Cognitio Juris
ISSN 2236-3009

A PRESERVAÇÃO DAS PROVAS DIGITAIS E A CADEIA DE CUSTÓDIA NO CONTEXTO DA FRAUDE ELETRÔNICA

THE PRESERVATION OF DIGITAL EVIDENCE AND THE CHAIN OF CUSTODY IN THE CONTEXT OF ELECTRONIC FRAUD

Artigo submetido em 25 de novembro de 2024
Artigo aprovado em 30 de novembro de 2024
Artigo publicado em 30 de dezembro de 2024

Cognitio Juris
Volume 14 – Número 57 – Dezembro de 2024
ISSN 2236-3009

.

Autor(es):
Maria Daniella de Sousa França[1]
Werna Karenina Marques de Sousa[2]

.

RESUMO

O presente estudo aborda a relevância da cadeia de custódia de provas digitais no Direito Penal, considerando os desafios trazidos pela evolução tecnológica e pelo aumento dos crimes cibernéticos, como fraudes eletrônicas. A regulamentação introduzida pelo Pacote

Anticrime (Lei nº 13.964/2019) é crucial para garantir a integridade e autenticidade das evidências digitais, tornando-as admissíveis em juízo. No entanto, a preservação dessas provas ainda enfrenta lacunas práticas e técnicas, decorrentes da volatilidade e da facilidade de manipulação dos dados digitais, mesmo com avanços como o art. 158-A do Código de Processo Penal. A pesquisa destaca a necessidade de padronizar procedimentos com base em normas como a ISO/IEC 27037:2013, que orienta a identificação, coleta e preservação de evidências digitais. Propõe-se também a adoção de tecnologias para registrar etapas da cadeia de custódia de forma imutável, e softwares de código hash, homologados para garantir a integridade dos dados. Capacitar continuamente operadores do Direito, policiais e peritos é essencial para acompanhar as melhores práticas no tratamento de provas digitais. Além disso, é recomendada a atualização do ordenamento jurídico, com protocolos específicos para o ambiente digital, prevendo sanções para violações e promovendo o uso de tecnologias modernas. Conclui-se que a validade e confiabilidade das provas digitais dependem de um sistema jurídico adaptado às especificidades tecnológicas, equilibrando eficiência processual e proteção de direitos fundamentais.

Palavras-chave: Cadeia de custódia. Provas digitais. Fraude eletrônica.

ABSTRACT

This study addresses the relevance of the chain of custody for digital evidence in Criminal Law, considering the challenges posed by technological advancements and the rise in cybercrimes, such as electronic fraud. The regulation introduced by the Anti-Crime Package (Law No. 13,964/2019) is crucial to ensuring the integrity and authenticity of digital evidence, making it admissible in court. However, the preservation of such evidence still faces practical and technical gaps, arising from the volatility and ease of manipulation of digital data, even with advances such as Article 158-A of the Code of Criminal Procedure. The research highlights the need to standardize procedures based on standards like ISO/IEC 27037:2013, which provides guidelines for the identification, collection, and preservation of digital

evidence. It also proposes adopting technologies such as blockchain to record each stage of the chain of custody immutably and using certified hash code software to ensure data integrity. Continuous training for legal professionals, law enforcement officers, and experts is essential to implementing best practices in handling digital evidence. Moreover, updating the legal framework with specific protocols for the digital environment is recommended, including sanctions for violations and encouraging the use of modern technologies. The conclusion is that the validity and reliability of digital evidence depend on a legal system adapted to technological specificities, balancing procedural efficiency and the protection of fundamental rights.

Keywords: Chain of custody. Digital evidence. Electronic fraud.

1 INTRODUÇÃO

Com o avanço tecnológico, as provas digitais adquiriram um papel crucial no direito, especialmente no âmbito do processo penal. Diante do aumento significativo de crimes virtuais, como a fraude eletrônica, surgiram novos desafios para a investigação criminal, sobretudo em relação à preservação da integridade das evidências digitais. Reconhecendo essa realidade, o Pacote Anticrime (Lei nº 13.964/2019) incluiu no Código de Processo Penal (CPP) a regulamentação da cadeia de custódia, estabelecendo procedimentos rigorosos para a coleta, preservação e descarte de vestígios materiais de crimes. De acordo com o art. 158-A do CPP, a cadeia de custódia é definida como “o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte” (art. 158-A, caput, CPP).

Esse processo é essencial para garantir a autenticidade e a integridade das provas digitais, de forma que sejam aceitas pelos tribunais. Em casos envolvendo crimes no ambiente virtual, nos quais os dados são facilmente manipuláveis, a cadeia de custódia serve para

garantir a conservação dos vestígios desde o primeiro contato até a destinação final dos materiais coletados, e qualquer interferência pode comprometê-la, resultando na perda da evidência e sua inutilidade.

A quebra da cadeia de custódia da prova levanta uma das questões mais controversas no processo penal contemporâneo: em que medida essa ruptura afeta a admissibilidade, validade e eficácia das provas apresentadas? Diante da volatilidade das evidências, especialmente no contexto das provas digitais, surge a necessidade de ponderar entre a proteção de direitos fundamentais, como o contraditório e a ampla defesa, e a busca pela verdade real. A questão central reside em determinar se a simples irregularidade na cadeia de custódia é suficiente para tornar a prova inadmissível ou se o juiz deve analisar outros elementos nos autos para aferir a autenticidade e integridade da evidência.

Em relação aos crimes virtuais, o crime de fraude eletrônica está entre os mais comuns, sendo uma novidade legislativa introduzida em 2021. Esse crime ocorre quando o criminoso consegue enganar a vítima, por meio das redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo para obter alguma vantagem ilícita (art. 171, § 2º-A do Código Penal).

Nessa perspectiva, o presente artigo se dispõe a analisar a cadeia de custódia e por que é importante em casos envolvendo provas digitais no processo penal brasileiro, especialmente em casos de fraude eletrônica. O estudo visa analisar (in) suficiência da legislação e jurisprudência atual e a omissão do legislador em relação às evidências digitais, uma vez que as normas vigentes se concentram predominantemente nos procedimentos relacionados às provas físicas e materiais. Ao não abordar de forma adequada os procedimentos específicos para coleta e preservação de provas digitais, que possuem características distintas de provas físicas, torna-se um desafio significativo dentro do ordenamento jurídico brasileiro.

Além disso, será evidenciada a adequação das normas legais e técnicas, como a Norma ABNT

ISO/IEC 27037:2013, que é essencial para assegurar que as evidências digitais sejam tratadas com um nível rigoroso de autenticidade e integridade, elementos fundamentais para sua validade em processos judiciais. Apesar de sua contribuição, a aplicação da norma enfrenta desafios práticos e de adaptação às realidades dos sistemas judiciário e policial brasileiros. Ademais, será analisada jurisprudência do Superior Tribunal de Justiça (STJ) sobre a admissibilidade e validade das provas digitais, com foco nas exigências para o cumprimento da cadeia de custódia.

Para uma análise detalhada da situação motora da cadeia de custódia e suas implicações no contexto jurídico, este estudo está organizado em cinco tópicos principais. Cada tópico abordará aspectos fundamentais para o entendimento da relevância e aplicação da cadeia de custódia no cenário contemporâneo, principalmente em provas digitais.

Serão discutidas, preliminarmente, a definição da cadeia de custódia e suas fases. Este tópico oferece uma introdução ao conceito de cadeia de custódia, abordando os procedimentos que visam garantir a integridade e a autenticidade das provas desde a coleta até o descarte. Também será analisada a cadeia de custódia e o sistema interamericano de direitos humanos, utilizando como exemplo o emblemático caso Favela Nova Brasília versus Brasil, nesta seção, a análise se volta para a importância da cadeia de custódia no contexto dos direitos humanos, usando como exemplo o emblemático caso Favela Nova Brasília versus Brasil, julgado pela Corte Interamericana de Direitos Humanos. Em seguida, a teoria geral da prova e provas digitais será explorada e os princípios fundamentais da teoria geral da prova, com uma comparação entre as provas tradicionais e as digitais e seus principais desafios.

No contexto dos crimes cibernéticos, serão abordados temas como tipificação legal, formas comuns de delitos virtuais (como invasão de dispositivos e fraude eletrônica) e a necessidade crescente de uma cadeia de custódia rigorosa para assegurar a validade das provas nesses casos. Por fim, será tratado o tópico de fraude eletrônica e a validade de provas digitais obtidas por meio de aplicativos como WhatsApp. A validade dessas provas e a facilidade com

que podem ser manipuladas tornam a cadeia de custódia fundamental para garantir a autenticidade e a integridade dos dados. O presente artigo ainda explora a relevância dos algoritmos, do aprendizado de máquina e do Big Data, destacando seus impactos em diferentes setores e a necessidade de alinhamento com princípios constitucionais, especialmente no contexto jurídico, para evitar violações de direitos fundamentais e garantir a segurança digital.

Portanto, justifica-se a realização desta pesquisa pela evidente precariedade legislativa e jurídica brasileira na área das provas digitais, especialmente no que tange à cadeia de custódia e à preservação da integridade das evidências digitais. A legislação atual enfrenta desafios consideráveis para acompanhar a rápida evolução tecnológica, uma vez que as normas vigentes foram, em grande parte, elaboradas em um contexto no qual as provas físicas eram predominantes, e a manipulação digital ainda não representava uma questão central para o direito processual.

2 DEFINIÇÃO DA CADEIA DE CUSTÓDIA E SUAS FASES

Segundo Nucci (2020), a cadeia de custódia deve seguir um procedimento rigorosamente estruturado e devidamente formalizado, registrando de forma detalhada toda a sequência cronológica da prova, conforme disposto no art. 158-A do CPP. Esse procedimento é essencial para garantir que a prova seja validada em tribunal e submetida ao necessário controle epistêmico. No que se refere às provas digitais, que possuem particularidades devido à facilidade de manipulação, a preservação é uma preocupação constante. Assim, o procedimento previsto no art. 158-A do CPP serve para assegurar a integridade dessas evidências.

Importante pontuar que, o art. 158-B do CPP, acrescentado ao Código de Processo Penal pela Lei n. 13.964/2019, estabelece rigorosas as etapas da cadeia de custódia das provas típicas, que inclui dez etapas fundamentais, sendo elas: (I) reconhecimento, (II) isolamento,

(III) fixação, (IV) coleta, (V) acondicionamento, (VI) transporte, (VII) recebimento, (VIII) processamento, (IX) armazenamento ao (X) descarte. Ademais, de acordo com Antônio Filho e Badaró (2020), o artigo 158-B detalha as etapas do rastreamento de vestígios de uma infração penal, bem como os procedimentos técnicos necessários que visam preservar, documentar e rastrear a trajetória de um vestígio, desde seu reconhecimento até o descarte.

Sendo assim, de acordo com o art. 158-B do CPP, a primeira fase é o reconhecimento do vestígio, que visa identificar um elemento como potencialmente relevante para a prova pericial. Na segunda fase, denominada de isolamento, o ambiente imediato e mediato é isolado para evitar que fatores externos alterem o estado original dos vestígios e o local do crime. A fase de fixação consiste em documentar minuciosamente o vestígio tal como ele foi encontrado no local de crime ou corpo de delito. Essa documentação pode incluir descrições escritas, fotografias, vídeos e até croqui, descritos no laudo pericial produzido pelo perito responsável.

Em relação à coleta, definida pelo ato de recolher o vestígio formalmente do local, respeitando as características físicas, químicas, biológicas e submetidas à análise pericial. Já o acondicionamento é o procedimento que envolve a embalagem individual de cada vestígio coletado, de acordo com sua especialidade para posterior análise, nessa fase, detalhes como data, hora, nome do agente responsável pela coleta e acondicionamento são registrados. Em relação à etapa do transporte, o vestígio é transferido do local de coleta para outro, seguindo condições adequadas para garantir a manutenção de suas características originais, bem como bem como o controle de sua posse.

A sétima fase é o recebimento, que é o ato formal de transferência da posse do vestígio, documentado com dados detalhados, incluindo número de procedimento, unidade de polícia, local de origem, nome de quem transportou, código de rastreamento e assinatura de quem o recebe. O processamento consiste no exame pericial propriamente dito, onde o vestígio é manipulado e analisado com a metodologia específica para suas características. Nesta etapa,

será formalizado o laudo produzido por perito.

No armazenamento refere-se à guarda do vestígio após o exame pericial, para fins de realização de contraperícia, descarte ou transporte. Por fim, a fase do descarte é o procedimento de liberação do vestígio após o encerramento do processo, seguindo as normas legais vigentes e, quando necessário, com autorização judicial (BRASIL, 1941).

Além das diretrizes legais, é importante mencionar as normas técnicas que orientam a coleta e tratamento das provas digitais, nas quais se aplicam também as etapas listadas no art. 158-B do CPP. Nesse contexto, exigem-se processos específicos como a Norma ABNT ISO/IEC 27037:2013. Oliveira (2019) explica que essa norma foi desenvolvida pela Organização Internacional de Padronização (ISO), retificada e gerenciada pela Associação Brasileira de Normas Técnicas (ABNT), em vigor no Brasil desde 09/01/2014. Ela fixa diretrizes que tratam acerca das práticas de coleta e tratamento das provas digitais, que servem para garantir sua autenticidade, estabelecendo orientações para identificação, coleta, aquisição e preservação de evidências digitais (PARODI, 2020).

Furlaneto Neto e Santos (2020) explicam que, de acordo com a Norma ABNT ISO/IEC 27037:2013, para uma evidência ser considerada válida, deve possuir três características essenciais: (a) relevância, quando contribui para comprovar ou contestar um aspecto específico do caso em investigação; (b) confiabilidade, que reflete o nível de precisão da informação em comparação com o original; e (c) suficiência, ou seja, a evidência digital deve ser suficiente para permitir a análise ou investigação adequada dos elementos questionados.

Além disso, os referidos autores esclarecem que, segundo a ABNT ISO/IEC 27037:2013, a evidência digital possui tanto uma dimensão física quanto lógica. A forma física refere-se aos dados contidos em um dispositivo tangível, enquanto a forma lógica envolve a representação virtual dos dados no dispositivo. A identificação da evidência digital requer a busca, reconhecimento e documentação dos dados, começando com a localização dos dispositivos

de processamento que podem armazenar essas informações. Este procedimento também deve priorizar a coleta com base na volatilidade dos dados, de modo a minimizar o risco de danos à prova digital. Além disso, é essencial conduzir buscas para identificar possíveis evidências ocultas, como arquivos excluídos ou adulterados. A identificação de mídias digitais engloba tanto aspectos físicos quanto lógicos, sendo esta última realizada por meio do cálculo de um valor de *hash*, utilizando algoritmos como MD5, SHA-1 e SHA-2, este último mais empregado atualmente. No que diz respeito à preservação, é fundamental proteger a integridade da prova digital para assegurar sua validade como evidência, o que implica na guarda cuidadosa tanto dos dados quanto do dispositivo, garantindo assim sua autenticidade.

Por outro lado, a violação ou descumprimento da cadeia de custódia pode levar à inadmissibilidade das provas, uma vez que a natureza volátil das provas digitais, é essencial implementar mecanismos que possam garantir a sua preservação, sem interferências que comprometam sua confiabilidade. O Superior Tribunal de Justiça tem sido enfático em reconhecer a fragilidade das provas obtidas sem respeito à cadeia de custódia e reiteradamente reconhecido sua imprestabilidade, quando não são utilizados os procedimentos recomendados pela ABNT que garantem a auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade:

(…) 6. Neste caso, não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular apreendido. Logo, evidentes o prejuízo causado pela quebra da cadeia de custódia e a imprestabilidade da prova digital. (STJ, 2024).

Para atestar a integralidade da prova digital, é fundamental a utilização de ferramentas especializadas, pois o registro detalhado do processo de coleta, armazenamento e transferência é crucial para garantir sua confiabilidade e aceitação em juízo. No caso em análise, observou-se que não foram seguidos os procedimentos necessários para assegurar a

integridade e a autenticidade dos dados extraídos de um celular apreendido, o que comprometeu a cadeia de custódia e a prova digital se tornou imprestável para o processo.

Conforme Badaró (2023), a documentação e o registro de todas as etapas de um procedimento técnico são essenciais, pois garantem o uso adequado das melhores práticas, especialmente ao lidar com dados probatórios voláteis e suscetíveis à alteração. Essa necessidade é ainda mais acentuada quando se considera a diferença ontológica entre a prova digital e a prova tradicional, já que a primeira utiliza uma linguagem digital em vez de uma linguagem natural, o que torna a cadeia de custódia detalhada ainda mais crucial.

A decisão também ressaltou a importância da utilização do código *hash*, uma função matemática essencial na preservação da cadeia de custódia digital. Segundo Guerra (2024, apud Sydow), o código *hash* gera uma sequência numérica única e irreversível, crucial para garantir a integridade dos dados armazenados em dispositivos digitais. Qualquer manipulação desses dados altera o código *hash*, sinalizando possíveis violações.

Sendo esse algoritmo, inclusive, mencionado pelo Ministro Ribeiro Dantas em seu voto no Agravo Regimental no Recurso Ordinário em Habeas Corpos nº 143.169/RJ, o qual vale a citação:

Aplicando-se uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo – uma espécie de impressão digital ou DNA, por assim dizer, do arquivo. Esse código hash gerado da imagem teria um valor diferente caso um único bit de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Mesmo alterações pontuais e mínimas no arquivo resultariam numa hash totalmente diferente, pelo que se denomina em tecnologia da informação de efeito avalanche: […]. (STJ, 2023).

A adoção do código *hash*, como evidenciado pelo voto do Ministro Ribeiro Dantas, é uma das ferramentas fundamentais na preservação da cadeia de custódia e reflete a crescente

preocupação com a vulnerabilidade das provas digitais. Sendo assim, a ausência de um software confiável, técnicas adequadas e verificáveis comprometem a integridade da prova digital.

Outro ponto crucial, também abordado pela jurisprudência atual, refere-se aos quatro aspectos essenciais no tratamento da evidência digital para avaliar o método utilizado na extração de dados. Conforme detalhado por Oliveira (2019), a evidência digital deve permitir a verificação de que todas as etapas foram devidamente seguidas, com registro claro de cada procedimento executado, caracterizando sua auditabilidade.

Além disso, é fundamental que a aplicação das mesmas etapas e instrumentos produza resultados idênticos, assegurando sua repetibilidade. Da mesma forma, ainda que sejam empregados métodos ou ferramentas diferentes, os resultados obtidos devem ser consistentes, garantindo sua reprodutibilidade. Por fim, os métodos e procedimentos adotados precisam ser respaldados pela melhor técnica disponível, justificando sua aplicação e validade, o que evidencia a justificabilidade da evidência digital.

A cadeia de custódia, portanto, atua como um protocolo que assegura o registro fiel de cada etapa, contribuindo, dessa forma, para a preservação da integridade da prova digital e sua admissibilidade em juízo ou fora dele. Além disso, a cadeia de custódia desempenha um papel importante na admissibilidade da prova digital, garantindo que os tribunais possam confiar em sua autenticidade e integridade. No contexto jurídico, a validade de uma prova digital depende não apenas de seu conteúdo, mas também da forma como foi obtida e preservada, para garantir direitos fundamentais, como o contraditório e a ampla defesa.

No entanto, há também entendimentos que permitem a análise da confiabilidade da prova com base em outros elementos disponíveis nos autos. A nulidade de uma prova em razão da quebra da cadeia de custódia não é automática. Para exemplificar, Badaró, (2017) explica “as irregularidades da cadeia de custódia não são aptas a causar ilicitude da prova, devendo

o problema ser resolvido, com redobrado cuidado e muito maior esforço justificativo, no momento da valoração". A respeito disso, a Sexta Turma do STJ já se posicionou sobre a controvérsia das consequências da quebra da cadeia de custódia da prova com o seguinte entendimento: "as irregularidades constantes da cadeia de custódia devem ser sopesadas pelo magistrado com todos os elementos produzidos na instrução, a fim de aferir se a prova é confiável" (STJ, 2021).

3 A CADEIA DE CUSTÓDIA E O SISTEMA INTERMAERICANO DE DIREITOS HUMANOS: CASO FAVELA NOVA BRASÍLIA VERSUS BRASIL

Discorrer sobre a relevância da cadeia de custódia é, inevitavelmente, discutir sobre o Sistema Interamericano e o caso Favela Nova Brasília Versus Brasil, julgado pela Corte Internacional de Direitos Humanos. O caso, em específico, data dos dias 18 de outubro de 1994 e em 8 de maio de 1995, e versa a respeito da responsabilidade estatal após a polícia do estado do Rio de Janeiro assassinar 26 homens e violentar sexualmente 3 mulheres no Complexo do Alemão (CNJ, 2021).

Ainda que o crime tenha ocorrido nos anos de 1994 e 1995, a condenação somente ocorreu em 16 de fevereiro de 2017, e, no que concerne à produção de provas, após as mortes, a polícia modificou a cena do crime, levando os corpos mortos para a praça central da Favela Nova Brasília (CNJ, 2021). É, pois, neste contexto, que se evidencia a importância da cadeia de custódia, de modo que sua ausência obteve grande destaque no caso em apreço, uma vez que resultou em grandes falhas no processo investigatório.

Resumidamente, do acima exposto se depreende que a cadeia de custódia é um assunto imprescindível ao direito penal, com relevância internacional, e que, no Brasil, a sua importância tem correlação direta com o caso Favela Nova Brasília, no qual as provas foram adulteradas uma vez ausentes uma cadeia de custódia adequada (MACHADO, 2023).

4 TEORIA GERAL DA PROVA E PROVAS DIGITAIS

Segundo Lopes Júnior (2019), O processo penal atua como um instrumento que permite a retrospecção e a reconstrução de eventos históricos, visando instruir o julgador sobre o ocorrido. Nesse sentido, as provas desempenham um papel fundamental, pois são os meios que possibilitam essa reconstituição dos fatos passados relacionados ao crime, ou seja, as provas são os meios para reconstrução o crime, servindo para convencimento do juiz sobre o fato.

Nucci (2020) explora a etimologia do termo “prova” em sua obra, explicando que ele deriva do latim *probatio*, o que envolve ideias de ensaio, verificação, exame e confirmação. A partir daí, o verbo *probare* surge, significando verificar, examinar, aprovar ou até persuadir. Dessa forma, o termo carrega em sua essência a ideia de confirmação e avaliação, características intrínsecas ao processo penal. A prova, portanto, é o elemento através do qual se busca convencer, com segurança, sobre a realidade dos fatos investigados, com vistas a uma decisão judicial justa e fundamentada.

De acordo com Rangel (2015), a prova pode ser entendida como um meio de verificação do *thema probandum*, sendo o objetivo central o convencimento do juiz acerca dos fatos apresentados no processo, torna-se um elemento indispensável na busca pela verdade.

Ao considerar o crescente uso da tecnologia e da internet na prática de crimes, as provas digitais, também conhecida como evidência digital (do inglês *digital evidence*), emergem como uma categoria crucial. Essas provas incluem informações armazenadas em aparelhos informáticos e dados eletrônicos, como e-mails, mensagens de texto, postagens em redes sociais, registros de acesso a sites e arquivos digitais. Para Furlaneto Neto e Souza (2020) as provas digitais podem estar tanto em posse do investigado quanto de terceiros, contendo dados relevantes para auxiliar na busca pela verdade dos fatos. Em seu entendimento, Ferreira (2020) afirma que a prova digital é considerada frágil, pois a manipulação de forma incorreta pode levar à perda da evidência.

No que diz respeito às provas digitais, elas são classificadas como provas atípicas, encontrando respaldo nos artigos 369 e 370 do Código de Processo Civil, aplicados analogicamente ao processo penal com base no artigo 3º do CPP. Esse reconhecimento pela doutrina jurídica atual reflete a adaptação do direito processual penal às novas formas de criminalidade. Em um cenário onde a prática de crimes digitais é cada vez mais comum, a prova digital, enquanto instrumento de verificação, assume uma função semelhante à das provas tradicionais, mas com peculiaridades que demandam cuidados específicos na sua coleta, preservação e apresentação.

Dessa forma, a prova digital adquire o mesmo propósito fundamental da prova tradicional: servir como meio para se alcançar a verdade dos fatos. Contudo, devido à sua natureza, ela exige protocolos diferenciados e a aplicação rigorosa de uma cadeia de custódia, de forma a assegurar sua integridade e autenticidade. A necessidade de controle sobre as evidências digitais torna-se evidente na medida em que esses dados são extremamente voláteis e passíveis de manipulação, razão pela qual os procedimentos de verificação e preservação precisam ser tecnicamente robustos para garantir a confiabilidade das informações trazidas aos autos.

5 CRIMES CIBERNÉTICOS

Os crimes cibernéticos, embora ainda careçam de uma definição consensual, são amplamente reconhecidos como delitos perpetrados por meio da internet e outras tecnologias digitais. Essas infrações incluem práticas como chantagem (art. 158 do CP), pornografia infantil (art. 241-B do CP), tráfico de drogas (art. 33, Lei nº 11.343/2006) e uma série de outras atividades ilícitas. Segundo o Ministério da Justiça e Segurança Pública, os crimes mais frequentemente reportados na esfera digital, respaldados pelo Código Penal, abrangem a ameaça (art. 147), calúnia (art. 138), difamação (art. 139), injúria (art. 140) e o uso de falsa identidade (art. 307).

A legislação brasileira tem avançado para enfrentar esses desafios com a Lei 12.737/2012, que introduziu a tipificação penal específica para crimes informáticos. Essa norma alterou o art. 154-A do Código Penal, criminalizando ações como a invasão de dispositivos computacionais, a violação de dados pessoais e o ataque a sites, com o intuito de proporcionar um arcabouço jurídico mais robusto para a repressão dessas condutas. Além disso, outras leis, como a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) disciplinam a proteção dos dispositivos informáticos e de dados pessoais, respectivamente, direcionando-se especialmente à privacidade individual (BITENCOURT, 2016).

De acordo com Souza (2024), a internet está atualmente na fase Web 3.0, marcada por inovações que transformaram a interação digital. Segundo o autor, esse estágio da cultura digital incorpora tecnologias avançadas, como inteligência artificial, que, embora proporcionem maior conectividade e autonomia aos usuários, também ampliam as possibilidades de exposição e vulnerabilidade. Em razão disso, Souza defende a necessidade de regulamentações mais rigorosas do que as que já estão em vigor.

Segundo Françoso e Nery (2024), o aumento do acesso à internet nos últimos anos facilitou a prática de crimes no ambiente virtual, o que resultou em uma proliferação de delitos informáticos. As autoras destacam que, além de crimes patrimoniais e fraudes, delitos de natureza sexual também passaram a ser cometidos através da rede mundial de computadores.

A exemplo disso, em Teresina/PI, no ano de 2017, foi noticiado o primeiro caso brasileiro do crime de estupro virtual, no qual o acusado usou um perfil falso no Facebook para coagir uma vítima a realizar atos sexuais em troca da preservação de suas imagens íntimas. A investigação contou com decretação de fornecimento das informações do usuário fornecidas pelo Facebook e apreensão de celulares, computador, pen drive e outros equipamentos eletrônicos com o fim de identificar e provar as ações do acusado, o que levou à sua prisão.

Percebe-se, com isso, a evolução constante dos crimes e suas modalidades dos delitos digitais, a qual exige que a legislação e o Poder Judiciário se adaptem a essa nova realidade, não apenas com a criação de leis específicas, mas também o aperfeiçoamento e implementações de protocolos rigorosos da cadeia de custódia para provas digitais com base nas peculiaridades da era digital.

6 FRAUDE ELETRÔNICA: PROVAS DIGITAIS E A SUA VALIDADE POR MEIO DO APLICATIVO WHATSAPP

Não há como falar de crimes cibernéticos sem mencionar o crime de fraude eletrônica, acrescentado, ao Código Penal, pela Lei n° 14.155/21. O diploma legislativo dispõe:

Art. 171 – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

§ 3º – A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência. (Brasil, 1943).

Como exposto, é um crime novo, com uma pena máxima consideravelmente alta, e o envolvimento da vítima e as redes sociais possuem grande destaque. Ligado a isso, cumpre

pontuar que, conforme dados divulgados pelo DataSenado (2024), golpes digitais vitimaram 24% (vinte e quatro por cento) da população brasileira, o que significa mais de 40,85 milhões de pessoas. Dentre tais fraudes, encontram-se clonagem de cartão, fraude na internet ou invasão de contas bancárias.

Durante a pesquisa, fora feito o seguinte questionamento: Nos últimos 12 meses, você perdeu dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão bancária? 24%, portanto, respondeu que sim, veja-se o gráfico:

“Nos últimos 12 meses, você perdeu dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias?”
24% Sim
75% Não

Fonte: Senado

Além disso, conforme dados divulgados pelo Fórum Brasileiro de Segurança Pública, entre 2018 e 2021, o estelionato por meio eletrônico cresceu quase 500% (Central de Notícias Uninter (2022). Assim, diante de todos os dados apresentados, as provas digitais merecem grande destaque e, sobre isto, entra-se na discussão a validade das provas produzidas pelo aplicativo whatsapp, este que, segundo o relatório de cibersegurança, elaborado pelo ThreatX, é o preferido pelo cibercriminosos (CLEARSALE, 2023).

A partir disso, acompanhando as modificações sociais, a jurisprudência do Superior Tribunal de Justiça discorreu sobre o tema, entendendo que, frente a grande facilidade de adulteração das provas digitais, é indispensável, para a sua validade, que as fases de obtenção sejam documentadas, com o devido registro das etapas da cadeia de custódia. Outrossim, deve haver a formalização do processo da cadeia de custódia, com laudo produzido por perito e esclarecimento das metodologias e ferramentas empregadas (STJ, 2024).

Em razão disso, percebe-se que a tipificação penal do crime de fraude eletrônica foi de

grande relevância para o combate de crimes digitais e que, intrínseco ao tema, está a produção de provas digitais, sobretudo as que são produzidas no aplicativo WhatsApp, devendo estas, como já defendido durante toda a pesquisa, respeitar a cadeia de custódia, de forma a garantir a ampla defesa, o devido processo legal e a sua própria legalidade/validade.

7 ALGORITMOS, INTELIGÊNCIA ARTIFICIAL E BIG DATA: DESAFIOS CONSTITUCIONAIS E JURÍDICOS NA ERA DIGITAL

Segundo Fuller (2008), os algoritmos são funções lógicas tão fundamentais que podem ser imperceptíveis para a maioria dos usuários. O professor também pondera que são blocos de construção fortemente formulados trabalhando para fazer, nomear, multiplicar, controlar e inter-relacionar a realidade. De modo geral, Lopes e Garcia (2002) explicam que algoritmos são conjuntos de instruções sequenciais finitas com o objetivo de solucionar problemas. Para os autores, um *software* de computador é um conjunto de algoritmos escritos em uma determinada linguagem de programação, linguagem que, através de outros processos, pode ser compreendida pelas máquinas.

De acordo com Baranauska (2007), o Aprendizado de Máquina, além de ser um ramo da Inteligência Artificial voltado para o desenvolvimento de técnicas computacionais relacionadas ao aprendizado e à criação de sistemas capazes de adquirir conhecimento automaticamente, também se refere a um programa de computador que toma decisões com base nas experiências acumuladas a partir de soluções bem-sucedidas para problemas anteriores.

Conforme a Equipe DSA (2018), organizações em uma grande variedade de indústrias já começaram a experimentar a aprendizagem de máquina, como, por exemplo, na detecção de fraudes em bancos, operadoras de cartão de crédito, como também na análise de streaming de dados: onde muitos dados, como *feeds* de redes sociais e transações de vendas

on-line, são atualizadas constantemente. As organizações usam a aprendizagem de máquina para encontrar intuições ou identificar problemas potenciais em tempo real dentre outras intervenções.

Conforme González (2016), *Big Data* é um termo que alude a um enorme crescimento em acessos e uso da informação automatizada. Profissionais da área defendem que com o tratamento de grande quantidade de dados gerados diariamente, seja possível permitir maior capacidade de acertos e definição de tomar o melhor caminho para alcançar os objetivos pretendidos. A autora supracitada também se refere ao *Big Data* como sendo as gigantescas quantidades de informações digitais controladas por empresas, autoridades e outras organizações, e que estão sujeitas a extensas análises com base no uso de algoritmos.

Callejón (2023) argumenta que a utilização de algoritmos no âmbito jurídico deve ser analisada sob a perspectiva constitucional, especialmente em relação ao sistema de direitos fundamentais, que não pode ser negligenciado em função de possíveis lesões decorrentes de procedimentos informatizados. Os algoritmos, apesar de serem ferramentas projetadas para otimizar processos e alcançar objetivos específicos, muitas vezes associados a ganhos econômicos, precisam ser compatíveis com os princípios constitucionais que regem a proteção dos direitos.

Nesse contexto, o uso de algoritmos para implementar políticas públicas jurídicas exige cuidado redobrado para evitar violações de direitos fundamentais, como a discriminação ou a restrição arbitrária de garantias individuais. Assim, a finalidade dos algoritmos e seu desenho devem ser compatíveis com os valores constitucionais, assegurando que a eficiência tecnológica não se sobreponha ao respeito pelos direitos básicos dos indivíduos.

Monteiro (2024) destaca que, mesmo diante dos evidentes limites das possibilidades de tutela legal, os brasileiros devem observar atentamente os movimentos em torno do Marco Regulatório de Inteligência Artificial e da regulamentação da proteção de dados nas

atividades de segurança pública. O que ressoa diretamente com os desafios apontados, especialmente no contexto da preservação das provas digitais no processo penal. A necessidade de regulamentações específicas e adequadas para o ambiente digital, alinhadas às evoluções tecnológicas e ao fortalecimento da segurança pública, é essencial para garantir a integridade e a admissibilidade das evidências digitais em um cenário jurídico cada vez mais complexo.

8 MÉTODO

Este estudo utiliza uma abordagem qualitativa, já que envolveu um procedimento analítico da doutrina, jurisprudência, norma técnica e legislação que utilizadas no presente estudo sobre o processo de cadeia de custódia de provas digitais no contexto processual penal. Como técnicas aplicadas, a análise documental e jurisprudencial permite identificar as especificidades e desafios que os dados digitais apresentam no processo penal brasileiro, incluindo os requisitos para a validade processual das provas.

O levantamento bibliográfico contempla fontes como livros de doutrina jurídica, artigos científicos e publicações especializadas em direito penal e digital, com foco no tratamento e preservação das provas digitais em conformidade com a legislação brasileira, como o Código de Processo Penal (CPP) e normas técnicas como a ISO/IEC 27037:2013. Já a análise jurisprudencial se concentra em decisões do Superior Tribunal de Justiça (STJ) e outros tribunais que abordam a aplicabilidade da cadeia de custódia digital e a importância do código hash e dos quatro princípios de tratamento da evidência digital.

A análise desses documentos, com apoio de doutrinas jurídicas e normativas técnicas, visa mapear lacunas, limitações e boas práticas na preservação de provas digitais. Essa metodologia proporciona uma compreensão aprofundada da necessidade de padronização e atualização legislativa no tratamento das provas digitais, com foco na adequação do sistema jurídico brasileiro às particularidades dos crimes cometidos em ambiente virtual.

O escopo descritivo, agregado a uma metodologia técnica bibliográfica, foi essencial para estabelecer relações entre os diferentes aspectos da cadeia de custódia. Isso incluiu a análise da importância da integridade das provas digitais, o impacto das tecnologias emergentes no processo penal e as implicações legais e sociais decorrentes das falhas na cadeia de custódia. A compreensão desses elementos é fundamental para aprimorar as práticas forenses e garantir a efetividade do sistema de justiça na proteção dos direitos individuais.

9 CONSIDERAÇÕES

O trabalho proposto alcançou os objetivos delimitados inicialmente, evidenciando a cadeia de custódia de provas digitais no contexto do Direito Penal em seus aspectos conceituais, práticos e normativos. A pesquisa permitiu analisar como a cadeia de custódia tem se adaptado ao ambiente digital, destacando sua relevância para garantir a integridade e a validade das provas no processo penal. Foram identificados os desafios enfrentados na preservação das evidências digitais, com ênfase nas técnicas e metodologias necessárias para assegurar a legalidade das provas, conforme as exigências do sistema jurídico brasileiro.

Diante dos desafios apresentados pela volatilidade e suscetibilidade à manipulação das provas digitais, algumas soluções e perspectivas inovadoras podem ser implementadas para fortalecer a cadeia de custódia e garantir a integridade e admissibilidade dessas evidências no processo penal.

Nesse sentido, verificou-se que a aceitação da prova digital como fonte probatória confiável depende diretamente da preservação da cadeia de custódia, por meio da adoção de procedimentos rigorosos e técnicos que assegurem a integridade e a autenticidade das evidências digitais. Esses procedimentos refletem a necessidade de um equilíbrio entre a rigidez das regras processuais e a busca pela verdade real, considerando a crescente

importância das provas digitais no cenário jurídico contemporâneo. A preservação da integridade dessas evidências é essencial para garantir a efetividade da justiça e assegurar que decisões judiciais sejam tomadas com base em provas fidedignas e bem preservadas, por mais que a cadeia de custódia não seja a prova em si, mas sim o modo de preservá-la, é essencial sua preservação.

A preservação eficaz das provas digitais requer a capacitação contínua de agentes como policiais, peritos e operadores do direito, aliada à adoção de tecnologias avançadas para registrar e rastrear cada etapa da cadeia de custódia de forma transparente e imutável. A padronização de ferramentas tecnológicas, como softwares de código hash homologados, é essencial para garantir a integridade das evidências, devendo sua aplicação ser regulamentada.

Além disso, é necessário atualizar o ordenamento jurídico para incluir protocolos específicos para provas digitais, prevendo sanções para violações e incentivando práticas modernas e auditáveis, assegurando a confiabilidade e admissibilidade das evidências no processo penal.

Por ser um tema relativamente novo, a cadeia de custódia aplicada às provas digitais ainda demanda maior exploração acadêmica e prática, visando aprofundar a compreensão das interações entre o Direito Penal e o ambiente virtual. A constante evolução das tecnologias digitais e o aumento significativo dos crimes cibernéticos impõem desafios jurídicos que exigem uma adaptação contínua das normas e procedimentos legais. Dessa forma, deve-se buscar assegurar não apenas a integridade das provas digitais, mas também a efetividade do processo penal em um cenário cada vez mais digitalizado.

REFERÊNCIAS

ACADEMY, Data Science. **Data Science Academy: 17 casos de uso de machine learning**. 17 CASOS DE USO DE MACHINE LEARNING. 2018. Disponível em: http://datascienceacademy.com.br/blog/17-casos-de-uso-de-machine-learning/#:~:text=Um

%20exemplo%20cl%C3%A1ssico%20de%20aprendizagem,acertos%2C%20at%C3%A9%20atingir%20seu%20objetivo. Acesso em: 24 nov. 2024.

ANTÔNIO FILHO; TORON, Alberto; BADARÓ, Gustavo. **Código de Processo Penal Comentado**. São Paulo (SP):Editora Revista dos Tribunais. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14.406:2018 – Cadeia de custódia de evidências digitais. Rio de Janeiro, 2018. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273. Acesso em: 03 nov. 2024.

BADARÓ, Gustavo Henrique. **A Cadeia de Custódia da Prova Digital**. In: OSNA, Gustavo et. al. Direito Probatório. Londrina: Thoth, 2023, p. 179.

BADARÓ, Gustavo Henrique. **A cadeia de custódia e sua relevância para a prova penal**. Temas atuais da investigação preliminar no processo penal. Tradução. Belo Horizonte: D'Plácido, 2017. p. 535/536.

BARANAUSKAS, José Augusto. **Aprendizado de Máquina Conceitos e Definições**. Disponível em: < http://dcm.ffclrp.usp.br/~augusto/teaching/ami/AM-I-ConceitosDefinicoes.pdf>. Acesso em: 24 nov. 2024

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial**. São Paulo: Saraiva, 2016, v. 2, p. 533.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm. Acesso em: 11 nov. 2024.

BRASIL. **Lei Federal 13.968, de 26 de dezembro de 2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar o crime de incitação ao suicídio e

incluir as condutas de induzir ou instigar a automutilação, bem como a de prestar auxílio a quem a pratique. Diário Oficial da República Federativa do Brasil, Brasília: DF, 26 dez. 2019b. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019 2022/2019/lei/L13968.htm>. Acesso em: 10 nov. 2024.

BRASIL. **Lei nº 11.343, de 23 de agosto de 2006**. Institui o Sistema Nacional de Políticas Públicas sobre Drogas – Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 2, 24 ago. 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 4 nov. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 4 nov. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 4 nov. 2024.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 17 mar. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 6 nov.

2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 nov. 2024.

BRASIL. **Lei 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da República Federativa do Brasil, Brasília: DF, 24 dez. 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 18 jan. 2020.

BRASIL. **Superior Tribunal de Justiça**. Agravo Regimental no Recurso em Habeas Corpus nº 143.169/RJ. Relator: Ministro Messod Azulay Neto; Relator para Acórdão: Ministro Ribeiro Dantas; Quinta Turma. Julgado em 7 fev. 2023. Diário da Justiça eletrônico, 2 mar. 2023. Acesso em: 06 nov. 2024.

BRASIL. **Superior Tribunal de Justiça**. Quinta Turma não aceita como provas prints de celular extraídos sem metodologia adequada. Portal de Notícias do STJ, 2 maio 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/02052024-Quinta-Turma-nao-aceita-como-provas-prints-de-celular-extraidos-sem-metodologia-adequada.aspx. Acesso em: 4 nov. 2024.

BRASIL. **Superior Tribunal de Justiça**. Habeas Corpus n.º 653515/SP. Relator Ministro Reynaldo Soares da Fonseca. 6ª Turma. Data do julgamento: 23/11/2021. Disponível em: https://processo.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28HC.clas.+e+%40num%3D%22653515%22%29+ou+%28HC+adj+%22653515%22%29.suce. Acesso em: 22 de nov. 2024.

BRASIL. **Superior Tribunal de Justiça**. Processual penal. Agravo regimental no habeas corpus. Tráfico de drogas. Apreensão de celular. Extração de dados. Captura de telas. Quebra da cadeia de custódia. Inadmissibilidade da prova digital. Agravo regimental provido. Relator: Ministro Joel Ilan Paciornik. AgRg no HC: 828054 RN 2023/0189615-0. Julgamento: 23 abr. 2024. Publicação: DJe 29 abr. 2024. Acesso em: 03 nov. 2024.

CALLEJÓN, Francisco Balaguer. **A constituição do algoritmo**. Tradução Diego Fernandes Guimarães – 1. Ed. – Rio de janeiro. Forense, 2023, p. 15.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Supervisão, no âmbito do Poder Judiciário, de sentença da Corte Interamericana de Direitos Humanos no caso Favela Nova Brasília vs. Brasil**: sumário executivo / Conselho Nacional de Justiça; Coordenadores Luis Geraldo Sant'ana Lanfredi; Valter Shuenquener de Araújo; Isabel Penido de Campos Machado. – Brasília: CNJ, 2021.

CONSULTOR JURÍDICO. **A cadeia de custódia de provas no processo penal brasileiro**. 11 dez. 2023. Disponível em: https://www.conjur.com.br/2023-dez-11/a-cadeia-de-custodia-de-provas-no-processo-penal-brasileiro/. Acesso em: 6 nov. 2024.

CLEARSALE. **Cibercriminosos preferem WhatsApp, revela relatório de cibersegurança**. Blog ClearSale, 19 jul. 2023. Disponível em: https://blogbr.clear.sale/cibercriminosos-preferem-whatsapp-revela-relatorio-de-ciberseguranca. Acesso em: 4 nov. 2024.

FERREIRA, **Rute Raquel Prates**. Violação do sigilo do whatsapp como meio de obtenção de provas no processo penal: análise jurisprudencial do superior tribunal de justiça. Orientador: Marcelo Almeida Ruivo. 2020. 27 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Católica do Rio Grande do Sul – PUCRS, Porto Alegre, 2020. Disponível em: https://www.pucrs.br/direito/wp-content/uploads/sites/11/2021/01/rute_ferreira.pdf. Acesso

em: 05 nov. 2024

FULLER, Matthew. **Software studies\ a lexicon**. London, England: The Mit Press, 2008. 349 p. Disponível em: https://monoskop.org/images/a/a1/Fuller_Matthew_ed_Software_Studies_A_Lexicon.pdf. Acesso em: 23 nov. 2024.

GONZÁLEZ, Elena Gil. **Big data, privacidad y protección de datos**. Madrid: Agencia Española de Protección de Datos y Boletín Oficial del Estado, 2016.

GUERRA, Maite Neves. **Regime democrático das provas digitais no processo penal: aquisição e qualificação**. 2024. 11 f. Dissertação (Mestrado em Ciência Jurídica) — Universidade do Vale do Itajaí, Itajaí, 2024. Disponível em: https://www.univali.br/Lists/TrabalhosMestrado/Attachments/3381/VERS%C3%83O%20FINAL%20DISSERTA%C3%87%C3%83O%20.pdf. Acesso em: 03 nov. 2024.

LOPES, A.; GARCIA, G. **Introdução à programação: 500 algoritmos resolvidos**. 6ª tiragem. Rio de Janeiro: Editora Elsevier, 2002. p. 469.

LOPES JUNIOR., Aury. **Direito processual penal**. – 16. ed. – São Paulo: Saraiva Educação, 2019. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Crimes digitais. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/crimes-digitais. Acesso em: 4 nov. 2024.

MONTEIRO, Pedro Diogo Carvalho. **Pensando A.I.A Generativa na Arquitetura Racial-Punitiva do Estado** In: SILVA, Tarcizio (org.). Inteligência Artificial Generativa: discriminação e impactos sociais. Online: Desvelar. Disponível em: https://desvelar.org/inteligencia-artificial-generativa-discriminacao-e-impactos-sociais/. Acesso em: 24 nov. 2024.

NUCCI, Guilherme de Souza. **Curso de direito processual penal**. – 17. ed. – Rio de Janeiro:

Forense, 2020.

PARODI, Lorenzo. **A cadeia de custódia da prova digital à luz da Lei 13.964/2019**. Consultor Jurídico, [S. l.], 18 jun. 2020. Disponível em: https://www.conjur.com.br/2020-jun-18/lorenzo-parodi-cadeia-custo-dia-prova-digital?utm_source=dlvr.it&utm_medium=twitter. Acesso em: 05 nov. 2024.

RANGEL, Paulo. **Direito processual penal**. 23. ed. São Paulo: Atlas, 2015.

SANTOS, José Eduardo Lourenço dos; FURLANETO NETO, Mário. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil**. Revista Em Tempo, [S.l.], v. 20, n. 1, nov. 2020. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 03 nov. 2024.

SENADO FEDERAL. **Portal de Notícias do Senado Federal**. Golpes digitais atingem 24% da população brasileira, revela DataSenado., 01 out. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado. Acesso em: 4 nov. 2024.

SOUZA, Bernardo; JACOB, Raphael. **Golpes Digitais** – Ed. 2024. São Paulo (SP): Editora Revista dos Tribunais. 2024.

OLIVEIRA, Vinícius Machado de. **ISO 27037 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital**. Academia de Forense Digital, [S. l.], 01 jan. 2019. Disponível em: https:// Revista da ESMESC, v.30, n.36, p.323-350, 2023349academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aqui-sicao-e preservacao-de-evidencia/. Acesso em: 05 nov. 2024

TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ. **Primeira prisão por estupro virtual no Brasil é decretada no Piauí**. Disponível em: https://www.tjpi.jus.br/portaltjpi/tjpi/noticias-tjpi/primeira-prisao-por-estupro-virtual-no-brasil-

e-decretada-no-piaui/. Acesso em: 11 nov. 2024.

UNINTER. Portal UNINTER. **Especialista alerta para aumento de crimes nas redes sociais**. 18 out. 2023. Disponível em: https://www.uninter.com/noticias/especialista-alerta-para-aumento-de-crimes-nas-redes-sociais. Acesso em: 6 nov. 2024.

---

[1] Graduanda do Curso de Direito da Universidade Federal do Rio Grande do Norte (UFRN/CERES).

[2] Professora Adjunta do Departamento de Direito da UFRN/CERES. Doutora em Direito pela Université Grenoble Alpes France em com tutela com a Universidade Federal da Paraíba - UFPB. Mestre em Direito pela Universidade Grenoble Alpes França com título reconhecido pela Universidade Federal de Minas Gerais -UFMG.