

ATUAÇÃO DO DELEGADO DE POLÍCIA NA GESTÃO DA PROVA DIGITAL: QUEBRA DE CADEIA DE CUSTÓDIA POR MANIPULAÇÃO PRÉVIA À PERÍCIA

THE ROLE OF THE POLICE DELEGATE IN THE MANAGEMENT OF DIGITAL
EVIDENCE: BREACH OF CHAIN OF CUSTODY DUE TO MANIPULATION
PRIOR TO FORENSIC EXAMINATION

Ciências Sociais Aplicadas • 04/06/2026

REGISTRO DOI: [10.70773/revistatopicos/780549065](https://doi.org/10.70773/revistatopicos/780549065)

Elimei Paleari do Amaral Camargo¹

Emanuele Giachini Botelho²

Maurício Rogério Botelho³

RESUMO

O artigo analisa a atuação do delegado de polícia na gestão da prova digital, com foco na cadeia de custódia e nas consequências de sua quebra. Parte-se da premissa de que a crescente digitalização das relações sociais impõe desafios ao processo penal, sobretudo quanto à preservação da integridade e da autenticidade das evidências digitais, marcadas pela imaterialidade, pela volatilidade e pela alta suscetibilidade a alterações. A cadeia de custódia é apresentada como mecanismo essencial de controle epistêmico, garantindo a rastreabilidade do vestígio desde a coleta até a sua apresentação em juízo. Com a Lei nº 13.964/2019, o instituto foi positivado no ordenamento brasileiro, estabelecendo etapas formais para o tratamento da prova. Contudo, sua efetividade enfrenta limitações estruturais, como a falta de capacitação técnica e a ausência de protocolos padronizados. No campo digital, destacam-se mecanismos como algoritmos *hash* e espelhamento forense, indispensáveis para assegurar a integridade dos dados. A atuação policial, especialmente no manuseio de dispositivos eletrônicos, é apontada como ponto crítico, sendo frequentes práticas inadequadas que comprometem a validade probatória. A jurisprudência do Superior Tribunal de Justiça (STJ) revela divergência quanto às consequências da quebra da cadeia de custódia, ora entendida como causa de inadmissibilidade da prova, ora como fator de redução de seu valor persuasivo. Conclui-se que a cadeia de custódia não é mera formalidade, mas condição de fidedignidade da prova digital, cuja violação compromete o devido processo legal e o potencial de convencimento do magistrado.

Palavras-chave: Prova digital; Cadeia de custódia; Processo penal; Integridade da prova; Perícia forense digital.

ABSTRACT

This article examines the role of the police chief in managing digital evidence, focusing on the chain of custody and the consequences of its breach. It is based on the premise that the increasing digitalization of social relations poses significant challenges to criminal procedure, particularly regarding the preservation of the integrity and authenticity of digital evidence, which is characterized by immateriality, volatility, and high susceptibility to alteration. The chain of custody is presented as an essential epistemic control mechanism that ensures the traceability of evidence from its collection to its presentation in court. With the enactment of Law No. 13,964/2019, this institute was formally incorporated into the Brazilian legal system, establishing procedural steps for handling evidence. However, its effectiveness is limited by structural constraints, such as insufficient technical training and the absence of standardized protocols. In the field of digital evidence, the study highlights key technical mechanisms, including hash algorithms and forensic imaging, which are crucial to ensuring data integrity. Police practices, particularly in handling electronic devices, are identified as a critical issue, as improper procedures frequently compromise evidentiary reliability. Case law from the Superior Court of Justice demonstrates divergent approaches to breaches of the chain of custody, sometimes leading to the inadmissibility of evidence and, in other cases, merely reducing its probative value. In digital contexts, however, stricter technical standards tend to prevail. The article concludes that the chain of custody is not a mere procedural formality, but a condition for the validity of digital evidence, and its violation may undermine due process and render evidence inadmissible.

Keywords: Digital evidence; Chain of custody; Criminal procedure; Evidence integrity; Digital forensics.

1. INTRODUÇÃO

A crescente digitalização das relações sociais, econômicas e comunicacionais tem produzido impactos profundos no âmbito do processo penal, especialmente no que se refere à produção, preservação e valoração da prova. Nesse cenário, a emergência da prova digital — constituída por dados binários suscetíveis de armazenamento, transmissão e manipulação em ambientes informacionais complexos — desafia as categorias tradicionais do Direito Probatório, exigindo a construção de novos parâmetros de confiabilidade e controle epistêmico.

Diferentemente das provas físicas convencionais, cuja materialidade permite a verificação sensorial direta e a identificação de alterações por meio de vestígios tangíveis, a prova digital apresenta características ontológicas que dificultam sua validação: imaterialidade, volatilidade e extrema sensibilidade a intervenções mínimas. Tal peculiaridade impõe ao sistema de justiça criminal a adoção de mecanismos rigorosos de preservação e rastreabilidade, sob pena de comprometimento da própria integridade do processo penal. Como destaca a doutrina: “a prova digital exige um modelo de controle que vá além da confiança nos agentes estatais, demandando verificabilidade técnica independente” (Prado, 2014, p. 88).

É nesse contexto que se insere o instituto da cadeia de custódia, concebido como um conjunto de procedimentos destinados a documentar a trajetória do vestígio, assegurando sua autenticidade e integridade desde a coleta até a sua apresentação em juízo. A positivação desse mecanismo no ordenamento jurídico brasileiro — por meio da Lei nº 13.964/2019, que introduziu os arts. 158-A a 158-F

no Código de Processo Penal — representa um marco relevante na tentativa de estruturar um modelo de controle probatório compatível com as exigências do Estado Democrático de Direito.

Todavia, a mera previsão normativa não é suficiente para garantir a efetividade do instituto, especialmente quando confrontada com a complexidade técnica das evidências digitais e com as limitações estruturais das instituições responsáveis pela persecução penal. A ausência de protocolos padronizados, a carência de capacitação técnica e a adoção de práticas informais no manuseio de dispositivos eletrônicos revelam um cenário em que a cadeia de custódia corre o risco de ser reduzida a uma formalidade esvaziada de conteúdo garantista.

Diante desse panorama, o presente artigo tem como objetivo analisar a cadeia de custódia da prova digital sob a perspectiva dos controles epistêmicos, investigando sua função como mecanismo de garantia da confiabilidade probatória e sua relação com os princípios estruturantes do processo penal. A hipótese orientadora é a de que, no âmbito das evidências digitais, a cadeia de custódia não pode ser compreendida como mera formalidade procedimental, mas como condição de possibilidade da própria validade da prova.

2. FUNDAMENTAÇÃO TEÓRICA: A CADEIA DE CUSTÓDIA DA PROVA DIGITAL NO PROCESSO PENAL

2.1. O Princípio da "Mesmidade" Como Corolário do Devido Processo Legal

A cadeia de custódia transcende a mera ritualística administrativa, configurando-se como um rigoroso sistema de controles epistêmicos indispensáveis à higidez do sistema acusatório. Sob a

perspectiva de Geraldo Prado (2014), o instituto funciona como uma "forma-garantia" voltada a assegurar o princípio da "mesmidade": a certeza de que o elemento probatório valorado pelo magistrado guarda identidade absoluta com o vestígio colhido na cena do crime. Conforme leciona Gustavo Badaró (2019), a autenticidade certifica a origem genuína do material, enquanto a integridade atesta a inexistência de modificações ou adulterações.

2.2. Contextualização Normativa no Brasil: O Advento da Lei N° 13.964/2019

Historicamente, o ordenamento jurídico brasileiro carecia de um regramento sistemático e legal sobre a cadeia de custódia, amparando-se predominantemente em atos administrativos e protocolos infralegais. O principal balizador era a Portaria n° 82/2014 da Secretaria Nacional de Segurança Pública (SENASP), que estabelecia diretrizes para os peritos criminais, mas possuía eficácia limitada no âmbito do controle jurisdicional da prova.

Tal cenário de insegurança jurídica foi substancialmente alterado pela Lei n° 13.964/2019 — o denominado "Pacote Anticrime" —, que positivou os artigos 158-A a 158-F no Código de Processo Penal. Esta reforma não apenas reconheceu a importância do instituto, mas detalhou minuciosamente o rastreamento do vestígio em dez etapas sucessivas:

1. Reconhecimento: identificação do potencial vestígio;
2. Isolamento: preservação do local para evitar contaminação;
3. Fixação: descrição detalhada do vestígio conforme encontrado;

4. Coleta: recolhimento do material para análise;
5. Acondicionamento: Embalagem Adequada para Transporte;
6. Transporte: transferência segura para o órgão pericial;
7. Recebimento: conferência e registro da entrada no órgão;
8. Processamento: o exame pericial propriamente dito;
9. Armazenamento: guarda em condições que garantam a integridade;
10. Descarte: destinação final após autorização judicial.

A lei define vestígio como "todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal". Conforme sustentado no desenvolvimento deste artigo, embora a literalidade da lei pareça voltada a objetos tangíveis, a doutrina moderna de Renato Brasileiro de Lima (2021) e Norberto Avena (2023) é uníssona em afirmar que este regramento é integralmente aplicável à prova digital. A natureza volátil dos dados binários exige que o cumprimento dessas etapas seja verificado com rigor ainda maior, visto que qualquer omissão no registro de uma dessas fases (especialmente na coleta e processamento) rompe a confiança técnica sobre a integridade do material, projetando efeitos diretos sobre a admissibilidade da prova em juízo.

2.3. A Ontologia da Prova Digital: Características e Desafios Hermenêuticos

A transposição da cadeia de custódia para o ambiente virtual exige a compreensão da natureza ontológica distinta da prova digital. Definida como dados processados a partir de uma lógica binária (*bits*), a evidência digital apresenta características que a diferenciam substancialmente das fontes de prova físicas. Segundo Andressa Olmedo Minto (2021), destacam-se quatro atributos fundamentais:

- Volatilidade: a possibilidade de desaparecimento ou alteração dos dados por eventos simples, como o registro automático de informações pelo sistema operacional ou o esgotamento de bateria;
- Fragilidade: a extrema suscetibilidade a manipulações imperceptíveis, em que a modificação de um único *bit* pode corromper a integridade do material de forma invisível a olho nu;
- Imaterialidade: o dado digital independe do suporte físico (*hardware*) em que está armazenado, sendo tecnicamente um elemento "imaterial" registrado eletronicamente;
- Replicabilidade e Dispersão: a facilidade de clonagem integral (cópia *bit a bit*) e a possibilidade de fragmentação dos dados em múltiplos locais, como nuvens e servidores transfronteiriços.

Diferente da prova física, cuja alteração geralmente deixa vestígios materiais, a prova digital demanda o que a doutrina denomina "princípio da desconfiança processual", exigindo protocolos técnicos específicos para sua validação. Sob essa ótica, a hermenêutica da prova digital não pode se limitar à análise do conteúdo aparente, mas deve alcançar a higidez do seu continente. Como bem assevera Geraldo Prado (2014), a ausência de um sistema de controles

epistêmicos que considere essas fragilidades ontológicas retira do elemento informativo a sua aptidão para o contraditório, transformando o dado binário em um elemento de arbítrio estatal.

2.4. Mecanismos Técnicos de Preservação e Rastreabilidade: A Ciência Forense Digital

Para mitigar os riscos intrínsecos à volatilidade e à fragilidade dos dados binários, a ciência forense digital utiliza protocolos técnicos rigorosos que devem integrar a custódia jurídica da prova. O principal mecanismo de controle de integridade é o algoritmo *hash*, frequentemente descrito pela doutrina como a "impressão digital" ou o "DNA" de um arquivo. Trata-se de uma função matemática que transforma um conjunto de dados de qualquer tamanho em uma sequência alfanumérica única e de comprimento fixo. Qualquer alteração mínima no conteúdo original — como a modificação de um único *bit* — resulta em um código *hash* completamente distinto, fenômeno conhecido como "efeito avalanche", o que permite denunciar imediatamente a quebra da integridade do vestígio.

Outro procedimento indispensável é o espelhamento forense, que consiste na realização de uma cópia integral, bit a bit, do dispositivo de armazenamento original. Este método assegura que a análise pericial seja realizada sobre a cópia (imagem forense), preservando o suporte bruto original de qualquer contaminação decorrente do manuseio. A rastreabilidade plena exige, ainda, que toda interação com a evidência digital seja documentada conforme normas técnicas internacionais, notadamente a ABNT NBR ISO/IEC 27037:2013, que estabelece diretrizes para a identificação, coleta, aquisição e preservação de evidências digitais, preconizando quatro princípios fundamentais:

1. Auditabilidade: a possibilidade de rastrear todas as ações realizadas sobre o vestígio;
2. Repetibilidade: a capacidade de se obter os mesmos resultados ao repetir o exame no mesmo material;
3. Reproduzibilidade: a obtenção dos mesmos resultados por diferentes peritos utilizando métodos distintos;
4. Justificabilidade: a fundamentação técnica para cada decisão tomada durante o manejo da prova.

Portanto, a validade jurídica da prova digital é indissociável de sua conformidade técnica. Sem a utilização de funções *hash* no momento da apreensão e sem a garantia de que o exame recaiu sobre cópia espelhada, a cadeia de custódia resta irremediavelmente comprometida, inviabilizando a verificação da "mesmidade" entre o dado colhido na delegacia e o apresentado em juízo.

2.5. Integração Interdisciplinar e as Consequências da Quebra da Cadeia

A validade jurídica da prova digital é indissociável da correção técnica de sua preservação. A interdisciplinaridade entre o Direito e a tecnologia torna-se imperativa, uma vez que o jurista não possui instrumentos isolados para aferir a integridade binária de um vestígio sem o suporte da ciência forense. No cotidiano das delegacias, contudo, a inobservância de registros mínimos no manuseio de dispositivos apreendidos gera a quebra da cadeia de custódia (*break on the chain of custody*), tema que suscita profunda divergência doutrinária e jurisprudencial.

Conforme detalhado no desenvolvimento deste estudo, a omissão legislativa do "Pacote Anticrime" quanto às consequências processuais específicas da quebra da cadeia permitiu a coexistência de duas vertentes principais:

Corrente da Inadmissibilidade: Liderada por Geraldo Prado (2014), defende que a cadeia de custódia é uma "forma-garantia" indissociável do devido processo legal. Assim, a interrupção de qualquer elo procedimental — como a falta de registro de um código *hash* — comprometeria a autenticidade da prova, tornando-a ilícita por violação de norma legal e constitucional, o que impõe a sua exclusão e desentranhamento dos autos (art. 157, CPP).

Corrente da Valoração: Capitaneada por Gustavo Badaró (2018), sustenta que a violação não deve conduzir automaticamente à inadmissibilidade, mas ser resolvida no campo da valoração probatória. Nesse sentido, o magistrado poderia atribuir menor valor persuasivo à evidência maculada, desde que outros elementos de prova legitimem seu conteúdo.

Não obstante essa disputa teórica, o Superior Tribunal de Justiça (STJ) tem consolidado o entendimento de que, em se tratando de fontes digitais, o ônus de comprovar a integridade da prova recai sobre o Estado. No emblemático julgamento do AgRg no RHC 143.169/RJ, a Quinta Turma reafirmou que é inadmissível presumir a veracidade de alegações estatais quando os protocolos de custódia são descumpridos. Portanto, a falta de rigor técnico na extração de dados — como o manuseio direto do aparelho pela polícia sem a devida perícia — retira a fiabilidade do material, projetando um vício que afeta a própria existência jurídica da prova.

2.6. Reflexão Crítica: O Descompasso Entre a Norma e a Realidade Estrutural

Não obstante a robustez teórica do modelo proposto e a clareza dos protocolos de preservação binária, a efetivação da cadeia de custódia digital enfrenta obstáculos severos na realidade institucional das polícias judiciárias brasileiras. O descompasso entre a densidade normativa da Lei nº 13.964/2019 e a pragmática do cotidiano investigativo revela o que a literatura empírica denomina "institucionalização da precariedade".

Conforme as pesquisas de Michel Misse (2010) e Eduardo Batitucci (2021), a escassez de recursos humanos qualificados, a sobrecarga de demandas e a ausência de *softwares* forenses certificados em diversas comarcas relegam a preservação de vestígios a métodos rudimentares. Essa "ilegalidade prática", muitas vezes justificada pela busca de eficiência imediata ou pela urgência na lavratura de flagrantes, acaba por mitigar as garantias fundamentais do investigado.

Nesse cenário, a ausência de Centrais de Custódia estruturadas (conforme previsto no art. 158-E do CPP) transforma as etapas de armazenamento e transporte em zonas de incerteza técnica. Sem o devido aparelhamento tecnológico e a profissionalização técnica contínua dos agentes, a cadeia de custódia corre o risco de tornar-se uma "folha de papel" — uma garantia meramente retórica que não resiste a um exame de auditabilidade. Portanto, a densificação teórica aqui proposta só atingirá sua finalidade democrática de controle do arbítrio estatal se for acompanhada por investimentos públicos massivos em infraestrutura pericial, garantindo que a prova

digital deixe de ser uma vulnerabilidade e passe a ser um instrumento genuíno de justiça.

3. A ATUAÇÃO DA POLÍCIA JUDICIÁRIA E A DINÂMICA DA CADEIA DE CUSTÓDIA DIGITAL: ENTRE O RIGOR EPISTÊMICO E A REALIDADE ESTRUTURAL

3.1. A Fenomenologia da Urgência nas Delegacias: O Tencionamento dos Controles Epistêmicos

A introdução sistemática da cadeia de custódia no ordenamento jurídico pátrio, por intermédio da Lei nº 13.964/2019 (Pacote Anticrime), estabeleceu um novo paradigma de integridade probatória corporificado nos arts. 158-A a 158-F do Código de Processo Penal. Sob a perspectiva de Prado (2019), o instituto configura um robusto sistema de controles epistêmicos, funcionando como uma "forma-garantia" voltada a assegurar a "mesmidade" do vestígio — ou seja, a identidade absoluta entre o elemento colhido no local do crime e aquele valorado pelo magistrado. Contudo, a literatura especializada aponta para um persistente descompasso entre a densidade normativa da lei e a dinâmica pragmática da polícia judiciária, marcada pela urgência na colheita de elementos informativos.

No cotidiano das unidades policiais, a pressão por resolutividade e os prazos exíguos para a lavratura de autos de prisão em flagrante impõem uma lógica de atuação em que o rigor pericial muitas vezes cede espaço à necessidade imediata de avançar na investigação. Azevedo e Vasconcellos (2011) demonstram que deficiências estruturais, como o déficit de recursos humanos qualificados e problemas logísticos, deterioram a qualidade do trabalho

investigativo, forçando a adoção de critérios gerenciais de produtividade em detrimento do protocolo técnico-científico. Esse cenário fragiliza as etapas iniciais de isolamento e fixação (art. 158-B, II e III), as quais são cruciais para evitar a contaminação de vestígios que, por sua natureza binária, gozam de extrema volatilidade e fragilidade.

3.2. A Função dos Agentes na Gestão da Prova Digital: O Manejo de Dispositivos Móveis

A autoridade policial, ao presidir o inquérito, assume o múnus de coordenar a arrecadação de elementos que lastreiem a futura ação penal, delegando ao escrivão a responsabilidade pela formalização e guarda dos objetos apreendidos. No contexto da prova digital, o manejo de dispositivos como smartphones revela-se o ponto de maior fricção entre a eficácia investigativa e a preservação da cadeia de custódia. A jurisprudência do Superior Tribunal de Justiça (STJ) tem enfrentado casos em que a denominada "vistoria policial" — o acesso direto e não documentado ao conteúdo de aparelhos pela equipe de investigação — acarreta a quebra irremediável da custódia probatória.

Embora o art. 158-C do CPP determine que a coleta deve ser realizada preferencialmente por perito oficial, a prática demonstra que o primeiro contato com o vestígio digital ocorre frequentemente por agentes de polícia judiciária sem formação técnica específica. Conforme aduz Badaró (2023), a falta de documentação minuciosa e o registro indevido de etapas, como a extração de dados via *print screens* sem a geração de código *hash*, retira a fiabilidade do material, pois impossibilita aferir se houve manipulação ou perda de dados durante o período em que o

dispositivo esteve sob tutela estatal. A integridade da prova, nestes termos, depende da observância de diretrizes como a NBR ISO/IEC 27037:2013, que preconiza a auditabilidade, repetibilidade e justificabilidade de cada interação com a fonte digital.

3.3. Limites da Discricionariedade e o Combate Às Práticas de Fishing Expedition

O poder discricionário conferido à autoridade policial para a requisição de diligências (art. 14, CPP) não é absoluto e encontra limites intransponíveis no direito à autodeterminação informacional e na privacidade do investigado. A ausência de regras específicas para a coleta de dados digitais na Lei nº 13.964/2019 criou lacunas normativas que, segundo a doutrina de Moraes da Rosa (2021), permitem a ocorrência de pescarias probatórias especulativas (*fishing expedition*), nas quais o Estado devassa a intimidade do sujeito em busca de crimes alheios ao objeto da investigação.

A legitimidade da atividade estatal é, portanto, objeto de controle de legalidade e não um parâmetro de confiança autoproclamado pelo Estado-acusação. A quebra da cadeia de custódia digital, pela inobservância do rito pericial adequado, projeta-se sobre a admissibilidade da prova. Atualmente, consolidam-se duas vertentes interpretativas: a primeira, defendida por Prado (2014), sustenta que a violação de qualquer elo da cadeia conduz à inadmissibilidade imediata da prova por violação ao devido processo legal. A segunda, observada em precedentes recentes da Sexta Turma do STJ, propõe que a irregularidade deve ser sopesada pelo magistrado no campo da valoração, podendo a prova ser mantida se outros elementos corroborarem sua higidez. Todavia, no campo das evidências binárias, a Quinta Turma do STJ tem reafirmado que é ônus do

Estado comprovar a integridade das fontes de prova, sendo inadmissível presumir a veracidade de laudos policiais quando descumpridos os protocolos de custódia.

3.4. Reflexão Crítica: O Abismo Entre o Modelo Teórico e a Institucionalização da Precariedade

Em conclusão a este tópico, a proposta teórica da cadeia de custódia digital é tecnicamente robusta e essencial para a higidez do Estado Democrático de Direito, funcionando como um freio contra arbítrios e erros judiciários. Contudo, sua efetivação no Brasil esbarra em um "Estado de Coisas Inconstitucional" que permeia as polícias judiciárias. A problematização das lacunas normativas revela que, sem a efetiva implementação de Centrais de Custódia (art. 158-E) e sem o aparelhamento tecnológico dos Institutos de Criminalística, a cadeia de custódia corre o risco de tornar-se uma "folha de papel" sem eficácia prática. A profissionalização técnica dos agentes e o abandono de uma cultura inquisitorial de "olhadinhas" informais são requisitos *sine qua non* para que a prova digital deixe de ser uma zona de incerteza e passe a ser um instrumento genuíno de justiça e proteção de garantias fundamentais.

4. A QUEBRA DA CADEIA DE CUSTÓDIA E OS DESAFIOS À HIGIDEZ DA PROVA DIGITAL: UMA ANÁLISE SOB O PRISMA DOS CONTROLES EPISTÊMICOS

A quebra da cadeia de custódia (*break on the chain of custody*) não se limita a uma mera irregularidade procedimental, mas configura a interrupção da sequência cronológica e lógica que assegura a rastreabilidade e a imutabilidade do vestígio. No contexto da prova digital, essa ruptura adquire contornos críticos devido à

imaterialidade, volatilidade e fragilidade intrínsecas aos dados binários, os quais podem ser alterados ou suprimidos de forma imperceptível por qualquer intervenção inadequada. Sob a perspectiva de Prado (2014), o instituto funciona como um dispositivo de proteção contra interferências externas capazes de falsificar o resultado da atividade probatória, sendo um elemento central de controle do decisionismo judicial e da integridade do processo penal.

4.1. A Divergência Jurisprudencial no STJ: Entre a Inadmissibilidade e a Valoração Probatória

A omissão legislativa no "Pacote Anticrime" (Lei nº 13.964/2019) quanto às consequências jurídicas específicas da quebra da cadeia de custódia gerou uma cisão interpretativa no Superior Tribunal de Justiça (STJ). Conforme aponta Badaró (2018), existem duas vertentes teóricas que se refletem nas decisões das turmas criminais:

1. Corrente da Inadmissibilidade: sustenta que a cadeia de custódia é uma "forma-garantia" indissociável do devido processo legal. A inobservância dos elos procedimentais acarretaria a ilicitude da prova por violação de norma legal e constitucional, impondo sua exclusão e desentranhamento físico dos autos (art. 157, CPP). Esse entendimento é fortalecido pela Quinta Turma do STJ, que, no julgamento do AgRg no RHC nº 143.169/RJ, decidiu que o ônus de comprovar a integridade da prova recai sobre o Estado, não se admitindo a presunção de legalidade quando o rito é ignorado.

2. Corrente da Valoração: adotada em alguns precedentes pela Sexta Turma do STJ, esta vertente defende que a quebra não enseja nulidade obrigatória, mas deve ser sopesada pelo magistrado no campo da valoração, diminuindo a força probante da evidência em face do grau de desconfiança gerado pela violação.

Todavia, em matéria de prova informática, a jurisprudência caminha para um rigor técnico superior. A ausência de registro do código *hash* e a falta de documentação do manuseio de aparelhos eletrônicos são vistas como falhas que retiram a fidedignidade do elemento informático, afetando diretamente a "mesmidade" da prova e a sua capacidade de suportar uma condenação.

4.2. O Impacto da "Vistoria Policial" e a Reserva de Jurisdição Sobre a Intimidade Digital

Um dos problemas mais agudos na prática das delegacias brasileiras, como discutido anteriormente, é a denominada "olhadinha" ou vistoria preliminar não periciada em dispositivos móveis. A autoridade policial, sob o pretexto de urgência, manuseia o celular e extrai *prints* de conversas antes do envio ao Instituto de Criminalística, comprometendo a integridade total do fluxo comunicativo.

A jurisprudência consolidada estabelece que o acesso aos dados telemáticos e de comunicações privadas exige autorização judicial específica, mesmo em prisões em flagrante, sob pena de nulidade absoluta. A extração unilateral de capturas de tela pela polícia judiciária, sem o uso de *softwares* certificados e auditáveis, viola os aspectos essenciais das evidências digitais: auditabilidade,

repetibilidade, reprodutibilidade e justificabilidade. Como assevera Lopes Jr. (2020), o contraditório deve ser garantido tanto na dimensão do direito à informação quanto na efetiva igualdade de armas, o que é impossibilitado quando o Estado apresenta uma prova cuja origem e integridade não podem ser tecnicamente conferidas pela defesa.

4.3. Propostas para Um Protocolo Policial Garantista e a Realidade Estrutural

A implementação de um protocolo de atuação policial garantista demanda a superação do "amadorismo investigativo". Propõe-se, em linha com a norma ABNT NBR ISO/IEC 27037:2013, a obrigatoriedade da realização de espelhamento forense (*bit a bit*) e a geração imediata de assinaturas digitais (código *hash*) no momento da apreensão.

Contudo, observa-se um descompasso entre a robustez teórica e a precariedade estrutural das polícias judiciárias. A ineficiência estatal no cumprimento das dez etapas do art. 158-B do CPP fragiliza a integridade probatória. A atuação do Juiz das Garantias, introduzida pela Lei nº 13.964/2019, surge como fiscal indispensável da legalidade probatória, devendo exercer um controle preventivo para evitar a contaminação do processo por provas obtidas com quebra de custódia.

5. CONSEQUÊNCIAS JURÍDICAS DA QUEBRA DA CADEIA DE CUSTÓDIA: O RIGOR TÉCNICO COMO CONDIÇÃO DE VALIDADE DA CONDENAÇÃO

5.1. Síntese dos Achados: A Indispensabilidade do Rigor Epistêmico

A análise transversal realizada revela que a observância da cadeia de custódia não constitui mera formalidade procedimental ou burocrática, mas um rigoroso sistema de controles epistêmicos indispensável à validade da prova no processo penal contemporâneo. A prova digital, por sua natureza ontologicamente distinta, exige uma "forma-garantia" que neutralize o "princípio da desconfiança processual". A utilização de mecanismos como o algoritmo *hash* e o espelhamento *bit a bit* deixou de ser uma escolha discricionária da autoridade policial para se tornar um requisito técnico de existência e validade da evidência.

5.2. O Paradigma Jurisprudencial do STJ e do STF

Conforme discutido, o STJ tem construído um balizamento progressivamente rigoroso. No emblemático julgamento do AgRg no RHC nº 143.169/RJ, a Quinta Turma estabeleceu que é ônus do Estado comprovar a integridade das fontes de prova, afastando a presunção de legalidade em casos de descumprimento do rito. No âmbito do Supremo Tribunal Federal (STF), a discussão converge para a proteção da privacidade e da autodeterminação informacional (Art. 5º, X e XII, CF/88). No julgamento do ARE 1.042.075/RJ (Tema 990) e na análise da ADI 6.298 (referente ao Juiz das Garantias), a Corte reforçou o papel do Judiciário como fiscal da legalidade na coleta da prova, impedindo que a urgência investigativa atropеле direitos fundamentais.

CONCLUSÃO

A análise desenvolvida permite afirmar que a cadeia de custódia da prova digital não se configura como mera formalidade procedimental, mas como um verdadeiro instrumento epistêmico

de legitimação da atividade probatória no processo penal contemporâneo. A natureza ontologicamente distinta da prova digital — caracterizada por sua imaterialidade e volatilidade — impõe a superação de modelos tradicionais baseados em presunções de veracidade absoluta dos agentes públicos.

A incorporação normativa pela Lei nº 13.964/2019 representa um avanço significativo, mas sua eficácia encontra limites na realidade estrutural das instituições brasileiras. O descompasso entre a densidade normativa e a prática investigativa cotidiana tensiona os fundamentos do Estado Democrático de Direito. Conclui-se que a quebra da cadeia de custódia da prova digital deve ser compreendida como um vício capaz de comprometer a própria existência jurídica da prova, uma vez que a ausência de rastreabilidade inviabiliza o exercício efetivo do contraditório e da ampla defesa. A validade da condenação está indissociadamente vinculada à higidez técnica; somente o cumprimento estrito do art. 158-B do CPP é capaz de afastar o arbítrio e legitimar o exercício do *jus puniendi*.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **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.

AVENA, Norberto. **Processo Penal**. 15. ed. Rio de Janeiro: Método, 2023.

AZEVEDO, Rodrigo Ghiringhelli de; VASCONCELLOS, Fernanda Bestetti de. O inquérito policial em questão. **Sociedade e Estado**,

Brasília, v. 26, n. 1, 2011.

BADARÓ, Gustavo Henrique. A cadeia de custódia e sua relevância para a prova penal. In: SIDI, Ricardo; LOPES, Anderson Bezerra (org.). **Temas atuais da investigação preliminar no processo penal**. Belo Horizonte: D'Plácido, 2018. p. 517-538.

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

BATITUCCI, Eduardo Cerqueira. **A produção da prova pericial na justiça criminal brasileira**. Belo Horizonte: Letra e Voz, 2021.

BRASIL. [Código de Processo Penal (1941)]. **Decreto-Lei nº 3.689**, de 3 de outubro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm.

BRASIL. **Lei nº 13.964**, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm.

LIMA, Renato Brasileiro de. **Manual de processo penal**: volume único. 10. ed. Salvador: JusPodivm, 2021.

LOPES JÚNIOR, Aury. **Direito processual penal**. 18. ed. São Paulo: Saraiva Educação, 2021.

MINTO, Andressa Olmedo. **A prova digital e a cadeia de custódia no processo penal**. São Paulo: Tirant lo Blanch, 2021.

MISSE, Michel. **O inquérito policial no Brasil:** uma pesquisa empírica. Rio de Janeiro: Booklink, 2010.

MORAIS DA ROSA, Alexandre. **Guia do processo penal conforme a teoria dos jogos.** 6. ed. Florianópolis: EMais, 2021.

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

PRADO, Geraldo. **Prova penal e sistema de controles epistêmicos:** a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

¹ Professora adjunta B 4 da Universidade Federal de Rondônia - UNIR, com trajetória acadêmica interdisciplinar entre o Direito e a Educação. Doutora em Educação pela UNIMEP/Piracicaba (2016), mestre em Direito pela Universidade de Ribeirão Preto - UNAERP- (2003) e graduada em Direito pela Instituição Toledo de Ensino de Bauru- ITE- (1996). Exerceu a função de chefe de departamento de direito de março de 2023 a março de 2024. Concluiu pós doutorado em ciência jurídica na UENP (Jacarezinho/PR) em fevereiro de 2026.

² Doutoranda em Direito na FUNIBER - Fundación Universitaria Iberoamericana) desde Janeiro/2026. Mestra em Ciência Jurídica pela Universidade Estadual Norte do Paraná - UENP. Professora de Direito em Regime Especial (CRES) na UENP - Universidade Estadual Norte do Paraná, desde 07/2024. Professora de Ensino Superior no Centro Estadual de Educação Tecnológica Paula Souza/ Faculdade de Tecnologia de Jahu desde 05/02/2026. Pesquisadora integrante do Igualdade, Reconhecimento e Inclusão Social: Minorias e Grupos Vulneráveis - IRIS (endereço de acesso:

dgp.cnpq.br/dgp/espelhogrupo/4411113930848069). Pesquisadora Integrante do Grupo de Pesquisa Direito, Democracia e Novas Tecnologias da UENP (endereço de acesso: <http://dgp.cnpq.br/dgp/espelhogrupo/825800>). Professora Coordenadora do Projeto de Extensão "CARTILHAS DE INFORMAÇÃO DO PROGRAMA "EU ME PROTEJO": CAPACITAÇÃO DE PROFESSORES DA EDUCAÇÃO INFANTIL E DOS PRIMEIROS ANOS DO ENSINO FUNDAMENTAL PARA ABORDAGEM DE TEMAS RELACIONADOS À PREVENÇÃO E COMBATE À VIOLÊNCIA INFANTIL" na UENP. Professora colaboradora do Projeto de Extensão "CARTILHAS DE INFORMAÇÕES SOBRE JULGAMENTO COM PERSPECTIVA DE GÊNERO: ESCLARECIMENTO AOS SERVIDORES DOS TRIBUNAIS DE JUSTIÇA E DO MINISTÉRIO PÚBLICO DO PARANÁ". Professora integrante da Comissão de Eventos da Uenp. Professora Coordenadora da comissão da IV Feira de Profissões 2025 da UENP no Campus de Jacarezinho/PR. Professora de Pós-graduação em Direito Previdenciário da UNOESTE - Campus de Jaú/SP. Advogada. Atuante desde 2004, avaliadora da Revista Direito e Cidadania da UEMG Passos (ISSN: 2526-4753).

³ Mestrando em direito pela Fundação Iberoamericana - Funiber (2026). Especialista em Direito Penal e Direito Processual Penal pela FAMART (2024). Especialista em gestão ambiental pelo Centro Universitário Claretiano (2009). Bacharel em Direito pelas Faculdades Integradas de Jahu (2018). Técnico em logística pela Fatec/Jaú (2006). Escrivão de polícia do estado de São Paulo.