REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

CADEIA DE CUSTÓDIA – PROVAS DIGITAIS

CHAIN OF CUSTODY – DIGITAL EVIDENCE

Ciências Sociais Aplicadas • 02/07/2026

REGISTRO DOI: 10.70773/revistatopicos/782795563

Jardson Ferreira da Silva

RESUMO

A crescente digitalização das relações sociais e a expansão dos crimes praticados em ambientes virtuais tornaram as provas digitais elementos cada vez mais relevantes na persecução penal contemporânea. Nesse contexto, a cadeia de custódia assume papel fundamental para assegurar a autenticidade, integridade, confiabilidade e rastreabilidade das evidências eletrônicas, desde sua coleta até sua apresentação em juízo. O presente artigo analisa o instituto da cadeia de custódia aplicado às provas digitais, abordando seus fundamentos conceituais, evolução histórica, disciplina normativa e etapas previstas no Código de Processo Penal após a Lei nº 13.964/2019. Examina-se, ainda, a jurisprudência recente do Superior Tribunal de Justiça acerca das consequências decorrentes da quebra da cadeia de custódia em evidências digitais, especialmente em casos envolvendo extração inadequada de dados, ausência de documentação técnica, corrupção de arquivos eletrônicos e falhas na preservação da integridade dos vestígios informáticos. Conclui-se que a cadeia de custódia constitui garantia indispensável ao devido processo legal, ao contraditório e à ampla defesa, funcionando como mecanismo de controle da confiabilidade da prova digital e limite ao exercício do poder punitivo estatal. Sua observância rigorosa é condição essencial para a admissibilidade e valoração legítima das evidências digitais no processo penal.

Palavras-chave: Cadeia de custódia; Provas digitais; Processo penal; Integridade; Autenticidade; Contraditório; Rastreabilidade.

ABSTRACT

The increasing digitalization of social relations and the expansion of crimes committed in virtual environments have made digital evidence an increasingly relevant element in contemporary criminal prosecution. In this context, the chain of custody plays a

fundamental role in ensuring the authenticity, integrity, reliability, and traceability of electronic evidence, from its collection to its presentation before the courts. This article analyzes the institute of the chain of custody applied to digital evidence, addressing its conceptual foundations, historical development, legal framework, and the procedural stages established by the Brazilian Code of Criminal Procedure after Law No. 13,964/2019. It also examines recent case law of the Brazilian Superior Court of Justice regarding the consequences of breaches in the chain of custody of digital evidence, particularly in cases involving improper data extraction, lack of technical documentation, corruption of electronic files, and failures in preserving the integrity of digital traces. The study concludes that the chain of custody constitutes an essential guarantee of due process of law, adversarial proceedings, and the right to a full defense, functioning as a mechanism for controlling the reliability of digital evidence and limiting the exercise of the State's punitive power. Its strict observance is an indispensable condition for the admissibility and legitimate evaluation of digital evidence in criminal proceedings.
Keywords: Chain of custody; Digital evidence; Criminal proceedings; Integrity; Authenticity; Adversarial principle; Traceability.

1. INTRODUÇÃO

A intensificação dos avanços tecnológicos e a progressiva informatização das relações sociais impuseram novos desafios à persecução penal, notadamente no que se refere à produção, conservação e valoração das provas digitais. A sociedade contemporânea, cada vez mais dependente de recursos informáticos, assiste também à migração dos delitos tradicionais para o ambiente virtual, culminando no surgimento de práticas

criminosas mediadas por sistemas computacionais — os denominados crimes cibernéticos ou delitos digitais.

Nesse cenário, os vestígios outrora limitados ao mundo físico passaram a se manifestar em suportes digitais. Os indícios relevantes à instrução penal — muitas vezes os únicos elementos hábeis à comprovação da materialidade e autoria delitivas — agora residem em ambientes eletrônicos, com estrutura e dinâmica próprias. Essa transição demanda não apenas o aprimoramento dos métodos investigativos, mas, sobretudo, a adoção de protocolos técnicos que garantam a autenticidade, integridade, confiabilidade e rastreabilidade das evidências digitais.

É nesse contexto que se impõe a importância do instituto da cadeia de custódia da prova digital, cujo objetivo precípuo é preservar, documentar e controlar, de forma contínua, todo o percurso da evidência, desde sua coleta no local do crime ou na fonte de armazenamento até sua apresentação em juízo. A ruptura ou inobservância dessa cadeia compromete, irremediavelmente, a validade probatória da evidência digital, com implicações diretas sobre os princípios do contraditório, da ampla defesa e da verdade real.

A dificuldade, contudo, reside na inadequação da legislação vigente. A Lei nº 13.964/2019, ao disciplinar a cadeia de custódia (arts. 158-A e seguintes do CPP), preocupou-se essencialmente com vestígios físicos, não oferecendo diretrizes específicas para os elementos de natureza digital. Essa lacuna normativa impõe ao intérprete e aos operadores do direito — em especial aos magistrados, membros do Ministério Público, delegados de polícia e advogados — o desafio de

adaptar os parâmetros legais aos contornos técnicos e voláteis das provas eletrônicas.

A prova digital exige cuidados excepcionais em virtude de sua alta volubilidade, facilidade de adulteração e risco de perda definitiva com simples manipulações. Nesse aspecto, a atuação de peritos criminais especializados em informática forense revela-se imprescindível, sendo esses os profissionais tecnicamente habilitados para realizar a extração, preservação, análise e interpretação dos dados eletrônicos de forma metodologicamente segura.

Para que a prova digital possa ser admitida e valorada validamente no processo penal, é imperativa a observância rigorosa dos protocolos de cadeia de custódia, assegurando a rastreabilidade de todos os atos de apreensão, armazenamento, transporte, análise e guarda da evidência. A ruptura não justificada desses elos pode ensejar a exclusão probatória, por força dos princípios da legalidade das provas (art. 5º, LVI, da CF) e da proibição de provas ilícitas.

Dessa forma, o Estado-juiz, ao avaliar provas digitais, deve verificar a regularidade procedimental da cadeia de custódia e, inexistindo registro completo e documentado de todas as fases de manuseio da evidência, deve proceder à sua desconsideração. A confiabilidade da prova não pode ser presumida — ela deve ser demonstrada, nos autos, de forma transparente e tecnicamente fundamentada.

Em conclusão, o processo penal moderno, diante da nova realidade informacional, exige a conciliação entre os princípios tradicionais do devido processo legal e as exigências técnicas inerentes à era digital. A cadeia de custódia da prova digital, portanto, emerge como

instrumento imprescindível para legitimar a atuação estatal no exercício do ius puniendi, garantindo não apenas a eficácia da persecução penal, mas, sobretudo, a proteção dos direitos fundamentais do acusado.

1. CONCEITO

Doutrinário

De acordo com o doutrinador **Douglas Fischer,** o conceito doutrinário da cadeia de custódia:

> *Nada mais é do que a preservação e o registro do caminho da prova, desde sua coleta até a apreciação pelo Poder Judiciário.*

O doutrinador Aury Lopes Jr. conceitua este instituto da seguinte forma:

> *A cadeia de custódia diz respeito ao conjunto de procedimentos concatenados, como uma corrente, que se destina a preservar a integridade da prova, sua confiabilidade e sua legalidade. Existem diferentes morfologias para a cadeia de custódia, conforme o tipo de prova penal.*

Legal

Já o conceito legal encontra-se no **artigo 158-A do Código de Processo Penal (CPP):**

> *Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.*

Observa-se que no conceito obtido através da legislação processual penal, é utilizado o termo vestígio, diferentemente da concepção estabelecida pelo doutrinador, que emprega a palavra prova.

Apesar da utilização de termos distintos, o significado de Cadeia de Custódia não é prejudicado, vez que nas palavras de Alexandre Herculano e Amanda Melo, os vestígios podem ser definidos como:

> *"Todos os tipos de objetos, marcas, ou sinais sensíveis que possam ter relação com o fato investigado. Assim, vestígio é todo objeto ou material bruto constatado e/ou recolhido em um local de crime para análise posterior"*

No momento que os peritos forenses chegam à conclusão de que tal vestígio está de fato relacionado ao evento periciado, ele deixará de ser um vestígio e passará a denominar-se evidência.

Já o termo prova, mesmo possuindo vários significados, é compreendido processualmente como a produção dos meios e atos praticados no processo de convencimento do juiz sobre a veracidade, ou não, de um fato que interesse à solução da lide.

Assim, partindo da análise dos conceitos supramencionados, entende-se que o instituto da cadeia de custódia é uma metodologia que visa comprovar, documental e ininterruptamente, os atos que sucederam a fonte de prova, desde sua recolha, o traslado e a conservação dos indícios e vestígios obtidos no curso de uma investigação criminal.

Para sua concretização, é imprescindível que sejam percorridas determinadas etapas concatenadas, de forma a assegurar a autenticidade, integridade e inalterabilidade das provas.

Trata-se, portanto, de um procedimento de documentação ininterrupta, que se inicia a partir do encontro do vestígio, até a sua juntada no processo, sendo certificado onde, como e sob qual supervisão foram mantidos os objetos que interessam à reconstrução verídica dos fatos.

Jurisprudencial

No âmbito jurisprudencial, o **Superior Tribunal de Justiça (STJ)** define:

> *"A cadeia de custódia da prova consiste no caminho que deve ser percorrido pela prova até a sua análise pelo magistrado, sendo certo que qualquer interferência indevida durante esse trâmite processual pode resultar na sua imprestabilidade" (STJ, 5ª Turma, RHC 77.836/PA, Rel. Min. Ribeiro Dantas, julgado em 05/02/2019).*

II. ORIGENS

Origens Históricas

O conceito de cadeia de custódia está relacionado à evolução do processo penal moderno e à valorização do **devido processo legal.** Entre os séculos XIX e XX, com o fortalecimento do Estado de Direito e das garantias processuais, cresceu a preocupação em evitar condenações injustas baseadas em provas corrompidas ou manipuladas.

A experiência dos sistemas jurídicos **anglo-saxões** (EUA e Reino Unido) foi determinante: nesses países, a noção de *chain of custody* consolidou-se como requisito essencial para a admissibilidade da prova, especialmente em processos criminais envolvendo evidências físicas, digitais ou toxicológicas.

Direito Comparado – Estados Unidos

Nos países de tradição *common law*, a *chain of custody* ganhou força a partir de casos emblemáticos em que a integridade da prova foi questionada:

O Caso mais famoso - O. J. Simpson

O exemplo mais famoso nos EUA ocorreu em 1994, quando o ex-jogador e ator **O. J. Simpson** foi acusado do assassinato de sua ex-esposa Nicole Brown Simpson e do amigo Ronald Goldman, em Los Angeles. O julgamento, transmitido ao vivo, tornou-se um marco do direito penal norte-americano.

A acusação baseava-se em provas físicas e biológicas, tais como:

- manchas de sangue encontradas no local do crime e no carro de Simpson;
- luvas ensanguentadas (uma na cena do crime e outra em sua residência);
- fios de cabelo e amostras de DNA.

Problemas na Cadeia de Custódia

A defesa explorou diversas falhas na custódia das provas, enfraquecendo o caso da promotoria:

Contaminação de provas biológicas:

Policiais foram acusados de manusear amostras sem luvas e sem os cuidados técnicos necessários, gerando risco de contaminação.

Armazenamento impróprio:

Amostras de sangue foram armazenadas em condições inadequadas, o que levou à degradação do material genético e

fragilizou os exames de DNA (então ainda recentes).

Documentação incompleta:

Houve falhas no registro do percurso das provas. Em alguns momentos, não era possível identificar quem havia manuseado os vestígios.

A luva ensanguentada:

Durante o julgamento, Simpson experimentou a luva encontrada, que aparentava ser pequena demais para suas mãos. A defesa sugeriu manipulação ou deterioração da prova, reforçando a falta de confiabilidade da custódia.

Resultado do Caso:

Em 1995, o júri absolveu O. J. Simpson, considerando que as falhas na cadeia de custódia tornaram as provas apresentadas pouco confiáveis.

Esse caso mostrou como brechas na cadeia de custódia podem comprometer até mesmo provas aparentemente irrefutáveis, como sangue, DNA e objetos com vestígios biológicos.

2. BRASIL – CONSOLIDAÇÃO DA CADEIA DE CUSTÓDIA

2.1. Casos Paradigmáticos

Caso da Escola Base (São Paulo, 1994)

Embora não tenha resultado em persecução penal final, este episódio é emblemático para demonstrar a importância da integridade probatória. A polícia e a imprensa divulgaram provas frágeis e mal preservadas que levaram à incriminação injusta dos proprietários da escola. A ausência de rigor na coleta e guarda dos indícios provocou uma tragédia social e jurídica, com consequências irreparáveis para os acusados.

Caso Isabella Nardoni (São Paulo, 2008)

O homicídio da menina Isabella chamou atenção nacional para a preservação da cena do crime. A defesa tentou contestar laudos periciais sobre marcas de sangue e fios de cabelo, alegando falhas na preservação do local. Embora a condenação dos acusados tenha sido mantida, o caso reforçou, perante a opinião pública e a comunidade pericial, a relevância da cadeia de custódia como garantia de confiabilidade das provas.

Operação Lava Jato (2014 em diante)

Nesta operação, diversas defesas questionaram a validade de provas digitais — e-mails, planilhas e registros extraídos de sistemas da Petrobras e de empreiteiras. Argumentou-se que não havia clareza quanto à cadeia de custódia desses arquivos eletrônicos, sobretudo em relação à apreensão e preservação da integridade dos dados. O debate jurídico sobre o tema foi um dos principais fatores que impulsionaram a formalização da cadeia de custódia no ordenamento jurídico brasileiro, consolidada pelo Pacote Anticrime (Lei nº 13.964/2019), que inseriu os artigos 158-A a 158-F no CPP.

3. EVOLUÇÃO LEGISLATIVA NO BRASIL

A consolidação legislativa da cadeia de custódia no Brasil ocorreu com a **Lei nº 13.964/2019 (Pacote Anticrime),** que acrescentou ao Código de Processo Penal os **arts. 158-A a 158-F.**

Principais Inovações Legislativas

- **Art. 158-A** – Define a cadeia de custódia como "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

- **Art. 158-B** – Estabelece as etapas da cadeia de custódia: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte.

- **Arts. 158-C a 158-F** – Regulam os responsáveis pela custódia, a forma de registro, os efeitos da quebra da cadeia e as consequências jurídicas decorrentes.

3.1. Marcos Normativos Complementares

Além do CPP, diversas normas reforçam a disciplina da cadeia de custódia no Brasil:

- **Constituição Federal (1988) –** Garante os fundamentos constitucionais: devido processo legal (art. 5º, LIV), contraditório e ampla defesa (art. 5º, LV) e inadmissibilidade de provas ilícitas (art. 5º, LVI).

- **Lei nº 11.690/2008 –** Alterou dispositivos do CPP relativos à prova, introduzindo a noção de vestígios e reforçando a centralidade da perícia oficial.

- **Resoluções do CNJ e do CNMP –** Definiram parâmetros técnicos para coleta, guarda e preservação de vestígios, especialmente em casos complexos ou envolvendo provas digitais.

III. ETAPAS DA CADEIA DE CUSTÓDIA.

As etapas da cadeia de custódia estão previstas no **artigo 158-B do Código de Processo Penal,** que disciplina o rastreamento do vestígio desde o seu reconhecimento até o descarte final.

A seguir, apresentam-se as fases enumeradas pela legislação:

I. **n Reconhecimento**
   Consiste no ato de identificar um elemento como de potencial interesse para a produção da prova pericial.

II. **Isolamento**
   Visa evitar alterações no estado das coisas, assegurando a preservação do ambiente imediato, mediato e relacionado aos vestígios e ao local do crime.

III. **Fixação**
   Refere-se à descrição detalhada do vestígio, conforme encontrado na cena do crime ou no corpo de delito, bem como à sua posição na área de exame. Essa etapa pode ser complementada por fotografias, filmagens ou croquis, sendo

indispensável sua descrição no laudo pericial elaborado pelo perito responsável.

IV. **Coleta**

Trata-se do ato de recolher o vestígio destinado à análise pericial, respeitando suas características e natureza específicas.

V. **Acondicionamento**

Etapa na qual cada vestígio coletado é embalado de forma individualizada, em conformidade com suas características físicas, químicas e biológicas. Deve conter anotação de data, hora e identificação do responsável pela coleta e pelo acondicionamento.

VI. **Transporte**

Consiste na transferência do vestígio de um local para outro, em condições adequadas (embalagens, veículos, temperatura etc.), de forma a garantir a preservação de suas características originais e o controle da posse.

VII. **Recebimento**

Ato formal de transferência da posse do vestígio, que deve ser devidamente documentado. O registro deve conter, no mínimo: número do procedimento, unidade policial relacionada, local de origem, nome de quem realizou o transporte, código de rastreamento, natureza do exame, tipo de vestígio, protocolo, assinatura e identificação de quem recebeu.

VIII. **Processamento**

Etapa correspondente ao exame pericial em si, em que o

vestígio é manipulado conforme metodologias adequadas às suas características físicas, químicas e biológicas. O resultado deve ser formalizado em laudo produzido pelo perito oficial.

IX. **Armazenamento**
Refere-se à guarda do vestígio em condições apropriadas, seja para posterior processamento, realização de contraperícia, descarte ou transporte. Essa etapa deve estar vinculada ao número do laudo correspondente.

X. **Descarte**
Etapa final, que consiste na liberação ou eliminação do vestígio, observando a legislação vigente e, quando aplicável, mediante autorização judicial.

XI. **CONSEQUÊNCIAS DA QUEBRA DA CADEIA DE CUSTÓDIA**

XII. A discussão sobre os efeitos da quebra da cadeia de custódia é relevante tanto na doutrina quanto na jurisprudência. Em síntese, existem posições mais **moderadas, intermediárias** e **rigorosas** acerca do tema.

1. Doutrina

Guilherme de Souza Nucci

Adota posição **moderada.** Para o autor, a quebra da cadeia de custódia pode levar à invalidação da prova, mas a consequência dependerá da análise do caso concreto e do grau de comprometimento da confiabilidade do material probatório.

Eugênio Pacelli

Defende uma posição **intermediária.** Reconhece que nem toda

falha enseja nulidade da prova, mas sustenta que, quando houver comprometimento da fidedignidade do vestígio, este deverá ser desconsiderado.

Aury Lopes Jr.
Possui posição **rigorosa.** Para o processualista, qualquer quebra na cadeia de custódia compromete imediatamente a confiabilidade da prova, tornando-a *imprestável*, por ferir garantias constitucionais como o devido processo legal e a ampla defesa.

2. JURISPRUDÊNCIA

No plano jurisprudencial, há duas correntes principais acerca das consequências da quebra da cadeia de custódia (*break on the chain of custody*):

- **1ª Corrente – Nulidade e ilicitude da prova**

  Defende que a quebra gera a exclusão da prova e, por consequência, a nulidade das provas dela derivadas. Considera-se, portanto, causa de *ilicitude probatória*. O Superior Tribunal de Justiça (STJ) já adotou essa linha em precedentes como o HC 160.662 e o REsp 1.795.341.

- **2ª Corrente – Análise do caso concreto**

Sustenta que a quebra da cadeia de custódia não leva, necessariamente, à ilicitude ou nulidade da prova. O impacto deve ser avaliado conforme as circunstâncias, levando-se em conta se a falha comprometeu ou não a fidedignidade do vestígio.

PARTE - II

TÓPICO 01

1 - AgRg no HC 902.195-RS, Rel. Min. Joel Ilan Paciornik. **Embora as regras específicas dos artigos 158-A a 158-F do Código de Processo Penal não retroajam, a cadeia de custódia deve ser preservada, mesmo para fatos anteriores à Lei n. 13.964/2019.** STJ. 5ª Turma.AgRg no HC 902.195-RS, Rel. Min. Joel Ilan Paciornik, julgado em 3/12/2024.

Cadeia de custódia e prova digital antes da Lei nº 13.964/2019: leitura acadêmica do AgRg no HC 902.195/RS (STJ, 5ª Turma)

A consolidação da prova digital como elemento central da persecução penal contemporânea reposicionou o debate sobre **confiabilidade epistêmica** e **garantias processuais** no processo penal. Diferentemente dos vestígios materiais clássicos (arma, projétil, manchas), os dados armazenados em dispositivos eletrônicos são voláteis, facilmente alteráveis e, em muitos casos, irrecuperáveis quando submetidos a procedimentos inadequados. Nesse cenário, a cadeia de custódia não pode ser compreendida como formalidade burocrática, mas como condição de possibilidade do contraditório efetivo e da decisão judicial racionalmente justificável.

É precisamente nesse ponto que o Superior Tribunal de Justiça, no **AgRg no HC 902.195/RS,** julgado em 03/12/2024, sob relatoria do Min. Joel Ilan Paciornik (5ª Turma), promove relevante esclarecimento: **embora as regras específicas dos arts. 158-A a 158-F do CPP não retroajam, a preservação da cadeia de custódia deve ser observada mesmo em fatos anteriores à Lei nº 13.964/2019.** A decisão, ao afastar um argumento recorrente — o de

que a ausência de disciplina legal expressa no período impediria o controle de idoneidade do vestígio — reforça a ideia de que a cadeia de custódia decorre de garantias estruturantes do processo penal: **devido processo legal, ampla defesa, contraditório e prova lícita.**

1. O CASO E O PROBLEMA JURÍDICO: QUANDO A PROVA "SOME" POR FALHA ESTATAL

No caso, o homicídio ocorreu em 2018. A polícia apreendeu o celular da vítima e, mediante autorização judicial, realizou a extração de dados. As mensagens obtidas foram utilizadas como base para imputação de homicídio qualificado ao acusado. O ponto de inflexão, contudo, surge quando, em 2022, uma perícia técnica conclui que o dispositivo estava danificado, apresentando erro decorrente de procedimento inadequado de "***root***" realizado durante a extração.

O dado decisivo não é apenas a constatação de dano físico ou lógico do aparelho, mas a consequência jurídica: **tornou-se impossível verificar a integridade e autenticidade das mensagens** supostamente extraídas. Em termos probatórios, isso significa que o conteúdo que fundamenta a acusação não supera um "teste mínimo de confiabilidade", pois não pode ser auditado, reproduzido ou confrontado pela defesa.

O Tribunal de Justiça negara o habeas corpus sustentando que não seria possível aplicar retroativamente os arts. 158-A a 158-F do CPP (introduzidos pelo Pacote Anticrime). O STJ, no entanto, desloca o eixo do debate: **não se trata de retroatividade normativa,** mas de **controle de confiabilidade da prova,** exigência presente mesmo antes da positivação sistemática da cadeia de custódia.

A discussão acerca da cadeia de custódia da prova penal, especialmente no contexto das evidências digitais, ganhou relevo significativo no processo penal brasileiro a partir da consolidação jurisprudencial do Superior Tribunal de Justiça, ainda que antes da positivação sistemática introduzida pela Lei nº 13.964/2019. O julgamento do **AgRg no HC 902.195/RS,** pela Quinta Turma do STJ, constitui marco relevante nesse debate ao afirmar que, embora as regras específicas dos arts. 158-A a 158-F do Código de Processo Penal não possuam aplicação retroativa, a preservação da cadeia de custódia sempre foi exigência imanente ao devido processo legal, inclusive para fatos ocorridos antes da vigência do chamado Pacote Anticrime.

Os fatos que deram origem ao referido julgamento são emblemáticos e reveladores das fragilidades inerentes ao tratamento inadequado da prova digital. Em 2018, foi encontrado o corpo de uma vítima de homicídio, ocasião em que a autoridade policial apreendeu o aparelho celular pertencente ao falecido, considerando-o potencial fonte de informações relevantes para a elucidação do crime. Instaurado o inquérito policial, o juízo competente autorizou a extração dos dados armazenados no dispositivo. A partir de mensagens de texto supostamente obtidas do celular, a polícia concluiu que determinado indivíduo teria sido o autor do homicídio, o que culminou no oferecimento de denúncia por homicídio qualificado.

No curso da persecução penal, a defesa requereu a realização de perícia técnica no aparelho celular da vítima, pleito que foi deferido. Todavia, quando a perícia foi efetivamente realizada, já no ano de 2022, constatou-se que o dispositivo estava danificado e não permitia o acesso aos dados originalmente extraídos. O laudo

pericial foi categórico ao apontar que o celular apresentava erro decorrente de procedimento técnico inadequado de “root” realizado pela própria polícia durante a fase de extração das informações. Esse procedimento comprometeu o funcionamento do aparelho e inviabilizou tanto a recuperação dos arquivos quanto a verificação da integridade, autenticidade e completude das mensagens que embasaram a acusação.

O perito responsável esclareceu que, diante do estado do aparelho, não era possível afirmar se houve adulteração do conteúdo nem se as mensagens atribuídas à vítima correspondiam, de fato, aos dados existentes no momento da apreensão. Em outras palavras, a fonte primária da prova havia sido irremediavelmente comprometida, impossibilitando qualquer controle técnico posterior. Diante desse cenário, a defesa impetrou habeas corpus, sustentando a ocorrência de quebra da cadeia de custódia, a violação ao contraditório e à ampla defesa e, por consequência, a necessidade de exclusão das provas extraídas do celular, com o trancamento da ação penal.

O Tribunal de Justiça, contudo, denegou a ordem sob o argumento de que, à época dos fatos e da extração dos dados (2018), ainda não existiam no Código de Processo Penal dispositivos específicos regulando a cadeia de custódia, razão pela qual não seria possível aplicar retroativamente os arts. 158-A a 158-F, introduzidos apenas em 2019. Tal fundamentação, embora formalmente correta quanto à irretroatividade da lei processual mais gravosa, desconsiderou a natureza garantística do instituto da cadeia de custódia e sua vinculação direta aos princípios constitucionais do processo penal.

Ao apreciar o agravo regimental, o Superior Tribunal de Justiça reformou esse entendimento. A Corte reconheceu que a perícia não

conseguiu identificar se o aparelho apreendido apresentava sinais de adulteração, tampouco foi capaz de recuperar os arquivos que teriam fundamentado a acusação. Essa impossibilidade comprometeu de forma decisiva a eficácia probatória dos elementos de convicção extraídos da fonte digital, uma vez que não se demonstrou minimamente sua integridade e confiabilidade.

O STJ destacou que a situação configurou intolerável mitigação do exercício do contraditório, pois a defesa foi impedida de averiguar a existência, a integridade e o contexto das mensagens supostamente trocadas, as quais sustentavam a persecução penal. Sem acesso à fonte íntegra e sem possibilidade de auditoria técnica, a prova deixa de ser verificável, tornando-se incompatível com um processo penal orientado por garantias. Nessas circunstâncias, impõe-se a exclusão dos dados e a vedação de qualquer referência a eles nos autos.

De modo particularmente relevante, o Tribunal esclareceu que não se tratava de aplicar retroativamente os arts. 158-A a 158-F do CPP. A questão central residia no reconhecimento de que a preservação da cadeia de custódia sempre foi exigível, mesmo antes da Lei nº 13.964/2019, como decorrência lógica do devido processo legal, do contraditório, da ampla defesa e do direito à prova lícita. A positivação posterior apenas sistematizou e detalhou etapas de um dever estatal que já existia.

2. COMENTÁRIO DOGMÁTICO: CADEIA DE CUSTÓDIA COMO GARANTIA, NÃO COMO "NOVIDADE" LEGISLATIVA

A decisão do STJ é especialmente relevante por separar, com precisão, dois planos:

1. **Plano normativo-específico:** os arts. 158-A a 158-F do CPP, enquanto disciplina detalhada de etapas, formulários, agentes responsáveis e procedimentos;

2. **Plano constitucional-garantístico:** a cadeia de custódia como exigência derivada do **devido processo,** do **contraditório** e do **direito à prova lícita,** que impõe ao Estado o dever de demonstrar que o vestígio apresentado em juízo é confiável.

Ao afirmar que as regras específicas não retroagem, mas que a cadeia de custódia deve ser preservada, o STJ adota uma leitura coerente com a lógica do processo penal democrático: **a prova não se legitima por existir, mas por poder ser controlada.** O contraditório, nessa perspectiva, não é mera chance formal de "falar sobre" a prova; é a possibilidade real de **verificar origem, contexto, integridade e percurso do vestígio.**

Esse raciocínio se conecta ao conceito jurisprudencial anterior ao Pacote Anticrime, já expresso no **RHC 77.836/PA** (STJ, 5ª Turma, Rel. Min. Ribeiro Dantas, julgado em 12/02/2019), segundo o qual **a cadeia de custódia abrange todo o caminho da prova até sua análise pelo magistrado, sendo que qualquer interferência pode resultar em imprestabilidade.** A decisão de 2024, portanto, não cria uma regra nova; ela **confirma a continuidade** de um entendimento: a confiabilidade do vestígio sempre foi exigência de validade, apenas posteriormente sistematizada em lei.

3. O NÚCLEO GARANTÍSTICO DO JULGADO: PREJUÍZO AO CONTRADITÓRIO E EXCLUSÃO DA PROVA

O STJ identifica que o dano causado ao aparelho impediu a perícia de responder perguntas essenciais: o celular estava adulterado? as

mensagens eram autênticas? havia contexto íntegro das conversas? A impossibilidade de realizar tais verificações gera aquilo que o Tribunal descreve como **“intolerável mitigação ao exercício do contraditório”,** pois a defesa fica impedida de examinar o material probatório em sua fonte e em sua totalidade.

Aqui, o comentário acadêmico indispensável é o seguinte: **quando o Estado danifica o vestígio digital, ele não apenas perde um objeto; ele destrói uma condição processual de controle.** Não se trata de vício meramente formal. É **vício substancial,** pois torna impossível aferir se o dado probatório é verdadeiro, completo e não manipulado. A consequência, coerente com a dogmática da prova ilícita/inadmissível, é a exclusão do material e a vedação de referência a ele nos autos, já que qualquer valoração judicial passaria a se apoiar em elementos não verificáveis.

4. IMPLICAÇÕES TEÓRICAS: A CADEIA DE CUSTÓDIA COMO “PONTE” ENTRE TÉCNICA E LEGITIMIDADE

O caso é exemplar para demonstrar que a prova digital demanda uma “ponte” entre técnica e direito. Termos como *root*, extração e preservação não são detalhes periféricos: eles determinam se a evidência será **auditável** e **reprodutível.** Sem isso, a prova perde sua legitimidade epistêmica e, por consequência, sua legitimidade jurídica.

A lição central do AgRg no HC 902.195/RS é, portanto, dupla:

- a cadeia de custódia é **garantia do acusado** e **ônus do Estado,** pois incumbe ao aparato persecutório preservar o vestígio de modo que possa ser controlado;

- a positivação de 2019 organizou etapas e nomenclaturas, mas não “inventou” o dever de confiabilidade: ele já era exigível como desdobramento do **devido processo legal probatório.**

Ao reconhecer a quebra da cadeia de custódia em fato anterior ao Pacote Anticrime, o STJ firma entendimento de alta relevância: **a prova digital não pode sustentar acusação penal quando o próprio Estado inviabiliza sua verificação.** A decisão reafirma que o processo penal não admite condenação baseada em “provas de fé pública”, imunes à auditoria defensiva. A cadeia de custódia, nesse marco, é menos um ritual legal e mais um mecanismo de controle democrático do poder punitivo, garantindo que a verdade processual seja construída sob critérios de confiabilidade mínima e sob contraditório substancial.

Em suma:

Embora as regras específicas dos artigos 158-A a 158-F do Código de Processo Penal não retroajam, a cadeia de custódia deve ser preservada, mesmo para fatos anteriores à Lei n. 13.964/2019. STJ. 5ª Turma.AgRg no HC 902.195-RS, Rel. Min. Joel Ilan Paciornik, julgado em 3/12/2024 (Info 837).

TÓPICO 02

2 - AgRg no HC 828.054-RN, Rel. Min. Joel Ilan Paciornik**. A falta de procedimentos para garantir a idoneidade e integridade dos dados extraídos de um celular apreendido resulta na quebra da cadeia de custódia e na inadmissibilidade da prova digital.**

A crescente utilização de provas digitais no processo penal tem imposto ao sistema de justiça desafios inéditos, especialmente no

que se refere à preservação da confiabilidade, autenticidade e integridade dos elementos probatórios extraídos de dispositivos eletrônicos. Nesse contexto, a jurisprudência do Superior Tribunal de Justiça vem desempenhando papel central na consolidação do instituto da cadeia de custódia como garantia indispensável do devido processo legal. O julgamento do **AgRg no HC 828.054/RN,** pela Quinta Turma do STJ, em 23 de abril de 2024, representa um marco relevante ao afirmar, de forma categórica, que a ausência de procedimentos técnicos aptos a assegurar a idoneidade da prova digital resulta em sua inadmissibilidade, bem como na nulidade das provas dela derivadas.

Os fatos que ensejaram o julgamento revelam, com clareza, os riscos inerentes ao tratamento inadequado da prova digital. No caso concreto, um indivíduo foi preso em flagrante pela suposta prática do crime de tráfico de drogas, ocasião em que a polícia apreendeu o aparelho celular que estava em sua posse. Suspeitando que o flagranteado pudesse estar envolvido em outros delitos, a autoridade policial obteve autorização judicial para a quebra do sigilo dos dados telemáticos referentes às comunicações enviadas e recebidas por meio do dispositivo apreendido. O celular foi, então, encaminhado à perícia para a realização do procedimento de extração de dados, abrangendo conversas mantidas em aplicativos como WhatsApp, Facebook e Instagram.

Decorridos alguns dias, o perito encaminhou relatório ao delegado responsável, informando que a extração dos dados havia sido realizada por meio da técnica de "*print screen*" dos diálogos, uma vez que os equipamentos de extração forense disponíveis — a exemplo do software *Cellebrite* — não teriam sido capazes de realizar a leitura do dispositivo. A análise, segundo o próprio laudo,

ocorreu mediante consulta direta ao aparelho, sem a utilização de ferramentas forenses certificadas, em razão de limitações técnicas da versão do software disponível à polícia.

Com base exclusivamente nessas informações, extraídas por meio de capturas de tela, a polícia concluiu pela possível existência de uma organização criminosa voltada ao tráfico de drogas, o que levou o juízo competente a deferir medidas de busca e apreensão nas residências de outros investigados mencionados nas conversas. A persecução penal, portanto, foi significativamente ampliada a partir de provas digitais cuja origem, integridade e confiabilidade não haviam sido tecnicamente asseguradas.

Diante desse cenário, a defesa dos investigados atingidos pelas medidas de busca e apreensão impetrou habeas corpus, sustentando que toda a atuação estatal estava fundada em "*print screens*" desprovidos de qualquer mecanismo de verificação de integridade, como a geração de código *hash*. Argumentou-se que esse método de extração não assegura a preservação da cadeia de custódia, por se tratar de técnica rudimentar, altamente manipulável e incapaz de garantir a mesmidade entre o dado originalmente coletado e aquele apresentado no processo. Em razão disso, pleiteou-se a nulidade das provas extraídas do celular e de todas as demais provas delas decorrentes.

O Tribunal de Justiça denegou a ordem, sob o argumento de que a defesa não teria comprovado, de forma concreta, a quebra da cadeia de custódia. Contudo, ao apreciar o agravo regimental, o Superior Tribunal de Justiça reformou esse entendimento, reconhecendo que, no caso, não foram adotados procedimentos minimamente

idôneos para garantir a integridade e a confiabilidade dos dados extraídos do aparelho celular apreendido.

O STJ ressaltou que o instituto da cadeia de custódia, disciplinado pelos arts. 158-A e seguintes do Código de Processo Penal, tem por finalidade assegurar que os elementos probatórios sejam tratados de modo a evitar interferências que comprometam sua confiabilidade, desde a coleta até a valoração judicial. Em se tratando de provas digitais, essa exigência assume contornos ainda mais rigorosos, em razão da natureza volátil e facilmente alterável dos dados telemáticos. A simples captura de telas, desacompanhada de procedimentos técnicos de preservação, não permite verificar se houve alterações, supressões ou acréscimos no conteúdo originalmente existente no dispositivo.

O Tribunal destacou que a documentação de todas as etapas da obtenção da prova digital é condição essencial para que o procedimento seja verificável e auditável pelas partes. A ausência de registros técnicos impede o exercício efetivo do contraditório, pois inviabiliza a conferência dos métodos utilizados e a reprodução da análise por peritos independentes. Conceitos como auditabilidade, repetibilidade, reprodutibilidade e justificabilidade passam a integrar o núcleo essencial da prova digital válida, sendo assegurados apenas mediante a adoção de metodologias técnicas reconhecidas e certificadas, como aquelas recomendadas por normas técnicas especializadas.

Nesse contexto, o STJ enfatizou o **princípio da mesmidade,** segundo o qual o elemento probatório valorado pelo magistrado deve ser exatamente o mesmo que foi originalmente coletado, sem qualquer modificação ao longo da cadeia de custódia. Esse princípio

garante que a prova apresentada em juízo corresponda integralmente ao vestígio arrecadado durante a investigação, permitindo que acusação, defesa e julgador atuem com segurança epistêmica. A violação da mesmidade compromete a confiabilidade da prova e impede sua utilização legítima no processo penal.

Uma das técnicas mais relevantes para assegurar a mesmidade da prova digital é o uso de algoritmos *hash*, que funcionam como verdadeira "impressão digital" dos arquivos. Qualquer alteração, ainda que mínima, no conteúdo original gera um código *hash* completamente distinto, permitindo a verificação objetiva da integridade dos dados. A ausência desse procedimento, especialmente quando substituído por simples capturas de tela, impede qualquer controle técnico sobre a autenticidade da prova.

O julgamento também reafirma entendimento consolidado na Quinta Turma do STJ no sentido de que **o ônus de provar a integridade e a confiabilidade da prova é do Estado,** não sendo admissível presumir a veracidade dos elementos apresentados quando os procedimentos da cadeia de custódia não são observados. Tal orientação já havia sido firmada, por exemplo, no **AgRg no RHC 143.169/RJ,** no qual se reconheceu a inadmissibilidade de provas digitais extraídas sem registro documental dos procedimentos adotados pela polícia para a preservação da integridade e autenticidade dos dados.

Em síntese, o **AgRg no HC 828.054/RN** consolida o entendimento de que a prova digital, para ser admissível, deve ser produzida e preservada segundo critérios técnicos rigorosos, devidamente documentados e passíveis de auditoria. A utilização de métodos precários, como o "*print screen*", desacompanhados de mecanismos

de verificação de integridade, configura quebra da cadeia de custódia e torna a prova imprestável, bem como todas as medidas investigativas e probatórias dela derivadas. Trata-se de afirmação relevante para a proteção do contraditório substancial e para a contenção do poder punitivo estatal em um cenário de crescente digitalização da prova penal.

Em suma:

A falta de procedimentos para garantir a idoneidade e integridade dos dados extraídos de um celular apreendido resulta na quebra da cadeia de custódia e na inadmissibilidade da prova digital. STJ. 5ª Turma. AgRg no HC 828.054-RN, Rel. Min. Joel Ilan Paciornik, julgado em 23/4/2024.

TÓPICO 03

3 - AgRg no RHC 184.003-SP, Rel. Min. Daniela Teixeira, Rel. p/ Acórdão Min. Ribeiro Dantas. **A CORRUPÇÃO DE PARTE DOS ARQUIVOS COMPROMETE A INTEGRALIDADE DA PROVA, INVIABILIZANDO SUA UTILIZAÇÃO.**

A admissibilidade da prova digital no processo penal contemporâneo encontra limites rigorosos na exigência de preservação de sua integridade e completude, sob pena de comprometimento do contraditório, da paridade de armas e da própria racionalidade da decisão judicial. Esse entendimento foi reafirmado de maneira paradigmática pelo Superior Tribunal de Justiça no julgamento do **AgRg no RHC 184.003/SP,** ao reconhecer que a corrupção parcial de arquivos digitais apreendidos inviabiliza a utilização de toda a prova, bem como das evidências dela derivadas, nos termos do art. 157, § 1º, do Código de Processo Penal.

O caso analisado pelo STJ envolveu investigação instaurada em 2017 para apurar a suposta prática de crimes financeiros por dois sócios de uma empresa, incluindo delitos tributários, lavagem de dinheiro e organização criminosa. No curso das investigações preliminares, o juízo autorizou diversas medidas cautelares, dentre elas a busca e apreensão de computadores e dispositivos eletrônicos da empresa. Durante o cumprimento dos mandados, fiscais da Secretaria da Fazenda Estadual, devidamente autorizados, acessaram os equipamentos e procederam à extração de arquivos considerados relevantes para a persecução penal.

O procedimento técnico adotado consistiu na conexão de um HD externo aos computadores da empresa e na utilização de software específico para cópia dos arquivos, com a geração de códigos *hash* correspondentes, os quais, em tese, permitiriam a verificação da integridade dos dados copiados. Todo o material foi armazenado em um único HD, posteriormente entregue ao Ministério Público, que permaneceu com a custódia exclusiva do dispositivo por vários anos, sem que a defesa tivesse acesso direto ao suporte físico original.

Somente em 2022, após determinação judicial, a defesa teve acesso ao conteúdo dos arquivos apreendidos, os quais foram disponibilizados pelo Ministério Público por meio de links em nuvem. Ao tentar examinar o material, os advogados constataram que parte significativa dos arquivos digitais estava corrompida e completamente inacessível. Diante dessa constatação, a defesa contratou empresa especializada em perícia digital, que produziu laudo técnico confirmando a impossibilidade de leitura de diversos arquivos. Questionado, o Ministério Público reconheceu que teria ocorrido “algum tipo de erro” durante a extração realizada pela

Secretaria da Fazenda, mas sustentou que os arquivos corrompidos não haviam sido utilizados para embasar a denúncia.

Em resposta, a defesa requereu ao juízo de primeira instância a entrega do HD original para realização de perícia independente, bem como a apresentação de documentação técnica detalhada acerca dos procedimentos de extração e esclarecimentos sobre a origem e o momento da falha que corrompeu os dados. Tais pedidos foram indeferidos sob o argumento de que a inacessibilidade dos arquivos afetaria igualmente acusação e defesa, inexistindo prejuízo concreto, além de se afirmar que o HD consistiria apenas em suporte material, já tendo os documentos sido disponibilizados em formato digital.

Após a denegação de habeas corpus pelo Tribunal de Justiça, os investigados interpuseram recurso ordinário para o Superior Tribunal de Justiça, sustentando, em síntese, que a impossibilidade de acesso integral aos dados inviabilizava a verificação da integridade das provas, comprometia a paridade de armas e tornava impossível saber se o Ministério Público teria tido acesso ao conteúdo dos arquivos antes de sua corrupção. Argumentou-se, ainda, que a prova digital, por sua própria natureza, exige completude e rastreabilidade, de modo que a perda parcial dos dados comprometeria a validade de todo o conjunto probatório.

Ao apreciar o recurso, o STJ deu-lhe provimento para declarar inadmissíveis todas as provas digitais obtidas na busca e apreensão, bem como as provas delas derivadas. O Tribunal partiu de um dado incontroverso: parte do material apreendido estava definitivamente inacessível em razão de corrupção dos arquivos, sem que houvesse explicação técnica satisfatória acerca das causas, do momento ou da

extensão dessa perda. Em consequência, a defesa não teve acesso à integralidade do material probatório originalmente extraído, circunstância que, por si só, compromete o exercício do contraditório substancial.

O voto condutor ressaltou que não se sabe quais arquivos foram perdidos, tampouco se o conteúdo extraviado poderia contribuir para a elucidação dos fatos ou mesmo favorecer a tese defensiva. Trata-se de lacuna probatória de alcance indeterminado, cuja responsabilidade recai exclusivamente sobre o Estado. Nessa perspectiva, não é juridicamente admissível presumir que os arquivos corrompidos seriam irrelevantes ou que não teriam sido previamente acessados pelo órgão acusador. A lógica da cadeia de custódia justamente impede que o processo penal se fundamente em presunções de boa-fé estatal, exigindo documentação técnica capaz de demonstrar, de forma objetiva, a integridade e a confiabilidade da prova.

Outro aspecto central destacado pelo STJ diz respeito à paridade de armas. A ausência de qualquer garantia objetiva de que o Ministério Público não teve acesso aos dados antes da corrupção dos arquivos gera desequilíbrio estrutural entre acusação e defesa. Ainda que tal acesso não possa ser comprovado, a simples impossibilidade de descartá-lo, em razão da falta de documentação e da recusa em permitir perícia independente, já é suficiente para comprometer a legitimidade da prova e da persecução penal dela decorrente.

Do ponto de vista dogmático, a decisão consolida duas teses de grande relevância. A primeira é a de que a prova digital deve ser completa e íntegra para ser admitida em juízo, pois somente assim pode ser submetida ao contraditório e à fiscalização técnica pelas

partes. A segunda é a de que a corrupção parcial dos arquivos compromete a integralidade da prova como um todo, inviabilizando sua utilização, uma vez que não é possível dissociar, com segurança, os dados íntegros daqueles perdidos, nem aferir o impacto da perda sobre o conjunto probatório.

Em síntese, o **AgRg no RHC 184.003/SP** reafirma que a cadeia de custódia da prova digital não se resume à preservação formal de suportes ou à geração inicial de códigos *hash*, mas exige a manutenção contínua da integridade, da rastreabilidade e da acessibilidade do material ao longo de toda a persecução penal. A perda ou corrupção de dados sob custódia estatal, aliada à ausência de documentação técnica e à negativa de produção de prova defensiva, conduz inevitavelmente à inadmissibilidade da prova digital e das evidências dela derivadas. Trata-se de decisão que reforça o papel da cadeia de custódia como garantia estruturante do processo penal democrático e como limite material ao exercício do poder punitivo estatal.

O STJ determinou que o juízo de origem identifique quais provas derivam das provas inadmissíveis, proceda ao seu desentranhamento dos autos e avalie se, após essa exclusão, ainda existem elementos probatórios suficientes para justificar o recebimento da denúncia.

Em suma:

A corrupção de parte dos arquivos digitais compromete a integralidade da prova, inviabilizando sua utilização. STJ. 5ª Turma. AgRg no RHC 184.003-SP, Rel. Min. Daniela Teixeira, Rel. para acórdão Min. Ribeiro Dantas, julgado em 10/12/2024 (Info 838).

TÓPICO 04

4 - RHC 143.169-RJ, Rel. Min. Messod Azulay Neto**. - SÃO INADMISSÍVEIS AS PROVAS DIGITAIS SEM REGISTRO DOCUMENTAL ACERCA DOS PROCEDIMENTOS ADOTADOS PELA POLÍCIA PARA A PRESERVAÇÃO DA INTEGRIDADE, AUTENTICIDADE E CONFIABILIDADE DOS ELEMENTOS INFORMÁTICOS.**

A prova digital assumiu papel central na persecução penal contemporânea, especialmente em investigações envolvendo crimes cibernéticos e delitos financeiros praticados por meio de sistemas informáticos. Todavia, a crescente relevância desse meio probatório exige rigor metodológico proporcional à sua fragilidade técnica. Nesse contexto, o julgamento do **RHC 143.169/RJ,** pela Quinta Turma do Superior Tribunal de Justiça, representa importante marco na consolidação da cadeia de custódia como garantia estrutural do processo penal e condição indispensável para a admissibilidade da prova digital.

O caso submetido ao STJ teve origem em operação policial deflagrada para investigar uma suposta organização criminosa de hackers, acusada de furtar valores de contas bancárias de diversos correntistas. Um dos investigados, João, foi preso e denunciado pelos crimes de furto, organização criminosa e lavagem de dinheiro. A imputação penal baseou-se, essencialmente, em provas digitais extraídas de computadores apreendidos na residência do acusado durante o cumprimento de mandados de busca e apreensão.

A defesa, ao impetrar habeas corpus, sustentou que as provas digitais apresentadas pelo Ministério Público eram inadmissíveis,

pois não havia qualquer registro documental acerca dos procedimentos adotados pela polícia para a coleta, preservação e análise dos dados informáticos. Argumentou-se que a ausência de documentação inviabilizava a verificação da integridade, autenticidade e confiabilidade dos arquivos, configurando quebra da cadeia de custódia nos termos do art. 158-A e seguintes do Código de Processo Penal. Diante disso, requereu-se o reconhecimento da inadmissibilidade das provas extraídas dos computadores apreendidos.

Ao apreciar a controvérsia, o Superior Tribunal de Justiça acolheu a tese defensiva. O Tribunal partiu da premissa de que a cadeia de custódia constitui decorrência lógica do próprio conceito de corpo de delito, previsto no art. 158 do CPP. Sua finalidade primordial é assegurar que os vestígios deixados pela infração penal correspondam exatamente àqueles arrecadados pela polícia, examinados pelos peritos e apresentados em juízo, sem qualquer adulteração durante o período em que permaneceram sob custódia estatal.

No caso concreto, a Corte verificou que inexistia qualquer documentação capaz de demonstrar como se deu o manuseio dos computadores apreendidos, quem teve acesso aos dispositivos, em que momentos ocorreram esses contatos e qual foi o trajeto administrativo percorrido pelos equipamentos desde a apreensão até a perícia. A ausência absoluta desses registros compromete a possibilidade de aferir a chamada mesmidade da prova, isto é, a identidade entre o vestígio originalmente apreendido e aquele que foi submetido à análise técnica e posteriormente valorado pelo órgão acusador.

O STJ ressaltou que, embora os dados digitais possuam natureza intrinsecamente volátil, já existem mecanismos técnicos suficientemente consolidados para garantir sua integridade. Entre eles, destaca-se a necessidade de cópia integral do conteúdo do dispositivo (*bit a bit*), mediante a criação de uma imagem fiel dos dados originais, bem como a aplicação de algoritmos *hash*. O *hash* funciona como verdadeira impressão digital do arquivo, permitindo verificar, com elevado grau de confiabilidade, se houve qualquer alteração, ainda que mínima, no conteúdo original. Qualquer modificação gera um código completamente distinto, fenômeno conhecido na tecnologia da informação como “efeito avalanche”.

Entretanto, no caso analisado, nem mesmo as providências mais elementares foram observadas. Não há comprovação de que o conteúdo dos computadores tenha sido devidamente espelhado, tampouco de que tenha sido gerado código *hash* para permitir a verificação posterior da integridade dos dados. Mais grave ainda, não houve sequer documentação básica sobre os procedimentos adotados pela autoridade policial. A Corte destacou que, diante dessa omissão, nem seria necessário avançar para discutir a adequação técnica da perícia, pois a ausência de registros documentais já inviabiliza qualquer controle sobre a confiabilidade da prova.

Outro aspecto relevante considerado pelo STJ foi o fato de que, antes mesmo da realização de perícia oficial pela polícia, os dados extraídos dos computadores teriam sido analisados por peritos da própria instituição financeira vítima dos crimes. O laudo produzido pelo banco, contudo, não esclareceu se houve acesso direto aos computadores apreendidos ou apenas a arquivos fornecidos pela polícia. Tampouco indicou a existência de códigos *hash* que

permitissem confrontar a cópia analisada com o conteúdo original, o que agrava ainda mais a quebra da cadeia de custódia e a incerteza quanto à autenticidade da prova.

Diante desse conjunto de falhas, o STJ concluiu que não era possível assegurar que os elementos informáticos periciados eram íntegros e idênticos àqueles existentes nos computadores do acusado no momento da apreensão. Tal circunstância configura ofensa direta ao art. 158 do CPP, com a consequente quebra da cadeia de custódia, tornando inadmissíveis as provas obtidas. Em aplicação analógica do art. 157, § 1º, do Código de Processo Penal, a Corte estendeu a inadmissibilidade também às provas derivadas, por falharem em um teste mínimo de confiabilidade.

Do ponto de vista dogmático, o julgamento do RHC 143.169/RJ reafirma que a cadeia de custódia não se reduz a um ritual procedimental ou a uma exigência meramente formal. Trata-se de garantia substancial do processo penal democrático, voltada a assegurar o contraditório efetivo e a paridade de armas. Sem a possibilidade de verificar tecnicamente a origem, o percurso e a integridade da prova digital, a defesa fica privada de exercer controle sobre o material probatório, e o juiz, impedido de proferir decisão racionalmente fundamentada.

Em síntese, o precedente consolida o entendimento de que são inadmissíveis as provas digitais desprovidas de registro documental acerca dos procedimentos adotados para a preservação de sua integridade, autenticidade e confiabilidade. Ao exigir a observância rigorosa da cadeia de custódia, o STJ reforça o papel do processo penal como instrumento de contenção do poder punitivo estatal, impedindo que acusações criminais se sustentem em provas

tecnicamente opacas, não auditáveis e imunes ao contraditório substancial.

Em suma:

São inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos.STJ. 5ª Turma.RHC 143169/RJ, Rel. Min. Messod Azulay Neto, Rel. Acd. Min. Ribeiro Dantas, julgado em 7/2/2023

CONCLUSÃO

A consolidação da prova digital como eixo central da persecução penal contemporânea impõe ao processo penal brasileiro um desafio inadiável: **conciliar eficiência investigativa com garantias fundamentais,** sob pena de transformar a tecnologia em vetor de decisões opacas e potencialmente injustas. Nesse cenário, a cadeia de custódia deixa de ser compreendida como formalidade procedimental e se afirma como **condição de legitimidade probatória,** pois é ela que permite demonstrar — e não presumir — a **autenticidade, a integridade, a confiabilidade e a rastreabilidade** dos vestígios digitais desde o reconhecimento até o descarte, nos termos do art. 158-A do CPP.

Ao longo do trabalho, verificou-se que a prova digital possui características próprias — **volatilidade, facilidade de adulteração, replicabilidade e risco de degradação por simples manipulações** — que ampliam a exigência de rigor metodológico em todas as etapas do art. 158-B do CPP. Se, na prova material clássica, a preservação do vestígio já é pressuposto de validade, nas evidências

eletrônicas esse cuidado se torna ainda mais crítico, pois pequenas intervenções técnicas (como acessos indevidos, extrações sem metodologia, procedimentos inadequados de "root" ou meras capturas de tela) podem inviabilizar a auditabilidade, a reprodutibilidade e a verificabilidade do conteúdo, esvaziando o contraditório e fragilizando a decisão judicial. Nesse sentido, ganha destaque o princípio da **mesmidade,** segundo o qual o elemento valorado em juízo deve corresponder exatamente ao conteúdo originalmente arrecadado, sem alterações ao longo do percurso de custódia — premissa que, no campo digital, é usualmente assegurada por técnicas como **espelhamento forense (*bit a bit*)** e **códigos *hash***.

A jurisprudência recente do Superior Tribunal de Justiça, analisada neste estudo, reforça essa perspectiva garantística ao reconhecer que **falhas relevantes na preservação e documentação** tornam a prova digital **inadmissível.** O STJ tem afirmado, de modo consistente, que a ausência de procedimentos idôneos e registros documentais mínimos compromete a confiabilidade do material e pode conduzir à sua exclusão, bem como às consequências sobre provas derivadas (art. 157, §1º, do CPP). É emblemático, nesse contexto, o entendimento de que, embora a disciplina detalhada dos arts. 158-A a 158-F tenha sido introduzida pelo Pacote Anticrime, a exigência de preservação da cadeia de custódia **decorre de garantias estruturantes** do processo penal (devido processo legal, contraditório, ampla defesa e proibição de prova ilícita), o que impede que a prova digital se sustente em "fé pública" imune à fiscalização defensiva. Assim, quando o próprio Estado inviabiliza a verificação técnica da evidência — por dano, corrupção de arquivos, ausência de documentação ou métodos precários de extração —

não se está diante de mero vício formal, mas de **prejuízo substancial** à paridade de armas e à racionalidade da decisão.

Conclui-se, portanto, que a cadeia de custódia das provas digitais deve ser tratada como **ônus institucional do Estado e garantia do acusado,** indispensável para que a verdade processual seja construída sob critérios mínimos de confiabilidade e sob contraditório efetivo. A insuficiência normativa específica para evidências digitais, mencionada na introdução, não autoriza flexibilizações incompatíveis com o modelo constitucional de processo penal: ao contrário, impõe aos operadores do direito a adoção de **protocolos técnicos reconhecidos,** a valorização da **perícia forense especializada** e a exigência de **documentação integral e contínua** do manuseio do vestígio. Em última análise, quanto mais digital é o vestígio, mais demonstrável deve ser sua integridade. Somente assim a prova tecnológica poderá cumprir seu papel legítimo: fortalecer a apuração penal sem comprometer as garantias que limitam, democraticamente, o poder de punir.

REFERÊNCIAS BIBLIOGRÁFICAS

BERGAMIN, Ana Letícia Marchiori. *A cadeia de custódia das provas digitais no processo penal brasileiro*. 2024. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2024.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. *Código de Processo Penal*. Brasília, DF: Presidência da República, 1941.

FERNANDES, Karen Bernardes de Paiva. *Provas digitais no processo penal: acesso aos dados armazenados, regime jurídico e a jurisprudência do STF*. Trabalho de Conclusão de Curso (Pós-Graduação em Direito Penal e Criminologia).

STJ. Agravo Regimental no Habeas Corpus nº 828.054/RN. 5ª Turma. Relator: Min. Joel Ilan Paciornik. Julgado em 23 abr. 2024.

STJ. Agravo Regimental no Habeas Corpus nº 902.195/RS. 5ª Turma. Relator: Min. Joel Ilan Paciornik. Julgado em 3 dez. 2024. Informativo STJ nº 837.

STJ. Agravo Regimental no Recurso em Habeas Corpus nº 184.003/SP. 5ª Turma. Relatora: Min. Daniela Teixeira. Relator para o acórdão: Min. Ribeiro Dantas. Julgado em 10 dez. 2024. Informativo STJ nº 838.

STJ. Recurso em Habeas Corpus nº 143.169/RJ. 5ª Turma. Relator: Min. Messod Azulay Neto. Relator para o acórdão: Min. Ribeiro Dantas. Julgado em 7 fev. 2023.