cadeia de custódia; prova digital; processo penal acusatório.

Abstract: *This article aims to analyze the precedents of the Superior Court of Justice (STJ) regarding digital evidence, mapping how precedents are reasoned when the defense requests the nullity of evidence due to a lack of integrity in the chain of custody, given the absence of a hash code in digital files. The research is justified by the current relevance of the subject, especially considering that in the last year five times more decisions were handed down than in the previous ten years, in a comparison with the research conducted by previous empirical analysis. To this end, a literature review on criminal procedure and digital evidence was used, as well as an empirical methodology through the systematic analysis of STJ decisions whose headnotes (ementa) contained the word hash. The descriptive and critical mapping of the decisions had its results presented through a combination of quantitative and qualitative methods. Consequently, it is verified that most precedents suffer from a justification deficit, removing from the prosecuting State the burden of proof regarding the validity of the digital evidence and placing upon the defense the task of proving prejudice in the specific case, in violation of the accusatory system.*

Keywords: *chain of custody; digital evidence; accusatory criminal procedure.*

Sumário: Introdução; 1. A cadeia de custódia na era digital; 2. A jurisprudência do Superior Tribunal de Justiça sobre provas digitais, cadeia de custódia e código *hash*; 2.1. Percurso metodológico; 2.2. Mapeamento descritivo e crítico das decisões; Considerações Finais; Referências.

Introdução

O presente estudo tem como objetivo a análise da jurisprudência do Superior Tribunal de Justiça (STJ) na temática da cadeia de custódia das

provas digitais, notadamente investigar a imprescindibilidade do código *hash* para possibilitar um contraditório amplo sobre os dados digitais. Precisamente, o escopo da pesquisa é considerar eventual déficit de justificação do precedente e não o seu resultado propriamente dito – de provimento ou desprovimento do recurso – avaliando a fundamentação que levou os Ministros a decidir de uma ou de outra forma.

A atualidade do tema é o principal motor de justificativa do estudo. Em que pese a proteção dos dados digitais tenha sido elevada a direito fundamental por meio da Emenda Constitucional 115/2022, o sistema processual penal brasileiro ainda é carente de normativas amplas sobre o tema. No intuito de concretizar a dignidade da pessoa humana como vetor axiológico que deve irradiar seus efeitos para todo o restante do ordenamento jurídico, o uso de dados digitais como prova no processo penal deve ser feito prezando pela presunção de inocência, pelo contraditório e pela materialização prática de um processo penal acusatório e constitucional. Nesse sentido, prescindir de um processo penal ancorado na absoluta auditabilidade das provas digitais, integralmente disponíveis à defesa desde o início da persecução penal judicial, é negar concretude a esse arcabouço principiológico, naturalizando condenações criminais com resquícios de sistema penal inquisitório e autoritário.

Por essa razão, a reflexão aqui proposta será apresentada em duas etapas:

Na primeira, será feita uma revisão de literatura sobre o processo penal digital, em busca do estado da arte atual sobre o uso das provas digitais no processo penal e a proteção da integridade da cadeia de custódia dos dados utilizados para a condenação. Aqui serão definidos os conceitos necessários para análise das decisões do STJ, tais como cadeia de custódia, código *hash* e dados brutos. Ademais, serão elencadas as principais normas legais e infralegais que regulamentam a perícia e a metodologia de extração de dados digitais em aparelhos eletrônicos. Na sequência, será apresentada uma análise das decisões do STJ sobre provas digitais, com mapeamento descritivo e crítico dos julgados, buscando um paralelo entre a fundamentação dos Ministros e a revisão de literatura realizada no item anterior.

Utiliza-se uma análise combinada de métodos qualitativos e quantitativos, após a devida categorização dos conceitos-chave presentes

nas decisões. A escolha dos códigos de leitura seguiu a metodologia de análise de julgados de Hall e Wright[2]; além do mapeamento de termos descritivos e valorativos da Metodologia de Análise de Decisões (MAD), de Freitas Filho e Lima[3], em busca de eventuais déficits de justificação. Ademais, foi feita uma análise comparativa com a pesquisa já realizada por Fisberg[4], por meio de uma investigação empírica e revisão documental sistemática das decisões do STJ, entre 03/07/2016 e 03/07/2026, cuja ementa contivesse a palavra *hash*.

Em respeito à Portaria do CNPq 2.664/2026, informa-se que a Inteligência Artificial Generativa "Gemini" foi utilizada da seguinte forma: i) auxílio em ideias para delimitação do recorte temático do artigo; ii) tradução do resumo e do título do português para o inglês; iii) organização final das referências bibliográficas pelo padrão ABNT; iv) organização e formatação da planilha de Excel com os dados brutos da pesquisa.

Como resultado, espera-se poder contribuir para um melhor entendimento da comunidade jurídica brasileira a respeito de como o STJ vem se utilizando de provas digitais para fundamentar condenações criminais, bem como se a fundamentação utilizada pelo Tribunal está em consonância com o processo penal acusatório.

1. A CADEIA DE CUSTÓDIA NA ERA DIGITAL

A Lei 13.964/19 introduziu normas expressas sobre cadeia de custódia nos artigos 158-A e seguintes do CPP. Contudo, não trouxe determinações específicas sobre prova digital, tampouco as consequências processuais práticas advindas de uma prova desprovida de cadeia de custódia íntegra ou do momento processual adequado para o exame da

---

2 HALL, Mark A.; WRIGHT, Ronald F. Systematic content analysis of judicial opinions. *California Law Review*. v. 96, p. 63-122, 2008.

3 FREITAS FILHO, Roberto; LIMA, Thalita Morais. *Metodologia de análise de decisões* - MAD. *Univ. JUS*, Brasília, n. 21, p. 1-17, jul./dez. 2010. Disponível em: https://www.rel.uniceub.br/jus/article/viewFile/1206/1149. Acesso em: 18 jul. 2026.

4 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.

sua regularidade[5]. Dada a complexidade do tema, é importante que os operadores do direito façam uma interpretação extensiva do texto legal, com auxílio de outras normas, sejam elas infralegais ou normas técnicas existentes no Brasil, adotando-as como referência metodológica para a perícia digital[6].

Sendo a computação forense disciplina científica de rápida evolução, as normas técnicas ajudam a evitar o engessamento no trato da matéria, fornecendo padrões de conduta com adaptações que nem sempre podem ser acompanhadas pelo ordenamento jurídico, dada a morosidade própria do processo legislativo[7]. Uma legislação que impusesse um método de coleta de provas digitais como necessariamente superior aos demais, correria o risco de tornar-se obsoleta em pouco tempo, superada pela aceleração das novidades tecnológicas[8]. Para além de um método perfeito e imutável para a extração de provas digitais no processo penal, o primordial é que sejam observadas práticas padronizadas, auditáveis e, acima de tudo, bem documentadas, possibilitando sua repetibilidade[9].

A título de exemplo, a Convenção de Budapeste sobre crimes cibernéticos[10] tem por objetivo tornar as investigações criminais mais

---

5 MATIDA, Janaina. A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes. Boletim IBCCRIM, São Paulo, v. 28, n. 331, p. 6–9, 2020. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/541. Acesso em: 18 jul. 2026.

6 FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. *Revista Acadêmica*, 2020. DOI: https://doi.org/10.26729/et.v20i1.3130. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 13 set. 2026.

7 CASEY, Eoghan (org.), *et al*. *Handbook of digital forensics and investigation*. San Diego: Elsevier, 2010. 567p.

8 DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di Diritto Processuale*, Milano, v. 66, n. 2, p. 283-298, mar./apr. 2011.

9 CASEY, Eoghan. *op. cit*.

10 Nesse sentido, dispõe o artigo 19.3 da convenção de Budapeste: "Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para apreender ou proteger dados de computador acessados de acordo com os parágrafos 1 ou 2. Estas medidas incluirão o poder de: a. apreender ou proteger um sistema de computador ou parte dele ou um meio de armazenamento de dados; b. fazer e guardar uma cópia desses dados de computador; c. manter a integridade dos dados

eficientes, possibilitando a regular obtenção de provas digitais. Dispondo especificamente sobre a busca e apreensão em computador, impõe que a autoridade competente guarde uma cópia de segurança dos dados digitais, de modo a manter a integridade do material original para análise futura, preservada, assim, a sua cadeia de custódia.

A cadeia de custódia pode ser definida como o procedimento que garante que os dados colhidos durante uma investigação sejam autênticos e resguardados desde a colheita até a sua efetiva utilização, mantendo registradas as informações do ciclo de vida do documento: pessoas que manusearam a prova, data/hora na qual foi colhida ou transferida, finalidade da transferência, além de detalhes que identifiquem de forma unívoca o aparelho digital em questão (como marca, modelo, número de série, dentre outros). Do ponto de vista técnico, a cadeia de custódia da prova digital não é caracterizada apenas por dados materiais/físicos, mas igualmente por técnicas e interações ocorridas internamente ou externamente ao aparelho, bem como por comandos em presença ou à distância. A alteração da cadeia de custódia de um dispositivo eletrônico pode se dar de forma voluntária/intencional, como também de forma não proposital – a exemplo da realização de backup periódico, com consequente sobreposição, substituição ou cancelamento de dados mais antigos, seja no dispositivo eletrônico, seja no armazenamento de dados em nuvens[11]. Por conseguinte, a indicação do sujeito responsável pela colheita da prova, da metodologia empregada para sua preservação e dos meios pelos quais foram custodiados não são informações que podem ser afastadas por argumentos a respeito da boa ou má-fé do agente público responsável[12].

A ABNT NBR ISO/IEC 27037:2013[13] apresenta diretrizes técnicas de segurança para a identificação, coleta, aquisição e preservação da evi-

---

de computador relevantes; d. tornar inacessíveis esses dados no sistema de computador acessado ou dele removê-los". Para mais informações: BRASIL. *Decreto nº 11.491, de 12 de abril de 2023*. Promulga a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001. Diário Oficial da União, Brasília, DF, 13 abr. 2023.

[11] DE VITA, Roberto. *La prova digitale nel processo penale*. Devitalaw: Roma, 2025.

[12] MATIDA, Janaina. *op. cit*.

[13] Em seu item 3, a norma apresenta a definição de uma série de termos técnicos e procedimentos para coleta da prova digital. A título de ilustração,

dência digital, fornecendo um método prático mundialmente reconhecido para possibilitar sua admissão como prova em processos judiciais. Apesar de ser uma norma técnica não dotada de coercitividade, possui validade internacional, propondo metodologias objetivas para a extração de dados digitais e registro adequado do caminho percorrido pela perícia, sendo uma maneira válida e eficaz de manter íntegra a cadeia de custódia para fins de utilização futura do material em um processo penal.

Em sentido similar, a Instrução Normativa DG/PF nº 299/2025 aponta que a prova digital deve ser dotada de rastreabilidade, integridade e proteção contra manipulações indevidas, colocando os princípios da documentação e da mesmidade como orientadores da atividade de polícia judiciária[14]. A norma define, em seu artigo 7, o conceito de dado digital: "aquele obtido diretamente da Internet, de ambiente de nuvem, de redes de computadores ou de outros espaços cibernéticos". Para a coleta desses dados digitais sem suporte físico, o artigo 10 da

citam-se alguns: 3.5. evidência digital: informações ou dados, armazenados ou transmitidos em forma binária, que podem ser invocados como evidência; 3.6. cópia de evidência digital: cópia de evidência digital que foi produzida para manter a confiabilidade da evidência, incluindo tanto a evidência digital como os meios de verificação nos quais o método de verificação pode ser incorporado ou ser independente das ferramentas utilizadas na verificação; 3.11. valor de *hash*: série de bits que são o resultado da função *hash*; 3.16. confiabilidade: propriedade de resultados e comportamentos pretendidos consistentes; 3.17. repetibilidade: propriedade de um processo conduzido para obter os mesmos resultados de testes em um mesmo ambiente de teste (mesmo computador, disco rígido, modo de operação etc.); 3.18. reprodutibilidade: propriedade de um processo para obter os mesmos resultados de testes em um diferente ambiente de teste (diferente computador, disco rígido, operador etc.). Para mais informações: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27037:* Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.

[14] Embora não apresente a definição do princípio da mesmidade, a norma informa, em seu artigo 3: "Os princípios que orientam a cadeia de custódia na Polícia Federal são os da documentação e da mesmidade, além daqueles aplicáveis à atividade de polícia judiciária". BRASIL. Ministério da Justiça e Segurança Pública. Polícia Federal. *Instrução Normativa DG/PF nº 299, de 24 de fevereiro de 2025*. Regulamenta a cadeia de custódia de elementos de interesse em formato digital no âmbito da Polícia Federal. Brasília, DF: Polícia Federal, 2025. Publicada no Boletim de Serviço nº 52, de 18 de março de 2025.

norma impõe a obrigatoriedade de uma documentação detalhada que contenha: data e local da extração de procedimentos, número de *hash* e identificação do dispositivo de armazenamento de dados, devendo sempre ser lacrado.

Embora em seu nível mais básico a evidência digital exista em um meio físico (como um disco magnético, um fio de cobre ou um sinal de rádio no ar), a análise forense raramente se debruça sobre a mídia física direta, ocorrendo através da intermediação de computadores e softwares para que os dados possam ser interpretados pela mente humana. Para tanto, os campos magnéticos são traduzidos, agrupados em códigos e logicamente organizados em arquivos e pastas. O perito acaba por examinar não o dado real, mas uma representação traduzida/abstrata dessa realidade, sendo que cada camada de abstração ou ferramenta empregada pode introduzir erros (*bugs)* ou acarretar perda das informações do arquivo original[15].

A diferenciação feita por Casey[16] entre aquisição física e aquisição lógica dos dados digitais fornece luz aos conceitos. Na aquisição física – método pelo qual se extraem os dados brutos (*raw data*), há uma cópia contínua, *bit* a *bit*, de toda a memória física de um dispositivo eletrônico, inclusive de arquivos eventualmente deletados. Não se trata de um documento estruturado, mas uma sequência de caracteres aparentemente incompreensíveis. Paralelamente, na aquisição lógica, é feita uma extração de dados já estruturados e organizados (como pastas de SMS, aplicativos de notas, contatos e histórico), mas ainda sem qualquer tratamento estético ou relatório visual de leitura. A limitação da aquisição lógica é o fato de ela recuperar apenas os dados ativos reconhecidos pela estrutura lógica do sistema operacional do aparelho periciado, sem acessar sua memória bruta, deixando de fora eventuais registros apagados.

Por essa razão, quando a defesa não tem acesso aos dados brutos (*raw data*), decorrentes da aquisição física, mas apenas ao relatório de leitura desses dados, gerados pelos mais diversos softwares forenses, acaba por ter acesso apenas a uma interpretação secundária dos dados

---

15 CASEY, Eoghan. *op. cit*.

16 *Ibidem*.

digitais. Para Lopes e outros[17], a disponibilização da integralidade da extração à defesa — incluindo a imagem forense (*raw data* / cópia *bit a bit*), os arquivos de projeto e metadados de extração (como as extensões proprietária .ufde .ufdx do software Cellebrite UFED)[18], os arquivos compactados e os *logs* de auditoria — é condição inegociável para a garantia do devido processo legal. Somente assim é possível fazer uma leitura primária/original dos dados digitais e, posteriormente, compará-los com o material produzido pela acusação.

Geraldo Prado[19] fundamenta a integridade da cadeia de custódia no princípio da mesmidade, ou seja, os dados encontrados na cena de um crime devem ser os mesmos utilizados na tomada da decisão judicial. Embora a definição do princípio da mesmidade tenha idêntica finalidade para a cadeia de custódia de qualquer material probatório, a imaterialidade das provas digitais impõe a adoção de padrões técnicos precisos, objetivando comprovar que os dados eletrônicos analisados no processo penal são os mesmos coletados durante a investigação.

Quando o perito realiza a extração física dos dados brutos, o software utilizado automaticamente calcula um algoritmo matemático que evidencia o conjunto total de bytes extraídos (como SHA-2 ou MD5)[20]. O código *hash* pode, então, ser definido como "um cálculo matemático que reduz um montante de dados em uma sequência alfanumérica fixa – um corte de *bits* e o processamento em um padrão, segundo um protocolo pré-determinado"[21]. O *hash* possibilita a comparação de um arquivo com

---

17 LOPES, Aury *et al*. Prova penal digital: relatório do Cellebrite pode ser insuficiente. *Consultor Jurídico (ConJur)*, São Paulo, 10 out. 2025. Disponível em: https://www.conjur.com.br/2025-out-10/prova-penal-digital-relatorios-do-cellebrite-podem-ser-insuficientes/. Acesso em: 18 jul. 2026.

18 O Cellebrite é um software especializado em periciar aparelhos celulares. Por meio da ferramenta chamada *Universal Forensic Extraction Device* (UFED), possibilita o desbloqueio do aparelho, a extração de seus dados e a elaboração de um relatório com o conteúdo dos dados extraídos. Para mais informações Cf.: KERR, Orin S. *The digital Fourth Amendment*: privacy and policing in our online world. New York: Oxford University Press, 2025.

19 PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. 1. ed. São Paulo: Marcial Pons, 2019.

20 FURLANETO NETO, Mario. *op. cit*.

21 FISBERG, Yuri. *op. cit*.

o seu similar de origem, já que ambos devem possuir o mesmo código alfanumérico identificador, uma espécie de impressão digital do arquivo, sendo certo que qualquer mínima alteração nele gera, automaticamente, uma alteração no código *hash* do arquivo[22].

Embora o *hash* seja de suma importância para a auditabilidade da prova digital, ele apenas atesta que um determinado conjunto de dados não foi modificado em relação ao estado em que se encontrava quando foi gerado. Se um print de tela de celular for tido como prova de um processo penal, a auditabilidade do arquivo por meio da geração de seu código *hash* não serve para distinguir, a título de exemplo, se uma foto foi criada por inteligência artificial, ou se um diálogo de WhatsApp corresponde a integridade da conversa entre as partes[23].

Nesse diapasão, o *hash* valida a conformidade de uma cópia com seu original sem, contudo, atestar a validade ou impedir a contaminação prévia do arquivo original. Daí ser um dever da autoridade competente pela apreensão da prova realizar "a cópia integral (*bit a bit*) do conteúdo do dispositivo, gerando assim uma imagem dos dados que espelha e representa de maneira fiel o conteúdo do original"[24]. Dada a complexidade da tarefa, a conferência da integridade das provas é facilitada quando a extração é feita com o uso de softwares específicos, como o *ADB*, o *Cellebrite*, o *Avilla Forensics* e o *IPED*. Tais programas são considerados de excelência para a extração de dados digitais, "por meio de extração lógica, física ou de imagens de unidade de armazenamento com ênfase na necessidade de garantir a cadeia de custódia para a admissibilidade das provas em processos judiciais"[25].

---

22 HERMEIRO, Andreia Carina Claúdio. *A cadeia de custódia da prova digital:* o uso da Tecnologia Blockchain como forma de preservação. 2023. 64p. Dissertação (Mestrado em Ciências Jurídico-Forenses) – Faculdade de Direito, Universidade de Coimbra, Coimbra, 2023.

23 FISBERG, Yuri. *op. cit*.

24 SILVA, Fernanda Pereira da. *A cadeia de custódia da prova digital na colaboração premiada:* fiabilidade probatória. 2023. 85 f. Dissertação (Mestrado Profissional em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, DF, 2023, p. 53.

25 SILVA, Marcos Alexandre de Araújo. Perícia em dispositivos móveis. *In*: SOUZA, Bernardo de Azevedo; SILVA, Marcos Lamas Santos da (coord.). *Perícias Digitais*. Indaiatuba, SP: Foco, 2025, p. 26.

Ainda assim, o uso de softwares especializados como os acima referidos servem como indício de mesmidade da prova digital, mas não garantem, por si sós, a integridade da cadeia de custódia. A dificuldade da perícia da prova digital reside no fato de cada aparelho ter seu próprio sistema operacional, sendo que cada sistema operacional necessita de uma linguagem única de leitura. A perícia feita com softwares especializados, embora seja facilitada em muitos aspectos, em outros acaba por fornecer uma leitura simplista da prova, com a perda de diferentes tipos de informação, seja por uma limitação do software em relação ao aparelho lido no caso concreto, seja pela falta de treinamento adequado dos peritos judiciais no uso do software[26].

Na sequência da regulamentação por normas infralegais, o arquivo denominado "Procedimentos Operacionais Padrão (POPs) de Perícia Criminal do Ministério da Justiça de 2024"[27] tem como objetivo orientar a perícia criminal no Brasil no trato da prova digital. Além de reforçar a adoção dos princípios da mesmidade e uso do código *hash*, impõe, no item 4.3, que um celular apreendido deva ser imediatamente desligado, ter seu cartão SIM removido, ser devidamente lacrado e inserido em uma *Faraday Bag*[28](ou envolto em três camadas de papel alumínio de modo a preservar o isolamento adequado do material, bloqueando eventuais sinais de internet que possam alterar o conteúdo interno do aparelho). Recomenda igualmente o uso de softwares adequados que permitam a compreensão e repetição do laudo futuramente, com o uso de uma cópia de segurança.

---

26 KERR, Orin. *op. cit*.

27 BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. *Procedimentos operacionais padrão:* perícia criminal: informática forense. Coordenação de Christhiane Pinto Cutrim e Liliane Pires. Brasília, DF: Secretaria Nacional de Segurança Pública, 2024. v. 5. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/pop/pop-pericia-criminal-2024-informatica-forense-vol-5-pdf.pdf/view. Acesso em: 14 set. 2026.

28 A *Faraday Bag* é uma das modalidades de isolamento de um dispositivo eletrônico de fatores externos, tais como interferências eletromagnéticas, baseada no princípio físico da gaiola de Faraday. Para mais informações: Cf. DE VITA, Roberto. *op. cit*.

De modo análogo, a Portaria SENASP 82/2014[29] define em seus "considerandos" que a cadeia de custódia é chave imprescindível para "garantir a idoneidade e a rastreabilidade dos vestígios, com vistas a preservar a confiabilidade e a transparência da produção da prova pericial até a conclusão do processo judicial". A observância técnica desse procedimento de forma rígida tem o potencial de validar "a evidência digital como elemento de reconstrução de um fato histórico e tornar viável o pleno exercício do contraditório sobre a prova"[30].

Como se percebe, a cadeia de custódia não é uma forma de obtenção de prova, mas sim de garantia da autenticidade e da integridade dos dados digitais, configurando "uma prova sobre a regularidade da prova produzida pelas partes"[31]. Segundo Badaró[32], do ponto de vista terminológico, não seria possível violar a cadeia de custódia, já que ela se refere à transparência do caminho percorrido pela prova, e não a prova em si mesma considerada, esta sim podendo ser violada.

Para que a cadeia de custódia seja considerada íntegra, de acordo com os artigos 158-A e seguintes do CPP, é preciso que se registrem os seguintes caminhos percorridos pela prova[33]: reconhecimento (ato de colocar o elemento como de potencial interesse para a produção da prova pericial); isolamento (lacre do elemento probatório); acondicionamento (guarda individual de cada elemento coletado); fixação (descrição detalhada de como se encontrava o elemento no ato da coleta, através de laudo

---

[29] BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. *Portaria SENASP nº 82, de 16 de julho de 2014*. Estabelece as Diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios. Diário Oficial da União: seção 1, Brasília, DF, p. 42, 18 jul. 2014. Disponível em: https://diariofiscal.com.br/ZpNbw3dk20XgIKXVGacL5NS8haIoH5PqbJKZaawfaDwCm/legislacaofederal/portaria/2014/senasp82.htm. Acesso em: 14 set. 2026.

[30] REIS, Rodrigo Casimiro. *Verdade e prova penal*: a cadeia de custódia da era digital. 1. ed. São Paulo: Amanuense, 2025, p. 25.

[31] *Ibidem*, p. 46.

[32] BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, v. 29, n. 343, p. 7–9, 2021. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 18 jul. 2026.

[33] SILVA, Fernanda. *op. cit.*

pericial); transporte (detalhamento de como foi feito eventual transporte do elemento de modo a manter as condições originais); recebimento (documentação formal da entrega do elemento em casos de transferência); processamento (manipulação do elemento através de uma metodologia adequada); descarte (eliminação do vestígio após autorização judicial).

Entende Nucci[34] que a forma prevista em lei para a concretização dos atos processuais, a exemplo da regulamentação sobre cadeia de custódia, não é um fim em si mesmo, mas formalidade que, caso infringida, gera tão somente uma nulidade relativa. Se o ato atingiu a sua finalidade, somente poderá ser nulificado caso se trate de nulidade absoluta[35]. Por outro lado, nos casos de nulidade relativa, a nulidade é decretada apenas quando for apontado algum prejuízo pelas partes, na forma do artigo 563 do CPP.

Tal posicionamento se coaduna com a posição majoritária adotada pelo Superior Tribunal de Justiça. O enunciado 1 da edição 69/2016 do seu compilado de "Jurisprudência em Teses"[36] aduz que: "A decretação da nulidade de ato processual requer prova inequívoca do prejuízo suportado pela parte, em face do princípio *pas de nullité sans grief*, previsto no art. 563 do Código de Processo Penal"[37]. Já o enunciado 1 da edição 105/2018 deixa claro que eventuais irregularidades na coleta de provas durante o inquérito policial não contaminam a ação penal dele decorrente.

---

[34] NUCCI, Guilherme de Souza. *Curso de direito processual penal*. 17. ed. Rio de Janeiro: Forense, 2020.

[35] Nucci define como nulidades relativas aquelas listadas no artigo 564 do CPP e que não podem ser sanadas na forma do artigo 572 do CPP, a exemplo da incompetência do juízo, nulidade de citação, ausência de exame de corpo de delito em crimes que deixam vestígio e a falta de nomeação de defensor a réu presente. Para mais informações: Cf. NUCCI, Guilherme. *op. cit*.

[36] A Jurisprudência em Teses do Superior Tribunal de Justiça é uma publicação periódica organizada pela Secretaria do Tribunal e que funciona como um catálogo organizado e temático dos precedentes. Cada edição conta com enunciados de teses, acompanhados dos julgados mais recentes que as sustentam. O acesso é gratuito e feito pelo site do tribunal. Mais informações na página oficial do Superior Tribunal de Justiça. Disponível em: https://scon.stj.jus.br/SCON/jt/jt.jsp. Acesso em: 25 set. 2026.

[37] Edição 69/2016 da Jurisprudência em Teses do STJ. Disponível em: https://scon.stj.jus.br/SCON/GetPDFJT?edicao=69. Acesso em: 18 set. 2026.

Em paralelo, as edições 279/2026, 280/2026 e 281/2026 do compilado de "Jurisprudência em Teses" do STJ tratam especificamente sobre direito penal e processual penal em ambiente digital. O enunciado 3 da edição 281/2026 afirma que para se manter íntegra e auditável a cadeia de custódia é necessária: "a possibilidade de exame técnico independente, o que pode incluir utilização de certificadores específicos como o algoritmo *hash*, em observância ao princípio da mesmidade"[38]. No entanto, não menciona se eventual irregularidade nessa cadeia de custódia da prova digital gera uma nulidade absoluta, com necessidade de desentranhamento dos autos, ou relativa, com possibilidade de manutenção no processo, salvo se a parte comprovar prejuízo. A leitura dos precedentes do STJ cuja ementa contenha expressamente a palavra *hash*, feita no próximo item, permitirá uma análise mais detida e crítica sobre o tema.

Para Badaró[39], as omissões e irregularidades leves no trato da prova digital – quando não haja indícios concretos nem de manipulação nem do uso de métodos que retirem seu valor epistêmico de prova – é lícita, e a valoração de seu peso probante deve ser feita pelo juiz no caso concreto. Ou seja, o material probatório permanece nos autos durante a instrução processual, mesmo com valor probatório reduzido, situação que será avaliada pelo juiz ao sentenciar o caso. Em contrapartida, se o método utilizado para a extração da prova for inadequado ou, sendo adequado "não houver comprovação de seu emprego por ausência de registro da cadeia de custódia, não há como garantir a tutela da genuinidade e não alteração do dado informático devido a sua natureza frágil e volátil"[40]. Nesse caso, ainda que a parte não comprove prejuízo, a prova digital deverá ser desentranhada dos autos, em respeito ao princípio da presunção de inocência.

Outro grupo de pesquisadores[41], ao qual essa pesquisa se filia, entende que a falta de integridade da cadeia de custódia torna a prova

---

[38] Edição 281/2026 da Jurisprudência em Teses do STJ. Disponível em: https://scon.stj.jus.br/SCON/GetPDFJT?edicao=281. Acesso em: 18 set. 2026.

[39] BADARÓ, Gustavo. Os standards metodológicos... *op. cit*.

[40] BADARÓ, Gustavo. Os standards metodológicos... *op.cit*.

[41] LOPES, Aury. Prova penal digital... *op. cit*.; MATIDA, Janaina. *op. cit*.; PRADO, Geraldo. *op. cit*.

nula de pleno direito, devendo ser desentranhada dos autos já na fase de instrução. Uma prova digital impossível de ser auditada pode dar ao julgador indícios de fatos que não correspondem à realidade, conferindo peso a uma narrativa potencialmente falsa. Manter a prova nos autos para avaliação posterior, ainda que somada a outros indícios de prova, pode levar à inferência no juízo premissas falsas a partir das quais o caso será julgado.

A tese da nulidade sem prejuízo (*pas nullité sans grief,* prevista no artigo 563 do CPP), além de ser espelho do ultrapassado regime de nulidades previsto nos artigos 563 a 573 do CPP, é arbitrária e indica uma compreensão civilista das nulidades, incompatível com o devido processo legal[42]. "Num cenário em que a opção é pelo aproveitamento das irregularidades, cabe reconhecer que o que se preserva é a ânsia por condenações - esta sim, custodiada da investigação à decisão de mérito"[43]. À diferença do processo civil, vige no processo penal o princípio da presunção de inocência, fazendo com que não exista uma obrigatoriedade de distribuição do ônus da prova, mas sim uma carga probatória que é incumbência exclusiva do órgão acusador, o Ministério Público[44].

Para Nucci[45], a finalidade da prova é convencer o juiz a respeito da verdade sobre um fato controverso, não devendo o magistrado se contentar com o acervo probatório que lhe é apresentado pelas partes, mas sim buscar provas de forma ativa, materializando o princípio da verdade real. É a partir da busca ativa da verdade real que o magistrado, tendo segurança nas provas colhidas, condena ou absolve o réu.

Em sentido oposto, para Morais da Rosa, a "verdade real é empulhação ideológica que serve para 'acalmar' a consciência de acusadores e julgadores"[46], dando ao juiz o poder de gestão da prova em nome da ilusória crença na existência de uma verdade real dentro do processo. A prática culmina no que Lopes denomina de "epistemologia da incerteza"

---

42 ROSA, Alexandre Morais da. *Guia compacto do processo penal conforme a teoria dos jogos*. 1. ed. Rio de Janeiro: Lumen Juris, 2013.

43 MATIDA, Janaina. *op. cit*.

44 LOPES, Aury. Prova penal digital... *op.cit*.

45 NUCCI, Guilherme. *op. cit*.

46 DA ROSA, Alexandre. *op. cit*.

e relatividade das verdades reais no processo penal, categorias que potencializam a insegurança da defesa, que precisa convencer o juiz de sua inocência, ao receber um ônus probatório que deveria ser da acusação[47].

Não obstante, o processo penal que abandona por completo a busca da verdade pode ensejar condenações fundadas em provas sabidamente falsas ou, ao contrário, em provas potencialmente verdadeiras, mas obtidas por meios ilícitos. Como resultado, existem limites intransponíveis à descoberta da verdade, uma vez que "a pretensão de descobrir a verdade perde a relevância sempre que se chocar com regras de contensão do poder, que gozam de primazia por assegurarem a liberdade e o conjunto de direitos e garantias fundamentais"[48].

O ideal seria, então, o abandono de posições extremadas. Se uma justiça penal totalmente ancorada em uma ideia de verdade constitui uma utopia, uma justiça penal que a abandone por completo pode levar a um sistema arbitrário. Partindo da premissa de que a verdade importa para o processo penal e nele deve se fazer presente, é preciso que ela seja colocada em seu devido lugar. Uma busca da verdade, entre aspas, como aponta Badaró[49], que não ocupa lugar central no processo, mas é condição necessária para a justiça da decisão. Funcionando, assim, dentro de um limite epistêmico que busca a reconstrução de fatos históricos, desde que não ofenda princípios de valor superior.

Nessa esteira, o sistema penal brasileiro possui uma clara matriz autoritária, com normas que remontam ao auge da ditadura Vargas, quando o tecnicismo jurídico de Francisco Campos tentou camuflar as ideias autoritárias do período com normas supostamente neutras que fossem estáveis no tempo[50]. O modelo foi similar ao implementado pelos irmãos Alfredo e Arturo Rocco na Itália fascista, com a presença de legislações técnicas que, se por um lado não modificavam as balizas da dogmática

---

47 LOPES, Aury. Prova penal digital... *op. cit.*, p. 257.

48 PINHO, Ana Cláudia; MELCHIOR, Antonio Pedro; CASARA, Rubens. *Teoria do processo penal brasileiro*. v. 1. Rio de Janeiro: Da Vinci Livros, 2025, p. 198.

49 BADARÓ, Gustavo Henrique. *Epistemologia judiciária e prova penal*. São Paulo: Thomson Reuters Brasil, 2019.

50 MAIA, Daniele Lovatte. Em torno de Francisco Campos: ideias autoritárias, Estado nacional e democracia substancial. *Revista Direito e Práxis*, Rio de Janeiro, v. 16, n. 2, p. 1-24, 2025. DOI: https://doi.org/10.1590/2179-8966/2025/86131.

jurídica, por outro atuavam por meio de legislações de exceção que conviviam com o restante do ordenamento jurídico, elaborado para ser estável no tempo, dada sua pretensa neutralidade[51]. A ideia de processo penal como meio de busca da verdade real igualmente tem relação com o Código Rocco de 1930, cuja ação prática tem seus alicerces na liberdade da prova e no livre convencimento do juiz, positivando que somente seriam nulidades absolutas aquelas que não pudessem ser sanadas nos moldes estabelecidos pela lei[52].

No Brasil, a ideia de um processo penal autoritário vai muito além da semântica do termo autoritarismo, sendo traduzida em um conjunto de regras e práticas processuais que convivem com os direitos fundamentais inaugurados na ordem jurídica pela Constituição Federal de 1988. Quando o juiz assume o monopólio do processo em busca da verdade e da justiça, frequentemente flexibiliza regras em prol da efetividade e minimiza o peso das nulidades processuais. O "processo autoritário concebe a forma processual como um grande obstáculo a ser vencido"[53], objetivando o alcance de finalidades extraprocessuais, como defesa social ou controle da criminalidade. O uso da instrumentalidade das formas, própria do processo civil, acaba por criar um processo penal autoritário que se afasta da lógica democrática da proteção da presunção de inocência e da ideia de processo penal enquanto garantia do cidadão contra o arbítrio estatal[54].

---

[51] MAIA, Daniele Lovatte. Metodologia técnico-jurídica e o Direito Penal fascista italiano: contribuições de Alfredo Rocco e Arturo Rocco. *Revista Quaestio Iuris*, Rio de Janeiro, v. 18, n. 1, p. 302-328, 2025. DOI: https://doi.org/10.12957/rqi.2025.91405.

[52] GLOECKNER, Ricardo Jacobsen. *Autoritarismo e processo penal:* uma genealogia das ideias autoritárias no processo penal brasileiro. v. 1. ed. Florianópolis/SC: Tirant Lo Blanch, 2018.

[53] *Ibidem*, p. 164.

[54] A crítica recai diretamente sobre a Escola Processualista de São Paulo, representada por autores como Enrico Tullio Liebman, Cândido Rangel Dinamarco, Ada Pellegrini Grinover. Na visão de Gloeckner, ao propor uma unidade metodológica entre processo civil e processo penal, por meio da Teoria Geral do Processo, tais autores acabaram por introduzir uma lógica privada – de processo enquanto meio de satisfação de interesses, pacificação de lides e aplicação eficiente da vontade da lei – ao direito público, esvaziando a lógica do processo penal acusatório. Para Gloeckner, a manutenção da

A sistemática do artigo 563 do CPP, inalterado desde a inauguração do diploma no ordenamento jurídico durante a ditadura Vargas, é a do máximo aproveitamento dos atos processuais. O juiz, enquanto gestor do processo, tem ônus argumentativo maior para excluir um ato processual do que para mantê-lo nos autos, uma vez que nesse caso basta invocar que eventual irregularidade não causou prejuízo, ou que a parte que a alegou não se desincumbiu do ônus de provar tal prejuízo em tempo oportuno[55].

A jurisprudência do STJ passou a nomear de nulidade de algibeira ou nulidade de bolso a alegação de nulidades pela defesa de forma extemporânea, sob o argumento de que a defesa, ciente da irregularidade, deixa para suscitá-la somente em momento posterior, quando o andamento processual lhe pareça desfavorável. Na visão de Nucci[56], se a parte silencia diante de uma nulidade relativa, na espera de um momento estratégico para sua alegação, eventual vício é sanado pela preclusão consumativa, já que a ninguém é dado beneficiar-se da própria torpeza. A título de exemplo, o entendimento é aplicado pelo STJ para a convalidação de eventuais vícios inerentes a integridade da cadeia de custódia da prova digital, considerada pelo Tribunal como uma nulidade relativa: "configuração de nulidade de algibeira: a tese de quebra da cadeia de custódia não foi arguida no momento processual oportuno, emergindo apenas em revisão criminal após o trânsito em julgado, atraindo a preclusão temporal (CPP, art. 571, II)"[57].

Atualmente, é possível encontrar na jurisprudência do STJ a aplicação da nulidade de algibeira até mesmo para o aproveitamento de nulidades absolutas: "a jurisprudência evoluiu para considerar que no

---

instrumentalidade no processo penal só pode existir caso venha acompanhada da ideia de processo enquanto garantia do acusado, e desacompanhado de relações finalísticas, "sejam elas metafísicas (justiça, equidade) ou econômicas (reduzir custos, aumentar a eficiência na resolução dos conflitos sociais). Para mais informações: *Cf.* GLOECKNER, Ricardo. *Autoritarismo e processo penal: uma genealogia... op.cit.*, p. 165.

55 GLOECKNER, Ricardo Jacobsen. *Autoritarismo e processo penal II:* autoritarismo cool e economia política do processo penal brasileiro. 1. ed. E-book São Paulo: Tirant Lo Blanch, 2023.

56 NUCCI, Guilherme. *op.cit*.

57 AgRg no HC 1.046.572/AP, 5ª Turma, julgado em 23/06/2026; AgRg no HC 1.046.896/AP, 5ª Turma, julgado em 23/06/2026.

processo penal, mesmo as nulidades absolutas exigem prejuízo e estão sujeitas à preclusão"[58]. Como apontado, o estabelecimento de uma preclusão temporal para a alegação de nulidade busca evitar uma espécie de abuso de direito pela defesa. Instituto original do direito civil, o abuso de direito foi transportado para o processo civil e dele para o processo penal[59], estando ligado ao conceito de boa-fé objetiva[60]. Trata-se de entendimento jurisprudencial sem qualquer consonância com o previsto em lei, fundamentado em uma teoria que confere maior valor à forma do que ao conteúdo do ato. Para Gloeckner, "abdicar de formas processuais penais solenes é um ato de servilismo à cultura autoritária"[61], sendo o sistema processual amorfo característica do processualismo inerente ao sistema autoritário-inquisitorial.

Em que pese a principiologia aplicada hoje ao processo penal ser a do livre convencimento motivado do juiz, a matriz autoritária do artigo 563 do CPP acima apontado é evidente, permitindo a presença no processo criminal de uma prova que apesar de nula, pode ser considerada para formação da culpa, pelo fato de a defesa não ter logrado identificar claramente o prejuízo da nulidade[62]. Como se a mera possibilidade de uma condenação criminal já não pudesse ser valorada como prova evidente de prejuízo ao acusado. Em suma, quando o juiz deixa de ser o principal

---

[58] AgRg no HC n. 593.029/MT, Rel. Ministro Rogerio Schietti, 6ª T., DJe 21/6/2022.

[59] GLOECKNER, Ricardo. *Autoritarismo e processo penal II:* autoritarismo cool... *op.cit*.

[60] Nesse sentido é o trecho da ementa do HC/STJ 171.753: "4. O princípio da boa-fé objetiva ecoa por todo o ordenamento jurídico, não se esgotando no campo do Direito Privado, no qual, originariamente, deita raízes. Dentre os seus subprincípios, destaca-se o *duty to mitigate the loss*. Na espécie, a serôdia insurgência, somente após a realização de diversos atos processuais, como o interrogatório, alegações finais e sentença, evidencia a consolidação da situação, sedimentando a tácita aceitação da ausência de oitiva da testemunha. Não deveria a parte insistir em marcha processual que crê írrita, sob pena de investir tempo e recursos de modo infrutífero". (STJ - HC: 171753 GO 2010/0082684-4, Relator.: Ministra MARIA THEREZA DE ASSIS MOURA, Data de Julgamento: 04/04/2013, T6 - SEXTA TURMA, Data de Publicação: DJe 16/04/2013).

[61] GLOECKNER, Ricardo. *Autoritarismo e processo penal II:* autoritarismo cool... *op.cit*., p. 420.

[62] GLOECKNER, Ricardo. *Autoritarismo e processo penal:* uma genealogia *op. cit*.

protetor da presunção de inocência para ser o principal ator processual de busca da verdade real, temos a materialização de um modelo autoritário para solucionar a equação segurança vs. liberdade[63].

2. A JURISPRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA SOBRE PROVAS DIGITAIS, CADEIA DE CUSTÓDIA E CÓDIGO *HASH*

O presente item está dividido em duas partes: na primeira serão discriminados os passos do percurso metodológico escolhido para análise das decisões colegiadas do STJ; na segunda será feito um mapeamento tanto descritivo quanto crítico dos precedentes. O objetivo principal é verificar se existe, na fundamentação das decisões do STJ, alguma similaridade com os conceitos relativos ao processo penal autoritário vistos no item anterior, com uma maior propensão a preservar a prova digital nos autos do processo do que a uma análise rigorosa da integridade da sua cadeia de custódia. Logo, o objeto de análise para considerar eventual déficit de justificação do precedente não foi o seu resultado – provimento ou desprovimento do recurso – mas sim a fundamentação que levou os Ministros a decidir de uma ou de outra forma.

2.1. Percurso Metodológico

A análise de documentos judiciais, notadamente decisões proferidas por órgãos colegiados, como é o caso presente, demandam precisão e rigor técnico-científico, de modo a conferir auditabilidade e replicabilidade ao estudo. Parte-se, nesta pesquisa, da premissa de que este tipo de análise não é feito por uma metodologia propriamente dita, mas por uma mistura de métodos qualitativos e quantitativos que funcionam como um guarda-chuva para o pesquisador, a depender do objetivo do estudo e do número de casos a serem analisados[64]. Nesse sentido, duas foram as

[63] PRADO, Geraldo. *op. cit.*

[64] VERBRUGGEN, Paul; WIJNTJENS, Lianne. Methodological accountability in systematic case law analysis: Empirical insights from the Netherlands.

lentes metodológicas escolhidas para a análise sistemática documental dos julgados do STJ.

A primeira delas foi a análise de conteúdo de decisões judiciais de Hall e Wright[65], indicada não como a melhor forma de leitura de precedentes judiciais, mas como um modelo de rigor técnico para o entendimento dos casos e melhor distinção empírica entre eles. Enquanto ferramentas convencionais se propõem à análise de um caso paradigma, ou um pequeno grupo de decisões consideradas excepcionais, a análise de conteúdo busca analisar julgados de mesmo peso em vista de padrões decisórios. Por essa razão, requer que o pesquisador explique a seleção de casos de forma detalhada e objetiva, permitindo a replicabilidade das etapas da pesquisa:

> A análise de conteúdo exige que o pesquisador explique a seleção de casos de forma objetiva, permitindo que outros estudos repliquem os caminhos metodológicos da pesquisa. A força de convencimento deste método depende da possibilidade de reprodução dos resultados pela comunidade acadêmica, e não do poder retórico do pesquisador ao proclamá-los[66].

Nesse sentido, para Hall e Wright[67], a pesquisa que se propõe a uma análise de conteúdo de decisões judiciais deve passar necessariamente por três etapas: i) seleção de casos; ii) codificação dos casos e; iii) análise dos casos codificados.

A seleção de casos desta pesquisa foi feita por meio da inserção do termo *hash* no menu de busca de jurisprudência disponível no site oficial do Superior Tribunal de Justiça, que contivessem o termo expressamente mencionado na ementa do julgado, com um recorte temporal de

---

European Journal of Empirical Legal Studies. v. 2, n. 1, art. 6, 2025. DOI: https://doi.org/10.62355/ejels.25885.

[65] *Ibidem*.

[66] *Ibidem*, p. 66. Tradução livre. No original: *Content analysis requires the researcher to explain the selection of cases and themes in enough objective detail to allow others to replicate the steps. This method's persuasiveness depends on the community's ability to reproduce the findings rather than the author's rhetorical power to proclaim them*.

[67] *Ibidem*.

03/07/2016 a 03/07/2026, de modo a realizar um estudo comparativo e dar continuidade à pesquisa já iniciada por Fisberg[68]. Dentro deste marco temporal, foram consideradas apenas decisões colegiadas de órgãos com competência criminal, de acordo com a divisão interna do STJ[69]. Como resultado, a pesquisa empírico-documental foi realizada em um total de 65 julgados, divididos entre precedentes da 5ª Turma, da 6ª Turma e da Corte Especial do STJ[70].

Na etapa de codificação dos casos, foram escolhidos os seguintes códigos: identificação do processo, órgão julgador (5ª Turma, 6ª Turma ou Corte Especial), data de publicação, origem da prova (celular, computador, nuvem, câmeras de rua), meio de extração da prova (manual ou software

---

68 FISBERG, Yuri. *op. cit*.

69 O procedimento gerou um total de 69 (sessenta e nove) decisões colegiadas, das quais foram removidas da análise: 3 (três) decisões provenientes da Terceira Turma e relativas ao direito civil, 1 (uma) decisão que estava em duplicidade, sendo ela: EDcl no AgRg no AgRg no AREsp 2682573/RO. Assim, a análise total foi feita em 65 (sessenta e cinco) julgados, colacionados em uma planilha de Excel, que contém a classificação dos precedentes nas seguintes colunas: A: número do processo; B: órgão julgador; C: data da publicação; D: origem da prova; E: meio de extração da prova; F: defesa reconhece a existência de *hash*; G: juízo reconhece a existência de *hash*; H: padrão técnico; I: dados brutos disponibilizados à defesa; J: termo descritivo; K: termo valorativo; L: déficit de justificação; M: fundamentação principal. Especificamente na coluna "M", foram inseridos trechos importantes do acórdão, que auxiliaram na classificação do precedente como "com déficit de justificação" ou "sem déficit de justificação". A planilha de Excel pode ser consultada em: MAIA, Daniele Lovatte. Conjunto de dados de: "Cadeia de custódia, Prova Digital e código hash: uma análise da jurisprudência do STJ à luz do processo penal acusatório". *Scielo Data,* v1, 2026. https://doi.org/10.48331/SCIELODATA.FSCX1S

70 Não se desconhece as limitações dessa escolha metodológica, que exclui da análise precedentes que, embora tratem de provas digitais, não mencionam em sua ementa o termo *hash*, a exemplo do HC 160.662/RJ, da 6ª Turma, julgado em 18/02/2014, que anulou as provas de interceptação telemática e telefônica da "Operação negócio da China", devido ao desaparecimento do seu material bruto e, consequentemente, impossibilidade de sua disponibilização à defesa. No entanto, em respeito ao rigor científico, optou-se por seguir a pesquisa apenas com os julgados coletivos que contivessem o termo *hash* em sua ementa, dentro do marco temporal assinalado, possibilitando sua replicabilidade em futuros estudos.

de apoio), defesa reconhece a existência de *hash*, juízo reconhece existência de *hash*, padrão técnico, dados brutos foram disponibilizados à defesa[71].

A terceira etapa do processo, qual seja, a análise crítica dos julgados codificados, foi feita apenas após o uso da Metodologia de Análise de Decisões Judiciais (MAD), ferramenta metodológica criada por Freitas Filho e Lima[72].

O objetivo da MAD é auxiliar o pesquisador a proceder, de forma controlada, na leitura de precedentes judiciais, por meio do qual é possível chegar a resultados apreciáveis, replicáveis e comparáveis. Para tanto, em um primeiro momento, é preciso: i) ter uma pesquisa exploratória (uso de provas digitais em investigações criminais); ii) recorte temático objetivo (como a questão do código *hash* vem sendo utilizada na seara da cadeia de custódia das provas digitais); iii) recorte institucional (decisões colegiadas proferidas pelo STJ, órgão responsável pela fiscalização do cumprimento das normas infraconstitucionais, de acordo com o artigo 105 da Constituição Federal).

Em um segundo momento do MAD, o pesquisador deve verificar como as decisões estão utilizando "conceitos, valores, institutos e princípios presentes nas narrativas decisórias"[73], para que, em um terceiro momento seja possível fazer uma distinção lógico-formal entre palavras de valor e palavras descritivas. Identificar em qual das duas categorias de palavra o julgado baseou sua decisão possibilita ao pesquisador afirmar se o caso concreto padeceu do que os autores chamam de "déficit de justificação".

---

71 O código "padrão técnico" se destinou a buscar, no acórdão, menção a alguma norma técnica, tais como: ABNT NBR ISO/IEC 27037:2013, ABNT NBR ISO/IEC 27042:2015, Portaria SENASP 82/2014; Resolução 408/2021 do Conselho Nacional de Justiça, Decreto 11.491/2023 – Convenção de Budapeste; Procedimentos Operacionais Padrão (POPs) de Perícia Criminal do Ministério da Justiça de 2024; ou a Instrução Normativa DG/PF nº 299/2025. Paralelamente, o código "dados brutos disponibilizados à defesa" foi considerado positivo sempre que o acórdão mencionava ou a disponibilização do aparelho digital à defesa (para retirada e perícia autônoma), ou a disponibilização em cartório do original dos dados brutos em mídia digital para que a defesa pudesse fazer uma cópia.

72 FREITAS FILHO, Roberto. *op. cit*.

73 FREITAS FILHO, Roberto. *op. cit*., p. 11.

Palavras descritivas são "aquelas que não têm sentido prescritivo, não têm significado relativo à qualidade de um objeto ou situação. Dizer que algo é um automóvel é usar a palavra 'automóvel' no sentido descritivo"[74]. Já por palavras de valor, tendo elas função qualificadora de um objeto, não possuem estabilidade semântica, necessitando que a decisão seja clara na motivação das circunstâncias descritivas presentes no caso:

> Assim, por exemplo, se um decisor diz que determinada prestação jurisdicional é devida por causa da dignidade da pessoa humana, a expressão "dignidade" tem de ser densificada de forma tal que, no caso concreto, seja possível identificar quais as circunstâncias presentes que determinam que tal situação gera "indignidade". Por causa da função lógica da palavra, que tem como significado descrever um estado desejável ("digno" significa algo valoroso), se o julgador não descreve, *ad nauseam*, as características descritivas, ou seja, quais as circunstâncias fáticas que determinam que a situação é "digna", o discurso acaba desbordando para a possibilidade de arbítrio, dada a falta de justificação plena. Há, portanto, o chamado "déficit de justificação". Esse é um pressuposto básico da MAD, sendo essa a sua especificidade[75].

No caso da presente pesquisa, foram considerados três termos descritivos na leitura dos precedentes: 1. a presença ou ausência de numeração *hash* nas provas digitais; 2. a forma como a prova digital foi extraída (de forma manual, por meio de softwares específicos e/ou com a utilização de procedimentos fundamentados em normas técnicas)[76] e; 3. a impossibilidade de análise do caso concreto, dada a ausência de manifestação madura sobre o tema nas instâncias ordinárias (risco de supressão de instância), seja pela impossibilidade de revolvimento fático-probatório no rito do habeas corpus ou no rito do recurso especial..

---

[74] *Ibidem*, p. 11.

[75] *Ibidem*, p. 11.

[76] Pela limitação metodológica da pesquisa, que se baseou tão somente na leitura do acórdão, a mera menção a um "protocolo" ou "protocolo interno do órgão" para extração das provas foi suficiente para que o termo descritivo 2 fosse considerado presente, ainda que o teor do dito protocolo não fosse mencionado na decisão.

Igualmente, três foram os termos valorativos escolhidos para a análise: 1. a boa-fé inerente à função pública (ou seja, a presunção de legitimidade da palavra do agente público que extraiu os dados digitais); 2. alegações genéricas da defesa a respeito da violação da cadeia de custódia (ou seja, invocação pelo STJ do artigo 563 do CPP e a necessidade de somente se declarar a nulidade de uma prova quando houver a demonstração de prejuízo concreto) e; 3. a existência de outras provas nos autos que sozinhas já teriam o potencial de sustentar a condenação.

Para conferir maior suporte técnico-metodológico à busca de eventual déficit de julgamento de um precedente, foi retomada a terceira etapa da análise de conteúdo de decisões judiciais de Hall e Wright[77], com o auxílio do software Excel.

Após a leitura individual dos precedentes para o preenchimento manual das colunas "A" a "K" da planilha, cada julgado foi novamente visitado para que se pudesse preencher as colunas "L: déficit de justificação" e "M: fundamentação principal". O primeiro indício para considerar como positivo ou negativo o déficit de justificação foi observar se os dados brutos das provas digitais haviam sido disponibilizados à defesa (coluna "I"). Sendo positiva a coluna "I", passou-se a uma avaliação de como foi feita a extração da prova digital. Se a extração dos dados foi feita utilizando algum protocolo de documentação dos atos (termo descritivo 2) o indício positivo era confirmado e o precedente classificado como "sem déficit de justificação". Por outro lado, se não houve qualquer tipo de documentação da cadeia de custódia, tendo a validade da prova digital sido fundamentada em qualquer dos três termos valorativos da coluna "K", o precedente era classificado como "com déficit de justificação". A contrario sensu, ainda que o precedente mencionasse a disponibilização da integralidade das provas digitais à defesa, se a autoridade competente não seguiu nenhum tipo de protocolo para a extração dos dados o precedente era declarado com déficit de justificação – estando ou não presentes qualquer dos termos valorativos.

Paralelamente, sendo negativa a coluna "I", ou sendo ela assinalada com a expressão "não menciona", pelo fato de os dados brutos ou não terem sido disponibilizados à defesa ou não ser possível aferir essa

[77] HALL, Mark. *op. cit*.

informação, passava-se à leitura dos termos descritivos da coluna "J". Somente nos casos em que estivessem presentes os termos descritivos 2 e 3 o indício inicial de precedente "sem déficit de justificação" era refutado e o precedente classificado como adequadamente justificado – ou seja, nos casos em que foi adotado algum tipo de protocolo para a extração da prova digital (termo descritivo 2) e os dados brutos ainda não tinham sido disponibilizados à defesa dada a fase em que o processo se encontrava (termo descritivo 3). Na ausência dos termos descritivos 1 e 2 e presença do termo descritivo 1 (número de *hash*), havia apenas um novo indício de decisão justificada, não sendo possível a confirmação.

2.2. Mapeamento descritivo e crítico das decisões

De início, o primeiro dado que chama atenção em relação à pesquisa anterior feita por Fisberg[78] é o elevado número de decisões proferidas pelo STJ no intervalo de 04/07/2025 a 03/07/2026 com a menção ao código *hash* na ementa da decisão. Dentro do marco temporal do estudo anterior[79], feito entre 2016, ano em que pela primeira vez o termo apareceu na jurisprudência do Tribunal e 03/07/2025, foram proferidas 11 (onze) decisões criminais cujas ementas continham a palavra *hash*; frente a 54 (cinquenta e quatro) decisões proferidas no ano seguinte. Trata-se de um aumento exponencial, tendo o STJ julgado cinco vezes mais casos em apenas um ano, quando comparado com um período anterior de dez anos, evidenciando um crescimento considerável do uso de provas digitais pelo judiciário brasileiro.

Do total de casos analisados, apenas duas decisões do segundo período (3,7%) consideraram ter havido violação à cadeia de custódia da prova digital[80], frente a quatro decisões (36,3%) do período anterior[81], uma

---

78 FISBERG, Yuri. *op. cit.*.

79 *Ibidem*.

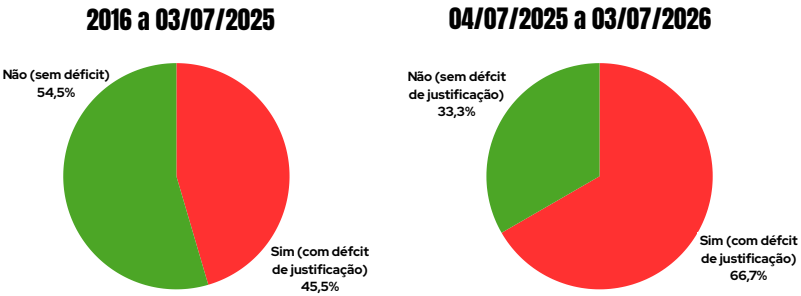
80 São elas: AgRg no RHC 198.632/SC, 5ª Turma, julgado em 09/03/2026 e AgRg no RHC 235.625/SP, 5ª Turma, julgado em 01/06/2026.

81 São elas: AgRg no RHC 143.169/RJ, 5ª Turma, julgado em 02/03/2023, AgRg no HC 8.280.54/RN, 5ª Turma, julgado em 29/04/2024, AgRg no RHC 186138/SP, 5ª Turma, julgado em 26/12/2024 e EDcl no AgRg no RHC 1.861.38/SP, 5ª Turma, julgado em 08/04/2025.

diminuição proporcional de quase de 89,1%. O percentual de aumento proporcional das decisões que não reconheceram a violação da cadeia de custódia e, consequentemente, da nulidade da prova digital, pouco significa em termos de segurança jurídica processual. Isso porque os novos precedentes podem ter se apresentado com autos mais bem instruídos e, portanto, com a integridade da cadeia de custódia preservada. Ou, por outro lado, os Ministros podem ter visualizado uma cadeia de custódia fragilizada e, ainda assim, optado por não decretar a nulidade das provas digitais.

Nesse sentido, a tabela abaixo mostra o comparativo dos precedentes em porcentagem, sendo que o aumento de decisões com déficit de justificação apenas pode ser colocado, na presente investigação, como um indício qualitativo de tendência[82].

Figura 1. comparativo em porcentagem das decisões do STJ sobre provas digitais com e sem déficit de justificação

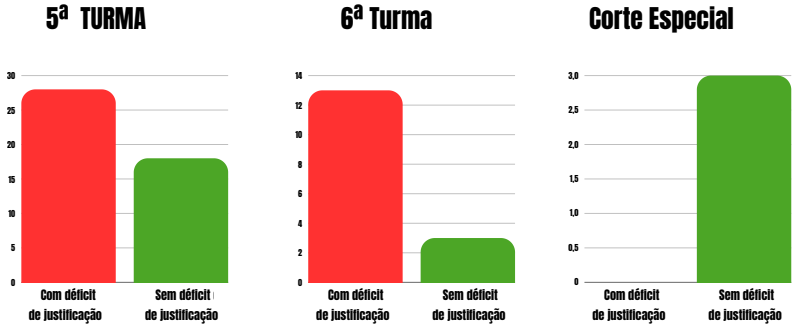


Fonte: elaboração própria

[82] Em números absolutos, entre 03/07/2016 e 03/07/2026 foram encontradas 5 (cinco) decisões com déficit de justificação frente a 6 (seis) decisões sem déficit de justificação; ao passo que entre 04/07/2025 e 03/07/2026 foram encontradas, 36 (trinta e seis) decisões com déficit e 18 (dezoito) decisões sem déficit. Embora tenham sido encontradas mais decisões com déficit de justificação no segundo período analisado, a discrepância no número de julgados em cada um dos períodos impossibilita a inferência estatística desse aumento. Consequentemente, os dados apontados não servem como prova estatística definitiva, mas como indício qualitativo de tendência.

Em contrapartida, a figura abaixo mostra os mesmos dados de déficit de justificação, mas considerando a forma como votou a 5ª Turma, a 6ª Turma, e a Corte Especial do STJ:

Figura 2. comparativo das decisões da 5ª Turma, 6ª Turma e Corte Especial do STJ sobre provas digitais com e sem déficit de justificação



Fonte: elaboração própria

Em nenhum dos precedentes a defesa reconheceu a presença de código *hash* nas provas digitais, ao passo que, para o STJ: i) 33 casos (51%) expressamente não reconheceram a existência de código *hash*; ii) 13 casos (20%) nada mencionaram e; iii) 18 casos (29%) expressamente reconheceram a presença do *hash* nas provas digitais. Para além da observação matemática, é interessante observar o mérito dos julgados: para o STJ, a presença de código *hash* funciona como prova automática de legalidade da prova digital. Em todos os casos em que o Tribunal considerou presente o *hash*, essa foi a fundamentação preponderante para que a prova fosse mantida nos autos, ainda que eventualmente um dos três termos valorativos fosse acrescentado.

No AREsp 2.972.295/MT, 5ª turma, julgado em 23/09/2025 o STJ entendeu que o fato de a prova digital ter sido lida por meio do software *Cellebrite*, com geração de relatório e número de *hash*, era suficiente para atestar a autenticidade da prova digital. Como já apontado, o código *hash* é uma ferramenta relevante, mas limitada, pois apenas atesta que um documento digital corresponde a exata integralidade de outro, nada informado sobre a veracidade do documento em questão. Logo, a geração

de *hash* por software especializado não confere mesmidade entre a prova digital periciada e a prova digital colhida.

Por outro lado, na ausência de *hash*, os precedentes se dividem: nos seis casos já informados em que as provas digitais foram consideradas nulas, não havia a presença de *hash* e esse dado foi considerado – não de forma isolada – mas em conjunto com os demais elementos dos autos para fundamentar a declaração de nulidade. Por outro lado, na integralidade dos demais precedentes, a ausência de código *hash* foi considerada como um dado secundário, que não tinha o condão de nulificar a prova digital. Nesse sentido:

> 6. A ausência de procedimentos técnicos padronizados de informática, como geração de código *hash*, clonagem forense ou protocolo de integridade, bem como a existência de alterações em nomes de arquivos, não evidenciam, por si sós, adulteração ou manipulação do conteúdo das provas digitais, nem configuram quebra da cadeia de custódia apta a acarretar nulidade, especialmente porque os agentes públicos esclareceram em juízo, sob contraditório, a dinâmica de coleta e análise dos dados. (AgRg no HC 1.080.226/PI, 6ª Turma, 14/04/2026).

No que tange à menção expressa de que à defesa foram disponibilizados os dados brutos das provas digitais, dos 65 (sessenta e cinco) julgados analisados, 42 (quarenta e dois) nada mencionaram, 10 (dez) expressamente afirmaram que a defesa não teve acesso aos dados brutos, e 13 (treze) chancelaram o acesso dos dados brutos pela defesa. Desses últimos, apenas 1 (um) foi considerado com déficit de justificação[83], uma vez que nele estava ausente o termo descritivo 2 (protocolo adotado para a extração das provas digitais). No que concerne aos casos de falta de acesso aos dados brutos, 2 (dois) precedentes estavam sem déficit de justificação[84], tendo esse sido um dos motivos da decretação de nulidade das provas digitais.

---

[83] HC 1.075.827/SP, 5ª Turma, julgado em 18/05/2026.

[84] AgRg no RHC 235.625/SP, 5ª Turma, julgado em 01/06/2026 e AgRg no HC 8.280.54/RN, 5ª Turma, julgado em 29/04/2024.

Sobre os julgados que reconheceram que a falta de acesso à defesa aos dados brutos é mera irregularidade sem aptidão para nulificar o uso das provas digitais como subsídio da condenação, os seguintes trechos merecem destaque:

> 3. O Tribunal de origem, ao afastar a alegação de quebra da cadeia de custódia, consignou que não basta a afirmação genérica da defesa para descredibilizar a prova, ressaltando que a extração das conversas de WhatsApp pelo inspetor de polícia e a forma de elaboração do relatório, ilustrado com fotografias das mensagens, conferem confiabilidade suficiente à prova, que todos os documentos que embasaram a condenação foram juntados aos autos, com viabilização do contraditório, e que em momento algum a defesa apontou adulterações concretas no conteúdo. (...) 5. A defesa não apresentou demonstração concreta de manipulação ou adulteração do material obtido com a extração de dados do telefone celular, limitando-se a alegações genéricas, o que não é suficiente para desconstituir a confiabilidade da prova digital produzida. (AgRg no HC 1.026.773/RS, da 5ª Turma, julgado em 23/04/2026).
>
> A mera inobservância de procedimentos técnicos de informática na extração de dados de aparelho celular, sem prova objetiva de adulteração, manipulação do conteúdo ou prejuízo ao contraditório, não configura quebra da cadeia de custódia apta a tornar ilícita a prova digital. A nulidade processual por alegada restrição de acesso à prova digital exige demonstração de efetiva negativa de acesso e de prejuízo concreto à defesa, não bastando a ausência de entrega de cópia forense integral quando o material relevante utilizado na condenação foi franqueado às partes. (AgRg no HC 1.080.226/PI, 6ª Turma, 14/04/2026).
>
> Não verifico irregularidade na guarda do material probatório dos autos, pois a prova digital teve origem conhecida, com menção às fontes de sua obtenção, para consulta e confirmação, com os respectivos códigos eletrônicos, de modo que não é possível afirmar que houve quebra da cadeia de custódia. Ademais, não se pode pressupor, sem prova, eventual má-fé dos agentes públicos no manuseio dos elementos probatórios por eles recebidos. (AgRg nos EDcl no AREsp 3.144.270/SP, 6ª Turma, 19/05/2026).

Sobre as provas digitais em si mesmas consideradas, os precedentes apresentaram as seguintes fontes: prints de tela de celular, aparelho de celular, notebook, iPad, vídeos (de câmeras de rua, de câmeras de comércio ou presentes nos aparelhos apreendidos), dados decorrentes de interceptação telefônica e arquivos em nuvem. No que tange à forma de extração dos dados digitais desses aparelhos, apenas um precedente mencionou o software *Avilla Forensics 3.0*, tendo nove mencionado o software *Cellebrite*. Nenhum outro software foi citado nos julgados.

Dentre as decisões com déficit de justificação, observou-se um uso mecânico da premissa de *pas nullité sans grief,* prevista no artigo 563 do CPP, alegando a impossibilidade de declaração de nulidade da prova digital quando a defesa não demonstrou o prejuízo daí advindo. Como exemplo: i) "A alegação de quebra da cadeia de custódia, desacompanhada de demonstração efetiva de prejuízo ou adulteração da prova, não é suficiente para gerar sua nulidade, conforme entendimento consolidado do STJ" (AgRg nos EDcl no RHC 222.911/ES, 5ª Turma, julgado em 30/03/2026 e AgRg nos EDcl no RHC 230.737/GO, 5ª Turma, julgado em 18/05/2026); ii) "Não há nos autos qualquer indicativo concreto de adulteração ou manipulação das provas, tampouco a defesa logrou demonstrar prejuízo efetivo decorrente da alegação suscitada, incidindo, na espécie, o princípio do *pas de nullité sans grief*" (AgRg no HC 1.062.682/RS, 5ª Turma, julgado em 11/05/2026)[85].

[85] Interessante notar que esse último precedente, em que pese ter se utilizado de argumentação incompatível com o sistema acusatório, foi considerado sem déficit de justificação, uma vez que assentou: "O Tribunal de origem consignou que a extração de dados dos aparelhos celulares foi regularmente autorizada por decisão judicial, posteriormente executada com o emprego de software especializado (Cellebrite), com utilização de algoritmos de verificação (*hash*) aptos a assegurar a integridade dos arquivos e conferir elevado grau de confiabilidade à prova digital produzida". Como não havia no acórdão informação sobre a presença ou ausência de disponibilização dos dados brutos das provas digitais à defesa, e dada a impossibilidade de consultas aos autos originais nesse momento, entendeu-se que os indícios evidenciam ausência de déficit de justificação. Ao contrário, no precedente AgRg no HC 1.004.935/DF, da 6ª Turma, julgado em 08/09/2025, mesmo tendo o Tribunal expressamente mencionado a existência de números *hash* extraídos pelo programa *cellebrite*, o precedente foi considerado com déficit de justificação, já que não analisou os argumentos da defesa: "ocorrência de nulidade absoluta decorrente da quebra da cadeia de custódia dos aparelhos celulares

Como apontado, colocar na defesa o ônus de indicar qual foi o prejuízo advindo de uma prova digital que não se pode afirmar verdadeira, dada a ausência de indícios mínimos de confiabilidade, autenticidade, e mesmidade para com o original, é fazer uso de um processo penal autoritário, pautado em premissas inquisitórias, com uso da sistemática de instrumentalidade das formas e princípio da eficiência, próprios do processo civil.

O mesmo pode ser dito para argumentos sobre a ausência de indícios de manipulação dos dados digitais, com a utilização acrítica de conceito derivado do direito administrativo, que confere premissa de legitimidade aos atos praticados por servidores públicos. Como exemplo: "os atos realizados por agentes públicos gozam de presunção de legitimidade. Portanto, alegações genéricas de que o formato (MP4) é 'facilmente manipulável' não bastam; cabe à defesa apontar objetivamente qual diálogo teria sido forjado" (AgRg no HC 1.069.875/ES, 6ª Turma, julgado em 09/04/2026).

O curioso é saber como o acusado poderia, em tese, provar a alteração de diálogo sem que a ele fosse disponibilizado os dados brutos referentes a extração desse diálogo ou, ao menos, a exibição de um protocolo rígido da forma como as provas foram extraídas do dispositivo digital, com a documentação sistemática da cadeia de custódia desse material. Na ausência dessas informações, demonstrar que o material apresentado em juízo está em desacordo com o original é tarefa impossível de ser feita pela defesa, ou por qualquer parte processual. Sendo inviável atestar a veracidade da prova que fundamenta a condenação do acusado, não há que se falar em condenação, dada a proteção constitucional que preconiza que, na dúvida, deve o acusado ser absolvido.

Outro precedente digno de nota é o AgRg nos EDcl no RHC 230.737/GO, da 5ª Turma, julgado em 18/05/2026. Nele, a condenação foi baseada, como aponta trecho da ementa, em "capturas de tela de mensagens, registros fotográficos e relatórios fornecidos por plataformas

---

apreendidos, em virtude do manuseio anterior à perícia oficial, sem lacre ou registro formal, além de gravações amadoras por terceiros não identificados", retirando, assim, os indícios mínimos presentes no caso anterior, de que os dados brutos teriam sido disponibilizados à defesa.

digitais, apresentados espontaneamente pela vítima no curso da investigação". Além do precedente não ter deixado claro o tipo de plataforma digital a que se fazia referência ou qual era o teor do relatório produzido, informou que o aparelho eletrônico nunca chegou a ser periciado, já que a vítima não mais se encontrava na posse do dispositivo quando da tentativa de realização da perícia. Ainda assim, entendeu o STJ que "a mera ausência da cadeia de custódia formal e de perícia no aparelho não autoriza, isoladamente, o desentranhamento na via estreita do *habeas corpus*".

A decisão ilustra bem a lógica do processo penal autoritário, ao minimizar o peso das nulidades processuais, flexibilizando as regras de documentação da cadeia de custódia em prol da eficiência processual. Abaixo trechos do inteiro teor do acórdão, que no original estão destacados em negrito:

> A decisão agravada concluiu que tais circunstâncias, por si sós, não autorizam o desentranhamento imediato do material probatório, notadamente porque os registros foram apresentados pela própria vítima inexistindo notícia de apreensão estatal do dispositivo, com posterior perda ou corrupção de dados sob custódia do Estado, devendo eventual discussão acerca de sua confiabilidade ser submetida ao contraditório no curso da instrução criminal.
>
> (...)
>
> Os elementos digitais questionados não decorrem de apreensão estatal com posterior quebra da cadeia de custódia, mas foram apresentados por particular, inexistindo, ao menos neste momento, notícia de que tenham sido submetidos a procedimento técnico de extração ou preservação. Não se trata, portanto, de ruptura de uma cadeia de custódia previamente estabelecida, mas de ausência de sua formação em sentido técnico desde a origem.
>
> (AgRg nos EDcl no RHC 230.737/GO e EDcl no AgRg nos EDcl no RHC 230.737/GO, 5ª Turma. DJe 18/05/2026).[86]

[86] Trata-se de posicionamento diametralmente oposto adotado pelo mesmo STJ no famoso precedente da "Operação negócio da China" (HC 160.662/RJ, da 6ª Turma, julgado em 18/02/2014), no qual a Corte entendeu que uma vez que parte do material decorrente da interceptação telefônica havia sido extraviada, o material remanescente nos autos não garantia a integridade e segurança do restante da prova colhida. O precedente não foi analisado neste

Já nos precedentes (AgRg no HC 1.046.572/AP, 5ª Turma, julgado em 26/06/2026; AgRg no HC 1.051.474/SP, 5ª Turma, julgado em 12/03/2026; e AgRg no RHC 215.572/SC, 6ª Turma, julgado em 08/09/2025), o STJ entendeu que a alegação de nulidade das provas digitais foi feita pela defesa de forma extemporânea (nulidade de algibeira), tendo havido sobre elas a preclusão consumativa, impossibilitando a apreciação da Corte. Tais precedentes tinham déficit de justificação – não pela preclusão consumativa do alegado pela defesa, pois esse dado não era objeto de análise – mas pela ausência de dados brutos disponibilizados à defesa, somada à ausência do termo descritivo 2 (protocolos de extração da prova).

Outro ponto que merece destaque no mapeamento das decisões é o fato de 76,3% dos casos analisados se referirem a demandas que chegaram ao STJ pela via do habeas corpus. Dentro desse montante, verificou-se que 20% dos casos foram inadmitidos, dentre outros argumentos, pelo fato de o habeas corpus ser um remédio processual que não comporta análise probatória e, outros 12%, sob o argumento de que a análise do tema em sede de habeas corpus configuraria supressão de instância.

Dada a conhecida morosidade do judiciário brasileiro, impedir que um caso de nulidade evidente chegue ao STJ por meio de habeas corpus, obrigando o acusado a aguardar o momento processual pertinente para ingresso com um recurso especial é desconsiderar o enorme ônus pessoal, social e financeiro de ser processado criminalmente.

Assim como no caso do habeas corpus, o STJ considerou o recurso especial como meio inadequado para se discutir a temática da cadeia de custódia das provas digitais, situação que ocorreu com 11 (onze) dos 12 (doze) precedentes analisados em sede de recurso especial. Desse montante, o único que efetivamente analisou o mérito recursal foi o AREsp 2.972.295/MT, 5ª turma, julgado em 23/09/2025. Todos os demais não se pronunciaram sobre a temática, por envolver análise de matéria fática, insuscetível de ser examinada por meio de recurso especial.

Contudo, quando consideramos a corrente doutrinária que advoga pela necessidade de exclusão dos autos da prova digital com cadeia de

estudo por não ter em sua ementa a palavra "*hash*" e, consequentemente, não ter passado pelo filtro inicial de coleta das decisões no site do STJ.

custódia violada[87], à qual esta pesquisa se filia, não se verifica qualquer óbice processual para análise do tema, seja em sede de habeas corpus, seja em recurso especial, pois toda a argumentação está baseada em prova documental pré-constituída, ou na ausência dela. Com isso, considera-se que somente haveria supressão de instâncias nos casos em que a matéria chegasse ao STJ sem qualquer oportunidade de manifestação das instâncias ordinárias, o que não se verificou nos casos estudados.

Ainda, considerar a verificação da integridade da cadeia de custódia como matéria estritamente documental possibilita a análise crítica dos precedentes em que a prova digital foi questionada ainda em sede de inquérito policial. 2 (dois) dos 3 (três) casos em que a matéria foi levada ao STJ antes mesmo da instauração da ação penal foram considerados sem déficit de justificação, já que neles havia informação expressa de que as diligências investigativas ainda estavam em andamento, impossibilitando que o material bruto das provas digitais fosse disponibilizado à defesa (em aplicação do termo descritivo 3). Caso o material já estivesse documentado nos autos do inquérito, a defesa teria direito ao acesso aos dados brutos, nos termos da Súmula Vinculante 14, antes mesmo da eventual propositura de ação penal.

Sobre o uso de normas técnicas, de todos os 65 (sessenta e cinco) julgados em questão, apenas 3 (três) fizeram uso de normas técnicas: i) O AgRg no HC 8.280.54/RN, da 5ª Turma, publicado em 29/04/2024, se utilizou da norma ABNT NBR ISO/IEC 27037:2013, bem como da analogia ao artigo 422, parágrafo 1º do CPC, para afirmar que no caso não houve adoção dos procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos através de extração de celular; ii) O Inq. 1.674, da Corte Especial, publicado em 11/05/2026 se utilizou da norma ABNT NBR ISO/IEC 27037:2013 e do POP/2024 para rejeitar o recurso da defesa e considerar íntegra a cadeia de custódia da prova digital, por seguir o disposto nas normas técnicas, apresentar a cronologia da prova e os respectivos códigos *hash* e; iii) O APn 1.076/DF, da Corte Especial, publicado em 28/05/2026, que se utilizou das mesmas normas técnicas referidas no item "ii" para considerar o fato de a polícia ter feito

[87] LOPES, Aury. *Prova penal digital...op. cit.*; MATIDA, Janaina.*op. cit.*; PRADO, Geraldo. *op.cit.*

uma cópia de segurança das provas digitais, foi suficiente para preservar a cadeia de custódia, ainda que não tenha sido disponibilizado o código *hash* dos documentos digitais.

A importância das normas técnicas já foi abordada no item anterior, notadamente o fato de terem maior facilidade de regulamentar o tratamento das provas digitais que uma legislação em sentido estrito, já que sua alteração pode ser feita por um processo menos rígido e moroso que a lei, possibilitando o acompanhamento da mudança acelerada das inovações tecnológicas. Malgrado a sua falta de coercitividade, dada a ausência de chancela formal do poder legislativo, trata-se da única forma atual existente no Brasil de padronizar a extração dos dados digitais para fins de produção probatória no processo penal. Apesar disso, a Convenção de Budapeste é norma legal válida, possui a mesma hierarquia normativa do Código de Processo Penal, e já traz em seu bojo parâmetros mínimos para a extração de dados em computador que podem ser utilizados por analogia em qualquer dispositivo digital. Desse modo, já existe previsão legal que obriga a perícia extrair uma cópia de segurança para preservação dos dados brutos originais e manutenção de sua integridade (artigo 19 do Decreto 11.491/2023).

Para além das críticas elaboradas para os precedentes acima elencados, é preciso enaltecer as decisões que julgaram o caso concreto tendo como filtro principal o sistema acusatório e o Estado como verdadeiro responsável por preservar a cadeia de custódia da prova digital, a exemplo do AgRg no RHC 186138/SP, da 5ª Turma, julgado em 26/12/2024.

O caso que melhor se coaduna com a fundamentação exposta no item anterior é o AgRg no RHC 143169/RJ, da 5ª Turma, julgado em 02/03/2023. Nele ficou constatado que a exclusão de provas digitais cuja cadeia de custódia tenha sido violada não é mero formalismo, mas sim forma de colocar no Estado acusador o ônus de provar a integridade e a confiabilidade das provas digitais:

> 4. A autoridade policial responsável pela apreensão de um computador (ou outro dispositivo de armazenamento de informações digitais) deve copiar integralmente (*bit* a *bit*) o conteúdo do dispositivo, gerando uma imagem dos dados: um arquivo que espelha e representa fielmente o conteúdo original. 5. Aplicando-se uma técnica de algoritmo *hash,* é possível obter uma assinatura única

> para cada arquivo, que teria um valor diferente caso um único *bit* de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Comparando as *hashes* calculadas. 7. No caso dos autos, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu. 8. Pela quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP. (AgRg no RHC 143169/RJ, da 5ª Turma, julgado em 02/03/2023)

A parte final do supracitado precedente é igualmente notável: "Caberá ao juízo de primeira instância desentranhar dos autos as provas inadmissíveis e avaliar se (e quais) outras delas decorrem, para que sejam também desentranhadas" (AgRg no RHC 143169/RJ, da 5ª Turma, julgado em 02/03/2023). Ou seja, invalidar as provas digitais não é necessariamente sinônimo de absolvição, devendo o caso retornar ao juízo de origem, para nova análise com base apenas em indícios de prova lícitos.

Em sentido contrário, diversos foram os precedentes em que a prova digital foi considerada válida com o argumento de que existiriam outros meios de prova que corroborariam a condenação, como exemplo: "conjunto probatório é composto não apenas pelos dados digitais obtidos dos dispositivos apreendidos, mas também pelo laudo pericial que confirmou a natureza ilícita das substâncias apreendidas e pelos depoimentos dos acusados" (AgRg no HC 1.004.935/DF, 6ª Turma, julgado em 08/09/2025). Em casos como este se observa duplo erro: manutenção de prova nula nos autos do processo e supressão de instâncias. Ao não invalidar a prova digital e afirmar que a condenação está suficientemente embasada em outros elementos de prova, o julgado mantém a nulidade e retira da instância ordinária seu direito de análise primária do caso concreto, considerando o novo cenário, de ausência do arcabouço das provas digitais ilícitas.

Também merece destaque a fundamentação utilizada pelo AgRg no HC 8.280.54/RN, da 5ª Turma, julgado em 29/04/2024, que anulou as provas digitais, por entender necessária a presença de mesmidade para considerar íntegra a cadeia de custódia, sendo a apresentação do código *hash* forma de garantir a auditabilidade da prova digital:

> 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. O referido documento técnico, embora não dotado de força obrigatória de lei, constitui relevante guia a ser observado pelos atores da persecução penal, a fim de assegurar, tanto quanto possível, a autenticidade da prova digital. Recomenda-se, na norma técnica, que o sujeito responsável pela aquisição e tratamento do material de interesse para uma investigação descreva, desde o início, toda a cronologia de movimento e manipulação da potencial evidência digital, convindo que o registro da cadeia de custódia contenha, no mínimo, informações sobre o identificador único da evidência; quem acessou a evidência, com registro de tempo e local; quem checou a evidência interna e externamente nas instalações de preservação da evidência, com respectivo registro de tempo e local; propósito de verificação da evidência; além de quaisquer alterações inevitáveis da potencial evidência digital, assim como o nome do indivíduo responsável para tanto e a justificativa para a introdução da alteração. (AgRg no HC 8.280.54/RN, da 5ª Turma, julgado em 29/04/2024)

Por fim, vale ressaltar que nenhum dos precedentes analisados fez qualquer menção à necessidade de se armazenar o dispositivo eletrônico dentro de recipiente que o isole de sinais de internet, a exemplo da *Faraday Bag*. O procedimento parece essencial para garantir que o conteúdo interno do aparelho apreendido permaneça íntegro, sem qualquer tipo de alteração ou apagamento de dados que inviabilizem seu uso como prova no processo penal.

Considerações Finais

O objetivo principal deste estudo era realizar uma investigação empírica sobre a forma como vem se posicionando o STJ em matéria de cadeia de custódia e prova digital. Considerando a pesquisa anterior elaborada por Fisberg[88], foi feito um recorte similar na busca online do Tribunal – artigos que contivessem o termo *hash* em sua ementa, entre 2016 e 2026, possibilitando a realização de um estudo comparativo.

A evolução digital da sociedade atrai para o campo do direito reflexos e consequências múltiplas, razão pela qual o recorte aqui estabelecido foi preciso: avaliar se o STJ em seus julgamentos colegiados em matéria criminal, analisa a integridade da cadeia de custódia fundamentado em premissas atinentes ao sistema acusatório, a presunção de inocência e ao contraditório. Após a pesquisa, confirmou-se a hipótese inicial, os precedentes estão aquém do rigor previsto pelas normas legais e técnicas em vigor no Brasil.

Através da codificação prévia dos precedentes e da categorização deles em palavras descritivas e palavras de valor, foi possível perceber que a maior parte das decisões do STJ possui um déficit de justificação ao se posicionar sobre a integridade da cadeia de custódia das provas digitais. Ao contrário do que preconiza o processo penal acusatório, transferem à defesa o ônus de comprovar eventual prejuízo causado pela prova, antes de analisar se a prova é nula em si mesma.

Trata-se de um padrão decisório arbitrário, que se coaduna com a matriz autoritária do Código de Processo Penal de 1941, que preza pela busca da verdade real a todo custo, de um lado com a flexibilização do sistema de nulidades e garantias processuais, e do outro com a importação da teoria da instrumentalidade das formas e do princípio da eficiência, próprios do processo civil. Paralelamente, para a análise das provas digitais, também foi observado o uso de conceitos próprios do direito administrativo, como a alegação de fé-pública e presunção de legitimidade dos atos do servidor público para fundamentar a integridade da cadeia de custódia.

---

[88] FISBERG, *op. cit*.

Sobre a forma de garantia de uma cadeia de custódia íntegra, verifica-se que o *hash* atesta a integridade do arquivo quando foi calculado, mas não garante a autenticidade desse arquivo, não assegura a ausência de eventual manipulação anterior à coleta e não confirma a sua mesmidade com o arquivo originalmente apreendido. Por essa razão, entende-se que a paridade de armas entre acusação e defesa somente é garantida com a disponibilização dos dados digitais brutos, sendo insuficiente apenas a apresentação do relatório gerado por softwares especializados, como o *Cellebrite*, ainda que contenha o código *hash* dos arquivos periciados.

O tema é complexo e a rapidez evolutiva das tecnologias digitais dificilmente conseguirá ser acompanhada por uma regulamentação legal apropriada. Logo, é imprescindível que todo o caminho percorrido pela prova digital, desde sua apreensão, armazenamento, perícia e posterior disponibilização integral para a defesa esteja documentado. Para tanto, as normas técnicas existentes no Brasil, a exemplo da ABNT NBR ISO/IEC 27037:2013, a Instrução Normativa DG/PF nº 299/2025 e os "Procedimentos Operacionais Padrão (POPs) de Perícia Criminal do Ministério da Justiça de 2024" devem servir de referência metodológica para a perícia digital, sendo a forma mais adequada de subsidiar eventuais lacunas na legislação processual penal.

Embora precedentes como o AgRg no RHC 143.169/RJ, AgRg no RHC 1.861.38/SP e o AgRg no HC 8.280.54/RN sejam dignos de nota, dada a fundamentação robusta determinando que cabe ao Estado acusador o ônus de provar a integridade da cadeia de custódia, são decisões isoladas e antigas quando comparadas com as demais. O que se percebe é que o STJ mantém para as provas digitais o mesmo padrão decisório historicamente utilizado para a análise de nulidades em geral, tais como o uso genérico do princípio *pas de nullité sans grief*, fundamentado no artigo 563 do CPP, além da lógica de vedação da nulidade de algibeira, convalidando o ato nulo pela preclusão consumativa.

Por fim, duas considerações conexas merecem destaque. A primeira é o fato de que a nulidade da prova digital por violação a sua cadeia de custódia é matéria que deve ser reconhecida pelo juízo já na instrução. Sendo nula a prova, deve ser imediatamente desentranhada dos autos, evitando a contaminação do processo com narrativas que não podem ser comprovadas de forma lícita. Em segundo lugar, sendo a questão passível

de análise através de provas documentais, ou da sua ausência, podem ser levadas ao STJ tanto por habeas corpus – com a devida manifestação prévia das instâncias ordinárias, quanto por recurso especial – uma vez que a temática não configura revolvimento fático do caso concreto.

Referências

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

BADARÓ, Gustavo Henrique. *Epistemologia judiciária e prova penal*. São Paulo: Thomson Reuters Brasil, 2019.

CASEY, Eoghan (org.), *et al*. *Handbook of digital forensics and investigation*. San Diego: Elsevier, 2010. 567 p.

CRUZ, Viviane Ramos da. Perícia em computadores. *In*: SOUZA, Bernardo de Azevedo; SILVA, Marcos Lamas Santos da (coord.). *Perícias Digitais*. Indaiatuba, SP: Foco, 2025.

DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di Diritto Processuale*, Milano, v. 66, n. 2, p. 283-298, mar./apr. 2011.

DE VITA, Roberto. *La prova digitale nel processo penale*. Devitalaw: Roma, 2025.

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. https://doi.org/10.22197/rbdpp.v11i3.1227

FREITAS FILHO, Roberto; LIMA, Thalita Morais. *Metodologia de análise de decisões* - MAD. *Univ. JUS*, Brasília, n. 21, p. 1-17, jul./dez. 2010. Disponível em: https://www.rel.uniceub.br/jus/article/viewFile/1206/1149. Acesso em: 18 jul. 2026.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. *Revista Acadêmica*, 2020, p. 12. https://doi.org/10.26729/et.v20i1.3130

GLOECKNER, Ricardo Jacobsen. *Autoritarismo e processo penal II:* autoritarismo cool e economia política do processo penal brasileiro. v. 2. 1. ed. São Paulo: Tirant Lo Blanch, 2023.

GLOECKNER, Ricardo Jacobsen. *Autoritarismo e processo penal:* uma genealogia das ideias autoritárias no processo penal brasileiro. v. 1. 1. ed. Florianópolis/SC: Tirant Lo Blanch, 2018.

HALL, Mark A.; WRIGHT, Ronald F. Systematic content analysis of judicial opinions. *California Law Review*, v. 96, p. 63-122, 2008.

HERMEIRO, Andreia Carina Claúdio. *A cadeia de custódia da prova digital:* o uso da Tecnologia Blockchain como forma de preservação. 2023. 64p. Dissertação (Mestrado em Ciências Jurídico-Forenses) – Faculdade de Direito, Universidade de Coimbra, Coimbra, 2023.

KERR, Orin S. *The digital Fourth Amendment*: privacy and policing in our online world. New York: Oxford University Press, 2025.

LOPES, Aury. *Fundamentos do Processo Penal – Introdução Crítica*. 11. ed. Rio de Janeiro: Saraiva Jur, 2025.

LOPES, Aury *et al*. Prova penal digital: relatório do Cellebrite pode ser insuficiente. *Consultor Jurídico (ConJur)*, São Paulo, 10 out. 2025. Disponível em: https://www.conjur.com.br/2025-out-10/prova-penal-digital-relatorios-do-cellebrite-podem-ser-insuficientes/. Acesso em: 18 jul. 2026.

MAIA, Daniele Lovatte. Em torno de Francisco Campos: ideias autoritárias, Estado nacional e democracia substancial. *Revista Direito e Práxis*, Rio de Janeiro, v. 16, n. 2, p. 1-24, 2025. https://doi.org/10.1590/2179-8966/2025/86131

MAIA, Daniele Lovatte. Metodologia técnico-jurídica e o Direito Penal fascista italiano: contribuições de Alfredo Rocco e Arturo Rocco. *Revista Quaestio Iuris*, Rio de Janeiro, v. 18, n. 1, p. 302-328, 2025. https://doi.org/10.12957/rqi.2025.91405

MAIA, Daniele Lovatte. Conjunto de dados de: "Cadeia de custódia, Prova Digital e código hash: uma análise da jurisprudência do STJ à luz do processo penal acusatório". *Scielo Data,* v1, 2026. https://doi.org/10.48331/SCIELODATA.FSCX1S

MATIDA, Janaina. A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes. Boletim IBCCRIM, São Paulo, v. 28, n. 331, p. 6–9, 2020. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/541. Acesso em: 18 jul. 2026.

PINHO, Ana Cláudia; MELCHIOR, Antonio Pedro; CASARA, Rubens. *Teoria do processo penal brasileiro*. v. 1. Rio de Janeiro: Da Vinci Livros, 2025.

PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. 1. ed. São Paulo: Marcial Pons, 2019.

REIS, Rodrigo Casimiro. *Verdade e prova penal*: a cadeia de custódia da era digital. 1. ed. São Paulo: Amanuense, 2025.

ROSA, Alexandre de Morais da. *Guia compacto do processo penal conforme a teoria dos jogos*. 1. ed. Rio de Janeiro: Lumen Juris, 2013.

SILVA, Fernanda Pereira da. *A cadeia de custódia da prova digital na colaboração premiada:* fiabilidade probatória. 2023. 85 f. Dissertação (Mestrado Profissional em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, DF, 2023.

SILVA, Marcos Alexandre de Araújo. Perícia em dispositivos móveis. *In*: SOUZA, Bernardo de Azevedo; SILVA, Marcos Lamas Santos da (coord.). *Perícias Digitais*. Indaiatuba, SP: Foco, 2025.

VERBRUGGEN, Paul; WIJNTJENS, Lianne. Methodological accountability in systematic case law analysis: Empirical insights from the Netherlands. *European Journal of Empirical Legal Studies*, v. 2, n. 1, art. 6, 2025. https://doi.org/10.62355/ejels.25885

Authorship information

Daniele Lovatte Maia. Doutora em Direito e Sociologia pela Universidade Federal Fluminense (UFF), com período de pesquisa (doutorado sanduíche) na Universidade *degli Studi di Macerata* (Itália). Mestre em Direito pela Universidade Federal do Rio de Janeiro. Graduada em Direito pela UFRJ. Advogada e Sócia do *T.F'A&M* – Tristão Farme d'Amoed Maia Advogados. Professora substituta de direito penal, direitos humanos e direito administrativo da Universidade Federal do Rio de Janeiro (2024-2026). Professora de Direito Penal, Prática Penal e Metodologia da UFF/Macaé (2019-2021). daniele.lovatte@gmail.com.

Additional information and author's declarations
(*scientific integrity*)

Conflict of interest declaration: the author confirms that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

Declaration of originality: the author assures that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; she also attests that there is no third party plagiarism or self-plagiarism.

Data Availability Statement: In compliance with open science policies, the dataset of this article is available in an open repository at the following link: MAIA, Daniele Lovatte. Conjunto de dados de: "Cadeia de custódia, Prova Digital e código hash: uma análise da jurisprudência do STJ à luz do processo penal acusatório". *Scielo Data,* v1, 2026. https://doi.org/10.48331/SCIELODATA.FSCX1S

IA Statement: The author declares that she is aware that the use of artificial intelligence must not supplant the human originality of the research, and that full responsibility for any errors or plagiarism rests entirely with the authors. The author declares that the Generative Artificial Intelligence 'Gemini' was used to assist in brainstorming the initial theme, ensuring alignment with this journal's call for papers on 'Judicial motivation and standards of justification in criminal proceedings.' Subsequently, Gemini was utilized to translate the abstract and the title from Portuguese into English, as well as to assist in formatting the references according to ABNT standards, and the excel.

Editorial process dates (https://revista.ibraspp.com.br/RBDPP/about)

- Submission: 20/07/2026
- Desk review and plagiarism check: 25/07/2026
- Review 1: 08/08/2026
- Review 2: 11/08/2026
- Preliminary editorial decision: 30/08/2026
- Correction round return 1: 25/09/2026
- Preliminary editorial decision 2: 28/09/2026
- Correction round return 2: 29/09/2026
- Final editorial decision: 29/09/2026

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 2

How to cite (ABNT Brazil):

MAIA, Daniele L. Cadeia de custódia, prova digital e código *hash*: uma análise da jurisprudência do STJ à luz do processo penal acusatório. *Revista Brasileira de Direito Processual Penal*, vol. 12, n. 3, e1593, set./dez. 2026. https://doi.org/10.22197/rbdpp.v12i3.1593

License Creative Commons Attribution 4.0 International.