



University of
Texas Libraries



e-revist@s



Centro Universitário Santo Agostinho

revista fsa

www4.fsnet.com.br/revista

Rev. FSA, Teresina, v. 22, n. 4, art. 4, p. 71-87, abr. 2025

ISSN Impresso: 1806-6356 ISSN Eletrônico: 2317-2983

<http://dx.doi.org/10.12819/2025.22.4.4>

DOAJ DIRECTORY OF
OPEN ACCESS
JOURNALS

WZB
Wissenschaftszentrum Berlin
für Sozialforschung



Cadeia de Custódia nas Provas Digitais: Desafios e Estratégias para a Preservação da Integridade Probatória

Chain of Custody in Digital Evidence: Challenges and Strategies for Preserving Evidence Integrity

Almir Santos Reis Junior

Doutor em Direito Penal pela Pontifícia Universidade Católica de São Paulo

Professor adjunto do curso de Direito da Universidade Estadual de Maringá

Professor convidado do curso de Doutorado em Direito Público, da Universidade Católica de Moçambique

E-mail: almir.crime@gmail.com

Ana Luiza Yumi Vargas

Graduada em Direito pela Universidade Estadual de Maringá, no Paraná.

Residente Jurídica do Ministério Público do Estado do Paraná.

E-mail: analuzayumi@hotmail.com

Endereço: Almir Santos Reis Junior

Rua Regina Marson Badan, 564 – Jd. Iguaçu – Maringá – PR – CEP 87060-160. Brasil.

Endereço: Ana Luiza Yumi Vargas

Rua Rio Jaguaribe, nº 595, Jardim Pinheiros 03, CEP: 87040-580, Maringá/PR. Brasil.

Editor-Chefe: Dr. Tonny Kerley de Alencar Rodrigues

Artigo recebido em 05/03/2025. Última versão recebida em 20/03/2025. Aprovado em 21/03/2025.

Avaliado pelo sistema Triple Review: a) Desk Review pelo Editor-Chefe; e b) Double Blind Review (avaliação cega por dois avaliadores da área).

Revisão: Gramatical, Normativa e de Formatação



RESUMO

O presente trabalho busca analisar o procedimento da cadeia de custódia nas provas digitais, introduzido na legislação brasileira por meio da Lei 13.964/2019, particularmente, nos artigos 158-A a 158-F, do Código de Processo Penal. Para tanto, apresenta-se o conceito de provas digitais e suas características. Partindo do pressuposto de que as provas digitais são dotadas de imaterialidade, fragilidade, volatilidade e dispersão, verifica-se que a documentação da cronologia da prova de forma detalhada se torna ainda mais necessária, a fim de garantir a integridade dos dados ao longo de todo o processo investigativo e judicial, sob risco de contrariar princípios como o da autenticidade (ou “mesmidade”), da ampla defesa, do contraditório, e ainda, a inadmissibilidade da prova ilícita no processo penal. Para execução deste trabalho adotou-se o método hipotético-dedutivo, a partir de hipóteses criadas e falseadas em busca de uma solução à problemática exposta, por meio do emprego da técnica de pesquisa bibliográfica a partir de livros, artigos, teses, jurisprudências e legislações. Ao final, chegou-se à conclusão de que a ausência de devida produção da prova digital com a quebra da cadeia de custódia relativiza os direitos e garantias fundamentais do investigado e, por isso, é imprescindível a utilização de práticas técnicas robustas e a especialização tanto para agentes públicos quanto para peritos forenses computacionais.

Palavras-chave: Cadeia de Custódia. Prova Digital. Investigação. Procedimento. Integridade Digital.

ABSTRACT

This paper aims to analyze the chain of custody procedure for digital evidence, introduced into Brazilian law by Law 13,964/2019, particularly in articles 158-A to 158-F of the Code of Criminal Procedure. To this end, the concept of digital evidence and its characteristics are presented. Assuming that digital evidence is immaterial, fragile, volatile, and dispersed, it is clear that documenting the chronology of the evidence in detail becomes even more necessary in order to guarantee the integrity of the data throughout the investigative and judicial process, at the risk of contradicting principles such as authenticity (or “sameness”), full defense, adversarial principle, and also the inadmissibility of illicit evidence in criminal proceedings. To carry out this work, the hypothetical-deductive method was adopted, based on hypotheses created and falsified in search of a solution to the problem exposed, through the use of the bibliographic research technique based on books, articles, theses, case law and legislation. In the end, it was concluded that the lack of due production of digital evidence with the breaking of the chain of custody relativizes the fundamental rights and guarantees of the investigated and, therefore, the use of robust technical practices and specialization is essential for both public agents and computer forensic experts.

Keywords: Chain of Custody. Digital Evidence. Investigation. Procedure. Digital Integrity.

1 INTRODUÇÃO

O tema central da presente investigação consiste na cadeia de custódia da prova digital, introduzida na legislação brasileira por meio da Lei 13.964/2019, nos artigos 158-A a 158-F, do Código de Processo Penal. A cadeia de custódia apresenta-se como um mecanismo garantidor da autenticidade das evidências coletadas, garantindo um registro detalhado de todo o percurso de uma prova obtida por meio eletrônico ou em formato digital, desde sua coleta inicial até sua apresentação e avaliação no processo judicial.

A autenticidade de uma prova utilizada no processo penal exige medidas para evitar sua contaminação. No tocante ao uso das provas digitais, que é um meio de prova atípico no processo penal, já que não encontra expressa previsão legal, a descrição dos sistemas informáticos utilizados e o relatório detalhado dos resultados obtidos são ainda mais imprescindíveis.

Verifica-se, na aplicação da cadeia de custódia na prova digital, a busca por propostas para as etapas da cadeia de custódia, quanto à individualização e apreensão dessas provas digitais, que devem ser seguidas rigorosamente, sob pena de a prova ser considerada inutilizável.

O presente estudo justifica-se pelo cenário jurídico contemporâneo, já que a ascensão das tecnologias digitais transformou drasticamente a maneira como as provas são coletadas, armazenadas e apresentadas em processos legais. A era digital trouxe consigo uma ampla gama de desafios e oportunidades, especialmente no que diz respeito à autenticidade e integridade das evidências digitais.

Para tanto, serão explorados os desafios do uso das provas digitais e a importância da cadeia de custódia da prova digital, bem como as consequências da violação da cadeia de custódia da prova digital relativamente aos meios de obtenção de provas digitais, que podem ter ocorrido no momento em que a prova foi colhida, até a apresentação à instrução processual.

Destaca-se, ainda, que há divergência na doutrina quanto às consequências da quebra da custódia das provas digitais, sendo que uma corrente defende que a prova digital decorrente da quebra da cadeia de custódia será inadmissível, enquanto a segunda corrente entende pela licitude da prova, contudo com valor probatório reduzido. Dessa maneira, é relevante realizar um estudo aprofundado sobre os impactos que a implementação da cadeia de custódia reflete nas provas digitais no processo penal brasileiro.

Ao final, analisam-se os desafios que surgirão com a aplicação da cadeia de custódia na prova digital e, sobretudo, verifica-se sua compatibilidade com os princípios estabelecidos pela Constituição, a fim de assegurar a integridade e a confiabilidade das evidências coletadas em formato digital dentro do Estado Democrático de Direito.

2 REFERENCIAL TEÓRICA

2.1 Provas Digitais

O ambiente digital está cada vez mais se destacando como o principal cenário para as interações humanas, e, como resultado, novas tecnologias têm ampliado a capacidade de adquirir e armazenar informações por meios eletrônicos.

O rápido avanço tecnológico, a diversidade de dispositivos e plataformas digitais, bem como a privacidade e segurança de dados justificam a necessidade de rigor técnico e procedimental quanto à cadeia de custódia das provas digitais.

Nessa perspectiva, Thiago Solon Gonçalves Albeche (2023) aponta que:

Vivemos a era *hibridismo existencial*, conjugando nossa existência no mundo cibernético com o mundo físico, alternando entre o estado “online” e o “offline”. Não há uma substituição do mundo físico pelo virtual, mas assumimos, cada vez mais, um modelo cultural *cyborgueano*, que conjuga a vida em uma parte orgânica e outra cibernética, sendo necessário assimilar que as interações que ocorrem no ambiente virtual também compõem a realidade.

O “ciberespaço” apresenta características como a ausência de localização geográfica específica, estando funcionalmente acessível em qualquer lugar; a transnacionalidade, que transcende as fronteiras dos Estados soberanos e não pertence a nenhum em particular, embora seja acessível a partir de todos; a neutralidade, permitindo aos usuários transmitir e acessar conteúdos livremente; a falta de centralização, sem um ponto central de origem ou disseminação, sendo global, coletivo e popular; e a possibilidade de ações anônimas e de ser alterado pelos próprios usuários (MINTO, 2021).

Qualquer recurso que possa contribuir à formação de uma prova é considerado uma fonte de prova. Em contraste, o meio de prova se refere ao instrumento pelo qual a prova é apresentada no processo. Entre a coleta de dados digitais e a apresentação da prova digital, é crucial seguir uma cadeia de custódia rigorosa. Se houver falhas nos meios de prova, isso pode resultar na nulidade da prova apresentada. Por outro lado, se houver falhas na obtenção da prova, a consequência poderá ser a inadmissibilidade, levando à sua exclusão do processo. Nesse contexto, o termo “prova digital” se refere a: (...) “dados produzidos e processados a

partir da lógica binária – dados digitais – e que têm potencial para serem utilizados como fonte de prova no Processo Penal” (MINTO, 2021, p. 15).

A importância dessas provas tem aumentado, especialmente em casos de crimes cibernéticos ou em situações nas quais, pelo menos, uma parte do crime tenha se desenvolvido por meios digitais, como redes sociais, aplicativos de mensagens, dispositivos criptografados ou armazenamento em nuvem, uma vez que permite demonstrar a materialidade e a autoria de um fato em um processo judicial (COUTINHO, 2024).

Na concepção de Gustavo Badaró (2023, p. 188), a prova digital tem por característica a ausência de materialidade e é altamente volátil, sujeita à constante alterabilidade, uma vez que: “(...) ainda que os dados digitais, em seu conteúdo informativo, possam ser diretamente percebidos por quem está em contato com eles, eles não possuem uma materialidade imediatamente constatável”.

Sobre a mesma temática, Andressa Olmedo Minto (2021) elenca as características da prova digital como sendo imaterialidade, fragilidade, volatilidade e dispersão, bem como aduz que as provas digitais necessitam de um método específico que não foi abrangido nas disposições sobre cadeia de custódia inseridas pela Lei 13.964/2019.

Sendo assim, a prova digital é imaterial, pois existe independentemente do suporte físico no qual está armazenada; é frágil, pois é passível de influências externas e uma manipulação descuidada pode resultar na perda de suas propriedades ou até mesmo na sua eliminação; é volátil, pois pode desaparecer tanto de forma intencional quanto não intencional; e possui a característica de dispersão porque pode estar localizada em vários locais diferentes (MINTO, 2021).

A prova digital, portanto, exige uma análise especializada por peritos em informática, que devem praticar ações somente dentro de sua área de competência e incluir a verificação de dados criptografados, a presença de metadados (como alterações nas datas e horas de criação ou acesso de arquivos), e-mails com destinatários em cópia oculta e fotografias que necessitam da identificação do número de série da câmera, para determinar quem usou o aparelho. Ademais, é essencial examinar a localização geográfica do dispositivo e o momento em que uma imagem foi capturada (MINTO, 2021).

Para os trabalhos de investigação de dados digitais, são sugeridas as seguintes ações: a) identificar o dispositivo de armazenamento que abarca o dado digital relevante para a investigação; b) capturar o dado digital por meio de técnicas de interceptação, quando se trata de comunicação em fluxo, ou através da apreensão e cópia ou espelhamento do dispositivo onde o arquivo de dados está armazenado; c) armazenar os dados digitais obtidos e copiados

em um local seguro e apropriado; d) analisar os dados obtidos – exclusivamente a partir da cópia do dispositivo de armazenamento – que sejam pertinentes ao foco da investigação; e) apresentar os resultados da investigação em tribunal, incluindo a produção de prova pericial e possíveis esclarecimentos verbais pelos peritos durante a audiência (BADARÓ, 2021).

O entendimento jurisprudencial aponta que outros aspectos das evidências digitais, garantidas pelo uso de metodologias da ABNT (Associação Brasileira de Normas Técnicas) são:

[...] as partes devem ter condições de aferir se o método técnico-científico para a extração dos dados foi devidamente observado (auditabilidade da evidência digital). Ainda, faz-se importante que a mesma sequência de etapas sempre redunde nos mesmos resultados, ou seja, que os mesmos procedimentos/instrumentos gerem a mesma conclusão (repetibilidade da evidência digital). Igualmente, ainda que sejam utilizados métodos diversos, os resultados devem ser os mesmos (reprodutibilidade da evidência digital). Por fim, os métodos e procedimentos devem ser justificáveis, sob a ótica da melhor técnica (justificabilidade da evidência digital) (STJ, 2024).

À vista do exposto acerca das provas digitais, a fim de garantir a validade e confiabilidade das provas digitais, é essencial que todas as alterações e ações sejam documentadas, a partir de um rigoroso controle por meio da cadeia de custódia, pois além de assegurar que as provas sejam admissíveis para valoração, também atua prevenindo alegações de adulteração ou contaminação, e, por consequência, eventuais nulidades processuais (COUTINHO, 2024).

3 RESULTADOS E DISCUSSÕES

3.1 Cadeia De Custódia Da Prova Digital

Com a crescente presença do digital na vida cotidiana, os eventos que acontecem total ou parcialmente no ambiente digital, e que são comprovados por meios eletrônicos, auxiliam na elucidação de como um crime ocorreu. No entanto, a eficácia dessas provas digitais/eletrônicas, conforme ensina Aury Lopes Junior (2020, p. 656): “[...] exige o estabelecimento de um procedimento regrado e formalizado, documentando toda a cronologia existencial daquela prova, para permitir a posterior validação em juízo e exercício do controle epistêmico”.

Ressalta-se que, por serem provas cuja produção ocorre fora do processo, é crucial que se demonstre, de forma documentada, a cadeia de custódia e toda a trajetória feita, da coleta até a inserção no processo e valoração judicial (LOPES JUNIOR, 2020).

Ademais, a cadeia de custódia em provas digitais assegura que a evidência mantenha sua integridade e não seja adulterada desde a coleta até sua apresentação em Juízo. Cada fase do processo (identificação, coleta, preservação e análise) é cuidadosamente registrada. Falhas na preservação dessa cadeia, como a falta de transparência ou documentação insuficiente, podem comprometer a integridade das evidências digitais, o que pode reduzir a influência dessas evidências na decisão do juiz (COUTINHO, 2024).

Segundo o disposto no art. 158-A do CPP, "Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte". Sobre a temática, a exposição vai de encontro com a posição de Renato Brasileiro de Lima, a qual ressalta que até a promulgação da Lei nº 13.964/19, que inseriu os artigos 158-A a 159-F, no Código de Processo Penal, não atribuía maiores cuidados à cadeia de custódia, tendo em vista que anteriormente a matéria era regulamentada apenas pela Portaria nº 82, de 16 de julho de 2014, da Secretaria Nacional de Segurança, e argumenta que a cadeia de custódia: "fundamenta-se no chamado princípio da "autenticidade da prova", um princípio básico pelo qual se entende que determinado vestígio relacionado à infração penal, encontrado, por exemplo, no local do crime, é o mesmo que o magistrado está usando para formar seu convencimento" (LIMA, 2020, p. 896).

Por outro lado, Geraldo Prado (2021) descreve o princípio da autenticidade da prova como sendo "lei da mesmidade", ou seja, "o mesmo" que se encontrou na cena do crime deve ser "o mesmo" a ser analisado pelo magistrado para fundamentar sua decisão. Para ele, há como exigência para a cadeia de custódia o princípio da "desconfiança processual", qual seja, nem tudo que ingressa no processo pode ter valor probatório, ou deve ser acreditado: "ninguém tem por que crer que algo é aquilo que a parte que o apresenta diz que é, simplesmente porque ela assim o diz", pois exige-se que tais provas sejam submetidas a um procedimento que demonstre que tais objetos correspondem ao que a parte alega ser.

Nesse contexto, a cadeia de custódia desempenha um papel importante para determinar a integridade das evidências digitais, estabelecendo a documentação sobre como as evidências são coletadas, transportadas, analisadas e transportadas.

Para estabelecer a cadeia de custódia, é obrigatória a documentação detalhada do tratamento das evidências a ser relatada por todas as pessoas que com ele estão em contato. O objetivo desta documentação é responder a uma série de perguntas como: Qual é a evidência? Como você conseguiu isso? Quando foi coletado? Quem cuidou disso? Por que essa pessoa

lidou com isso? Para onde viajou e onde foi armazenado? Por quanto tempo a evidência digital foi acessada pelos indivíduos autorizados? (MOHAMMED, 2018).

Ademais, a responsabilidade pela documentação da cadeia de custódia recai sobre as pessoas que lidam com a fonte de prova armazenada. Portanto, em uma investigação criminal, conduzida por órgãos oficiais, como no caso do inquérito policial, o dever de registrar e documentar a cadeia de custódia é atribuído aos funcionários públicos que possuem contato com os materiais que servem como provas (BADARÓ, 2021).

Somando a isso, Andressa Olmedo Minto (2021) esclarece que a investigação de evidências digitais demanda conhecimentos específicos em matéria informática, sobretudo porque não se pode afirmar, com segurança, se o procedimento de cadeia de custódia previsto no Código de Processo Penal pode ser aplicado à prova digital ou, se aplicado, de que forma o seria concretizado. O ideal seria que fosse suplementado por disposições específicas, dado que as provas digitais possuem características peculiares.

Este também é o posicionamento de Gustavo Badaró (2021), contudo o autor também pondera que seria inviável para o legislador estabelecer regras detalhadas acerca da cadeia de custódia nas provas digitais, em razão de não existirem, neste momento, meios e técnicas uniformemente aceitos. No mais, a ciência da computação está em constante mutação e evolução, o que faz com que os integrantes do poder judiciário se vejam forçados a adaptar os meios tradicionais de prova para lidar com as particularidades de coleta dos dados digitais.

Mário Furlaneto Neto e José Eduardo Lourenço dos Santos (2020) também destacam a complexidade dos vestígios digitais. Eles apontam que, devido à diversidade de linguagens e suportes nos quais esses vestígios podem se manifestar, bem como ao fato de estarem frequentemente ocultos em uma grande quantidade de dados e informações, é necessário discutir a padronização dos métodos de recuperação de vestígios digitais no âmbito científico.

Não obstante, para a investigação em ambiente digital, foram sugeridas quatro etapas: a recolha, o exame, a análise e o relatório. A etapa de recolha se refere aos atos de identificação das evidências digitais, na qual geralmente ocorre em contexto de busca domiciliar ou pessoal, a sua recolha propriamente dita, com a apreensão dos equipamentos informáticos ou a cópia dos dados, rotulagem, registro e atos complementares destinados a garantir a integridade dos dados. Efetuado o exame e a análise, o relatório deve conter linguagem e nomenclatura acessível, com a sugestão de elaboração de um glossário de termos, para os conceitos e termos técnicos informativos (MINTO, 2021).

Em relação à cadeia de custódia da prova digital, a Convenção de Budapeste, um tratado internacional focado em crimes cibernéticos, e um instrumento internacional sobre

crimes cibernéticos e provas eletrônicas, abarca diversas medidas de investigação no âmbito virtual e influencia diretamente a cadeia de custódia da prova digital.

O Brasil ratificou a Convenção em 2022 e a promulgou internamente com o Decreto 11.491/2023, a fim de estabelecer diretrizes para a cooperação internacional na investigação e combate a crimes cometidos por meio de computadores e redes digitais. Com efeito, a Convenção de Budapeste enfatiza a importância de métodos seguros e documentados para coletar, armazenar e apresentar evidências digitais em processos legais. Isso inclui garantir a autenticidade, integridade e admissibilidade dessas provas perante os tribunais, seguindo procedimentos claros para preservar a sua validade e aceitação no processo judicial internacional.

Conforme o artigo 18 da Convenção de Budapeste, os Estados signatários podem adotar medidas legislativas no sentido de permitir às respectivas autoridades que ordenem, a quem tenha sob sua posse ou controle dados informáticos específicos, que os apresente ou permita que as autoridades tenham acesso a eles. A finalidade não é conservar dados nem solicitar acesso a quem os detenha, mas sim a apreensão de dados sem qualquer comunicação anterior a quem os possua.

Para garantir a agilidade necessária na cooperação jurídica internacional em questões probatórias, a Convenção estabelece dois tipos de medidas cautelares. A primeira é o pedido de preservação de dados armazenados em computador, que deve ser feito quando há risco de perda ou alteração das informações, com a intenção de possibilitar um futuro pedido de acesso, busca e apreensão, guarda ou revelação desses dados, prevista no artigo 29 da referida Convenção. Já a segunda medida consiste na solicitação de revelação de dados específicos de tráfego, que visa obter informações urgentes para identificar a origem dos dados, incluindo o provedor de serviços e o caminho percorrido pelas informações, prevista no artigo 30 da Convenção de Budapeste.

Além disso, a Convenção prevê três instrumentos específicos para a obtenção de provas digitais: o pedido de busca, acesso, apreensão, guarda ou revelação de dados armazenados em computador (artigo 31); o pedido de interceptação de dados de tráfego em tempo real (artigo 33); e o pedido de interceptação ou gravação em tempo real do conteúdo de comunicações específicas transmitidas por meio de um sistema de computador (artigo 34).

Ademais, a legislação processual penal brasileira tem sido atualizada para se adaptar a essa nova realidade. Atualmente são identificados quatro diplomas legais específicos que tratam dos meios de obtenção de evidências digitais: a) a Lei n. 9.296/96 (que regula as Interceptações Telefônicas, Interceptações Telemáticas e Captação Ambiental); b) a Lei n.

12.965/14 (Marco Civil na Internet); c) a Lei n. 8.069/90 (Estatuto da Criança e do Adolescente); e d) a Lei n. 12.850/13 (Lei das Organizações Criminosas). A possibilidade da interceptação do fluxo de comunicações de natureza telemática e informática trata-se de meio de obtenção de prova excepcional, que não será admitido quando não ocorrer qualquer das seguintes hipóteses: I - não houver indícios razoáveis da autoria ou participação em infração penal; II - a prova puder ser feita por outros meios disponíveis; III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção (artigo 2º da Lei n. 9.296/96).

Nesse sentido, nos termos do artigo 5º, XII, da Constituição Federal de 1988, é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, em último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Noutra vertente, a Lei 12.965/14, conhecida como Marco Civil da Internet, estabelece princípios e garantias, direitos e deveres para o uso da Internet no Brasil, bem como prevê a guarda ou armazenamento dos registros de acesso ao provedor de conexão. Além disso, a Lei 13.441/17 alterou o Estatuto da Criança e do Adolescente para fins de introduzir no ordenamento jurídico a denominada infiltração policial virtual, com o objetivo de auxiliar na investigação de crimes contra a dignidade sexual de crianças e adolescentes, prevista nos artigos 240, 241, 241-A a 241-D. Essa infiltração de agentes de polícia na internet necessita de autorização judicial, mediante requerimento do Ministério Público ou representação da Autoridade Policial, bem como não pode exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda 720 (setecentos e vinte) dias (BADARÓ, 2021).

Por fim, a Lei 12.850/13, conhecida como Lei das Organizações Criminosas, também prevê a infiltração virtual no âmbito dos crimes praticados por organizações criminosas, nos artigos 10-A a 10-D, autorizada por até 06 (seis) meses, sem prejuízo de eventuais renovações, desde que o total não exceda 720 (setecentos e vinte) dias, de modo que ao final deverá ser confeccionado relatório circunstanciado de todos os atos eletrônicos praticados durante a operação.

Em que pese a introdução da cadeia de custódia nos artigos 158-A a 158-F, do Código de Processo Penal, a Lei nº 13.964/19 não indica os critérios objetivos para determinar quando ocorre a quebra da cadeia de custódia. Nesse cenário, Aury Lopes Junior (2020, p. 660) sustenta que a consequência da quebra da cadeia de custódia:

Sem dúvida deve ser a proibição de valoração probatória com a consequente exclusão física dela e de toda a derivada. É a “pena de inutilizzabilità” consagrada pelo direito italiano. Mas é importante que não se confunda a “teoria das nulidades” com a “teoria da prova ilícita”, ainda que ambas se situem no campo da ilicitude processual, guardam identidades genéticas distintas. É por isso que não se aplicam às provas ilícitas as teorias da preclusão ou do prejuízo. Esse é um diferencial crucial, não raras vezes esquecido.

Lopes Junior (2020, p. 718) complementa ao afirmar que: “[...] a prova produzida não pode servir apenas aos interesses do órgão acusado, sendo imprescindível a preservação da sua integralidade, sem a qual se mostra inviabilizado o exercício da ampla defesa”.

Ademais, acerca das consequências da quebra da cadeia de custódia, aduz que:

De um lado, há quem entenda que a quebra inviabiliza o efetivo exercício do contraditório pela parte que não tem acesso à prova integral. Sob a ótica da teoria dos frutos da árvore envenenada, os elementos remanescentes serão contaminados, logo, ilícitos, em virtude da lacuna decorrente da supressão de outros elementos que poderiam configurar argumentos persuasivos em sentido contrário à tese deduzida no processo. Houve, portanto, violação ao contraditório, como condição de validade constitucional do ato processual, daí por que há de se reconhecer a ilicitude da prova remanescente, nos termos do art. 157 do CPP. Em sentido diverso, com a introdução do regramento atinente à cadeia de custódia pela Lei n. 13.964/19, parte da doutrina prefere afirmar que eventual violação à nova sistemática adotada pelos arts. 158-A a 158-F do CPP poderá acarretar a ilegitimidade da prova, haja vista a violação a regras de direito processual, com a consequente aplicação da teoria das nulidades (nossa posição). (LOPES JUNIOR, 2020, p. 720).

Destarte, Alexandre Cebrian Araujo Reis, Victor Eduardo Rios Gonçalves e Pedro Lenza (2022, p. 121) ressaltam que a inobservância das recomendações legais relativas à cadeia de custódia: “(...) só ensejará a inadmissibilidade da prova pericial se demonstrada a existência de prejuízo concreto e relevante para a confiabilidade do material analisado, no tocante à origem e preservação das características”.

Nesse contexto, o autor Gustavo Badaró justifica que:

A parte que pretende a produção de uma prova digital tem o ônus de demonstrar previamente a sua integridade e autenticidade, por meio da documentação da cadeia de custódia. (...) Nesse caso, num sistema que respeite a presunção de inocência, não se poderá exigir do acusado a demonstração do prejuízo pela não utilização das melhores práticas segundo a *computer forensics*, devendo a prova ser destituída de valor probatório (Badaró, 2021, p. 3).

Sendo assim, há situações nas quais podem ocorrer apenas omissões ou irregularidades menores, sem evidências claras de que a fonte de prova foi modificada, adulterada ou substituída. Nesses casos, a questão deve ser abordada durante a fase de avaliação das provas (BADARÓ, 2021).

Ante o exposto, é possível concluir que há divergência doutrinária quanto às consequências da quebra da cadeia de custódia nas provas digitais. De um lado, autores como

Geraldo Prado, Aury Lopes Junior e Marcos Eberhardt compreendem que, uma vez quebrada a cadeia de custódia, a prova obtida deve ser considerada ilícita e inadmissível ao processo, com sua exclusão, uma verdadeira proibição de valoração probatória, bem como a inutilização das provas derivadas. De outro lado, Gustavo Badaró e Rogério Sanches Cunha, em sentido contrário, discorrem que a prova obtida a partir da quebra da cadeia de custódia pode ser valorada pelo magistrado conforme sua proporcionalidade, podendo ter um valor menor, e não a sua invalidade (VAZ, 2023).

Com efeito, as provas digitais têm se revelado como recursos valiosos, capazes de comprovar a existência ou inexistência de um fato ou circunstância, sendo extensivamente utilizadas em contextos jurídicos ligados ao direito penal, razão pela qual Geraldo Prado (2021, p. 25) apresenta o entendimento de que:

A cadeia de custódia das provas digitais é uma garantia de natureza constitucional e não mera consequência lógica do sistema de preservação do corpo de delito digital. Por meio da cadeia de custódia das provas digitais são tutelados os direitos fundamentais à confidencialidade e garantia da integridade dos sistemas de tecnologia da informação, à proteção do entorno digital, da identidade digital, do domicílio digital e, por óbvio, da privacidade associada ao direito de decidir o que tornar público ou não relativamente a essa esfera da vida.

Diante do referido posicionamento, reforça-se o entendimento de que o não cumprimento de uma regra legal não necessariamente leva à imediata invalidação da prova, uma vez que a confiabilidade pode ser demonstrada por outros meios.

De maneira correspondente, uma prova pode perder sua confiabilidade mesmo na ausência de violação de uma norma específica. Isso ocorre porque, como observa o autor Geraldo Prado, o cumprimento técnico das regras não garante que a prova não possa ser manipulada por alguém, como um perito, se agir de má-fé.

Sobre esse tema, para o Superior Tribunal Federal, deve-se buscar a origem da possível contaminação probatória e o magistrado deve sopesar se houve sinais de incorreta manipulação, guarda ou deterioração das provas apreendidas que comprometam a confiabilidade da perícia e integralidade da prova, bem como eventual ocorrência de violação de direitos fundamentais do investigado (ATHENIENSE, 2024).

No mesmo sentido, avalia-se caso a caso se a prova digital foi a única a fundamentar a ação penal ou se coexistem provas independentes aptas a motivar o livre convencimento do magistrado. Diferentemente, quando não são adotados procedimentos que assegurem a idoneidade e a integridade dos elementos obtidos a partir da extração dos dados de um celular apreendido, o entendimento jurisprudencial é no sentido de que é incontestável o prejuízo

causado pela quebra da cadeia de custódia, resultando na invalidade da prova digital (STJ, 2024).

Em síntese, como entende o Superior Tribunal de Justiça, alegações sobre a quebra da cadeia de custódia que não apresentam evidências de adulteração, manipulação de provas contra a defesa ou falta de cuidado no manuseio das evidências enquanto elas estiveram sob a guarda do Ministério Público não são acolhidas, mantendo a validade das provas digitais. Isso nos leva a concluir que a quebra da cadeia de custódia configura uma questão ligada à eficácia da prova, a qual deve ser analisada em cada caso específico.

4.2 Utilização de Novas Tecnologias na Investigação e a Preservação das Garantias Fundamentais

Ao mesmo tempo em que o número de crimes relacionados com computadores e outros dispositivos aumentou, trazendo maior dificuldade para delimitar a autoria, o avanço da tecnologia vem reconfigurando a maneira pela qual uma infração penal pode ser esclarecida, pois a perícia forense de computadores e redes evoluiu para apresentar resultados (MOHAMMED , 2018). Nesse cenário, enquanto se busca atender ao interesse público na obtenção de provas para a resolução de crimes, é igualmente importante garantir a proteção dos direitos fundamentais dos indivíduos envolvidos, especialmente aqueles relacionados à intimidade e à vida privada. Isso porque o legislador infraconstitucional, ao criminalizar a invasão de dispositivos informáticos alheios, visou proteger a liberdade individual, garantindo a inviolabilidade da intimidade e da vida privada (BADARÓ, 2021).

É preciso refletir que o telefone celular, por exemplo, se transformou em uma extensão dos direitos da personalidade dos sujeitos; por isso, uma vez apreendido e periciado, se torna imprescindível a elaboração de laudos fortes bem como demonstração cabal de que a acusação fundamentada em uma evidência digital seja realmente verdadeira.

Ora, as relações sociais estão cada vez mais sujeitas a constante monitoramento, devido à maior capacidade de captação de sons e imagens que acabam sendo utilizados como provas de infrações penais. No sistema de justiça penal que opera com a presunção de inocência e o devido processo legal, a defesa deve ter não apenas conhecimento da acusação, mas também estar informada das fontes e métodos de prova disponíveis.

Existem casos, como o espelhamento de tela do aplicativo *WhatsApp Web*, em que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta da

legitimidade dos atos dos investigadores, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica (MINTO, 2021).

Somado a isso, o entendimento majoritário do Colendo Superior Tribunal de Justiça colaciona que: “[...] é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia” (STJ, 2024).

Sendo assim, não se trata apenas de investigar a boa ou má-fé dos agentes policiais ou estatais que manusearam a prova. O objetivo não é presumir a honestidade ou desonestidade, mas estabelecer um procedimento objetivo que assegure e valide a prova, independentemente das questões subjetivas relacionadas ao agente. A discussão sobre a subjetividade deve ser substituída por critérios objetivos e empiricamente verificáveis, que não dependam da comprovação de má-fé ou da integridade do agente estatal (LOPES JUNIOR; ROSA, 2015).

Diferentemente, mesmo sem autorização judicial, a polícia pode acessar conversas do aplicativo *WhatsApp* de uma vítima falecida, cujo aparelho celular foi entregue pela esposa para ser investigado. Nesse caso, não há violação à intimidade da vítima, detentora do direito ao sigilo, uma vez que a finalidade da prova pericial, a título exemplificativo, é esclarecer a causa da morte, em delito de homicídio. Em suma, é fundamental a devida produção da prova digital, já que afeta diretamente direitos e garantias fundamentais do investigado, tais como sua intimidade, vida privada e inviolabilidade de domicílio e das comunicações privadas (MINTO, 2021).

Em consequência, é essencial que haja uma especialização tanto para policiais federais e civis quanto para peritos forenses computacionais, a fim de melhorar a eficácia do uso de provas digitais, bem como a sua integridade assegurada por uma cadeia de custódia.

Por fim, além de promover o aperfeiçoamento e a especialização, é necessário equipar adequadamente as Delegacias de Polícia e os Núcleos de Criminalística para lidar com a crescente demanda por investigações de crimes digitais, como muito bem advoga Badaró.

5 CONSIDERAÇÕES FINAIS

A implementação de um conjunto de atos que documentem a cronologia da prova de forma detalhada se torna ainda mais evidente devido à diferença ontológica entre a prova

digital e a prova tradicional, além do fato de que a prova digital utiliza uma linguagem digital em vez de uma linguagem natural.

No contexto dos crimes digitais, a integridade da cadeia de custódia é garantida por meio de algoritmos que funcionam como uma impressão digital para cada arquivo. Para garantir o direito de defesa, é crucial permitir a comparação entre a cópia analisada e o arquivo original, a fim de verificar sua autenticidade e confirmar a correspondência entre o conteúdo do processo e o material original.

Nesse sentido, os meios de obtenção de prova digital ocorrem por iniciativa dos órgãos investigatórios ou acusatórios e dependem de autorização judicial para serem efetivados.

O entendimento jurisprudencial acerca da inadmissibilidade de provas colhidas em razão da quebra da cadeia de custódia, em síntese, evidencia que a ausência de perícia técnica no dispositivo que possibilitou obter a prova digital torna impossível o reconhecimento da autenticidade da prova, uma vez que impede a realização de contraprova, violando os princípios da ampla defesa e contraditório e devido processo legal.

Em síntese, para assegurar a autenticidade e integridade das provas digitais, é crucial seguir rigorosamente os métodos informáticos estabelecidos para sua obtenção, registro, armazenamento, análise e apresentação, alinhando-se às melhores práticas nacionais e internacionais. A apresentação dessas provas nos tribunais brasileiros deve ser realizada por meio de perícia técnica, e a documentação completa da cadeia de custódia é indispensável para garantir seu valor epistêmico adequado.

REFERÊNCIAS

ALBECHE, T. S. G.. **Prova digital, investigação cinética e o princípio da parametrização do novo meio de obtenção de prova**. 10 out. 2023. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2023/10/10/prova-digital-investigacao-cinetica-e-o-principio-da-parametrizacao-do-novo-meio-de-obtencao-de-prova/>. Acesso em: 10 maio 2024.

ATHENIENSE, A. **A importância da preservação da cadeia de custódia das provas digitais**. Diretório Nacional da Advocacia. Disponível em: <https://analise.com/opinio/a-importancia-da-preservacao-da-cadeia-de-custodia-das-provas-digitais>. Acesso em: 06 jun. 2024.

BADARÓ, G. H. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, ano 29, n. 343, p. 7-9, jun./2021.

BADARÓ, G. **A cadeia de custódia da prova digital. Direito probatório.** Londrina: Thoth, p. 175-188, 2023.

COUTINHO, T. M. **Provas digitais e cadeia de custódia:** desafio e implicações no processo penal. *Consultor Jurídico*. 22 julho 2024. Disponível em: <https://www.conjur.com.br/2024-jul-22/provas-digitais-e-cadeia-de-custodia-desafios-e-implicacoes-no-processo-penal/>. Acesso em: 24 jul. 2024.

FURLANETO NETO, M; SANTOS, J. E. L. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil.** *Revista Em Tempo*, v. 20, n. 1, novembro 2020. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Em_Tempo_n.20.02.pdf. Acesso em: 17 maio 2024.

LIMA, Re. B. **Manual de processo penal.** 8. ed. rev., ampl. e atual. Salvador: JusPodivm, 2020.

LOPES JUNIOR, A. **Direito processual penal.** 17. ed. São Paulo: Saraiva Educação, 2020.

LOPES JUNIOR, A. L; ROSA, A. M. A importância da cadeia de custódia para preservar a prova penal. In: **Consultor Jurídico**. 16 jan. 2015. Disponível em: <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal/>. Acesso em: 17 maio 2024.

MINTO, A. O. **A prova digital no processo penal.** São Paulo: LiberArs, 2021.

MOHAMMED, J. T. Adoption of chain of custody improves digital forensic investigation process. **Iraqi Journal of Information and Communication Technology**, v. 1, n. 2, p. 13–23, 2018. Disponível em: <https://ijict.edu.iq/index.php/ijict/article/view/14>. Acesso em: 07 jun. 2024.

PRADO, G. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. **Revista Consultor Jurídico**, v. 26, p. 25, 2021- Disponível em: <https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/>. Acesso em: 10 maio 2024.

REIS, A. C. A; LENZA, P; GONÇALVES, V. E. R. **Direito processual penal.** 11. ed. São Paulo: SaraivaJur, 2022.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Habeas Corpus nº 828054/RN.** Relator: Joel Ilan Paciornik. Quinta Turma. Data de Publicação: Dje 29/04/2024.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Habeas Corpus nº 900613/MG.** Relator: Reynaldo Soares da Fonseca. Quinta Turma. Data de publicação: Dje 25/07/2024.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso em Habeas Corpus nº 182.310/RJ.** Relator: Jesuíno Rissato. Sexta Turma. Data de publicação: Dje 14/05/2024.

SUPREMO TRIBUNAL FEDERAL. **Informativo de Jurisprudência.** n. 04, Brasília, 31 jan. 2022. Disponível em:

[https://processo.stj.jus.br/jurisprudencia/externo/informativo/?aplicacao=informativo&acao=pesquisar&livre=@CNOT=%27018781%27#:~:text=%22a%20cadeia%20de%20cust%C3%B3dia%20fundamenta,judicial%22%20\(PRADO%2C%20Geraldo. Acesso em: 07 jun. 2024.](https://processo.stj.jus.br/jurisprudencia/externo/informativo/?aplicacao=informativo&acao=pesquisar&livre=@CNOT=%27018781%27#:~:text=%22a%20cadeia%20de%20cust%C3%B3dia%20fundamenta,judicial%22%20(PRADO%2C%20Geraldo. Acesso em: 07 jun. 2024.)

VAZ, M. F. A preservação da cadeia de custódia como pressuposto de admissibilidade da prova digital. **Revista da ESMESC**, v. 30, n. 36, p. 323-350, 2023.

Como Referenciar este Artigo, conforme ABNT:

A. S. REIS JUNIOR, A. L. Y. VARGAS, Cadeia de Custódia nas Provas Digitais: Desafios e Estratégias para a Preservação da Integridade Probatória. **Rev. FSA**, Teresina, v. 22, n. 4, art. 4, p. 71-87, abr. 2025.

Contribuição dos Autores	A. S. Reis Junior	A. L. Y. Vargas
1) concepção e planejamento.	X	X
2) análise e interpretação dos dados.	X	X
3) elaboração do rascunho ou na revisão crítica do conteúdo.	X	X
4) participação na aprovação da versão final do manuscrito.	X	X