A INTEGRIDADE DA PROVA DIGITAL COMO VETOR DA MODULAÇÃO DA NULIDADE: REPERCUSSÕES DA QUEBRA DA CADEIA DE CUSTÓDIA

THE INTEGRITY OF DIGITAL EVIDENCE AS A VECTOR FOR MODULATING NULLITY: REPERCUSSIONS OF BREAKING THE CHAIN OF CUSTODY

Melhym Pereira Quemel
Mestre em direito pela Universidade Estácio de Sá (UNESA). Advogado. Especialista em Advocacia cível pela Fundação Escola Superior do Ministério Público/RS (FMP). Especialista em Ciências Penais e Segurança Pública pelo Instituto Rogério Greco.
E-mail: mpquemel@gmail.com

Recebido em: 01/07/2025 | Aprovado em: 23/07/2025

Resumo: O presente artigo analisa os efeitos da quebra da cadeia de custódia em provas digitais e a modulação da nulidade processual (relativa/absoluta). Investiga as consequências práticas via caso paradigma (descoberta por IA Google/NCMEC). Metodologia: análise documental, revisão bibliográfica (prova digital, cadeia de custódia, Lei nº 13.964/19) e jurisprudencial (STJ). Discute preservação, metadados, *standards* técnicos e argumentos de defesa/acusação. Conclui pela tendência à nulidade relativa condicionada a prejuízo concreto, sobretudo se a integridade da prova for confirmada por outros meios (perícia, *hashes*). Aponta a relevância da IA e cooperação internacional na persecução de cibercrimes.

Palavras-chave: cadeia de custódia, prova digital, nulidade processual, inteligência artificial, processo penal.

Abstract: *This article analyzes the effects of breaking the chain of custody for digital evidence and the modulation of procedural nullity (relative/absolute). Investigates the practical consequences using a case paradigm (discovery via Google/NCMEC AI). Methodology: documentary analysis, literature review (digital evidence, chain of custody, Law 13,964/19), and jurisprudential analysis (STJ). Discusses preservation, metadata, technical standards, and defense/prosecution arguments. Concludes there is a tendency towards relative nullity conditioned on*

concrete prejudice, especially if the evidence's integrity is confirmed by other means (forensics, hashes). Points out the relevance of AI and international cooperation in the prosecution of cybercrimes.

***Keywords**: chain of custody, digital evidence, procedural nullity, artificial intelligence, criminal procedure.*

INTRODUÇÃO

A crescente digitalização da sociedade reverbera intensamente no sistema de justiça criminal, onde algoritmos de inteligência artificial (IA) já não são apenas personagens de ficção científica, mas ferramentas ativas na descoberta de crimes complexos, como demonstra o caso que inspira este estudo.

A capacidade de sistemas automatizados identificarem padrões suspeitos em volumes massivos de dados digitais inaugura uma nova era na investigação, mas também impõe desafios sem precedentes à garantia da validade processual das provas assim obtidas. Neste cenário, o tema central deste artigo é a cadeia de custódia aplicada a arquivos digitais, um mecanismo fundamental para assegurar a idoneidade da prova em juízo.

A relevância do tema é multifacetada: reside na necessidade de adaptar institutos processuais clássicos à natureza volátil e intangível da prova digital; na insegurança jurídica gerada por interpretações divergentes sobre as consequências da violação dessa cadeia, especialmente após as inovações trazidas pela Lei nº 13.964/2019 ("Pacote Anticrime"); e na urgência de se discutir o impacto de tecnologias disruptivas, como a IA, e da cooperação internacional (exemplificada pela atuação do National Center for Missing and Exploited Children – NCMEC) na persecução penal.

O problema de pesquisa que norteia este trabalho é: Qual o efeito prático da alegação de quebra da cadeia de custódia sobre arquivos digitais no processo penal brasileiro, especialmente quando a integridade do conteúdo pode ser aferida por outros meios, e como a jurisprudência tem modulado os efeitos dessa nulidade?

O objetivo geral é analisar a modulação dos efeitos da nulidade (relativa ou absoluta) decorrente da quebra da cadeia de custódia em arquivos digitais. Como objetivos específicos, busca-se: (a) contextualizar a prova digital e a importância da cadeia de custódia, abordando a Lei nº 13.964/2019; (b) descrever e analisar um caso concreto paradigma onde a prova digital foi central e sua cadeia de custódia questionada, destacando o papel da IA e da cooperação internacional; (c) examinar a jurisprudência pertinente do Superior Tribunal de Justiça (STJ); e (d) discutir a aplicação do princípio do prejuízo (*pas de nullité sans grief*) na matéria.

A abordagem metodológica combina a revisão bibliográfica e documental de fontes doutrinárias sobre processo penal, prova digital e computação forense (utilizando as fontes bibliográficas como base), com a análise de jurisprudência selecionada do STJ e o estudo de caso aprofundado do Processo nº 0800337-68.2023.8.19.0058, que tramita no Tribunal de Justiça do Rio de Janeiro, servindo como ilustração prática dos desafios teóricos.

Para alcançar os objetivos propostos, o artigo está estruturado da seguinte forma: o Capítulo 1 abordará os conceitos fundamentais da prova digital e da cadeia de custódia, incluindo as alterações legislativas recentes. O Capítulo 2 detalhará o caso paradigma, desde a descoberta do crime pela IA do Google até os questionamentos processuais levantados pela defesa. O Capítulo 3 analisará criticamente a alegada quebra da cadeia de custódia no caso concreto, à luz da doutrina, dos *standards* técnicos e da jurisprudência sobre a modulação da nulidade. Finalmente, a Conclusão sintetizará os achados, responderá à questão de pesquisa e apontará desdobramentos e sugestões para casos futuros.

1. A PROVA NA ERA DIGITAL E A CADEIA DE CUSTÓDIA

A transição da prova predominantemente física para a digital representa uma das transformações mais significativas no campo probatório do processo penal contemporâneo. Este capítulo introduz as especificidades da prova digital em contraste com as provas tradicionais, ressaltando os desafios inerentes à sua natureza volátil e intangível.

Em seguida, apresenta a cadeia de custódia como resposta metodológica essencial para garantir a confiabilidade dessa prova, culminando na análise da sua recente positivação no ordenamento jurídico brasileiro pela Lei nº 13.964/2019.

1.1. Da Prova Tradicional à Prova Digital: Natureza e Desafios

As provas tradicionalmente conhecidas no processo penal, como um documento em papel, uma arma de fogo ou um depoimento testemunhal, possuem uma materialidade ou uma forma de apreensão sensorial direta que facilita, em certa medida, a verificação de sua autenticidade e integridade ao longo do tempo.

A prova digital, por outro lado, é definida como "informação gerada ou armazenada sob formato digital (numérico), que pode ser utilizada como meio de prova"[1]. Ela existe como sequências de bits (zeros e uns) que requerem um dispositivo computacional para serem acessadas e interpretadas[2]. Essa natureza imaterial e a "congênita mutabilidade"[3] trazem desafios únicos.

Arquivos digitais podem ser copiados, alterados ou excluídos com facilidade, muitas vezes sem deixar vestígios evidentes, ao contrário de uma rasura em um documento físico. Como aponta a doutrina especializada em computação forense, a simples ação de ligar um computador ou acessar um arquivo pode alterar metadados cruciais (datas de acesso, modificação, etc.), contaminando a evidência[4].

Além disso, a prova digital frequentemente reside em ambientes complexos e dinâmicos, como sistemas em nuvem, dispositivos móveis ou redes sociais, cuja coleta e preservação exigem conhecimentos técnicos específicos e procedimentos rigorosos[5]. A volatilidade é outra característica

1 LIMA, Renato Brasileiro de. **Manual de processo penal:** volume único. 8. ed. rev., ampl. e atual. Salvador: Ed. JusPodivm, 2020. p. 649, 655, 1725.

2 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

3 BADARÓ, Gustavo Henrique Righi Ivahy. **Epistemologia judiciária e prova penal**. São Paulo: Revista dos Tribunais, 2019.

4 CARVALHO, Romullo Wheryko Rodrigues de. A Importância da Cadeia de Custódia na Computação Forense. **Revista Brasileira de Criminalística,** v. 9, n. 2, p. 134-138, 2020. DOI: http://dx.doi.org/10.15260/rbc.v9i2.463.

5 OLIVEIRA, Lurã Azevedo de; BEZERRA MEDINA, Lucas Arieh. A cadeia de custódia das provas colhidas em aparelhos móveis de gravação. **Boletim IBCCRIM**, [S. l.], v. 31, n. 364, p. 16-19, 2024. Disponível em: <https://publica-

marcante; dados armazenados em memória RAM, por exemplo, podem ser perdidos simplesmente ao desligar o equipamento[6].

Essas características distinguem fundamentalmente a prova digital da prova física e demandam uma abordagem metodológica diferenciada para sua admissão e valoração em juízo.

1.2. A Cadeia de Custódia como Garantia Epistêmica

Diante dos desafios impostos pela natureza da prova digital, a cadeia de custódia emerge como um procedimento indispensável para assegurar sua "validade epistêmica"[7], ou seja, sua capacidade de demonstrar fidedignamente um fato relevante para o processo.

O conceito de cadeia de custódia, importado de áreas como a criminalística tradicional e a medicina legal, refere-se ao "conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

Aplicada à prova digital, a cadeia de custódia visa garantir que o dado digital apresentado em juízo é o mesmo que foi coletado na origem e que não sofreu alterações indevidas ou não documentadas durante as fases de identificação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte[8].

A documentação meticulosa de cada etapa e de quem teve acesso ao vestígio digital é crucial. Isso inclui, por exemplo, o uso de técnicas como o cálculo de *hash* (uma assinatura digital única para um arquivo ou conjunto de dados) no momento da coleta e em fases subsequentes para verificar a integridade do material[9].

---

coes.ibccrim.org.br/index.php/boletim_1993/article/view/1584>. Acesso em: 19 abr. 2025.

6 CAPOZZI, Ricardo Andrian; BATISTA, Peterson; FARIA, Petterson. Aplicação da coleta e preservação de provas em ambientes digitas e formação da cadeia de custódia segundo ISO 27.037, a Lei 13.964 e PL 4939/2020. **Revista Perícia em Foco**, São Paulo/Brasil, v. 1, n. 1, 2024. DOI: 10.5281/zenodo.13894346. Disponível em: <https://periciaemfoco.com.br/pfoco/article/view/1>. Acesso em: 19 abr. 2025.

7 BADARÓ, Gustavo Henrique Righi Ivahy. **Epistemologia judiciária e prova penal**. São Paulo: Revista dos Tribunais, 2019.

8 CARVALHO, 2020; CAPOZZI; BATISTA; FARIA, 2024.

9 LIMA, Renato Brasileiro de. **Manual de processo penal:** volume único. 8. ed. rev., ampl. e atual. Salvador: Ed.

A observância de *standards* metodológicos próprios da computação forense, como os previstos na norma ISO/IEC 27037[10], torna-se, assim, não um mero formalismo, mas uma condição para a confiabilidade da prova. Como adverte Righi[11], sem a documentação completa e integral da cadeia de custódia, a prova digital perde sua rastreabilidade e, consequentemente, sua força probante.

1.3. A Positivação da Cadeia de Custódia: A Lei nº 13.964/2019

Embora a necessidade da cadeia de custódia já fosse reconhecida pela doutrina e, em certa medida, pela jurisprudência, a Lei nº 13.964/2019 (Pacote Anticrime) representou um marco ao inserir expressamente o instituto no Código de Processo Penal (CPP), nos artigos 158-A a 158-F. Essa positivação buscou conferir maior segurança jurídica e padronizar os procedimentos relativos à preservação de vestígios em geral, com aplicabilidade direta à prova digital[12].

O artigo 158-A define a cadeia de custódia e estabelece seu início ("com a preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a presença de vestígio") e fim ("com o descarte"). O artigo 158-B detalha as etapas que compreendem a cadeia de custódia, desde o reconhecimento do vestígio até seu processamento e armazenamento, exigindo que todas as etapas sejam formalmente documentadas.

O artigo 158-C especifica quem são os responsáveis pela sua preservação (o agente público que reconhecer o elemento como de potencial interesse). O artigo 158-D trata do acondicionamento do vestígio, exigindo recipiente adequado, lacre, numeração individualizada e documentação da data, hora, nome de quem coletou e do perito

JusPodivm, 2020. p. 649, 655, 1725.

10 CAPOZZI, Ricardo Andrian; BATISTA, Peterson; FARIA, Petterson. Aplicação da coleta e preservação de provas em ambientes digitas e formação da cadeia de custódia segundo ISO 27.037, a Lei 13.964 e PL 4939/2020. **Revista Perícia em Foco**, São Paulo/Brasil, v. 1, n. 1, 2024. DOI: 10.5281/zenodo.13894346. Disponível em: <https://periciaemfoco.com.br/pfoco/article/view/1>. Acesso em: 19 abr. 2025.

11 BADARÓ, Gustavo Henrique Righi Ivahy. **Epistemologia judiciária e prova penal**. São Paulo: Revista dos Tribunais, 2019.

12 PACELLI, Eugênio; FISCHER, Douglas. **Comentários ao Código de Processo Penal e sua Jurisprudência.** 13. ed. rev., atual. e ampl. São Paulo: Atlas, 2021.

responsável pela análise. Os artigos 158-E e 158-F abordam o tratamento de vestígios em geral, incluindo a central de custódia.

Essa regulamentação, embora genérica para todos os tipos de vestígios, fornece um arcabouço legal claro para a exigência da cadeia de custódia. Contudo, como alerta Fischer[13], a aplicação desses dispositivos à prova digital ainda suscita debates, especialmente sobre quais etapas são factíveis e como documentá-las adequadamente no ambiente virtual (por exemplo, a coleta de dados na nuvem ou a preservação de logs de acesso).

A interpretação e aplicação desses artigos, particularmente no que tange às consequências de sua inobservância, tornaram-se centrais nos debates forenses, como será explorado nos capítulos seguintes à luz do caso paradigma e da jurisprudência.

Compreendidas as particularidades da prova digital e a fundamental importância da cadeia de custódia, positivada pela Lei nº 13.964/2019, torna-se possível analisar como esses conceitos se manifestam na prática. O próximo capítulo mergulhará no caso concreto que serve de paradigma a este estudo, detalhando como a tecnologia e a cooperação internacional levaram à descoberta de um crime grave e como a cadeia de custódia da prova digital se tornou o ponto fulcral da controvérsia processual.

2. O CASO PARADIGMA: DA NUVEM AO PROCESSO PENAL

A complexidade da cadeia de custódia em arquivos digitais e as nuances da modulação dos efeitos de sua eventual quebra podem ser mais bem compreendidas por meio da análise de um caso concreto que atraiu significativa atenção jurídica e midiática. Trata-se de processo criminal[14] originado na Comarca de Saquarema, Estado do Rio de Janeiro, cujos contornos fáticos e processuais ilustram vividamente os desafios contemporâneos da prova digital.

13 FISCHER, Douglas. Cadeia de custódia da prova no processo penal: comentários aos arts. 158-A a 158-F do CPP (Lei 13.964/2019). In: CUNHA, Rogério Sanches; GOMES, Luiz Flávio; PINTO, Ronaldo Batista (Coord.). **Pacote Anticrime**: Lei nº 13.964/2019: Comentários artigo por artigo. Salvador: JusPodivm, 2021.

14 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

2.1. A Notícia Crime Transnacional e o Papel da Inteligência Artificial

A investigação teve início de forma inusitada, extrapolando as fronteiras nacionais e adentrando o domínio da inteligência artificial aplicada à vigilância de conteúdo on-line. Conforme relatado nos autos do Inquérito Policial nº 947-01253-2022 (posteriormente redistribuído sob o nº 0800337-68.2023.8.19.0058)[15], a ignição processual deu-se de uma comunicação oriunda do National Center for Missing and Exploited Children (NCMEC), entidade norte-americana dedicada ao combate à exploração infantil[16].

Essa comunicação, por sua vez, foi motivada por um alerta gerado por sistemas de inteligência artificial da Google LLC. Algoritmos da empresa, projetados para detectar automaticamente material relacionado à exploração sexual infantojuvenil (CSAM – *Child Sexual Abuse Material*) armazenado em suas plataformas de nuvem (como o Google Drive ou Google Photos), identificaram arquivos suspeitos associados a uma conta vinculada ao investigado, A.E.O.C., médico anestesista de nacionalidade estrangeira residente no Rio de Janeiro[17].

A Google, em cumprimento a obrigações legais e termos de serviço, reportou suas suspeitas ao NCMEC, que, por meio de acordos de cooperação internacional, encaminhou a informação à Polícia Federal brasileira.

Esse ponto inicial é crucial, pois demonstra a crescente relevância de atores privados e tecnologia de IA na detecção de ilícitos, levantando debates sobre privacidade, vigilância e a própria natureza da "descoberta" da prova em ambientes digitais[18]. A investigação não partiu de uma denúncia humana direta ou de uma vigilância estatal tradicional, mas de uma análise automatizada de dados em servidores estrangeiros.

15 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

16 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

17 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

18 BADARÓ, 2024. p. 58, 59, 87; LOPES JR., 2020.

2.2. A Investigação Preliminar e a Atuação Policial

Recebida a comunicação via NCMEC, a Polícia Federal realizou diligências preliminares e, constatando que os fatos teriam ocorrido no Estado do Rio de Janeiro, declinou a atribuição para a Polícia Civil fluminense, especificamente para a Delegacia da Criança e Adolescente Vítima (DCAV)[19].

A investigação da DCAV, conforme detalhado nos relatórios policiais e nos depoimentos dos agentes responsáveis, como Guilherme Vieira da Costa e Bernardo de Castro Mendonça (cujos relatos constam sumarizados nas alegações finais do Ministério Público[20]), concentrou-se em corroborar as informações recebidas e aprofundar a apuração. Iniciou-se com a identificação formal do titular da conta Google e do endereço IP associado aos *uploads*/armazenamento dos arquivos suspeitos, chegando-se ao investigado A.E.O.C.[21] (Relatório DCAV).

A análise inicial das informações fornecidas pela Google/NCMEC, que incluíam metadados dos arquivos (como nomes, datas e, crucialmente, códigos *hash*), permitiu à autoridade policial ter um panorama preliminar do material. O código *hash* (como MD5 ou SHA-256) funciona como uma "impressão digital" do arquivo, um identificador único gerado de seu conteúdo.

A preservação e comparação desses *hashes* ao longo das etapas investigativas são fundamentais para a manutenção da cadeia de custódia, garantindo que o arquivo analisado posteriormente é o mesmo que foi originalmente encontrado[22]. No caso em tela, os *hashes* dos arquivos identificados pela Google foram informados e, teoricamente, serviriam de parâmetro para a verificação de integridade do material que viesse a ser apreendido[23] (comunicação NCMEC/PF).

19 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

20 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

21 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

22 CARVALHO, 2020; CAPOZZI; BATISTA; FARIA, 2024.

23 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

Diante dos indícios, a autoridade policial representou por mandados de busca e apreensão, visando coletar dispositivos eletrônicos (computadores, *smartphones*, mídias de armazenamento) que pudessem conter os arquivos originais ou outras provas digitais relevantes[24]. A decisão judicial que deferiu as buscas baseou-se na plausibilidade das informações transnacionais e na necessidade de aprofundamento para confirmação da materialidade e autoria delitiva[25].

2.3. A Apreensão dos Dispositivos e os Desafios da Coleta

O cumprimento dos mandados de busca e apreensão resultou na coleta de diversos equipamentos eletrônicos nos endereços ligados ao investigado A.E.O.C.[26] (Auto de Apreensão). Aqui, a aplicação prática dos procedimentos de cadeia de custódia, conforme delineados nos artigos 158-A a 158-F do Código de Processo Penal (com redação dada pela Lei nº 13.964/2019), torna-se central.

Os agentes policiais envolvidos na busca, conforme seus depoimentos[27], relataram os procedimentos adotados para o acondicionamento e lacre dos materiais apreendidos. A descrição detalhada de quem coletou, como coletou, onde e como acondicionou e quem transportou cada item é vital para a rastreabilidade da prova. A utilização de invólucros adequados e lacres numerados, com registro em ata, visa garantir a idoneidade do material que será posteriormente periciado[28].

Contudo, é justamente nessa fase que surgem potenciais questionamentos. A defesa do investigado A.E.O.C., em suas manifestações processuais[29] (Defesa Prévia; Alegações Finais), combativamente suscita

24 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

25 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

26 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

27 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

28 AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas.** 6. ed. São Paulo: Thomson Reuters Brasil, 2021.

29 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

dúvidas sobre a estrita observância de todos os passos da cadeia de custódia.

Argumenta-se, por exemplo, sobre a ausência de registros fotográficos de todos os lacres no momento da apreensão, a forma de espelhamento (cópia forense) dos dados dos dispositivos apreendidos e, principalmente, a maneira como os arquivos digitais originais, aqueles que motivaram o alerta da Google, foram acessados e preservados pelas autoridades brasileiras.

2.4. A Perícia Digital e a Questão da Integridade

Os dispositivos eletrônicos apreendidos foram encaminhados ao Instituto de Criminalística Carlos Éboli (ICCE) para perícia[30] (Guia de Encaminhamento). O laudo pericial de informática forense[31] (Laudo ICCE nº 0257/2023) descreve os procedimentos técnicos adotados para extrair e analisar os dados contidos nos equipamentos.

Idealmente, a perícia inicia com o espelhamento do conteúdo original dos dispositivos (criação de uma cópia bit a bit) em uma nova mídia, utilizando-se de técnicas que impeçam a alteração dos dados originais (como bloqueadores de escrita) e calculando-se o *hash* tanto do dispositivo original quanto da cópia gerada. A coincidência desses *hashes* demonstra que a cópia é idêntica ao original[32]. Todo o trabalho pericial subsequente deve ser realizado sobre essa cópia espelhada, preservando-se o dispositivo original intacto.

O laudo pericial no caso paradigma detalha a recuperação de arquivos, análise de metadados, registros de acesso e outras informações digitais relevantes encontradas nos aparelhos de A.E.O.C.[33]. Parte crucial da análise pericial consistiu em verificar se os arquivos encontrados nos dispositivos apreendidos correspondiam àqueles originalmente reportados pela Google/NCMEC. Isso é feito comparando-se os códigos *hash* dos arquivos

30 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

31 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

32 FISCHER, Douglas. Cadeia de custódia da prova no processo penal: comentários aos arts. 158-A a 158-F do CPP (Lei 13.964/2019). In: CUNHA, Rogério Sanches; GOMES, Luiz Flávio; PINTO, Ronaldo Batista (Coord.). **Pacote Anticrime**: Lei nº 13.964/2019: Comentários artigo por artigo. Salvador: JusPodivm, 2021.

33 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

encontrados pela perícia com os *hashes* informados na comunicação inicial[34] (Tabela Comparativa de *Hashes*).

A defesa, por sua vez, questiona a validade dessa comparação, argumentando que a forma como a própria Google acessou e gerou os *hashes* iniciais não teria seguido um protocolo forense auditável, ou que a polícia brasileira, ao receber a informação e antes mesmo da apreensão, poderia ter acessado a nuvem do investigado de forma a comprometer a cadeia de custódia original[35].

Levanta-se a hipótese de que a "árvore envenenada" (prova ilícita originária) poderia contaminar todo o material subsequente, mesmo que a coleta e perícia dos dispositivos físicos tenham seguido os protocolos[36]. Este embate técnico-jurídico sobre a origem da prova (IA em nuvem estrangeira), os procedimentos de coleta (busca e apreensão) e a análise pericial (espelhamento, *hashes*, metadados) compõe o cerne da discussão sobre a cadeia de custódia no caso A.E.O.C., servindo como pano de fundo para a análise da modulação dos efeitos da nulidade que será abordada nos capítulos seguintes.

3. ANÁLISE DA QUEBRA DA CADEIA DE CUSTÓDIA E A MODULAÇÃO DA NULIDADE

Tendo apresentado o caso paradigma e os argumentos processuais nele desenvolvidos, este capítulo dedica-se à análise crítica da alegada quebra da cadeia de custódia dos arquivos digitais. Serão examinados os potenciais pontos de fragilidade no manuseio da prova digital à luz dos procedimentos recomendados pela doutrina e pelos standards técnicos.

Em seguida, será explorada a jurisprudência do Superior Tribunal de Justiça (STJ) sobre o tema, com foco nos julgados indicados[37]. Por fim, discutir-se-á a teoria das nulidades no processo penal, especificamente a distinção entre nulidade relativa e absoluta e a aplicação do princípio

34 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

35 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

36 PACELLI, Eugênio. **Curso de Processo Penal.** 24. ed. São Paulo: Atlas, 2020.

37 Agravo Regimental no Recurso em Habeas Corpus nº 182.310/RJ e Recurso em Habeas Corpus nº 79.848/SP.

do prejuízo (*pas de nullité sans grief*) na avaliação da quebra da cadeia de custódia, conectando a teoria com a possibilidade de aferição da integridade da prova por meios alternativos.

3.1. Identificando Pontos Críticos na Cadeia de Custódia do Caso

A cadeia de custódia da prova digital, no caso paradigma, iniciou-se em um ponto atípico: a detecção por um ente privado (Google) em servidores localizados no exterior. A transmissão subsequente para o NCMEC (outra entidade privada estrangeira) e, depois, para as polícias Federal e Civil brasileiras, envolveu múltiplos intermediários e potenciais transferências de dados. Cada uma dessas etapas apresenta desafios sob a ótica da ISO 27037[38] e dispositivo legal, artigo 158-B do CPP.

Questionamentos poderiam surgir, por exemplo, sobre a documentação da coleta original: como o Google preservou e documentou a coleta inicial dos arquivos e metadados? Foram gerados *hashes* na origem? Essa documentação acompanhou os *reports* enviados ao NCMEC e, posteriormente, às autoridades brasileiras? A ausência dessa documentação inicial detalhada é um ponto frequentemente explorado pelas defesas.

Outro ponto crítico envolve a transferência entre entidades: como se deu a transferência dos arquivos entre Google, NCMEC e Polícias? Foram utilizados canais seguros? Houve registro formal de recebimento e envio em cada etapa? A integridade dos dados foi verificada a cada transferência (e.g., comparação de *hashes*)?

A análise preliminar pela DCAV também suscita dúvidas: ao receber os dados, a DCAV realizou uma cópia forense (bit a bit) do material original antes de iniciar a análise? Ou a análise foi feita diretamente sobre os arquivos recebidos? A metodologia de extração e análise dos metadados foi documentada conforme os padrões da computação forense[39]?

38 CAPOZZI, Ricardo Andrian; BATISTA, Peterson; FARIA, Petterson. Aplicação da coleta e preservação de provas em ambientes digitas e formação da cadeia de custódia segundo ISO 27.037, a Lei 13.964 e PL 4939/2020. **Revista Perícia em Foco**, São Paulo/Brasil, v. 1, n. 1, 2024. DOI: 10.5281/zenodo.13894346. Disponível em: <https://periciaemfoco.com.br/pfoco/article/view/1>. Acesso em: 19 abr. 2025.

39 CAPOZZI, Ricardo Andrian; BATISTA, Peterson; FARIA, Petterson. Aplicação da coleta e preservação de provas em ambientes digitas e formação da cadeia de custódia segundo ISO 27.037, a Lei 13.964 e PL 4939/2020. **Revista Perícia em Foco**, São Paulo/Brasil, v. 1, n. 1, 2024. DOI: 10.5281/zenodo.13894346. Disponível em: <https://periciaemfoco.com.br/pfoco/article/view/1>. Acesso em: 19 abr. 2025.

Finalmente, a preservação pós-apreensão: após a apreensão dos dispositivos do acusado, como foi realizada a extração dos dados neles contidos? Foi feita cópia forense? Os dispositivos foram lacrados e acondicionados corretamente (Art. 158-D, CPP)?

Embora os autos do processo[40] detalhem a investigação subsequente à comunicação do NCMEC, a fase pré-processual envolvendo Google e NCMEC pode carecer da formalidade documental exigida pelos artigos 158-A e seguintes do CPP, que pressupõem a atuação de agentes públicos desde o início. Essa lacuna formal é o terreno fértil para a alegação de quebra da cadeia de custódia. Contudo, a simples existência de pontos críticos formais não implica, automaticamente, a invalidade da prova, como será discutido adiante.

3.2. A Jurisprudência do STJ sobre Cadeia de Custódia e Prova Digital: Entre a Eficácia Probatória e a Inadmissibilidade

A interpretação do Superior Tribunal de Justiça (STJ) acerca das consequências da quebra da cadeia de custódia, mormente no que tange à prova de natureza digital, revela-se um campo dinâmico e essencial para compreender a aplicabilidade do instituto no cenário processual penal brasileiro. A análise detida de julgados selecionados permite identificar as nuances argumentativas e a *ratio decidendi* que moldam o entendimento da Corte, oscilando entre a concepção da falha como vício de nulidade relativa, dependente da demonstração de prejuízo, e o reconhecimento da inadmissibilidade da prova quando comprometida sua própria confiabilidade essencial.

Um dos entendimentos consolidados pelo STJ, exemplificado no julgamento do AgRg no RHC 182.310/RJ[41], aborda a quebra da cadeia de custódia sob o prisma da eficácia probatória. Neste caso, envolvendo a análise de um HD entregue por colaboradores, a Corte manteve a decisão de origem que afastou a nulidade. O fundamento central foi que a defesa, ao

40 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

41 BRASIL. Superior Tribunal de Justiça**. Agravo Regimental no Recurso em Habeas Corpus nº 182.310/RJ.** Relator: Ministro Reynaldo Soares da Fonseca. Quinta Turma. Julgado em 19/09/2023. DJe 26/09/2023.

arguir a quebra, não apresentou qualquer indício concreto de adulteração ou manipulação da prova durante o período de custódia estatal.

A *ratio decidendi* desse julgado assenta-se na premissa de que a alegação desacompanhada de elementos mínimos que sugiram a violação da integridade do vestígio digital não é suficiente para invalidar a prova. Considerou-se que sua verificação demandaria um revolvimento fático-probatório incompatível com a via estreita do *habeas corpus*. Nessa linha, a quebra da cadeia de custódia "não se trata [...] de nulidade processual, senão de uma questão relacionada à eficácia da prova, a ser vista em cada caso"[42]. Tal entendimento transfere à defesa o ônus de demonstrar a adulteração ou o comprometimento da prova, aplicando o princípio *pas de nullité sans grief* (art. 563, CPP) e tratando a inobservância procedimental como nulidade relativa.

No mesmo sentido, o RHC 79.848/SP[43] já sinalizava essa abordagem ao analisar a validade de investigação iniciada com base em *prints* de conversas de WhatsApp obtidos por um dos integrantes do grupo e entregues anonimamente. O Tribunal considerou que a prova digital (os *prints*) não era o único elemento a embasar a investigação, havendo outras diligências (oitivas, requisições) que a corroboravam.

Ademais, diferenciou a captação da conversa por um interlocutor da interceptação clandestina, validando a prova inicial por não vislumbrar ilegalidade manifesta e por existirem outros meios probatórios a conferir lastro à persecução[44]. A *ratio* aqui também aponta para a necessidade de analisar o contexto probatório como um todo, relativizando a falha formal na origem da prova digital quando outros elementos conferem verossimilhança aos fatos.

Contudo, a jurisprudência do STJ não é monolítica e reconhece situações em que a falha na preservação da prova digital assume contornos mais graves, levando à sua exclusão. O julgamento do AgRg no RHC

42 BRASIL. Superior Tribunal de Justiça**. Agravo Regimental no Recurso em Habeas Corpus nº 182.310/RJ.** Relator: Ministro Reynaldo Soares da Fonseca. Quinta Turma. Julgado em 19/09/2023. DJe 26/09/2023.

43 BRASIL. Superior Tribunal de Justiça**. Recurso em Habeas Corpus nº 79.848/SP.** Relator: Ministro Nefi Cordeiro. Sexta Turma. Julgado em 06/03/2018. DJe 12/03/2018.

44 BRASIL. Superior Tribunal de Justiça**. Recurso em Habeas Corpus nº 79.848/SP.** Relator: Ministro Nefi Cordeiro. Sexta Turma. Julgado em 06/03/2018. DJe 12/03/2018.

133.430/PE[45], revisitando o mesmo caso do RHC 79.848/SP[46], introduziu uma distinção crucial ao analisar especificamente a prova obtida por espelhamento via WhatsApp Web. Citando como fundamento o RHC 99.735/SC[47], a Sexta Turma declarou expressamente nulas e determinou o desentranhamento das mensagens obtidas por esse método[48].

A *ratio decidendi* baseou-se na intrínseca falta de confiabilidade da ferramenta WhatsApp Web para fins probatórios: a possibilidade técnica de o investigador (ou terceiro) enviar e excluir mensagens sem deixar vestígios, alterando o conteúdo original de forma indetectável, compromete irremediavelmente a autenticidade e a integridade da prova. Nesse cenário, a quebra da cadeia de custódia não é meramente formal, mas material, afetando a essência da prova. Importante notar que, mesmo declarando nula a prova obtida pelo espelhamento, o STJ manteve as demais provas produzidas por fontes independentes[49].

Essa linha de raciocínio, que foca na impossibilidade de garantir a "mesmidade" da prova digital devido a falhas graves no procedimento de coleta ou preservação, foi levada a um patamar ainda mais incisivo no julgamento do AgRg no RHC 143.169/RJ[50]. Em voto vencedor divergente, a Quinta Turma reconheceu a quebra da cadeia de custódia de computadores apreendidos em virtude da completa ausência de documentação por parte da polícia sobre quaisquer dos procedimentos adotados (coleta, acondicionamento, cálculo de *hash*, espelhamento, análise).

A *ratio decidendi* aqui foi contundente: a necessidade de preservar a cadeia de custódia antecede a Lei nº 13.964/2019, sendo indissociável do conceito de corpo de delito (art. 158, CPP). Diante da omissão estatal em seguir procedimentos técnicos mínimos (como cópia bit a bit e cálculo

45 BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 133.430/PE.** Relator: Ministro Rogerio Schietti Cruz. Sexta Turma. Julgado em 15/12/2020. DJe 18/12/2020.

46 BRASIL. Superior Tribunal de Justiça**. Recurso em Habeas Corpus nº 79.848/SP.** Relator: Ministro Nefi Cordeiro. Sexta Turma. Julgado em 06/03/2018. DJe 12/03/2018.

47 BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 99.735/SC.** Relator: Ministro Nefi Cordeiro. Sexta Turma. Julgado em 20/11/2018. DJe 27/11/2018.

48 BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 133.430/PE.** Relator: Ministro Rogerio Schietti Cruz. Sexta Turma. Julgado em 15/12/2020. DJe 18/12/2020.

49 BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 133.430/PE.** Relator: Ministro Rogerio Schietti Cruz. Sexta Turma. Julgado em 15/12/2020. DJe 18/12/2020.

50 BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ.** Relator: Ministro Ribeiro Dantas. Quinta Turma. Julgado em 22/06/2021. DJe 01/07/2021.

de *hash*) e em documentar suas ações, inverteu-se o ônus da prova: não caberia à defesa provar a adulteração (prova diabólica), mas sim ao Estado comprovar a integridade e a confiabilidade da fonte de prova por ele apresentada. Como a polícia falhou completamente em oferecer qualquer garantia de que o conteúdo permaneceu íntegro, a Corte declarou as provas extraídas dos computadores e as delas derivadas inadmissíveis, com base no art. 157, § 1º, do CPP, por violação direta da confiabilidade probatória[51].

Essa análise jurisprudencial evidencia uma tensão: de um lado, a regra geral que trata a quebra da cadeia de custódia como nulidade relativa, exigindo demonstração de prejuízo pela defesa[52]; de outro, o reconhecimento de que falhas procedimentais graves, que impeçam a verificação da autenticidade e integridade da prova digital – como a falta total de documentação[53] ou o uso de métodos intrinsecamente manipuláveis[54] –, maculam a prova em sua origem, tornando-a inadmissível e invertendo o ônus de demonstrar sua confiabilidade para o Estado.

Aplicando essas diretrizes ao caso paradigma[55], observa-se que a defesa invocou a quebra da cadeia de custódia de forma genérica, questionando a trajetória da prova desde o Google/NCMEC até a perícia brasileira, mas sem apontar indícios de adulteração ou contestar o conteúdo dos vídeos e metadados que formaram a materialidade delitiva[56]. Nesse contexto, a jurisprudência majoritária[57] tenderia a rejeitar a alegação de nulidade, por ausência de demonstração de prejuízo concreto.

A possibilidade técnica de realizar perícia nos arquivos digitais apreendidos para aferir sua integridade, mediante comparação de *hashes* ou análise forense, reforçaria essa perspectiva, permitindo verificar

51 BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ.** Relator: Ministro Ribeiro Dantas. Quinta Turma. Julgado em 22/06/2021. DJe 01/07/2021.

52 BRASIL. Superior Tribunal de Justiça**. Agravo Regimental no Recurso em Habeas Corpus nº 182.310/RJ.** Relator: Ministro Reynaldo Soares da Fonseca. Quinta Turma. Julgado em 19/09/2023. DJe 26/09/2023.

53 BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ.** Relator: Ministro Ribeiro Dantas. Quinta Turma. Julgado em 22/06/2021. DJe 01/07/2021.

54 Agravo Regimental no Recurso em Habeas Corpus nº 133.430/PE e Recurso em Habeas Corpus nº 99.735/SC.

55 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

56 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

57 BRASIL. Superior Tribunal de Justiça**. Agravo Regimental no Recurso em Habeas Corpus nº 182.310/RJ.** Relator: Ministro Reynaldo Soares da Fonseca. Quinta Turma. Julgado em 19/09/2023. DJe 26/09/2023.

a confiabilidade da prova a despeito de eventuais falhas formais na documentação da fase internacional inicial.

Contudo, a ausência de documentação detalhada sobre como se deu a transferência e o recebimento inicial dos dados pelas autoridades brasileiras poderia, em tese, atrair a aplicação da *ratio* do RHC 143.169/RJ[58], caso se entenda que essa lacuna inicial impede por completo a aferição segura da "mesmidade" da prova.

A questão central, portanto, reside em definir se as falhas formais apontadas foram de tal monta que impossibilitaram qualquer verificação posterior da integridade da prova digital ou se, apesar das falhas, a autenticidade do material pôde ser razoavelmente assegurada por outros meios técnicos e processuais. A jurisprudência do STJ, ao modular os efeitos da quebra da cadeia de custódia, impõe essa análise casuística, ponderando o rigor procedimental com a busca pela verdade e a efetiva demonstração de prejuízo à defesa.

3.3. Nulidade Relativa *versus* Absoluta: O Princípio do Prejuízo (*Pas de nullité sans grief*)

A distinção entre nulidade relativa e absoluta é crucial. A nulidade absoluta viola normas de interesse público, ligadas a garantias constitucionais fundamentais (como o devido processo legal, a ampla defesa), e pode ser declarada de ofício, independentemente da demonstração de prejuízo. A nulidade relativa atinge normas de interesse predominantemente das partes e depende de arguição oportuna e da demonstração do efetivo prejuízo sofrido[59].

No contexto da cadeia de custódia, a questão é se sua violação representa uma afronta direta a uma garantia fundamental (gerando nulidade absoluta) ou se é um vício procedimental cuja gravidade depende do impacto na confiabilidade da prova e do prejuízo causado à defesa (nulidade relativa).

58 BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ.** Relator: Ministro Ribeiro Dantas. Quinta Turma. Julgado em 22/06/2021. DJe 01/07/2021.

59 LIMA, 2020. p. 649, 655, 1725; FISCHER, 2021.

A doutrina majoritária[60] e a jurisprudência do STJ (conforme análise anterior) têm se alinhado à segunda corrente. Argumenta-se que a cadeia de custódia é um procedimento para garantir a autenticidade e integridade da prova, mas sua violação formal nem sempre resulta na perda dessas características. Incide aqui o princípio do *pas de nullité sans grief*, positivado no art. 563 do CPP ("Nenhum ato será declarado nulo, se da nulidade não resultar prejuízo para a acusação ou para a defesa").

Assim, mesmo que se constate uma falha formal na cadeia de custódia (e.g., falta de um lacre específico, documentação incompleta da transferência inicial Google-NCMEC), a defesa precisaria demonstrar como essa falha específica comprometeu a prova ou prejudicou seu direito de defesa.

No caso paradigma, a defesa alegou a quebra, mas não apontou adulteração nos vídeos nem contestou que o conteúdo mostrava o réu cometendo o ato, tampouco explicou como a suposta falha procedimental inicial (envolvendo Google/NCMEC) teria impactado a essência da prova digital[61]. A ausência dessa demonstração de prejuízo concreto fortalece a tese da nulidade meramente relativa, passível de convalidação se o vício não for arguido oportunamente ou se o prejuízo não for demonstrado.

3.4. A Possibilidade de Aferição da Integridade da Prova Digital

Um fator determinante na aplicação do princípio do prejuízo é a possibilidade de aferir a autenticidade e a integridade da prova digital por outros meios, mesmo que a cadeia de custódia formal apresente falhas. No caso dos arquivos digitais, isso é tecnicamente viável em muitas situações.

Como sugerido pelo membro do MP na descrição do caso[62], uma perícia técnica posterior poderia recalcular os *hashes*. Os arquivos de vídeo originais, da forma como foram recebidos e preservados pela polícia brasileira (idealmente em uma cópia forense armazenada em mídia segura,

60 LIMA, 2020. p. 649, 655, 1725; FISCHER, 2021.

61 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

62 BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

como um pen drive ou HD externo lacrado), poderiam ter seus códigos *hash* calculados novamente.

Também seria possível comparar com *hashes* anteriores. Se os *reports* originais do Google ou do NCMEC continham os *hashes* dos arquivos detectados, a comparação entre os *hashes* originais e os recalculados poderia atestar se os arquivos permaneceram íntegros desde a detecção inicial. Mesmo que os *hashes* originais não estivessem disponíveis, a análise pericial do conteúdo dos arquivos e de seus metadados (consistência interna, ausência de sinais de edição) poderia oferecer fortes indícios de sua autenticidade.

Essa possibilidade de verificação *a posteriori* da integridade da prova digital enfraquece o argumento da nulidade absoluta baseada apenas em falhas formais na cadeia de custódia inicial. Se a perícia demonstra que o arquivo apresentado em juízo é idêntico ao coletado (ou, no caso, ao detectado pelo Google), a falha procedimental na documentação da transferência, embora indesejável, pode não ter gerado prejuízo à defesa quanto à essência da prova.

É claro que isso não isenta o Estado de cumprir rigorosamente a cadeia de custódia (Art. 158-A), mas modula as consequências de sua eventual violação.

A análise da doutrina, da jurisprudência do STJ e do caso paradigma sugere que a quebra da cadeia de custódia da prova digital tende a ser tratada como nulidade relativa, exigindo demonstração de prejuízo concreto pela defesa. A possibilidade de aferição técnica da integridade dos arquivos digitais desempenha um papel crucial nessa avaliação. Resta, agora, consolidar essas observações e extrair as conclusões finais do estudo.

CONCLUSÃO

Este artigo propôs-se a analisar a modulação dos efeitos da nulidade decorrente da quebra da cadeia de custódia em arquivos digitais no processo penal brasileiro, utilizando como fio condutor um caso paradigmático emblemático dos desafios contemporâneos. O percurso iniciou-se com a exploração das características singulares da prova digital e da importância

crucial da cadeia de custódia como garantia de sua idoneidade, destacando a positivação do instituto pela Lei nº 13.964/2019 (Capítulo 1).

Em seguida, mergulhou-se no caso concreto, revelando como a inteligência artificial e a cooperação internacional podem deflagrar investigações complexas e como a cadeia de custódia se tornou o epicentro da batalha processual (Capítulo 2). Por fim, analisou-se criticamente a alegada quebra à luz dos *standards* técnicos, da jurisprudência do STJ e da teoria das nulidades, evidenciando a prevalência da abordagem da nulidade relativa, condicionada à demonstração de prejuízo (Capítulo 3).

Todavia, reconhece-se que este estudo possui limitações. A análise do caso paradigma baseou-se nos documentos fornecidos e em informações contextuais, não abrangendo o exame completo de todo o processo judicial, incluindo a sentença final e eventuais recursos. A seleção jurisprudencial, embora focada nos julgados indicados, representa um recorte do vasto universo de decisões sobre prova digital. Além disso, a dinâmica tecnológica e legislativa impõe contínua atualização das discussões aqui travadas.

As discussões fomentadas neste artigo apontam para importantes desdobramentos. Primeiro, reforça-se a necessidade de aprimoramento contínuo dos protocolos de coleta, preservação e análise de provas digitais por parte das autoridades policiais e periciais, com documentação rigorosa de todas as etapas da cadeia de custódia, inclusive nas fases que envolvem cooperação internacional ou interação com entes privados, buscando aderência máxima aos artigos 158-A e seguintes do CPP e às normas técnicas internacionais (como a ISO/IEC 27037).

Segundo, sugere-se, como ferramenta prática em casos de questionamento da cadeia de custódia, a realização de perícia técnica focada na verificação da integridade dos arquivos digitais, comparando, sempre que possível, os *hashes* atuais com os registrados em etapas anteriores (como os *reports* do Google/NCMEC no caso paradigma), como forma de suprir eventuais lacunas documentais e demonstrar a ausência de adulteração.

Terceiro, o caso analisado lança luz sobre a crescente importância da inteligência artificial como ferramenta investigativa, o que demanda futuras pesquisas sobre os limites éticos e legais de seu uso, a transparência

dos algoritmos e a própria admissibilidade processual de provas geradas ou pré-selecionadas por IA. Quarto, a relevância da cooperação jurídica internacional e da colaboração com entidades como o NCMEC merece estudos aprofundados, visando otimizar os fluxos de informação e garantir a compatibilidade dos procedimentos com as garantias processuais internas.

Portanto, conclui-se que, embora a observância rigorosa da cadeia de custódia seja um dever do Estado e uma garantia para o acusado, a jurisprudência brasileira, em sintonia com a doutrina majoritária e o princípio do *pas de nullité sans grief* (art. 563, CPP), tem se consolidado no sentido de tratar a sua quebra, especialmente em relação à prova digital, como uma nulidade relativa. Sua decretação depende da demonstração de prejuízo concreto para a parte que a alega, não bastando a mera irregularidade formal.

No caso paradigma, a ausência de contestação sobre a autenticidade do conteúdo dos vídeos e a falta de demonstração de como a suposta falha procedimental inicial teria alterado a essência da prova, aliadas à possibilidade técnica de aferir sua integridade, apontam para a dificuldade de reconhecimento de uma nulidade, sobretudo de natureza absoluta.

Nesse sentido, o estudo aponta para a necessidade de um equilíbrio entre o rigor formal na preservação da prova e a busca pela verdade processual, valorando-se a prova digital que, apesar de eventuais percalços em sua cadeia de custódia, mantém-se íntegra e autêntica quanto ao seu conteúdo essencial. A era digital exige adaptação, rigor técnico e uma interpretação processual que contemple suas especificidades sem sacrificar as garantias fundamentais.

REFERÊNCIAS

AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas.** 6. ed. São Paulo: Thomson Reuters Brasil, 2021.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, [S. l.], v. 29, n. 343, p. 7-9, 2024. Disponível em: <https://

publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325>. Acesso em: 19 abr. 2025. p. 58, 59, 87.

BADARÓ, Gustavo Henrique Righi Ivahy. **Epistemologia judiciária e prova penal**. São Paulo: Revista dos Tribunais, 2019.

BRASIL. Superior Tribunal de Justiça**. Agravo Regimental no Recurso em Habeas Corpus nº 182.310/RJ.** Relator: Ministro Reynaldo Soares da Fonseca. Quinta Turma. Julgado em 19/09/2023. DJe 26/09/2023.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ.** Relator: Ministro Ribeiro Dantas. Quinta Turma. Julgado em 22/06/2021. DJe 01/07/2021.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 133.430/PE.** Relator: Ministro Rogerio Schietti Cruz. Sexta Turma. Julgado em 15/12/2020. DJe 18/12/2020.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 99.735/SC.** Relator: Ministro Nefi Cordeiro. Sexta Turma. Julgado em 20/11/2018. DJe 27/11/2018.

BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Processo nº 0800337-68.2023.8.19.0058.** [Peças processuais diversas, incluindo denúncia, manifestações MP/Defesa]. Rio de Janeiro, 2023.

BRASIL. Superior Tribunal de Justiça**. Recurso em Habeas Corpus nº 79.848/SP.** Relator: Ministro Nefi Cordeiro. Sexta Turma. Julgado em 06/03/2018. DJe 12/03/2018.

CAPOZZI, Ricardo Andrian; BATISTA, Peterson; FARIA, Petterson. Aplicação da coleta e preservação de provas em ambientes digitas e formação da cadeia de custódia segundo ISO 27.037, a Lei 13.964 e PL 4939/2020. **Revista Perícia em Foco**, São Paulo/Brasil, v. 1, n. 1, 2024. DOI: 10.5281/zenodo.13894346. Disponível em: <https://periciaemfoco.com.br/pfoco/article/view/1>. Acesso em: 19 abr. 2025.

CARVALHO, Romullo Wheryko Rodrigues de. A Importância da Cadeia de Custódia na Computação Forense. **Revista Brasileira de Criminalística,** v. 9, n. 2, p. 134-138, 2020. DOI: http://dx.doi.org/10.15260/rbc.v9i2.463.

FISCHER, Douglas. Cadeia de custódia da prova no processo penal: comentários aos arts. 158-A a 158-F do CPP (Lei 13.964/2019). In: CUNHA, Rogério Sanches; GOMES, Luiz Flávio; PINTO, Ronaldo Batista (Coord.). **Pacote Anticrime**: Lei nº 13.964/2019: Comentários artigo por artigo. Salvador: JusPodivm, 2021.

LIMA, Renato Brasileiro de. **Manual de processo penal:** volume único. 8. ed. rev., ampl. e atual. Salvador: Ed. JusPodivm, 2020. p. 649, 655, 1725.

LOPES JR., Aury. **Direito Processual Penal.** 17. ed. São Paulo: Saraiva Educação, 2020.

OLIVEIRA, Lurã Azevedo de; BEZERRA MEDINA, Lucas Arieh. A cadeia de custódia das provas colhidas em aparelhos móveis de gravação. **Boletim IBCCRIM**, [S. l.], v. 31, n. 364, p. 16-19, 2024. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1584>. Acesso em: 19 abr. 2025.

PACELLI, Eugênio; FISCHER, Douglas. **Comentários ao Código de Processo Penal e sua Jurisprudência.** 13. ed. rev., atual. e ampl. São Paulo: Atlas, 2021.

PACELLI, Eugênio. **Curso de Processo Penal.** 24. ed. São Paulo: Atlas, 2020.