REVISTA INTELECTO PRODUÇÃO CIENTÍFICA FEMA

*Volume 8 ▪ Dezembro de 2025 ▪ **ISSN: 2596-0806***
Fundação Educacional do Município de Assis - Fema

A CADEIA DE CUSTÓDIA EM PROVAS DIGITAIS

DOI: 10.5281/zenodo.19007707

Beatriz Vasconcelos Barbosa de PAULA; Dr. Luciano Tertuliano da SILVA

beatrizvbdepaula@gmail.com

RESUMO: O presente artigo científico explora a crescente relevância das provas digitais no processo penal brasileiro, analisando seus conceitos, critérios de admissibilidade, a fundamental importância da cadeia de custódia e os desafios tecnológicos inerentes à sua produção e valoração. Com a digitalização da sociedade, a criminalidade também migrou para o ambiente virtual, tornando as evidências digitais indispensáveis para a elucidação de diversos delitos. Contudo, a natureza volátil e a facilidade de manipulação desses dados impõem rigorosos requisitos para sua validade jurídica, especialmente no que tange à autenticidade e integridade. Serão abordados os aspectos legais, doutrinários e jurisprudenciais que permeiam o tema, com foco nas garantias constitucionais e nos direitos fundamentais envolvidos, bem como nas inovações tecnológicas que visam assegurar a confiabilidade dessas provas.

PALAVRAS-CHAVE: Prova Digital; Processo Penal; Cadeia de Custódia; Perícia Digital; Admissibilidade da Prova.

ABSTRACT: This scientific article explores the growing relevance of digital evidence in the Brazilian criminal process, analyzing its concepts, admissibility criteria, the fundamental importance of the chain of custody, and the technological challenges inherent in its production and evaluation. With the digitalization of society, criminality has also migrated to the virtual environment, making digital evidence indispensable for clarifying various crimes. However, the volatile nature and ease of manipulation of this data impose strict requirements for its legal validity, especially regarding authenticity and integrity. Legal, doctrinal, and jurisprudential aspects surrounding the topic will be addressed, focusing on constitutional guarantees and fundamental rights involved, as well as technological innovations aimed at ensuring the reliability of such evidence.

KEYWORDS: Digital Evidence; Criminal Procedure; Chain of Custody; Digital Forensics; Evidence Admissibility.

Introdução

A cadeia de custódia em provas digitais é um processo fundamental no campo da investigação forense, assegurando que as evidências virtuais, coletadas em dispositivos eletrônicos, mantenham sua integridade desde a coleta até a apresentação em tribunal. Ademais, as provas digitais emergiram como elementos cruciais para a investigação e persecução penal, tornando-se, em muitos casos, a única fonte de comprovação da materialidade e autoria do crime.

Diante desse cenário, há um percentual de aumento significativo da dependência de dispositivos eletrônicos, meios de comunicação, inteligências artificiais e internet. Com isso, crimes cibernéticos têm se tornado cada vez mais comuns, tornando a gestão de provas digitais essencial para a garantia da justiça no mundo. "O ambiente digital tornou-se não apenas meio de prática delitiva, mas também a principal fonte de rastros probatórios, exigindo novas técnicas de preservação e controle da prova." *(LAZZARINI, André. Provas Digitais e o Princípio da Legalidade. Revista Brasileira de Direito Penal, v. 12, n. 2, 2017, p. 92).*

Portanto, a presente pesquisa busca explorar os desafios significativos ao sistema de justiça, análises jurisprudenciais e ensinamentos de doutrinadores renomados do Direito penal e processual penal, apreciando de maneira descritiva e qualitativa como a cadeia de custódia tem sido aplicada no dia a dia. A relevância deste estudo, reside no fato de que, em um mundo cada vez mais digitalizado, a manipulação das provas pode aferir tanto a garantia do devido processo legal, quanto as garantias fundamentais dos indivíduos. Assim, faz-se necessária a presença de profissionais qualificados na área da perícia, a propiciar a integridade às provas digitais, assegurando-as a confiabilidade de sua utilização nas decisões dos tribunais.

1. Conceitos de Prova em Geral

1.1 Definição de prova digital e sua importância no processo penal atual

De acordo com *Lazzarini* (*2017, p. 90),* "a prova digital se caracteriza por sua imaterialidade e pela necessidade de um meio eletrônico para sua percepção e interpretação". Por isso, as provas são registradas, originalmente, em formato de dados binários, armazenados em softwares, que dependem de dispositivos tecnológicos, como computadores, celulares, redes sociais, e-mail, vídeos, áudios, imagens, entre outros. Nesse sentido, diante do processo penal, e com o rápido avanço ao mundo remoto, as provas são essenciais para a elucidação dos crimes, como fraudes eletrônicas, invasão de dispositivos, ataques em sistemas, lavagem de dinheiro, crimes contra a honra e pornografia infantil. Diante de um mundo cada vez mais conectado, diversos crimes deixam rastros, que se tornam as principais ou as únicas evidências disponíveis em um processo. Contudo, com o auxílio de provas lícitas, busca-se a identificação dos infratores, a resolução da problemática e a aplicação da lei de forma correta. Pois, sem elas, a persecução penal seria inviabilizada em muitos casos, gerando impunidade e comprometendo a segurança jurídica e pessoal.

1.2 Diferença entre prova digital e outros tipos de prova

Embora a prova digital compartilhe da finalidade de outros meios de prova – a busca pela verdade real –, ela possui características distintivas que as diferenciam. A principal delas é sua natureza

imaterial e binária. “A prova digital distingue-se das demais por sua estrutura lógica e não física, o que impõe critérios próprios de obtenção e preservação.”

(GOMES, Luiz Flávio. Direito Penal: Parte Geral. São Paulo: RT, 2020, p. 201).

Ademais, enquanto a prova testemunhal é baseada na memória humana, a prova documental física é sensível, a prova pericial tradicional se baseia em vestígios materiais, e a prova digital reside em bits e bytes, exigindo equipamentos e softwares específicos para sua coleta, análise e apresentação. Outra diferença fundamental, reside na sua facilidade de alteração; um documento físico pode ser adulterado, mas os mecanismos de detectação da falsificação, é, muitas vezes, mais simples. Dados digitais, por outro lado, podem ser facilmente apagados, modificados ou corrompidos, sem deixar vestígios a olho nu. Essa característica exige um cuidado redobrado na sua preservação e como será detalhado na seção sobre cadeia de custódia.

Além disso, a prova digital é frequentemente transversal, ou seja, pode ser obtida de diversas fontes e em diferentes formatos, exigindo uma abordagem multidisciplinar, combinada de conhecimentos jurídicos, tecnológicos e forenses. A interpretação de metadados, logs de acesso e informações criptografadas, demanda alta capacidade técnica, que não se faz necessária para a análise de provas tradicionais.

1.3 Desafios relacionados à preservação da autenticidade das provas digitais

A preservação da autenticidade das provas digitais, é um dos mais complexos desafios no processo penal. Essa, refere-se à garantia de que a prova não foi alterada desde o momento de sua coleta. Dito isso, os desafios mais recorrentes são:

- VOLATILIDADE: dados em sistemas de nuvem podem ser instáveis, e desaparecer rapidamente se não forem apreendidos de forma adequada e imediata.

- ATAQUES MALICIOSOS: a prova pode enfrentar problemas, como o ataque de hackers ou a tentativa de alteração das evidências e exclusão por parte dos investigados.

- FRAGMENTAÇÃO: a informação que se obtém a partir da prova digital, pode ser espalhada em diversas plataformas, exigindo a coleta de múltiplos fragmentos a fim de que forme a perspectiva correta.

- ALTERAÇÃO INADVERTIDA: caso tenha um simples acesso à prova digital, como a data de último acesso ou pesquisas, pode ser que haja modificação desses dados, comprometendo sua eficácia e integridade.

“A autenticidade da prova digital depende da demonstração inequívoca de que os dados permaneceram inalterados desde sua coleta.”

(ROSA, Luiz Carlos. Cadeia de Custódia Digital: Aspectos Jurídicos e Práticos. RBPP, v. 5, n. 1, 2020, p. 49). Portanto, para enfrentar esses e outros tipos de desafios, é necessário a alta capacitação de peritos, técnicas forenses e a estrita observação da cadeia de custódia.

1.4 Métodos para assegurar a integridade da prova desde sua obtenção, até o julgamento

A integridade, é a garantia de que a prova digital não foi alterada ou corrompida, seguindo os trâmites corretos de sua coleta até sua apresentação em juízo. Conforme o explicado, a seguir estão os procedimentos empregados:

- HASHING: também conhecido como "impressões digitais", sua função é gerar um código alfanumérico único para um conjunto de dados. Ou seja, qualquer mínima alteração, resultará em um sistema de hash completamente diferente. Contudo, quando uma prova é coletada, um sistema de hash único é registrado. Se, em alguma etapa posterior o hash da prova for diferente do original, indica-se que houve alteração. Rosa (2020, p. 55) enfatiza que "o hash é a espinha dorsal da garantia de integridade da prova digital na cadeia de custódia".

- DOCUMENTAÇÃO DETALHADA: cada etapa da manutenção, manuseio, armazenamento e análise da prova deve ser documentada cuidadosamente. Isso inclui data, horário, local, pessoas envolvidas, hash da prova, software atualizados e quaisquer observações que aparecerem durante o processo. "A ausência de registros claros e contínuos sobre a manipulação da prova compromete sua credibilidade processual." *(PRADO, Geraldo. A cadeia de custódia da prova no processo penal. São Paulo: Marcial Pons, 2021, p. 63).*

- IMAGENS FORENSES (BIT-STREAM COPY): é fundamental criar uma imagem forense exata do dispositivo de armazenamento de dados. Essa, é uma cópia de bit a bit de todo o conteúdo do disco, incluindo dados apagados, que podem conter informações cruciais. Entretanto, a imagem forense é verificada, também, com um hash, para garantir a eficácia.

- ASSINATURAS DIGITAIS E CRIPTOGRAFIA: em alguns casos, a prova digital pode ser assinada digitalmente ou criptografada para garantir sua autenticidade e confiabilidade durante a transmissão ou armazenamento.

- AMBIENTES CONTROLADOS: a análise e o armazenamento das provas, deve ser realizado em um ambiente controlado e seguro, com acesso restrito e monitorado para evitar adulterações.

1.5 Privacidade e direitos fundamentais

A Constituição Federal, em seu artigo 5°, incisos X e XII, garantem a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o sigilo das comunicações. Dessa

forma, a coleta e a análise das provas digitais, frequentemente envolvem o acesso a informações pessoais dos indivíduos, abordando sérias questões sobre a privacidade e seus direitos fundamentais. "A prova digital somente é legítima quando obtida em conformidade com os direitos fundamentais." *(BADARÓ, Gustavo H. R. I. A Cadeia de Custódia e a Admissibilidade da Prova Digital. RBPP, 2021, p. 128).*

A obtenção de provas digitais, especialmente aquelas que envolvem dados de comunicação (e-mails, mensagens) ou dados armazenados em dispositivos pessoais, deve ser realizada com estrita observância dos princípios da legalidade, proporcionalidade e necessidade. Medidas como a quebra de sigilo de dados e comunicações telemáticas exigem autorização judicial prévia e fundamentada, conforme a Lei nº 9.296/96 (Lei de Interceptação Telefônica, aplicável por analogia a comunicações digitais).

Contudo, *Fernando Capez (2018, p. 125*) ressalta que "a busca pela verdade real não pode se sobrepor aos direitos e garantias individuais, sob pena de nulidade da prova e violação do devido processo legal". Ou seja, a prova obtida ilicitamente, em desrespeito às normas constitucionais, é inadmissível no processo penal, conforme o artigo. 5°, inciso LIV, da Constituição Federal.

Portanto, a doutrina e a jurisprudência têm debatido incansavelmente os limites da atuação estatal na coleta de provas digitais, buscando um equilíbrio entre a efetividade da persecução penal e a proteção dos direitos fundamentais.

2. Admissibilidade e Validade Jurídica

2.1 critérios de admissibilidade das provas digitais no processo penal

A admissibilidade da prova no processo penal, refere-se à capacidade de ser considerada válida para a formação do convencimento do perito. Para as provas digitais, esses critérios são ainda mais rigorosos devido às suas características peculiares. *Nucci (2019, p. 345)* ressalta que "a prova, para ser admitida, deve ser lícita, pertinente e relevante". Logo, os principais critérios de admissibilidade incluem:

- LEGALIDADE: as provas devem ser obtidas em conformidade com a Constituição Federal e o Processo Penal. Isso significa que a coleta de dados digitais não pode ferir os direitos fundamentais, como o sigilo e a privacidade de comunicações, sem a devida autorização judicial. Ademais, provas obtidas por invasão de dispositivos sem mandado, por exemplo, são consideradas ilícitas.
- PERTINÊNCIA E RELEVÂNCIA: é necessário que a prova digital tenha relação com os fatos e, ao mesmo tempo, influencie na decisão do possível órgão julgador.

- CONTRADITÓRIO E AMPLA DEFESA: a parte contrária deverá dispor de seu direito de contradizer, de ter acesso aos métodos de coleta das provas e sua análise, a fim de que possa produzir sua contestação.

- AUTENTICIDADE E INTEGRIDADE: a prova deve ser genuína, sem alterações. A autenticidade é garantida por meio da cadeia de custódia e das técnicas de hashing. Já, a integridade, observa qualquer modificação intencional ou acidental, desde o momento de sua coleta.

- CONFIABILIDADE: devem ser produzidas por profissionais qualificados da área, assegurando a aceitação científica. Assim sendo, Gustavo Badaró sustenta a validade epistêmica, isto é, sua capacidade de gerar conhecimento confiável para fins de decisão judicial, dependendo de padrões metodológicos específicos de forense computacional.

2.2 Desafios enfrentados pelos magistrados, na avaliação da confiabilidade e validade das provas

A magistratura enfrenta desafios diariamente, no que diz respeito a avaliação e a confiabilidade das provas digitais. Dito isso, a complexidade técnica envolvida na sua análise, exige um conhecimento que, muitas vezes, transcende a formação jurídica convencional, como:

- RÁPIDA EVOLUÇÃO TECNOLÓGICA: no mundo atual, novas formas de comunicação, armazenamento de dados e softwares surgem constantemente, tornando cada vez mais difícil para o sistema jurídico acompanhar essas mudanças e estabelecer parâmetros transparentes para a admissibilidade das provas.

- DIFICULDADE DE COMPREENSÃO TÉCNICA: a natureza dos metadados, logs, criptografia, algoritmos e sistemas operacionais, podem ser dificilmente compreendidas pelos Juízes e Promotores, por não possuírem formação em tecnologia. Isso pode levar ao julgamento inadequado ou à dificuldade em identificar falhas nas provas. “A dependência excessiva do laudo pericial impõe ao magistrado o dever de compreender minimamente os fundamentos técnicos apresentados*” (NUCCI, Guilherme de Souza. Código de Processo Penal Comentado. São Paulo: Forense, 2019, p. 350).*

- JURISPRUDÊNCIA EM CONSTRUÇÃO: significa que não há uma matéria consolidada de decisões que sirvam de diretrizes claras para o esclarecimento dos casos abordados, gerando insegurança jurídica.

- DEPENDÊNCIA DE PERITOS: a avaliação da prova digital frequentemente depende do laudo de peritos técnicos. A qualidade e a imparcialidade das perícias são cruciais, e o magistrado precisa ser capaz de questionar e interpretar tais conclusões.

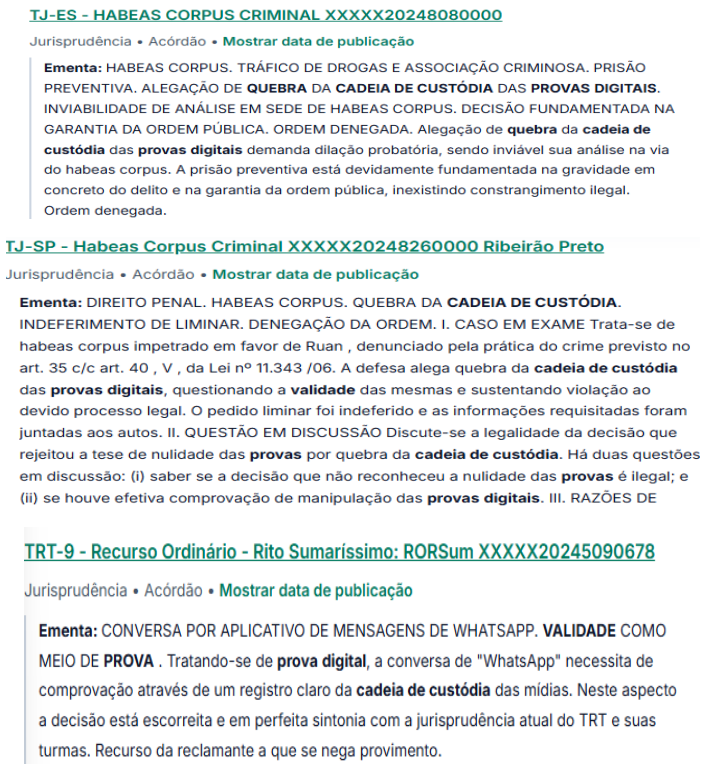
Conforme a analogia de Gustavo Badaró, “o amicus curiae amplia o contraditório e a legitimidade democrática da decisão judicial, permitindo que vozes qualificadas participem da construção da solução jurídica”. Portanto, é imprescindível o auxílio desse mecanismo nos processos digitais.

2.3 Jurisprudências relacionadas ao uso de provas digitais

A jurisprudência brasileira tem desempenhado papel fundamental na consolidação dos critérios de admissibilidade e valoração das provas digitais, especialmente diante da insuficiência normativa para acompanhar a rápida evolução tecnológica.

Os tribunais superiores, em especial o Supremo Tribunal Federal e o Superior Tribunal de Justiça, têm reiteradamente afirmado que a validade da prova digital está condicionada à observância dos direitos fundamentais, da legalidade na obtenção dos dados e da preservação da cadeia de custódia. Nesse sentido, decisões recentes têm reconhecido a ilicitude de provas obtidas por acesso direto a dispositivos eletrônicos sem autorização judicial, bem como têm invalidado elementos probatórios quando verificada a ausência de documentação adequada sobre o manuseio da prova digital.

Conforme destaca Badaró, a jurisprudência atua como verdadeiro parâmetro interpretativo, ao estabelecer limites e standards probatórios capazes de assegurar segurança jurídica e confiabilidade na utilização das provas digitais no processo penal (BADARÓ, Gustavo Henrique Righi Ivahy. *Prova Penal: Fundamentos, Exame e Valoração*. São Paulo: Revista dos Tribunais, 2020, p. 141).



TJ-ES - HABEAS CORPUS CRIMINAL XXXXX20248080000

Jurisprudência • Acórdão • Mostrar data de publicação

Ementa: HABEAS CORPUS. TRÁFICO DE DROGAS E ASSOCIAÇÃO CRIMINOSA. PRISÃO PREVENTIVA. ALEGAÇÃO DE **QUEBRA** DA **CADEIA DE CUSTÓDIA** DAS **PROVAS DIGITAIS**. INVIABILIDADE DE ANÁLISE EM SEDE DE HABEAS CORPUS. DECISÃO FUNDAMENTADA NA GARANTIA DA ORDEM PÚBLICA. ORDEM DENEGADA. Alegação de **quebra** da **cadeia de custódia** das **provas digitais** demanda dilação probatória, sendo inviável sua análise na via do habeas corpus. A prisão preventiva está devidamente fundamentada na gravidade em concreto do delito e na garantia da ordem pública, inexistindo constrangimento ilegal. Ordem denegada.

TJ-SP - Habeas Corpus Criminal XXXXX20248260000 Ribeirão Preto

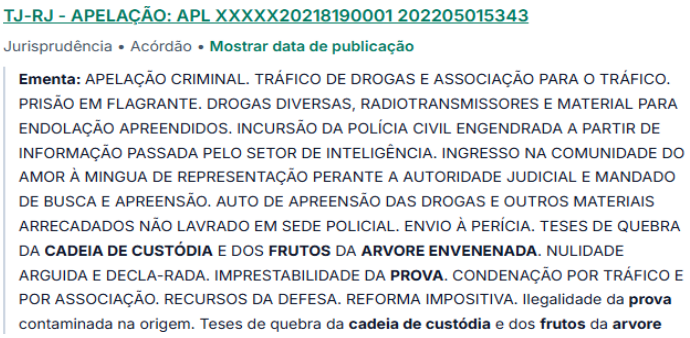
Jurisprudência • Acórdão • Mostrar data de publicação

Ementa: DIREITO PENAL. HABEAS CORPUS. QUEBRA DA **CADEIA DE CUSTÓDIA**. INDEFERIMENTO DE LIMINAR. DENEGAÇÃO DA ORDEM. I. CASO EM EXAME Trata-se de habeas corpus impetrado em favor de Ruan , denunciado pela prática do crime previsto no art. 35 c/c art. 40 , V , da Lei nº 11.343 /06. A defesa alega quebra da **cadeia de custódia** das **provas digitais**, questionando a **validade** das mesmas e sustentando violação ao devido processo legal. O pedido liminar foi indeferido e as informações requisitadas foram juntadas aos autos. II. QUESTÃO EM DISCUSSÃO Discute-se a legalidade da decisão que rejeitou a tese de nulidade das **provas** por quebra da **cadeia de custódia**. Há duas questões em discussão: (i) saber se a decisão que não reconheceu a nulidade das **provas** é ilegal; e (ii) se houve efetiva comprovação de manipulação das **provas digitais**. III. RAZÕES DE

TRT-9 - Recurso Ordinário - Rito Sumaríssimo: RORSum XXXXX20245090678

Jurisprudência • Acórdão • Mostrar data de publicação

Ementa: CONVERSA POR APLICATIVO DE MENSAGENS DE WHATSAPP. **VALIDADE** COMO MEIO DE **PROVA** . Tratando-se de **prova digital**, a conversa de "WhatsApp" necessita de comprovação através de um registro claro da **cadeia de custódia** das mídias. Neste aspecto a decisão está escorreita e em perfeita sintonia com a jurisprudência atual do TRT e suas turmas. Recurso da reclamante a que se nega provimento.



TJ-RJ - APELAÇÃO: APL XXXXX20218190001 202205015343

Jurisprudência • Acórdão • **Mostrar data de publicação**

Ementa: APELAÇÃO CRIMINAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO PARA O TRÁFICO. PRISÃO EM FLAGRANTE. DROGAS DIVERSAS, RADIOTRANSMISSORES E MATERIAL PARA ENDOLAÇÃO APREENDIDOS. INCURSÃO DA POLÍCIA CIVIL ENGENDRADA A PARTIR DE INFORMAÇÃO PASSADA PELO SETOR DE INTELIGÊNCIA. INGRESSO NA COMUNIDADE DO AMOR À MINGUA DE REPRESENTAÇÃO PERANTE A AUTORIDADE JUDICIAL E MANDADO DE BUSCA E APREENSÃO. AUTO DE APREENSÃO DAS DROGAS E OUTROS MATERIAIS ARRECADADOS NÃO LAVRADO EM SEDE POLICIAL. ENVIO À PERÍCIA. TESES DE QUEBRA DA **CADEIA DE CUSTÓDIA** E DOS **FRUTOS** DA **ARVORE ENVENENADA**. NULIDADE ARGUIDA E DECLA-RADA. IMPRESTABILIDADE DA **PROVA**. CONDENAÇÃO POR TRÁFICO E POR ASSOCIAÇÃO. RECURSOS DA DEFESA. REFORMA IMPOSITIVA. Ilegalidade da **prova** contaminada na origem. Teses de quebra da **cadeia de custódia** e dos **frutos** da **arvore**

3. Cadeia de Custódia das Provas Digitais

3.1 Origem e delineamentos

"A cadeia de custódia é o caminho percorrido pela prova, com registros formais de cada etapa, garantindo que o material praticado ou a informação digital seja o mesmo coletado na origem" *(Badaró, Gustavo).* Contudo, seu objetivo principal é assegurar que a prova apresentada em juízo, é a mesma que foi coletada durante a prática de um crime, sem ter sofrido qualquer tipo de adulteração. Com o advento das provas digitais, a cadeia de custódia adquiriu uma nova dimensão, com base na fragilidade e facilidade de manipulação dos dados eletrônicos. Entretanto, o delineamento da cadeia de custódia envolve a documentação minuciosa de cada etapa do acolhimento das provas, incluindo um documento sobre quem coletou, quando, onde, como, quem armazenou, quem analisou-a e teve acesso a ela. Portanto, cada transferência deverá ser registrada, adquirindo histórico ininterrupto, do qual ateste a integridade de cada vídeo, foto, print e áudio.

3.2 Etapas da cadeia de custódia em provas digitais

As etapas são rigorosas a fim de garantir a integridade e autenticidade dos dados, descrevendo-as principalmente como:

- RECONHECIMENTO: identificação de fontes potenciais de provas digitais, como computadores, pendrives, servidores próprios, celulares e nuvem.

- ISOLAMENTO E PRESERVAÇÃO DA CENA: proteção do ambiente onde a prova é encontrada para evitar contaminação ou alteração. Também, pode incluir no desligamento de dispositivos e isolar redes de forma controlada.

- COLETA: a fase mais crítica. A prova digital deve ser coletada por profissionais capacitados, utilizando ferramentas forenses que garantam a integridade dos dados (por exemplo, criação de imagens forenses com hashing). É fundamental que a coleta seja "não invasiva", ou seja, que não altere os dados originais.

- ACONDICIONAMENTO: embalagem e lacração dos dispositivos ou mídias digitais de forma segura, com identificação clara e hash dos dados.

- TRANSPORTE: movimentação da prova digital de forma segura, com registro de quem transportou, quando e como.

- RECEBIMENTO: registro detalhado da entrada da prova no laboratório ou local de armazenamento, com conferência do hash e das condições de lacre.

- ANÁLISE: a perícia propriamente dita. A análise deve ser feita em cópias forenses da prova digital, nunca nos originais, para preservar a integridade da fonte. Todos os procedimentos devem ser documentados.

- ARMAZENAMENTO: guarda da prova digital em local seguro, com controle de acesso e condições ambientais adequadas para evitar danos.

- DESCARTE: destinação final da prova após o trânsito em julgado do processo, seguindo as normas legais.

"A quebra em qualquer etapa da cadeia compromete a confiabilidade de todo o conjunto probatório." *(ROSA, Luiz Carlos. Cadeia de Custódia Digital. 2020, p. 60).*

3.3 Conflitos relacionados à coleta de provas digitais em conformidade com a lei

A coleta de provas digitais muitas vezes entra em conflito com direitos fundamentais, exigindo equilíbrio entre investigação e proteção da privacidade e do sigilo.

- ACESSO A DADOS PESSOAIS: a obtenção de dados de celulares, computadores ou e-mails sem autorização judicial viola o Art. 5º, XII, da CF. A jurisprudência tem considerado ilícitas provas obtidas por "invasão" de dispositivos sem mandado.

- QUEBRA DE SIGILO: a interceptação de comunicações telemáticas exige autorização judicial e deve seguir a Lei nº 9.296/96. Persistem divergências sobre o que se caracteriza como "comunicação" e "dado armazenado".

- ACESSO A DADOS EM NUVEM: o uso crescente de serviços como Google Drive e Dropbox gera dúvidas sobre jurisdição e validade de mandados para dados armazenados em servidores estrangeiros.

- PRIVACIDADE: a coleta de provas digitais pode expor dados de pessoas não investigadas, levantando questões sobre a proteção da privacidade de terceiros.

- PROVAS ILÍCITAS POR DERIVAÇÃO: pela teoria dos "frutos da árvore envenenada", provas obtidas ilicitamente tornam ilícitas também todas as provas delas derivadas.

3.4 Manutenção da cadeia de custódia e os riscos de adulteração e manipulação

A manutenção da cadeia de custódia é fundamental para garantir a credibilidade da prova digital. Como afirma Prado (2021), ela assegura a confiabilidade da evidência, evitando questionamentos sobre sua integridade.

- ADULTERAÇÃO: alteração intencional do conteúdo para criar falsas evidências. Lazzarini (2017), destaca que adulterações violam o princípio da legalidade probatória.
- MANIPULAÇÃO: mudança de metadados sem alterar o conteúdo principal. Para Rosa (2020), isso já compromete a narrativa temporal necessária à investigação.
- CONTAMINAÇÃO: inclusão de dados estranhos ou alterações acidentais por manuseio inadequado. Dalagnol (2015), reforça que qualquer interferência indevida rompe o vínculo lógico entre a fonte e a prova.
- PERDA DE DADOS: exclusão, formatação ou falhas de hardware que eliminam informações. Nucci (2019), observa que a perda probatória prejudica a reconstrução dos fatos.

A falta de registros claros sobre o acesso à evidência abre margem para contestação. Para Capez (2018), somente controles rigorosos garantem autenticidade. Assim, uma cadeia de custódia bem documentada preserva a integridade da prova desde sua origem.

3.5 Integridade da cadeia de custódia

A integridade da cadeia de custódia é o pilar da confiabilidade da prova digital. Como observa Prado (2021), somente uma cadeia sólida e contínua garante que a evidência permaneça autêntica. Cada etapa deve ser rigorosamente controlada para evitar qualquer questionamento futuro.

-DOCUMENTAÇÃO EXAUSTIVA: todas as ações devem ser registradas de forma detalhada. Para Fernando Capez (*Curso de Direito Penal – Parte Geral*. São Paulo: Saraiva, 2018, p.132)., a documentação minuciosa é o que permite demonstrar a autenticidade da prova.

-FERRAMENTAS FORENSES CERTIFICADAS: o uso de hardware e software validados evita alterações acidentais e assegura resultados reproduzíveis. Lazzarini (*Provas Digitais e o Princípio da Legalidade*. Revista Brasileira de Direito Penal, v. 12, n. 2, 2017, p. 101), destaca que a confiabilidade técnica é parte essencial da legalidade probatória.

-TREINAMENTO E CAPACITAÇÃO: profissionais devem ter formação específica em perícia digital. Dalagnol (*A lógica das provas no processo: prova direta, indícios e presunções*. Porto Alegre: Livraria do Advogado, 2015, p.68), aponta que o correto manejo técnico é indispensável para manter a lógica e consistência da prova.

-CONTROLE DE ACESSO: o acesso deve ser restrito e monitorado, garantindo rastreabilidade. Nucci (*Código de Processo Penal Comentado*. São Paulo: Forense, 2019, p. 352, ressalta que o controle sobre quem manipula a prova reforça sua credibilidade processual.

-VERIFICAÇÃO DE HASH: a geração e conferência de hashes comprovam a integridade em cada etapa. Conforme Rosa (*Cadeia de Custódia Digital: Aspectos Jurídicos e Práticos*. Revista Brasileira

de Direito Processual Penal, v. 5, n. 1, 2020, p. 58), o hash é o principal mecanismo técnico de proteção contra alegações de adulteração.

-AMBIENTE SEGURO: O laboratório deve ter segurança física e lógica para prevenir contaminações. Gomes (*Direito Penal: Parte Geral*. São Paulo: Editora Revista dos Tribunais, 2020, p. 210), enfatiza que a proteção estrutural é parte inseparável da preservação da prova.

4. Perícia digital e desafios tecnológicos em sua custódia

4.1. Importância da perícia técnica na análise de provas digitais

A perícia técnica é essencial para a análise de provas digitais, pois permite compreender, validar e apresentar adequadamente dados eletrônicos em juízo. Como destaca Badaró, a prova digital exige critérios científicos rígidos para garantir confiabilidade. A atuação de peritos capacitados é indispensável diante da complexidade desses vestígios

-EXTRAÇÃO FORENSE: a coleta deve seguir métodos validados para não alterar dados originais, conforme lembram Prado e Lazzarini, que reforçam a necessidade de procedimentos tecnicamente reprodutíveis. (PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. São Paulo: Marcial Pons, 2021, p. 84; LAZZARINI, André. *Provas Digitais e o Princípio da Legalidade*. Revista Brasileira de Direito Penal, v. 12, n. 2, 2017, p. 97).

-INTERPRETAÇÃO E ANÁLISE: O perito deve interpretar logs, metadados e mensagens, contextualizando informações, como apontam Dalagnol e Rosa (DALAGNOL, Deltan. A lógica das provas no processo: prova direta, indícios e presunções. Porto Alegre: Livraria do Advogado, 2015, p. 73; ROSA, Luiz Carlos. Cadeia de Custódia Digital: Aspectos Jurídicos e Práticos. Revista Brasileira de Direito Processual Penal, v. 5, n. 1, 2020, p. 52).

-RECONSTITUIÇÃO DE EVENTOS: A partir de artefatos digitais, é possível reconstruir cronologias e identificar autores.

-VALIDADE E AUTENTICIDADE: Hashes, assinaturas digitais e técnicas de verificação garantem integridade — elemento central segundo Rosa em sua obra *Cadeia de Custódia Digital: Aspectos Jurídicos e Práticos*. 2020, p. 58).

-LAUDO TÉCNICO E SUPORTE AO JULGADOR: O perito traduz tecnicidade ao magistrado, permitindo adequada valoração da prova, como destaca Nucci (*Código de Processo Penal Comentado*. São Paulo: Forense, 2019, p. 356).

4.2 Problemas técnicos e a complexidade na interpretação de dados digitais

A análise de dados digitais envolve diversos desafios técnicos e interpretativos. Como destacam Luiz Carlos Rosa e Geraldo Prado, a complexidade da prova digital exige domínio técnico e rigor metodológico.

- VOLUME DE DADOS: a quantidade de dados gerados e armazenados diariamente é colossal. Analisar terabytes de informações em um celular ou servidor pode ser uma tarefa demorada e dispendiosa.
- DIVERSIDADE DE SISTEMAS: a multiplicidade de formatos, aplicativos e sistemas operacionais demanda do perito amplo conhecimento tecnológico, conforme observa Lazzarini (*Provas Digitais e o Princípio da Legalidade*. 2017, p. 103), ao tratar da diversidade das fontes digitais.
- CRIPTOGRAFIA: a proteção cada vez mais robusta dificulta o acesso e exige métodos avançados para obtenção de chaves ou descriptografia.
- DADOS FRAGMENTADOS OU APAGADOS: a recuperação de conteúdos deletados ou dispersos requer técnicas especializadas, nem sempre eficazes.
- METADADOS ALTERÁVEIS: metadados podem ser facilmente manipulados, o que, segundo Guilherme Nucci (*Código de Processo Penal Comentado*. 2019, p. 351), exige cautela redobrada na verificação de autenticidade.
- CONTEXTO E SIGNIFICADO: a extração não basta; é preciso interpretar o contexto para compreender o real sentido das informações, como ensina Dalagnol, em sua obra descrita acima, ao tratar da lógica probatória.
- FALSIFICAÇÃO DE EVIDÊNCIAS: a facilidade de criação de conteúdos digitais falsos impõe ao perito a habilidade de identificar edições, adulterações e deepfakes.

Em síntese, a análise de dados digitais demanda conhecimento técnico profundo, atenção ao contexto e métodos rigorosos de verificação, pois, como afirma Capez (*Curso de Direito Penal – Parte Geral*. São Paulo: Saraiva, 2018, p. 130), a credibilidade da prova depende da precisão e confiabilidade de sua produção.

4.3 Rapidez nas mudanças tecnológicas e seu impacto no Processo Penal

A velocidade vertiginosa das mudanças tecnológicas é um dos maiores desafios para o processo penal no que diz respeito às provas digitais. Novas tecnologias, aplicativos e formas de comunicação surgem e se popularizam em um ritmo muito mais rápido do que a capacidade do legislador e do sistema judiciário de se adaptar. Sendo assim, o impacto dessa rapidez inclui:

-LEGISLAÇÃO DESATUALIZADA: as normas não acompanham as inovações, criando lacunas e incertezas sobre a legalidade e validade de provas digitais — problema já apontado por Lazzarini

(LAZZARINI, André. *Provas Digitais e o Princípio da Legalidade*. Revista Brasileira de Direito Penal, v. 12, n. 2, 2017, p. 108) ao tratar da insuficiência normativa.

- FERRAMENTAS FORESNSES OBSOLETAS: softwares e equipamentos precisam de atualização contínua para funcionar com novos sistemas, formatos e criptografias; caso contrário, tornam-se incapazes de extrair dados corretamente.

-JURISPRUDÊNCIA ATRASADA: como observa Nucci (NUCCI, Guilherme de Souza. *Código de Processo Penal Comentado*. São Paulo: Forense, 2019, p. 354), a jurisprudência depende dos casos concretos, formando entendimentos lentamente e gerando decisões divergentes em temas tecnológicos recentes.

-CAPACITAÇÃO PERMANETE: operadores do direito e peritos devem se atualizar constantemente, pois, como destaca Dalagnol (DALAGNOL, Deltan. *A lógica das provas no processo: prova direta, indícios e presunções*. Porto Alegre: Livraria do Advogado, 2015, p. 82), a correta interpretação e utilização da prova depende do domínio técnico.

Essa dinâmica exige que o sistema de justiça desenvolva mecanismos mais céleres e adaptáveis, garantindo que a inovação tecnológica não comprometa a segurança jurídica nem os direitos fundamentais.

4.4. Dificuldades na atualização de técnicas jurídicas para lidar com novas formas de comunicação e armazenamento de dados

As dificuldades na atualização das técnicas jurídicas para lidar com as novas formas de comunicação e armazenamento de dados são evidentes. O direito, por sua natureza, é mais conservador e lento em suas mudanças do que a tecnologia.

- PRINCÍPIO DA LEGALIDADE ESTRITA: a prova deve ter amparo legal, e a falta de regulamentação específica para certas evidências digitais gera dúvidas quanto à sua validade, problema apontado por Lazzarini em sua obra (*Provas Digitais e o Princípio da Legalidade*. Revista Brasileira de Direito Penal, v. 12, n. 2, 2017, p. 105) ao tratar da insuficiência normativa sobre tecnologia.

- INÉRCIA LEGISLATIVA: O processo legislativo lento impede que a lei acompanhe a velocidade das inovações. (GOMES, Luiz Flávio. *Direito Penal: Parte Geral*. São Paulo: Editora Revista dos Tribunais, 2020, p. 198).

- FALTA DE ESPECIALIZAÇÃO: a carência de conhecimento técnico entre operadores do direito dificulta a compreensão e aplicação adequada das provas digitais, como observado por Dalagnol

(DALAGNOL, Deltan. *A lógica das provas no processo: prova direta, indícios e presunções*. Porto Alegre: Livraria do Advogado, 2015, p. 70, ao tratar da complexidade probatória.

- CONFLITOS DE COMPETÊNCIA: a dimensão transnacional dos dados — muitos armazenados em servidores no exterior — gera conflitos de jurisdição e obstáculos na obtenção de provas, como também destaca Nucci (*Código de Processo Penal Comentado*. São Paulo: Forense, 2019, p. 359).

- EQUILÍBRIO ENTRE SEGURANÇA E LIBERDADE: a modernização jurídica deve preservar direitos fundamentais, mantendo o equilíbrio entre investigação e garantias individuais, conforme reforça Prado (PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. São Paulo: Marcial Pons, 2021, p. 102), ao discutir limites da atuação penal.

Assim, o desafio central está em adaptar o direito penal e processual penal à realidade digital sem comprometer a legalidade, a segurança jurídica e as liberdades constitucionais.

4.5 O sistema Hash e a criptografia como garantia da efetividade da cadeia de custódia nas provas digitais

O hash, enquanto função matemática que gera um identificador único para um conjunto de dados, permite verificar qualquer alteração mínima no arquivo, garantindo sua integridade. Como destacam os autores Rosa e Prado, o hash é um dos principais mecanismos de demonstração técnica da autenticidade da prova digital. (ROSA, Luiz Carlos. *Cadeia de Custódia Digital: Aspectos Jurídicos e Práticos*. 2020, p. 57; PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. 2021, p. 88).

A garantia de integridade decorre da comparação entre o hash obtido no momento da coleta e os recalculados ao longo da custódia: hashes idênticos indicam preservação; divergências revelam manipulação. Já, a criptografia protege os dados contra acessos indevidos e assegura a confidencialidade no transporte e armazenamento, além de possibilitar assinaturas digitais que garantem autenticidade e não repúdio.

A doutrina de Gustavo Badaró reforça que a cadeia de custódia deve assegurar "rastreabilidade, autenticidade e confiabilidade", e mecanismos tecnológicos como hash e criptografia concretizam esses requisitos no âmbito das provas digitais. Assim, a combinação de ambos fornece um sistema robusto de segurança, essencial para a validade jurídica e a credibilidade probatória no processo penal contemporâneo.

4.6 Mecanismos extratextuais e disposição do julgador à confiabilidade na custódia das provas digitais

A confiabilidade na custódia das provas digitais não depende apenas de aspectos técnicos e legais, mas também de fatores extratextuais que influenciam a percepção do julgador. A padronização de procedimentos por meio de normas e guias de boas práticas fortalece a credibilidade das perícias, assim como a acreditação de laboratórios, que garante conformidade com padrões técnicos reconhecidos. A formação e reputação dos peritos também exerce papel decisivo, pois peritos qualificados e transparentes tendem a ter seus laudos mais valorizados.

Outro elemento essencial é a transparência e o contraditório, permitindo que a defesa acesse dados brutos, metodologias e ferramentas, e produza contraprova — algo que, conforme destaca Badaró, reforça a legitimidade e a confiabilidade da prova ao assegurar efetivo controle pelas partes. A capacitação dos magistrados em temas digitais também influencia sua disposição em valorar corretamente a prova técnica. Por fim, precedentes jurisprudenciais consistentes ajudam a consolidar critérios e aumentar a previsibilidade das decisões.

Dessa forma, a confiança na custódia das provas digitais resulta da união entre a integridade técnica da prova e fatores externos, como padronização, qualificação profissional e coerência jurisprudencial.

Conclusão

As provas digitais representam um avanço inegável na busca pela verdade real no processo penal, adaptando o sistema de justiça à realidade da criminalidade na era digital. Sua capacidade de revelar informações cruciais para a elucidação de crimes as torna indispensáveis. Contudo, sua natureza imaterial, volátil e de fácil manipulação impõe desafios significativos que exigem uma abordagem rigorosa e multifacetada.

A observância da cadeia de custódia emerge como o pilar fundamental para a garantia da autenticidade e integridade dessas provas. Desde o reconhecimento do vestígio digital até seu armazenamento final, cada etapa deve ser meticulosamente documentada e controlada, com o uso de ferramentas tecnológicas como o *hash* e a criptografia, que conferem segurança e rastreabilidade aos dados. A quebra da cadeia de custódia, como tem sido reiterado pela jurisprudência, pode levar à inadmissibilidade da prova, comprometendo a persecução penal.

A perícia digital, por sua vez, é a chave para a compreensão e valoração dessas evidências. A expertise dos peritos em extrair, analisar e interpretar dados digitais, superando as complexidades técnicas e a rapidez das mudanças tecnológicas, é crucial para transformar bits e bytes em informações juridicamente relevantes. Os desafios enfrentados pelos magistrados na avaliação dessas provas, dada a sua complexidade técnica e a constante evolução tecnológica, ressaltam a necessidade de capacitação contínua e de uma maior interação entre o direito e a tecnologia.

Por fim, a proteção dos direitos fundamentais, especialmente a privacidade e o sigilo das comunicações, deve ser o balizador de toda a atividade de coleta e análise de provas digitais. A busca pela verdade real não pode justificar a violação de garantias constitucionais, e a prova obtida por meios ilícitos deve ser rechaçada.

Em suma, a efetividade da justiça na era digital depende da capacidade do sistema jurídico de se adaptar aos novos paradigmas probatórios, investindo em tecnologia, capacitação profissional e, acima de tudo, garantindo que a busca pela verdade seja sempre pautada pela legalidade, pela ética e pelo respeito aos direitos fundamentais. A prova digital, quando obtida e custodiada de forma correta, não é apenas um meio de prova, mas uma ferramenta poderosa para a construção de um processo penal mais justo e eficaz.

REFERÊNCIAS BIBLIOGRÁFICAS

BADARÓ, Gustavo Henrique Righi Ivahy. *Curso de Processo Penal*. São Paulo: Thomson Reuters Brasil, 2019.

_____. *Prova Penal: Fundamentos, Exame e Valoração*. São Paulo: Revista dos Tribunais, 2020.

_____. A Cadeia de Custódia e a Admissibilidade da Prova Digital. *Revista Brasileira de Direito Processual Penal*, v. 7, n. 2, p. 120–145, 2021.

_____. *Standards Probatórios no Processo Penal*. São Paulo: Marcial Pons, 2022.

_____. *A cadeia de custódia da prova digital*. In: *Direito Probatório*. São Paulo: Thomson Reuters Brasil, 2023.

BADARÓ, Gustavo Henrique Righi Ivahy; BOTTINI, Pierpaolo Cruz. *Prova Penal e Habeas Corpus*. São Paulo: Revista dos Tribunais, 2018.

CAPEZ, Fernando. *Curso de Direito Penal – Parte Geral*. São Paulo: Saraiva, 2018.

DALAGNOL, Deltan. *A lógica das provas no processo: prova direta, indícios e presunções*. Porto Alegre: Livraria do Advogado, 2015.

GOMES, Luiz Flávio. *Direito Penal: Parte Geral*. São Paulo: Editora Revista dos Tribunais, 2020.

LAZZARINI, André. Provas Digitais e o Princípio da Legalidade. *Revista Brasileira de Direito Penal*, v. 12, n. 2, p. 90–110, 2017.

NUCCI, Guilherme de Souza. *Código de Processo Penal Comentado*. São Paulo: Forense, 2019.

PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. São Paulo: Marcial Pons, 2021.

ROSA, Luiz Carlos. Cadeia de Custódia Digital: Aspectos Jurídicos e Práticos. *Revista Brasileira de Direito Processual Penal*, v. 5, n. 1, p. 45–67, 2020.