

A Valoração de Elementos Probatórios Digitais no Processo Penal Brasileiro: Fundamentos Teóricos, Natureza Jurídica e Cadeia de Custódia

The Evaluation of Digital Evidence in Brazilian Criminal Procedure:

Theoretical Foundations, Legal Nature and Chain of Custody

Adriano Procópio de Souza¹

Gustavo Henrique de Andrade Cordeiro²

Resumo: O crescente volume de dados digitais produzidos nas relações contemporâneas impôs ao processo penal brasileiro o desafio de adequar suas categorias tradicionais à realidade das evidências eletrônicas. O presente artigo examina os fundamentos teóricos, a natureza jurídica e o regime de custódia das provas digitais no ordenamento jurídico pátrio. Por meio de pesquisa bibliográfica e documental, com método dedutivo de abordagem, analisa-se a teoria da prova sob o paradigma do sistema acusatório, as especificidades técnicas das evidências eletrônicas, sua distinção em relação ao documento convencional e as implicações da cadeia de custódia para sua admissibilidade. Conclui-se que a prova digital constitui categoria probatória autônoma e que a integridade da cadeia de custódia é condição de admissibilidade das evidências eletrônicas no processo penal, não mera questão de valoração, impondo ao Estado o ônus de demonstrar a autenticidade e a confiabilidade dos dados apresentados em juízo.

Palavras-chave: Prova digital. Cadeia de custódia. Processo penal acusatório. Teoria da prova. Autenticidade probatória.

Abstract: The growing volume of digital data produced in contemporary relations has imposed on Brazilian criminal procedure the challenge of adapting its traditional categories to the reality of electronic evidence. This article examines the theoretical foundations, legal nature, and custody regime of digital evidence in the Brazilian legal system. Through bibliographic and documentary research, using a deductive method, the theory of evidence is analyzed under the accusatorial system paradigm, the technical specificities of electronic evidence, its distinction from conventional documents, and the implications of the chain of custody for admissibility. It concludes that digital evidence constitutes an autonomous evidentiary category and that chain of custody integrity is a condition of admissibility of electronic evidence in criminal proceedings, not merely a question of evidentiary weight, placing on the State the burden of demonstrating the authenticity and reliability of data presented in court.¹²

Keywords: Digital evidence. Chain of custody. Accusatorial criminal procedure. Theory of evidence. Evidentiary authenticity.

¹ Mestrando em Direito pelo Centro Universitário Eurípides de Marília (UNIVEM). Graduado em Direito pela Universidade de Marília (UNIMAR). ORCID: 0000-0002-4035-1628

² Doutor em Direito pela Instituição Toledo de Ensino (ITE). Promotor de Justiça do Ministério Público do Estado de São Paulo e Pró-Reitor Acadêmico do Centro Universitário Eurípides de Marília (UNIVEM). ORCID: 0000-0002-4035-1628.

1 INTRODUÇÃO

A inserção da tecnologia no cotidiano contemporâneo provocou transformações expressivas sobre o sistema de justiça criminal. O ambiente digital, que permeia desde as comunicações interpessoais até as transações financeiras e as atividades delitivas, passou a produzir rastros eletrônicos que assumem papel central nas investigações penais. No Brasil, a digitalização acelerada dos últimos anos criou um cenário em que as provas de natureza eletrônica transitaram de elemento probatório excepcional para instrumento corriqueiro da persecução penal. Ao mesmo tempo que esse fenômeno oferece ao Estado ferramentas investigativas de grande eficácia, ele impõe ao sistema processual desafios consideráveis quanto à adequação de suas categorias jurídicas tradicionais a uma realidade probatória radicalmente nova, para a qual o legislador ainda não forneceu respostas normativas suficientemente precisas.

Diante desse cenário, emerge um questionamento central: em que medida o ordenamento jurídico brasileiro oferece fundamentos normativos e doutrinários suficientes para assegurar a validade, a autenticidade e a admissibilidade das provas digitais no processo penal, considerando as peculiaridades técnicas dessas evidências e a ainda incipiente regulamentação de sua produção e valoração? A tensão entre as potencialidades investigativas das evidências eletrônicas e os riscos de manipulação e adulteração coloca em xeque tanto a eficácia da jurisdição penal quanto a preservação dos direitos fundamentais dos investigados. Esse dilema torna-se mais agudo quando se constata que a fragilidade inerente aos dados digitais, facilmente alteráveis, replicáveis e dependentes de aparatos tecnológicos para sua leitura, não encontra resposta satisfatória nas categorias processuais clássicas.

O presente estudo tem por objetivo geral analisar criticamente os fundamentos teóricos, a natureza jurídica e o regime de custódia das provas digitais no processo penal brasileiro, identificando as condições em que tais evidências podem ser produzidas, admitidas e valoradas de forma constitucionalmente adequada. Para tanto, estabelecem-se os seguintes objetivos específicos: (a) examinar a evolução da teoria da prova em face das inovações tecnológicas e seus reflexos sobre o sistema acusatório; (b) investigar as especificidades técnicas das provas digitais e sua distinção em relação ao documento; (c) analisar o instituto da cadeia de custódia como condição de integridade e autenticidade das evidências eletrônicas; (d) avaliar as consequências jurídicas da ruptura da cadeia de custódia, à luz da doutrina e da jurisprudência dos tribunais superiores.

Quanto à metodologia, adota-se o método dedutivo de abordagem, partindo-se de premissas gerais acerca dos princípios constitucionais que regem o processo penal, notadamente a presunção de inocência, o contraditório e a ampla defesa, para alcançar conclusões específicas sobre o regime jurídico das provas digitais. O procedimento é monográfico, com recorte temático centrado na valoração probatória e na cadeia de custódia no processo penal brasileiro. A pesquisa é de natureza bibliográfica e documental, de caráter exploratório e explicativo, valendo-se de fontes primárias, como legislação e jurisprudência dos tribunais superiores, e de fontes secundárias, como doutrina nacional e estrangeira e artigos científicos publicados em periódicos especializados. A abordagem qualitativa permite não apenas descrever o estado atual da disciplina normativa, mas sobretudo problematizar suas lacunas à luz das exigências de um processo penal democrático.

O primeiro eixo temático dedica-se ao exame das evidências no processo criminal, investigando como o avanço tecnológico transformou a teoria da prova e os modelos de persecução penal. A adoção do sistema acusatório pelo ordenamento constitucional de 1988, e sua reafirmação pela Lei n.º 13.964/2019, estabeleceram balizas fundamentais para a atividade probatória, impondo clara separação entre as funções de acusar, defender e julgar. Nesse contexto, serão examinadas a função da teoria da prova na garantia dos direitos constitucionais do acusado e as categorias fundamentais de fonte de prova e meio de prova, pressupostos indispensáveis à compreensão do estatuto jurídico das evidências digitais.

O segundo eixo aborda as especificidades técnicas e a natureza jurídica das provas digitais, problema que tem desafiado a doutrina e a jurisprudência diante da inadequação das categorias tradicionais. Serão examinadas as características que distinguem as evidências eletrônicas das provas físicas, como a imaterialidade, a volatilidade, a replicabilidade ilimitada e a dependência de recursos tecnológicos, bem como o debate doutrinário sobre seu enquadramento jurídico. A questão de se as provas digitais devem ser tratadas como documentos ou constituem categoria probatória autônoma revela implicações práticas significativas para a definição dos requisitos de admissibilidade e valoração no processo penal.

O terceiro eixo examina o instituto da cadeia de custódia das provas digitais, especialmente após sua positivação nos artigos 158-A a 158-F do Código de Processo Penal pelo Pacote Anticrime. Será investigada a origem desse instituto, seu desenvolvimento doutrinário no Brasil, com destaque para os conceitos de mesmidade e desconfiança, e as consequências jurídicas de sua ruptura. A análise da jurisprudência recente do Superior Tribunal de Justiça revela progressiva consolidação do entendimento de que a integridade da cadeia de custódia constitui condição de admissibilidade das provas digitais, e não mera questão

formal ou de valoração, o que reforça o papel central desse instituto na proteção das garantias processuais fundamentais.

O enfrentamento dessas questões revela-se essencial não apenas para a adequação técnico-normativa do processo penal às demandas da era digital, mas, sobretudo, para a preservação dos direitos fundamentais do acusado em um contexto em que o poder investigativo do Estado dispõe de instrumentos tecnológicos cada vez mais sofisticados. A análise proposta busca contribuir para a construção de parâmetros jurídicos mais precisos para a produção, admissão e valoração das provas digitais no Brasil, fomentando debate qualificado sobre os limites e as possibilidades da incorporação tecnológica ao processo penal democrático.

2 AS EVIDÊNCIAS NO PROCESSO CRIMINAL

2.1 O impacto das inovações tecnológicas e a evolução da teoria da prova na esfera processual penal

O desenvolvimento tecnológico provocou mudanças estruturais na dinâmica da persecução penal. Historicamente, as apurações criminais valiam-se de meios probatórios de natureza essencialmente física: documentos em papel, objetos apreendidos, laudos periciais sobre vestígios materiais e testemunhos presenciais. Essa realidade transformou-se de forma acelerada com a disseminação dos sistemas de vigilância eletrônica, dos smartphones e da conectividade em rede, que passaram a registrar e transmitir, continuamente, volumes expressivos de dados sobre comportamentos, deslocamentos, comunicações e transações. A persecução penal contemporânea viu-se diante de um novo universo probatório, caracterizado pela ubiquidade dos dados digitais e pela complexidade técnica de sua obtenção e análise (BADARÓ, 2021).

O mesmo progresso que beneficiou as investigações criminais também possibilitou o surgimento de novas modalidades delitivas, praticadas total ou parcialmente em ambiente virtual. Crimes como a fraude eletrônica, o estelionato informático, a extorsão virtual, a pornografia infantil e a organização criminosa com suporte tecnológico tornaram-se desafios permanentes para as agências de persecução. Diante disso, os investigadores precisaram adaptar técnicas e métodos ao ambiente digital, o que evidencia a relação dialética entre tecnologia e criminalidade e impõe ao sistema processual penal a urgência de desenvolver respostas normativas e hermenêuticas suficientemente ágeis para acompanhar a velocidade das transformações (LOPES JÚNIOR, 2022).

A teoria da prova, nesse contexto, desempenha papel central, pois é o instrumento que permite a reconstrução dos fatos e a verificação da responsabilidade penal do acusado, conferindo à atividade jurisdicional parâmetros de racionalidade e controlabilidade. Como observa Taruffo (1992), a prova não é um instrumento de acesso à verdade absoluta, mas o meio pelo qual se produz, no processo, um grau de certeza suficiente e racionalmente justificável para fundamentar a decisão judicial. Essa concepção epistemológica da prova assume importância ainda maior no contexto digital, em que a aparência de objetividade dos dados eletrônicos pode mascarar vulnerabilidades técnicas significativas, inacessíveis ao julgador sem o suporte de conhecimentos especializados.

A inexistência de regulamentação específica sobre a admissibilidade e a disciplina normativa das provas digitais no Brasil torna o apelo à teoria da prova ainda mais indispensável. Na ausência de normas próprias, os intérpretes recorrem aos princípios gerais do processo penal e às categorias doutrinárias disponíveis para equacionar problemas para os quais o legislador não ofereceu respostas adequadas. Esse estado de insuficiência normativa, embora não impeça a utilização de evidências eletrônicas, gera insegurança jurídica significativa e abre espaço para decisões inconsistentes que comprometem a isonomia do sistema (CARVALHO, 2020).

A teoria da prova é, ademais, imprescindível para resguardar os direitos constitucionais do acusado. A presunção de inocência, consagrada no artigo 5.º, inciso LVII, da Constituição Federal de 1988, que estabelece que ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória, impõe que a condenação só possa fundar-se em provas lícitas, obtidas em conformidade com as garantias do devido processo legal. De acordo com a jurisprudência do Superior Tribunal de Justiça, o direito ao silêncio configura garantia essencial da dignidade humana, assegurando ao acusado a prerrogativa de não colaborar para sua própria incriminação, sendo vedada qualquer interpretação desfavorável de sua recusa em produzir prova contra si mesmo (BRASIL, STJ, HC 179.486/GO, 2011).

Embora a busca da verdade seja finalidade do processo penal, é preciso reconhecer que a verdade absoluta é inacessível. Por isso, Laudan (2013) sustenta que o processo penal trabalha com verdades aproximadas, construídas a partir de evidências disponíveis e submetidas a regras epistêmicas que garantem sua confiabilidade. A chamada verdade processual, aquela estabelecida dentro dos limites legais e com base em evidências legitimamente produzidas, não é, portanto, mera convenção formal, mas o resultado de um processo de reconstrução racional dos fatos, cujo rigor garante tanto a eficácia da persecução quanto a proteção das garantias fundamentais. Essa compreensão epistemológica é especialmente relevante para o tratamento

das evidências digitais, cuja confiabilidade depende do cumprimento de exigências técnicas e procedimentais ainda não consolidadas no processo penal brasileiro.

2.2 Sistema acusatório no âmbito penal

O modelo acusatório de processo penal caracteriza-se, essencialmente, pela separação entre as funções de acusar, defender e julgar, atribuídas a sujeitos processuais distintos e autônomos. Essa divisão estrutural distingue o sistema acusatório do inquisitório, no qual o julgador acumulava concomitantemente os papéis de acusador e de árbitro, comprometendo de forma irremediável sua imparcialidade. O Código de Processo Penal brasileiro, com a redação conferida pela Lei n.º 13.964/2019, incorporou expressamente o modelo acusatório em seu artigo 3.º-A, estabelecendo que o processo penal terá estrutura acusatória, vedando a iniciativa do juiz na fase de investigação e a substituição da atuação probatória do órgão de acusação (LOPES JÚNIOR, 2022).

Nesse arranjo, o acusado é reconhecido como sujeito de direitos, titular das garantias da ampla defesa, do contraditório e do direito ao silêncio, não podendo ser compelido a colaborar com sua própria incriminação. A separação entre as funções processuais não é, portanto, mero arranjo organizacional: ela é a condição de possibilidade de um julgamento imparcial, no qual o magistrado decide com base nas provas trazidas pelas partes, sem comprometer-se previamente com qualquer hipótese acusatória (BADARÓ, 2021). A imparcialidade do julgador, nesse sentido, não é apenas uma garantia do acusado, mas um requisito de legitimidade epistêmica da decisão judicial, pois só pode ser verdadeira a decisão proferida por quem não está comprometido de antemão com nenhuma das versões em disputa.

A distinção entre meios de prova e meios de obtenção de prova, positivada em ordenamentos como o Código de Processo Penal de Portugal (1987) e o da Itália (1988), é fundamental para a compreensão das provas digitais. Os meios de prova servem diretamente para convencer o juiz sobre a veracidade de uma alegação fática, enquanto os meios de obtenção de prova consistem em técnicas destinadas a localizar fontes ou elementos probatórios que só posteriormente ingressarão no processo. A interceptação telemática, a busca e apreensão de dispositivos eletrônicos e a quebra de sigilo de dados são exemplos de meios de obtenção que precedem e viabilizam a produção da prova digital em sentido estrito, submetendo-se a regimes jurídicos específicos previstos na Constituição Federal e na legislação infraconstitucional (BADARÓ, 2021). Gössel (2007) observa que o princípio do Estado de Direito exige que o acusado disponha de meios efetivos de controle sobre a validade das provas que lhe são opostas.

2.3 Conceituações sobre prova

A palavra "prova" comporta, no léxico jurídico, pelo menos três acepções distintas: prova como atividade, que corresponde ao processo de produção probatória; prova como resultado, relativa à convicção formada no julgador; e prova como meio, referente aos instrumentos legalmente previstos para a formação da convicção judicial. Essa tríplice perspectiva, identificada por Ferrua (2004), é metodologicamente relevante porque permite situar o debate sobre as provas digitais em diferentes planos: o da produção (como se obtém e formaliza a evidência digital), o da admissibilidade (quais requisitos deve satisfazer) e o da valoração (qual peso deve ter na formação da convicção judicial).

A distinção entre fonte da prova, meio de prova, elemento probatório e resultado da prova é igualmente relevante. A fonte da prova é qualquer pessoa, objeto ou coisa capaz de fornecer informações relevantes à decisão judicial, existindo antes e independentemente do processo. O meio de prova é o veículo formal pelo qual as informações da fonte são introduzidas nos autos, submetendo-se ao contraditório. O elemento probatório é o dado bruto extraído da fonte, ainda não apreciado judicialmente. Por fim, o resultado da prova é a conclusão do magistrado sobre a confiabilidade da fonte e a relevância dos dados apresentados (BADARÓ, 2021). No campo das evidências digitais, um arquivo eletrônico é a fonte da prova; o laudo pericial que o examina é o meio de prova; os dados extraídos do arquivo são elementos probatórios; e a conclusão sobre sua autenticidade e integridade é o resultado da prova.

Além disso, a teoria da prova exerce papel primordial na definição dos limites da atividade estatal: ao estabelecer parâmetros claros para a obtenção e apresentação das evidências, contribui para fortalecer a credibilidade do sistema de justiça e impede práticas abusivas por parte do Estado. As regras que disciplinam a colheita e a produção de provas servem para assegurar o respeito aos direitos constitucionais do acusado em todas as fases do procedimento criminal, desde a investigação policial até a sentença definitiva. Um processo penal democrático exige, necessariamente, uma teoria probatória que coloque a dignidade da pessoa humana e as garantias fundamentais no centro de suas escolhas metodológicas (NUCCI, 2020).

3 DAS PROVAS DIGITAIS

3.1 Especificidades das provas digitais

As provas digitais configuram modalidade qualitativamente distinta de evidência, em razão de características técnicas que as diferenciam estruturalmente das provas físicas

convencionais. A principal particularidade reside em sua natureza imaterial: os dados digitais existem na forma de sequências binárias, que só se tornam inteligíveis ao ser humano mediante o uso de dispositivos capazes de decodificá-las e convertê-las em linguagem compreensível. Essa característica tem implicações diretas sobre a forma de coleta, preservação e apresentação em juízo das evidências eletrônicas, exigindo protocolos técnicos específicos que o processo penal tradicional não contempla de forma satisfatória, seja do ponto de vista normativo, seja do operacional (RODRIGUES, 2009).

A volatilidade é outra característica fundamental das evidências digitais. Diferentemente dos documentos físicos, que em geral preservam sua forma e conteúdo enquanto não são fisicamente destruídos ou alterados, os dados digitais podem ser apagados, modificados ou corrompidos de forma extremamente rápida, por vezes de modo inadvertido, como ocorre quando um dispositivo eletrônico é ligado após a apreensão, sobrescrevendo dados armazenados. Esse risco de perda ou adulteração acidental impõe que a coleta de provas digitais seja realizada com técnicas específicas de forense computacional, que incluem o espelhamento bit a bit do dispositivo e a verificação da integridade por meio de algoritmos hash, procedimentos que ainda carecem de regulamentação normativa expressa no ordenamento jurídico brasileiro (CARVALHO, 2020).

A replicabilidade ilimitada é uma terceira característica que distingue as evidências digitais. Ao contrário dos objetos físicos, os dados digitais podem ser copiados indefinidamente sem degradação de qualidade: cada cópia é idêntica ao dado de origem, tornando impossível, em princípio, a identificação de um exemplar original único. Essa propriedade facilita a preservação das evidências, pois permite que cópias sejam realizadas para análise sem comprometer o dado originalmente coletado; mas, ao mesmo tempo, cria riscos de adulteração indetectável, caso os procedimentos de verificação de integridade não sejam rigorosamente observados. A técnica da clonagem ou espelhamento, amplamente utilizada na forense computacional, busca justamente assegurar que as análises periciais sejam realizadas sobre cópias fidedignas, preservando o dado original (ZICCARDI, 2015).

Além da imaterialidade, da volatilidade e da replicabilidade, as provas digitais caracterizam-se pela dependência de aparatos tecnológicos para sua leitura e interpretação. Dados armazenados em formatos proprietários, criptografados ou fragmentados em múltiplos dispositivos só são acessíveis mediante ferramentas técnicas especializadas, inacessíveis à maioria dos atores processuais sem formação específica em forense digital. Essa dependência cria assimetrias informacionais significativas entre acusação e defesa, especialmente quando os meios de obtenção das evidências são controlados pelo Estado e a defesa carece de recursos

técnicos para questionar, de forma embasada, a autenticidade das evidências que lhe são opostas (GAHTAN, 1998). Fontenele Lemos, Cavalcante e Mota (2021) destacam que a ausência de regulamentação normativa específica agrava essas assimetrias, deixando ao intérprete a tarefa de colmatar lacunas por meio de analogia e princípios gerais, com riscos evidentes de inconsistência.

Os dados digitais podem ser capturados tanto quando armazenados em dispositivos, no âmbito da informática, quanto durante sua transmissão em redes, no âmbito da telemática. No primeiro caso, trata-se de dados em repouso, acessíveis mediante busca e apreensão do dispositivo; no segundo, de dados em trânsito, cujo acesso exige a interceptação da comunicação no momento em que ocorre. Ambas as situações submetem-se a regimes jurídicos distintos, previstos na Constituição Federal (artigo 5.º, incisos X, XI e XII) e na legislação infraconstitucional, e demandam protocolos técnicos diferenciados para assegurar a integridade das evidências obtidas. Essa distinção é metodologicamente relevante porque determina tanto as autoridades competentes para a obtenção das evidências quanto os requisitos formais que devem ser observados para que elas sejam consideradas válidas (BADARÓ, 2021).

3.2 A natureza jurídica das provas digitais

A questão da natureza jurídica das provas digitais tem sido objeto de debate doutrinário intenso, polarizado entre duas posições principais: aquela que enquadra a evidência eletrônica como espécie de documento, sujeitando-a ao regime processual da prova documental; e aquela que sustenta a autonomia categorial da prova digital, defendendo a necessidade de um regime jurídico próprio. A escolha entre essas posições tem implicações práticas decisivas sobre os requisitos de admissibilidade, os ônus de autenticação e os meios de impugnação disponíveis às partes no processo penal.

O Código de Processo Penal brasileiro, em seu artigo 232, conceitua documento de forma limitada, como quaisquer escritos, instrumentos ou papéis, públicos ou particulares. Essa definição, concebida em 1941, é claramente insuficiente para abranger a complexidade das evidências eletrônicas contemporâneas. A jurisprudência tem interpretado o conceito de documento de forma mais ampla, reconhecendo como tal diversas formas de expressão do pensamento humano; contudo, essa extensão interpretativa não resolve os problemas específicos das provas digitais, cuja natureza imaterial e cuja independência em relação ao suporte físico escapam às categorias do documento tradicional, concebido como objeto material portador de informação inscrita de forma duradoura (NUCCI, 2020).

A doutrina identifica duas grandes teorias sobre o conceito de documento: a teoria do escrito, que vincula o documento à ideia de permanência e durabilidade de um conteúdo escrito em suporte físico, e a teoria da representação, que compreende como documento qualquer elemento portador de informação, independentemente do suporte. Francesco Carnelutti, em formulação clássica recorrentemente citada na doutrina processual penal, define documento como algo capaz de representar um fato, formulação que serviu de base para as concepções mais amplas de documento em suporte não físico. Contudo, mesmo essa definição ampla não capta adequadamente as particularidades das evidências digitais, cuja essência imaterial e cuja independência em relação ao suporte físico as diferenciam dos documentos convencionais em aspectos que não podem ser ignorados (FERRUA, 2012).

A doutrina estrangeira desenvolveu distinção metodologicamente relevante entre computer-generated evidence, referente a provas produzidas digitalmente como simulações e animações por computador, e computer-derived evidence, correspondente a dados extraídos diretamente de arquivos informáticos. Apenas esta última categoria deve ser compreendida como prova digital em sentido estrito. Essa distinção, ainda pouco difundida na doutrina e jurisprudência brasileiras, é relevante porque permite identificar com precisão o objeto da regulamentação necessária e distinguir categorias probatórias que demandam tratamentos jurídicos distintos (GAHTAN, 1998).

Diante das insuficiências das categorias tradicionais, a posição mais adequada é a que reconhece a prova digital como categoria probatória autônoma, análoga ao documento, mas com características singulares que reclamam regime jurídico próprio. Essa autonomia categorial fundamenta-se em quatro elementos diferenciadores: (a) a imaterialidade, que torna o dado digital independente de suporte físico determinado; (b) a volatilidade, que exige protocolos específicos de preservação; (c) a replicabilidade, que inviabiliza a identificação de um exemplar original único; e (d) a dependência tecnológica, que torna a leitura e a interpretação dos dados condicionadas a aparatos técnicos especializados (RODRIGUES, 2009). O tratamento da prova digital como mero documento eletrônico subestima essas diferenças e cria riscos significativos de inadequação normativa, comprometendo a efetividade das garantias processuais do acusado (CARVALHO, 2020).

Uma distinção frequentemente negligenciada na prática forense brasileira é aquela entre documento eletrônico e prova digital. O documento eletrônico é um arquivo digital criado com a finalidade de representar um ato ou fato jurídico de forma duradoura, como um contrato eletrônico assinado digitalmente, cujos requisitos de autenticidade são definidos por mecanismos de criptografia e certificação digital. A prova digital, por sua vez, é mais

abrangente: inclui dados que não foram criados com finalidade probatória, mas que se tornaram evidência de um fato criminoso, como mensagens trocadas em aplicativos de comunicação instantânea, registros de navegação na internet ou logs de acesso a sistemas informatizados. Os requisitos de autenticidade aplicáveis ao documento eletrônico não são automaticamente transferíveis à prova digital, que exige mecanismos próprios de verificação baseados em protocolos de forense computacional (FONTENELE LEMOS; CAVALCANTE; MOTA, 2021).

4 ACERCA DA CADEIA DE CUSTÓDIA

4.1 Conceituação de cadeia de custódia

O instituto da cadeia de custódia das provas encontra suas raízes na tradição jurídica norte-americana, no contexto da qual se desenvolveu como mecanismo de garantia da integridade das evidências ao longo de todo o procedimento criminal, desde sua coleta no local do crime até sua apresentação ao tribunal. A lógica subjacente ao instituto é de enorme relevância epistêmica: para que uma evidência possa ser racionalmente valorada pelo julgador, é necessário demonstrar que o objeto ou dado apresentado em juízo é o mesmo que foi originalmente coletado, e que permaneceu inalterado ao longo de toda a cadeia de manuseio. Sem essa demonstração, não há como afirmar, com o grau de certeza exigido pelo processo penal democrático, que a evidência apresentada corresponde à realidade dos fatos investigados (PRADO, 2019).

No Brasil, a cadeia de custódia foi expressamente positivada pela Lei n.º 13.964/2019 (Pacote Anticrime), que inseriu os artigos 158-A a 158-F no Código de Processo Penal. O artigo 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 crime, com a finalidade de rastrear sua posse e manuseio a partir de seu reconhecimento até seu descarte. Embora essa positivação mereça reconhecimento, a doutrina aponta que a definição legal apresenta limitações: ao vincular a obrigatoriedade da cadeia de custódia predominantemente às provas de natureza pericial, não disciplina de forma específica o tratamento das evidências digitais, que possuem peculiaridades técnicas que demandam protocolos próprios e mais rigorosos (BADARÓ, 2021).

Geraldo Prado, principal referência doutrinária brasileira sobre o tema, apresenta a cadeia de custódia como um método por meio do qual se pretende preservar a integridade do elemento probatório e assegurar sua autenticidade, cuja finalidade última é prevenir o erro

judiciário e melhorar a qualidade da prestação jurisdicional (PRADO, 2014, p. 86). Para o autor, dois princípios fundamentam o instituto: a mesmidade, que garante que a prova valorada pelo juiz é exatamente a mesma que foi coletada na cena do crime; e a desconfiança, que impõe uma postura crítica sobre as informações apresentadas pelas partes, exigindo verificação independente de sua autenticidade. Esses dois princípios atuam de forma complementar: a mesmidade define o objetivo a ser alcançado, e a desconfiança estabelece a atitude epistêmica necessária para garanti-lo ao longo de todo o procedimento probatório.

O Superior Tribunal de Justiça tem reconhecido expressamente a relevância funcional do instituto, afirmando que a principal finalidade da cadeia de custódia é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo (BRASIL, STJ, AgRg no RHC 143.169/RJ). Essa formulação jurisprudencial sintetiza com precisão a função epistêmica da cadeia de custódia: não se trata de mera exigência burocrática, mas de condição necessária para que as evidências apresentadas ao processo possam ser racionalmente valoradas como representação fiel dos fatos investigados. Sem a cadeia de custódia, o juiz estaria valorizando um dado cuja autenticidade não pode ser verificada, comprometendo irremediavelmente a racionalidade da decisão judicial.

No âmbito das provas digitais, as exigências da cadeia de custódia assumem especificidades técnicas próprias. O Superior Tribunal de Justiça, em paradigmático acórdão, consolidou o entendimento de que é ônus do Estado-acusação comprovar a integridade, a autenticidade e a confiabilidade do material extraído de dispositivos eletrônicos, sendo inadmissível presumir a veracidade das alegações estatais quando descumpridos os procedimentos da cadeia de custódia. O acórdão exige documentação completa e adoção de métodos auditáveis, repetíveis e reproduzíveis, com observância de padrões técnicos reconhecidos, incluindo a verificação de integridade por hash e o registro de logs de acesso, sob pena de imprestabilidade da prova (BRASIL, STJ, AgRg no HC 828.054/RN, 2024). Essa orientação representa uma mudança paradigmática: a cadeia de custódia deixa de ser tratada como formalidade acessória e passa a ser reconhecida como condição de validade epistêmica das evidências digitais.

A doutrina espanhola, com reflexos na brasileira, introduziu o conceito de mesmidade da prova, assegurando que a evidência exibida ao tribunal seja exatamente a mesma recolhida na cena do fato. Esse conceito implica a adoção de formalidades rigorosas no tratamento e na custódia das evidências: cada pessoa que manuseia a prova deve ser identificada, o momento exato do contato deve ser registrado, e o estado do objeto ou dado deve ser documentado antes

e depois de cada intervenção. Sem essas formalidades, torna-se impossível demonstrar, com base em critérios racionais e controláveis pelas partes, que a evidência apresentada ao julgador não foi substituída, adulterada ou modificada ao longo do procedimento (PRADO, 2019). A cadeia de custódia não é, portanto, apenas um instrumento de controle administrativo, mas uma garantia constitucional implícita do devido processo legal.

4.2 Da ruptura ou quebra da cadeia de custódia das provas digitais

A chamada quebra da cadeia de custódia das provas digitais é objeto de intensa controvérsia doutrinária e jurisprudencial, que gira em torno de dois problemas centrais: o que configura, efetivamente, uma ruptura na cadeia de custódia; e quais são as consequências processuais dessa ruptura. A compreensão precisa desses problemas é fundamental para evitar tanto o excesso, que tornaria inadmissível qualquer prova obtida sem o cumprimento rigoroso de todas as formalidades, quanto a omissão, que permitiria ao Estado apresentar evidências de autenticidade duvidosa como representações fidedignas dos fatos investigados.

Do ponto de vista terminológico, a expressão quebra da cadeia de custódia é tecnicamente imprecisa: o que ocorre, na realidade, é a ausência de documentação integral do percurso da evidência, o que pode ou não corresponder a uma adulteração efetiva da fonte probatória. Uma cadeia de indivíduos que manejaram o vestígio sempre existirá; o que pode falhar é o registro documental dessa cadeia. Se inexistirem anotações sobre as pessoas que tiveram contato com a evidência, os momentos de cada intervenção e o estado do objeto ou dado antes e depois de cada manuseio, a cadeia de custódia, no sentido de documentação comprobatória, não poderá ser estabelecida, tornando impossível qualquer verificação sobre a integridade da fonte probatória (PRADO, 2014).

A doutrina divide-se entre duas correntes principais sobre as consequências jurídicas da ruptura da cadeia de custódia. A corrente da inadmissibilidade sustenta que a ausência de documentação integral compromete irremediavelmente a admissibilidade da prova: sem a demonstração de que a evidência é autêntica e íntegra, não há como valorá-la racionalmente, pois o juiz estaria em posição de ignorância sobre se o dado apresentado corresponde ao que foi efetivamente coletado. A corrente da relativização, por sua vez, defende que falhas pontuais na cadeia de custódia, desprovidas de indícios concretos de adulteração, não implicam automaticamente a inadmissibilidade da prova, mas afetam seu peso probatório, competindo ao juiz avaliar o conjunto do material disponível para determinar se as falhas comprometeram efetivamente a confiabilidade das evidências (LIMA, 2022).

O Superior Tribunal de Justiça tem desenvolvido, nos últimos anos, jurisprudência progressivamente mais rigorosa sobre o tema. No julgamento do AgRg no RHC 184.003/SP, a Corte afirmou que provas digitais colhidas sem a devida observância da cadeia de custódia são inadmissíveis, por colocarem em risco os princípios do contraditório e da ampla defesa. O voto condutor destacou que a prova digital deve ser completa e íntegra para ser admitida em juízo e que a corrupção de parte dos arquivos compromete a integralidade da prova, inviabilizando sua utilização (BRASIL, STJ, AgRg no RHC 184.003/SP). Essa orientação revela uma compreensão mais exigente sobre a qualidade técnica das evidências eletrônicas e sobre as responsabilidades das autoridades encarregadas de sua coleta e preservação.

Em decisão proferida em 2025, o Tribunal declarou inadmissíveis provas extraídas de um celular apreendido porque a autoridade policial limitou-se a realizar capturas de tela das conversas em aplicativo de mensagens, sem adotar protocolos técnicos adequados de preservação da cadeia de custódia digital, como o espelhamento bit a bit e a verificação de integridade por algoritmos hash. A Corte foi categórica ao afirmar que é ônus do Estado comprovar a integridade e a confiabilidade das fontes de prova por ele apresentadas, sendo incabível presumir a veracidade das alegações estatais quando descumpridos os procedimentos referentes à cadeia de custódia (BRASIL, STJ, HC 1.036.370, 2025). Esse acórdão sinaliza uma mudança estrutural no tratamento jurisprudencial das evidências digitais: não cabe ao acusado provar que a prova é falsa, mas ao Estado provar que ela é verdadeira e foi obtida de forma íntegra.

A falta de comprovação técnica acerca da integridade e da autenticidade dos dados digitais deve conduzir à inadmissão da prova já na fase de análise de admissibilidade, e não apenas na etapa de valoração probatória. Como ressalta a doutrina italiana, a preservação da autenticidade das provas eletrônicas constitui valor absoluto ao qual as autoridades investigativas devem se submeter, sob pena de inutilização do material obtido por ausência de credibilidade e de capacidade epistêmica para representar fidedignamente os fatos criminosos (RODRIGUES, 2009). Ao réu compete apenas apontar que os métodos de apreensão, preservação e registro não obedeceram aos padrões forenses reconhecidos; incumbe à acusação demonstrar que, a despeito das irregularidades procedimentais, os dados específicos apresentados ao processo mantiveram sua integridade e autenticidade (PRADO, 2019).

5 CONCLUSÃO

O presente estudo dedicou-se à análise crítica dos elementos probatórios digitais no processo penal brasileiro, examinando seus fundamentos teóricos, suas especificidades

técnicas, sua natureza jurídica e o regime de custódia que lhes deve ser aplicado. O ponto de partida foi o reconhecimento de que a digitalização acelerada da sociedade contemporânea gerou um novo universo probatório, caracterizado pela ubiquidade dos dados eletrônicos e pela complexidade técnica de sua obtenção, preservação e análise, que o ordenamento jurídico brasileiro ainda não regulamentou de forma suficientemente específica e sistemática. Esse estado de insuficiência normativa não impede a utilização de evidências eletrônicas no processo penal, mas impõe aos intérpretes o desafio de construir soluções hermenêuticas que conciliem a efetividade da persecução com a proteção dos direitos fundamentais do acusado.

Buscando responder ao questionamento sobre os fundamentos normativos e doutrinários disponíveis no ordenamento jurídico brasileiro para assegurar a validade, a autenticidade e a admissibilidade das provas digitais, o estudo examinou, por meio de pesquisa bibliográfica e documental com método dedutivo, as categorias da teoria da prova, as especificidades das evidências eletrônicas e o regime da cadeia de custódia. O percurso analítico permitiu identificar os pontos de inadequação das categorias processuais tradicionais, os critérios doutrinários e jurisprudenciais progressivamente construídos para suprir as lacunas normativas e os desafios que permanecem sem solução satisfatória no ordenamento vigente.

No primeiro eixo de análise, constatou-se que o avanço tecnológico transformou de forma estrutural a dinâmica probatória do processo penal, tornando as evidências digitais componente indispensável de um número crescente de investigações criminais. A adoção expressa do sistema acusatório pela Lei n.º 13.964/2019 reafirmou os princípios da imparcialidade judicial, do contraditório e da presunção de inocência como pilares da atividade probatória, impondo que a coleta e a valoração das provas digitais se subordinem a garantias processuais robustas. A teoria da prova revelou-se instrumento indispensável para a construção de critérios racionais de admissibilidade e valoração dessas evidências, operando como filtro epistemológico que distingue as evidências confiáveis das que não satisfazem os requisitos mínimos de autenticidade e integridade.

No segundo eixo, verificou-se que as provas digitais possuem características técnicas que as distinguem estruturalmente das provas físicas convencionais: a imaterialidade, a volatilidade, a replicabilidade ilimitada e a dependência de aparatos tecnológicos para sua leitura e interpretação. Essas características inviabilizam o tratamento das evidências eletrônicas como simples modalidade de prova documental, revelando a necessidade de reconhecê-las como categoria probatória autônoma, com regime jurídico próprio. A distinção entre documento eletrônico e prova digital mostrou-se metodologicamente relevante, pois os requisitos de autenticidade aplicáveis ao primeiro não são automaticamente transferíveis à

segunda, que exige mecanismos próprios de verificação baseados em protocolos de forense computacional.

No terceiro eixo, a análise da cadeia de custódia revelou ser esse instituto o principal mecanismo disponível no ordenamento jurídico brasileiro para assegurar a autenticidade e a integridade das provas digitais. A positivação dos artigos 158-A a 158-F do Código de Processo Penal pelo Pacote Anticrime representou avanço significativo, ao estabelecer obrigação expressa de documentação do percurso cronológico das evidências. Contudo, a legislação vigente apresenta limitações importantes: ao vincular a cadeia de custódia predominantemente às provas periciais, deixa sem regulamentação específica os protocolos aplicáveis às evidências digitais, cujas peculiaridades técnicas demandam exigências ainda mais rigorosas do que as previstas para as provas físicas convencionais.

Diante do exposto, conclui-se que o ordenamento jurídico brasileiro, embora disponha de fundamentos normativos e doutrinários relevantes para a regulamentação das provas digitais, ainda não oferece respostas normativas suficientemente específicas e sistemáticas para os desafios que essas evidências apresentam. A jurisprudência do Superior Tribunal de Justiça tem avançado significativamente no preenchimento dessas lacunas, reconhecendo progressivamente que a integridade da cadeia de custódia constitui condição de admissibilidade, e não mera questão de valoração, das evidências eletrônicas, e que o ônus de demonstrar a autenticidade das provas digitais recai sobre o Estado-acusação. Essa construção jurisprudencial, embora necessária, não substitui a urgência de uma regulamentação normativa específica que estabeleça, com clareza e segurança jurídica, os protocolos técnicos aplicáveis à obtenção, preservação e apresentação das provas digitais no processo penal.

Reconhece-se que o debate sobre as consequências jurídicas da ruptura da cadeia de custódia comporta posições divergentes. De um lado, sustenta-se que qualquer falha na documentação do percurso da evidência torna inadmissível a prova digital, sob o fundamento de que, sem demonstração de integridade, o julgador estaria valorando um dado cuja correspondência com os fatos investigados é incerta, violando os princípios da presunção de inocência e do devido processo legal. De outro, argumenta-se que falhas pontuais e de menor gravidade na cadeia de custódia, desprovidas de indícios concretos de adulteração, não devem conduzir à inadmissibilidade automática, mas à redução do peso probatório, competindo ao juiz avaliar o conjunto do material disponível. Ambas as perspectivas apresentam fundamentos legítimos, e sua resolução depende de exame cuidadoso das circunstâncias concretas de cada caso.

Ao término desta investigação, entende-se que a adoção de uma postura epistemicamente rigorosa sobre as provas digitais, que exija a demonstração de autenticidade e integridade como condição de admissibilidade e que atribua ao Estado o ônus dessa demonstração, é a que melhor se compatibiliza com os princípios do sistema acusatório e com a proteção da presunção de inocência. A incorporação tecnológica ao processo penal é inevitável e pode contribuir para a efetividade da persecução e para a qualidade da justiça criminal; contudo, não pode prescindir de salvaguardas processuais robustas que impeçam que a sofisticação técnica sirva de instrumento de substituição das garantias fundamentais do acusado. Para pesquisas futuras, sugere-se o aprofundamento dos debates sobre os padrões técnicos aplicáveis à forense computacional no Brasil, a criação de protocolos normativos específicos para cada categoria de evidência digital e a formação continuada dos operadores do direito para a compreensão das tecnologias envolvidas na produção e no controle dessas evidências.

REFERÊNCIAS

- BADARÓ, Gustavo Henrique. Processo penal. 9. ed. São Paulo: Revista dos Tribunais, 2021.
- BENNASAR, Andrés Jaume. La validez del documento electrónico y su eficacia en sede procesal. Valladolid: Lex Nova, 2010.
- BENUCCI, Renato Luis. A tecnologia aplicada ao processo judicial. Campinas: Millenium Editora, 2006.
- BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 mar. 2025.
- BRASIL. Decreto-Lei n.º 3.689, de 3 de outubro de 1941. Código de Processo Penal. Diário Oficial da União, Rio de Janeiro, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 10 mar. 2025.
- BRASIL. Lei n.º 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal e os meios de obtenção da prova. Diário Oficial da União, Brasília, DF, 5 ago. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 10 mar. 2025.
- BRASIL. Lei n.º 13.441, de 8 de maio de 2017. Altera o Estatuto da Criança e do Adolescente para prever a infiltração de agentes de polícia na internet. Diário Oficial da União, Brasília, DF, 9 maio 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13441.htm. Acesso em: 10 mar. 2025.

BRASIL. Lei n.º 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União, Brasília, DF, 24 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113964.htm. Acesso em: 10 mar. 2025.

BRASIL. Superior Tribunal de Justiça. Quinta Turma. Agravo Regimental no Habeas Corpus n.º 828.054/RN. Relator: Ministro Joel Ilan Paciornik. Julgamento em: 23 abr. 2024. Disponível em: <https://www.stj.jus.br>. Acesso em: 10 mar. 2025.

BRASIL. Superior Tribunal de Justiça. Quinta Turma. Agravo Regimental no Recurso em Habeas Corpus n.º 143.169/RJ. Relator para acórdão: Ministro Ribeiro Dantas. Disponível em: <https://www.stj.jus.br>. Acesso em: 10 mar. 2025.

BRASIL. Superior Tribunal de Justiça. Quinta Turma. Agravo Regimental no Recurso em Habeas Corpus n.º 184.003/SP. Disponível em: <https://www.stj.jus.br>. Acesso em: 10 mar. 2025.

BRASIL. Superior Tribunal de Justiça. Quinta Turma. Habeas Corpus n.º 179.486/GO. Relator: Ministro Jorge Mussi. Julgamento em: 14 jun. 2011. Disponível em: <https://www.stj.jus.br>. Acesso em: 10 mar. 2025.

BRASIL. Superior Tribunal de Justiça. Quinta Turma. Habeas Corpus n.º 1.036.370. Relator: Ministro Joel Ilan Paciornik. Julgamento em: set. 2025. Disponível em: <https://www.stj.jus.br>. Acesso em: 10 mar. 2025.

CARVALHO, Paulo Roberto de Lima. Prova cibernética no processo penal brasileiro. São Paulo: Saraiva Educação, 2020.

FERRUA, Paolo. Il libero convincimento del giudice penale: i limiti legali. Milano: Giuffrè, 2004.

FERRUA, Paolo. Il 'giusto processo'. 2. ed. Bologna: Zanichelli, 2012.

FONTENELE LEMOS, Diego; HOMSI CAVALCANTE, Larissa; GONÇALVES MOTA, Rafael. A prova digital no direito processual brasileiro. Revista Acadêmica Escola Superior do Ministério Público do Ceará, v. 13, n. 1, p. 11-34, 2021. DOI: 10.54275/raesmpce.v13i1.147. Disponível em: <https://revistaacademica.mpce.mp.br/revista/article/view/147>. Acesso em: 2 mar. 2025.

GAHTAN, Alan M. Computer crimes. Aurora: Canada Law Book, 1998.

GÖSSEL, Karl Heinz. El principio de Estado de Derecho en su significado para el proceso penal. In: GÖSSEL, Karl Heinz. El derecho procesal penal en el Estado de Derecho. Obras completas. Santa Fé: Rubinzal-Culzoni, 2007.

LAUDAN, Larry. Verdad, error y proceso penal: un ensayo sobre epistemología jurídica. Tradução de Carmen Vázquez e Edgar Aguilera. Madrid: Marcial Pons, 2013.

LIMA, Renato Brasileiro de. Manual de processo penal. 11. ed. Salvador: Juspodivm, 2022.

LOPES JÚNIOR, Aury. Direito processual penal. 19. ed. São Paulo: SaraivaJur, 2022.

NUCCI, Guilherme de Souza. Código de Processo Penal comentado. 19. ed. Rio de Janeiro: Forense, 2020.

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

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

RODRIGUES, Benjamim Silva. Direito penal. Parte especial, I: direito penal informático-digital. Coimbra: Coimbra Editora, 2009.

TARUFFO, Michele. La prova dei fatti giuridici. Milano: Giuffrè, 1992.

ZICCARDI, Giovanni. Informática jurídica: direito e tecnologia da informação. São Paulo: Saraiva, 2015.