A CADEIA DE CUSTÓDIA DA PROVA DIGITAL: DISSENSOS E CONSENSOS ENTRE TEORIA E PRÁXIS

THE CHAIN OF CUSTODY OF DIGITAL EVIDENCE: DIVERGENCES AND CONVERGENCES BETWEEN THEORY AND PRACTICE

Cláudio Saad Netto[1]
Universidade de Brasília, UnB, Brasil
claudioprocessopenal@gmail.com

Luiz Francisco Torquato Avolio[2]
Universidade de São Paulo, USP, Brasil
lfavolio@hotmail.com

Luiz Antonio Borri[3]
Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Brasil
luiz@advocaciabittar.adv.br

DOI: https://doi.org/10.5281/zenodo.19697006

Resumo: O artigo analisa a cadeia de custódia da prova digital, assinalando a posição da doutrina jurídica e da área informática, que sustentam a exigência de cautelas adicionais com essa espécie probatória, em decorrência da sua volatilidade. A seguir, examina-se posições absolutamente divergentes fixadas pelo Superior Tribunal Justiça em relação à matéria, apontando para a necessidade de harmonização do posicionamento da Corte. Partindo da compreensão de que existe um direito à prova pericial, defende-se que a uniformização da matéria observe rígidas regras para a custódia probatória do vestígio digital.

Palavras-chave: prova pericial; vestígio digital; jurisprudência; cadeia de custódia; prova ilícita.

Abstract: This article analyzes the chain of custody applicable to digital evidence, emphasizing the converging positions of legal scholarship and computer science literature that highlight the need for heightened safeguards in light of the intrinsic volatility of such evidentiary material. It further scrutinizes the markedly divergent approaches adopted by the Superior Court of Justice, revealing significant inconsistencies that call for doctrinal and jurisprudential harmonization. Grounded in the understanding that there is a right to expert evidence, it is argued that the standardization of this matter should adhere to strict rules regarding the evidentiary custody of digital evidence.

Keywords: expert evidence; digital evidence; case law; chain of custody; exclusionary rule.

[1] Pós-Doutor em Direito pela Universidade de Brasília (https://ror.org/02xfp8v59). Doutor e Mestre em Direito Processual Penal, ambos pela PUC-SP. Especialista em Gestão de Políticas de Segurança Pública (ANP/DF). Bacharel em Direito, Engenharia Civil e Ciências Contábeis. Articulista em livros jurídicos. Palestrante. Perito Criminal Federal (Aposentado). ORCID: https://orcid.org/0009-0006-3434-7338. Currículo Lattes: http://lattes.cnpq.br/1402230225242409. Instagram: @claudiosnetto.

[2] Doutor e Mestre em Direito Processual pela Faculdade de Direito da Universidade de São Paulo (https://ror.org/036rp1748). Especialista em Direito Penal Econômico pela Universidade de Coimbra. Advogado, pesquisador científico e parecerista. ORCID: https://orcid.org/0000-0002-6622-5523. Currículo Lattes: http://lattes.cnpq.br/8091754283817494. Instagram: @lfavolio.

[3] Doutor em Ciências Criminais pela PUCRS (https://ror.org/025vmq686). Mestre em Ciências Jurídicas pelo Cesumar. Advogado. ORCID: https://orcid.org/0000-0001-7649-1270. Currículo Lattes: http://lattes.cnpq.br/1414046440611495.

1. Fundamentos jurídicos e científicos sobre a validade da prova digital

Como descreve **Giulio Illuminati** (2022, p. 945), o significado de vestígio digital é amplo, abarcando "qualquer dado codificado em formato numérico segundo o sistema binário, de modo que possa ser lido por um dispositivo eletrônico, pois é representado por dois impulsos elétricos de intensidades distintas: ligado/desligado, ou seja, zero e um".

Os chamados vestígios digitais não se limitam a um corpo físico, podendo, em tese, ser duplicados perfeita e indefinidamente, mantendo o seu conteúdo.

Esse modo de ver a prova digital[1] alinha-se à compreensão doutrinária de estabelecer que a validade epistêmica das provas digitais no processo penal demanda a obediência aos standards metodológicos para a *computer forensics*, pois os dados digitais são conservados e transmitidos em linguagem não natural, sendo características desse elemento de prova a desmaterialização e a dispersão (**Badaró**, 2021, p. 7).

Por isso, para que uma prova digital seja admitida, diferentemente do que ocorre no processo civil, em que, simplesmente, é reputada válida se não houver impugnação (art. 422 do CPC), no processo penal, por força da presunção de inocência, superável tão somente pelo mais elevado *standard* probatório, deve-se comprovar a sua autenticidade, integridade e confiabilidade, qual seja, a sua mesmidade.

A fim de assegurar a mesmidade da prova (**Prado**, 2014, p. 16-17), no AgRg no *HC* 943.895/PR, o Superior Tribunal de Justiça (STJ) estabeleceu quatro aspectos como essenciais da provas digitais: i) auditabilidade: as partes devem ter condições de aferir se o método técnico-científico para a extração foi devidamente observado; ii) repetibilidade: a mesma sequência de etapas deve sempre produzir os mesmos resultados; iii) reprodutibilidade: ainda que empregando métodos diversos, os resultados devem ser os mesmos; e iv) justificabilidade: os métodos e procedimentos devem ser justificáveis, sob a óptica da melhor técnica **(Brasil**, 2025a).

Por essa razão, adverte **Geraldo Prado** (2023, p. 315-330) sobre a importância de se conservar o caminho digital percorrido pela informação, precavendo-se contra manipulações acidentais ou intencionais, supressões ou acréscimos, seja em relação a dispositivos físicos, comunicações telefônicas ou sistemas operacionais *in the cloud*.

Nesse contexto, tanto a doutrina quanto a perícia científica têm visto no código *hash*[2] um instrumento adequado para assegurar a mesmidade da prova digital.

Como explica **Evandro Mário Lorens** (2025, p. 237), uma particularidade do vestígio digital é que ele não se limita por corpo físico, ou seja, pode ser perfeitamente duplicado, mantendo integralmente todas as características de seu conteúdo. Destaca o autor que os principais meios atualmente disponíveis para armazenamento podem ser sensíveis a diversas condições, como umidade, calor, impacto, falhas de alimentação elétrica e defeitos eletrônicos dos dispositivos. Além do mais, intervenções de processamento indevidas podem destruir, de forma definitiva, os vestígios digitais.

Ao reconhecer precauções a serem adotadas nos exames periciais digitais diante do risco de quebra da cadeia de custódia, realça **Lorens** (2025) a importância de normas técnicas como a ABNT NBR ISO 27037 e o regramento legal da Lei 13.964/2019, destacando que, na condução do exame propriamente dito, devem ser adotadas diversas providências para a preservação da cadeia de custódia dos vestígios digitais, entre elas: duplicação forense do material recebido, realização do exame sobre as cópia da duplicação forense, acondicionamento adequado do material, controle de acesso aos vestígios, utilização exclusivamente de ferramentas forenses certificadas, registro formal de eventuais atividades invasivas no exame (**Lorens**, 2025, p. 247-249).

2. A cadeia de custódia da prova digital no CPP

O instituto da cadeia de custódia foi inserido pela Lei 13.964/2019 — que incluiu os artigos 158-A a 158-F no CPP — e visa a garantir a higidez da fonte de prova[3], e a afastar incertezas que poderão gravitar em torno da preservação dos vestígios deixados pela infração penal. Discorrer sobre cadeia de custódia da prova implica discutir a qualidade da prova, ou seja, reconhecer se uma fonte de prova encontrada no local de crime ou correlato, na vítima ou no agressor[4], corresponde àquilo que foi submetido examinado e consequentemente transportado ao processo penal.

Esse diploma legal foi responsável por incluir na legislação nacional o conceito de vestígio, prescrevendo no art. 158-A, §3º, do CPP que: "vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal".

De uma leitura superficial do art. 158-A, § 3º, do CPP subsistiria limitação à vinculação das provas digitais ao instituto da cadeia de custódia da prova, posto que permaneceria restrita ao suporte físico dos dados.

Tal conclusão, contudo, não seria razoável, visto que o vestígio digital, difundido à custa do uso constante de dispositivos eletrônicos como *smartphones*, *tablets* e computadores, representa, atualmente, uma das mais acessíveis fontes de prova. Como bem definiu o Min. Edson Fachin, a respeito da autodeterminação informativa, seria o acesso a uma espécie de "casa imaterial cibernética" do indivíduo, onde se concentram todos os dados de sua vida privada, profissional e financeira (**Brasil**, 2025c, p. 23).

Logo, a regulação legal da cadeia de custódia deve ser interpretada de forma ampla, incluindo os vestígios imateriais, assim como os de natureza digital (**Bittar; Soares**, 2021, p. 78; **Bruni**, 2020, p. 127-128; **Duarte**, 2020, p. 26).

3. As linhas de divergência jurisprudencial na 5ª Turma do STJ

Passando a examinar a cadeia de custódia da prova digital à luz da jurisprudência do STJ, despontam, no entanto, nítidas contradições, em especial em acórdãos da 5ª Turma[5], do entendimento firmado acima que, por vezes, contrastam com as diretrizes científicas da área de informática.

3.1. STJ – 5ª Turma: Agravo Regimental em *Habeas Corpus*

Numa primeira linha, afinada com os avanços científicos, a 5ª Turma do STJ, ao julgar o AgRg no HC 943.895/PR, entre 28/8/2025 e 3/9/2025, em acórdão de relatoria do Min. Joel Ilan Paciornik.

Tratava-se de agravo regimental, interposto pelo Ministério Público Federal, em face de decisão monocrática que concedeu a ordem de *habeas corpus*, de ofício. Na origem, imputou-se a prática dos crimes do art. 288 do Código Penal, art. 38-A e art. 49 da Lei 9.605/98 e a defesa arguiu o trancamento da ação penal por nulidade decorrente da violação da cadeia de custódia na extração dos dados obtidos em aparelho de celular.

A tese defensiva era de que o aparelho celular de corréu foi manuseado diretamente pela autoridade policial que produziu um relatório de análise de extração de dados baseado em *printscreen* de diálogos de WhatsApp, sem atender às diretrizes legais da cadeia de custódia.

Estabeleceu o Relator três teses relevantes sobre a cadeia de custódia de vestígio digital: (i) A quebra da cadeia de custódia de provas digitais compromete sua fidedignidade e integridade da prova; (ii) O Estado possui o ônus de comprovar a integridade e confiabilidade das provas apresentadas; e (iii) A ausência de documentação da cadeia de custódia torna a prova inadmissível no processo penal.

https://doi.org/10.5281/zenodo.19697006

Sobre esse ponto específico, o acórdão consignou a seguinte informação:

> após o cumprimento do mandado de busca e apreensão do celular do corréu Victor Bereza e antes do encaminhamento do aparelho ao Instituto de Criminalística para extração dos dados com a técnica científica adequada que assegure a preservação da prova e a fidedignidade dos dados, a autoridade policial procedeu com o manuseio do aparelho, inclusive confrontando o proprietário acerca das conversas encontradas e elaborando relatório contendo *prints* de conversas encontradas em aplicativos de mensagens (**Brasil**, 2025a, p. 12).

Resgatando a compreensão estabelecida no AgRg no *HC* 828.054/RN, julgado em 23/4/2024, o acórdão recorda as características das provas digitais, reconhecendo a maior volatilidade dos dados telemáticos, bem como sua maior suscetibilidade a alterações, a denotar a relevância de mecanismos de preservação dos vestígios probatórios digitais (**Brasil**, 2025a).

O acórdão realça, ainda, a relevância de se atender às regras mínimas que garantam a autenticidade de novos meios de prova, notadamente com observância à NBR ISO/IEC 27037:2013 que versa sobre diretrizes no manuseio de vestígios digitais, compreendendo a sua identificação, coleta, aquisição e preservação.

Diante desse cenário, o agravo regimental foi desprovido, mantendo-se a concessão da ordem de *HC* que reconheceu a inadmissibilidade das provas obtidas a partir do aparelho celular apreendido do corréu, assim como daquelas derivadas.

Na mesma linha, no julgamento do RHC 143.169/RJ, em acórdão relatado pelo Ministro Ribeiro Dantas, tratava-se de caso em que

> 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 (**Brasil**, 2023).

Conforme destacado na ementa, o que passa a ser um princípio garantístico do processo penal, é "ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas", sendo incabível simplesmente "presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia".

Como consequência, foi reconhecida a quebra da cadeia de custódia, tornando inadmissíveis as provas extraídas dos computadores do acusado, bem como as provas delas derivadas, em aplicação analógica do art. 157, § 1º, do CPP.

3.2. STJ – 5ª Turma: Agravo Regimental no Recurso Ordinário em *Habeas Corpus*

Já, numa segunda linha de entendimento, a 5ª Turma, na mesma sessão virtual ocorrida entre 28/8/2025 e 3/9/2025, no julgamento do AgRg no RHC 212.606/PR, posicionou-se em sentido diametralmente oposto, ao definir que o fornecimento de *prints* de WhatsApp por corréu, interlocutor das conversas, que renunciou ao sigilo dos seus dados, constitui prova válida (**Brasil**, 2025b).

Segundo o julgado, apesar de o aparelho celular não haver sido apreendido:

> o ônus de demonstrar a adulteração de um documento — e a captura de tela foi considerada como tal pelas instâncias ordinárias — recai sobre quem alega, e a simples conjectura de que a prova poderia ter sido modificada não é suficiente para invalidá-la, sobretudo quando as instâncias ordinárias atestaram a coerência cronológica e a ausência de indícios de fraude (**Brasil**, 2025b, p. 8).

A questão central que se coloca, pois, é a seguinte: como se pode atestar a coerência cronológica e a falta de indícios de fraude se o aparelho que constitui a fonte daqueles *prints* não foi apreendido?

4. Necessidade de harmonização da matéria, à luz do art. 926 do CPC

Observa-se do quanto abordado, ausência de estabilidade, bem como de coerência e de integração (art. 926, CPC) com a jurisprudência nessa matéria da admissibilidade da prova digital.

Partindo-se das cautelas legais que visam a assegurar a mesmidade da prova, e das recomendações da perícia técnica da área de informática, é inevitável concluir-se, como sustenta **Geraldo Prado** (2023, p. 340), que:

> a volatilidade da prova digital é de quase impossível detecção e à semelhança da prova de DNA manipulada, a inversão do ônus da prova para exigir dos acusados que demonstrem o dano causado por eventual modificação intencional dos dados consistiria na temível "prova diabólica", isto é, naquela inatendível.

5. Da necessidade de perícia criminal: pressupostos e direito à prova pericial

O cenário atual, pois, é preocupante, sobretudo diante dos riscos de condenação lastreada em prova ilícita, pois o exercício do contraditório e da ampla defesa são severamente comprometidos com a utilização de *prints* de WhatsApp obtidos sem a respectiva apreensão do aparelho celular, bem como sem a adoção de providências necessárias para a extração de seu conteúdo.

O artigo 158 do CPP estabelece a indispensabilidade do exame de corpo de delito, direto ou indireto, para comprovar a materialidade de crimes que deixam vestígios, não podendo a confissão do acusado suprir essa prova.

Dadas as peculiaridades dos diversos tipos de perícias, a doutrina reputa essa incompleta regulamentação da cadeia de custódia, verdadeira "norma processual penal em branco", pois devem ser observados protocolos administrativos e científicos específicos para cada modalidade de exame pericial.

O exame pericial da prova digital, a princípio, já compreende a observância de duas cadeias de custódia, a do dispositivo (*hardware*) ou suporte dos dados, e o dos arquivos, programas e dados nele contidos (*software*).

Mais que um simples suporte de armazenamento, como o disco rígido de um computador ou a memória de um dispositivo portátil, muitas vezes se torna necessário o acesso a dados armazenados nas nuvens (*cloud computing*).

Segundo **José Nogueira** (2025, p. 217-234), especialista em perícias informáticas, o processo de extração e armazenamento dos dados é facilitado pelo emprego da inteligência artificial, na automação da coleta e análise dos dados, em grandes volumes de dados, no reconhecimento de anomalias (algoritmos de aprendizado), possibilitando a geração de relatórios e laudos automatizados.

Utiliza-se, para assegurar a mesmidade e autenticidade dos vestígios, o código *hash* de cada arquivo, que deveria ser uma fonte original, mas poderia se tratar de cópia, devidamente autenticada.

Afinal, como assinala a doutrina, o dever legal insculpido no art. 158, do CPP, da obrigatoriedade da perícia, importa no reconhecimento de um correspondente direito, qual seja, do direito à prova pericial no processo penal. Pois, assim, quanto mais confiável e garantidor se apresentar o meio probante eleito para o exercício do direito à prova, mais efetivo se mostrará o rito probatório (**Saad Netto *et al.***, 2023).

Naturalmente, o direito à prova pericial só pode ser assegurado se a fonte de prova for adequadamente preservada contra manipulações intencionais ou involuntárias não bastando a invocação de um truque hermenêutico (verdadeira prova diabólica) para justificar a integridade da prova, pois incumbe ao Estado acusador demonstrar — como consectário da presunção de inocência — a idoneidade daquilo que pretende utilizar em desfavor do cidadão acusado. Em suma, as fontes de prova não se tornam idôneas porque o acusado deixou de questionar alguma adulteração, mas porque foram adotadas as providências científicas para a custódia da prova.

Informações adicionais e declarações dos autores (integridade científica)

Declaração de conflito de interesses: os autores confirmam que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de autoria:** somente os pesquisadores que cumprem os requisitos de autoria deste artigo são listados como autores; todos os coautores são totalmente responsáveis por este trabalho em sua totalidade.

Declaração de originalidade: os autores garantiram que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; eles também atestam que não há plágio de terceiros ou autoplágio.

Como citar (ABNT Brasil)

SAAD NETTO, Cláudio; AVOLIO, Luiz Francisco Torquato; BORRI, Luiz Antonio. A cadeia de custódia da prova digital: dissensos e consensos entre teoria e práxis. *Boletim IBCCRIM*, São Paulo, v. 34, n. 403, p. 18-21, 2026. DOI: 10.5281/zenodo.19697006. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2761. Acesso em: 1 jun. 2026.

Notas

[1] Embora consagrada pela doutrina jurídica, em verdade, a expressão "prova digital" se sujeita a críticas uma vez que não há confundir suporte digital (registros, vestígios) com a função probatória (documental ou pericial). Ou seja, o "digital" não define a natureza da prova — apenas o meio de existência do vestígio ou do registro. Em suma: não existe prova digital como categoria autônoma. Existe um regime probatório diferenciado aplicável a provas documentais e periciais de origem digital.

[2] Como se vê na doutrina "o mecanismo de controle de integridade dos dados copiados em um processo de duplicação ou cópia forense, ou de extração forense é usualmente realizado por algoritmos de resumo criptográfico, conhecidos também como funções *hash*, ou simplificadamente *hash*. Os algoritmos de resumo criptográfico são funções matemáticas unidirecionais que transformam uma entrada de dados de tamanho variável em um valor de tamanho fixo, o *hash*" (Lorens, 2025, p. 240).

[3] Compreende-se por fontes de prova tanto coisas quanto pessoas. Nesse sentido, cite-se como exemplo os vestígios, tais como objetos, substâncias etc. (coisas) e os peritos criminais (pessoas). É a partir das fontes de prova que se permite obter a prova.

[4] Para uma crítica à percepção de que a cadeia de custódia se limita ao local do crime ou à vítima indica-se a consulta à obra de Amaral (2023, p. 127-128).

[5] As ideias debatidas no presente texto partem de premissas fixadas em Saad Netto, Avolio e Borri (2025).

Referências

AMARAL, Maria Eduarda Azambuja. *Entre a ciência forense e o processo penal*: um modelo interdisciplinar da cadeia de custódia. Belo Horizonte, São Paulo: D'Plácido, 2023.

BADARÓ, Gustavo. 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, junho/2021. Disponível em: https://www.publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325. Acesso em: 30 mar. 2026.

BITTAR, Walter Barbosa; SOARES, Rafael Junior. Capítulo 4 – Código de Processo Penal – Decreto-Lei 3.689/41. *In*: BITTAR, Walter Barbosa (org). *Comentários ao Pacote Anticrime*: Lei 13.964/2019 (artigo por artigo – incluindo a rejeição de vetos). São Paulo: Tirant lo Blanch, 2021. p. 39-101.

BRASIL. Superior Tribunal de Justiça (Quinta Turma). *AgRg no HC n. 828.054/RN*. Relator Ministro Joel Ilan Paciornik, julgado em 23/4/2024, DJe de 29/4/2024.

BRASIL. Superior Tribunal de Justiça (Quinta Turma). *AgRg no HC 943.895/PR*. Relator Ministro Joel Ilan Paciornik, julgado em sessão virtual de 28/08/2025 a 03/09/2025a.

BRASIL. Superior Tribunal de Justiça (Quinta Turma). *AgRg no RHC n. 143.169/RJ*. Relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, julgado em 7/2/2023, DJe de 2/3/2023.

BRASIL. Superior Tribunal de Justiça (Quinta Turma). *AgRg no RHC 212.606/PR*. Relator Ministro Carlos Cini Marchionatti (Desembargador Convocado), julgado em sessão virtual de 28/08/2025 a 03/09/2025b.

BRASIL. Supremo Tribunal Federal. *ARE 1042075*. Relator: Ministro Dias Toffoli, Tribunal Pleno, julgado em 25/06/2025c.

BRUNI, Aline Thaís. Cadeia de Custódia. *In*: SALVADOR NETTO, Alamiro Velludo *et al.* (org.). *Pacote Anticrime*: Comentários à Lei 13.964/2019. São Paulo: Almedina, 2020. p. 121-141.

DUARTE, Daniel Nascimento. Restrição legal de aplicabilidade da cadeia de custódia da prova penal. *Boletim IBCCRIM*, v. 28, n. 335, p. 25-28, 2020. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/920. Acesso em: 30 mar. 2026.

ILLUMINATI, Giulio. Prova digitale e ammissibilità. *In*: VALENTE, Manuel Monteiro Guedes; WUNDERLICH, Alexandre (org.). *Direito e liberdade*: estudos em homenagem ao professor doutor Nereu José Giacomolli. São Paulo: Almedina, 2022. p. 945-959.

LORENS, Evandro Mário. Perícias em vestígios digitais e a cadeia de custódia. *In*: SAAD NETTO, Cláudio; AVOLIO, Luiz Francisco Torquato; BORRI, Luiz Antonio (org.). *Nulidades no processo penal e a cadeia de custódia*. São Paulo: Revista dos Tribunais, 2025. p. 235-249.

NOGUEIRA, José Helano Matos. Perícia em dados em nuvem, tecnologia blockchain e a cadeia de custódia. *In*: SAAD NETTO, Cláudio; AVOLIO, Luiz Francisco Torquato; BORRI, Luiz Antonio (org.). *Nulidades no processo penal e a cadeia de custódia*. São Paulo: Revista dos Tribunais, 2025. p. 217-234.

PRADO, Geraldo. Ainda sobre a "quebra da cadeia de custódia das provas". *Boletim IBCCRIM*, São Paulo, v. 22, n. 262, p. 16-17, 2014. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/issue/view/130. Acesso em: 30 mar. 2026.

PRADO, Geraldo. Investigação criminal digital e processo penal. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 199, p. 315-350, nov.-dez. 2023.

SAAD NETTO, Claudio (org.). *O Direito à prova pericial no processo penal*. São Paulo: Thomson Reuters, 2023.

SAAD NETTO, Cláudio; AVOLIO, Luiz Francisco Torquato; BORRI, Luiz Antonio (org.). *Nulidades no processo penal e a cadeia de custódia*. São Paulo: Revista dos Tribunais, 2025.

Recebido: 5 mar. 2026. Aprovado: 30 mar. 2026. Última versão dos autores: 11 abr. 2026.