UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO
LINHA DE PESQUISA: DIREITO, JURISDIÇÃO E INTELIGÊNCIA ARTIFICIAL
PROJETO DE PESQUISA: DEMOCRACIA, PROCESSO E JURISDIÇÃO

REGIME DEMOCRÁTICO DAS PROVAS DIGITAIS NO PROCESSO PENAL: AQUISIÇÃO E QUALIFICAÇÃO

MAITE NEVES GUERRA

Itajaí (SC), junho de 2024.

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO
LINHA DE PESQUISA: DIREITO, JURISDIÇÃO E INTELIGÊNCIA ARTIFICIAL
PROJETO DE PESQUISA: DEMOCRACIA, PROCESSO E JURISDIÇÃO

REGIME DEMOCRÁTICO DAS PROVAS DIGITAIS NO PROCESSO PENAL: AQUISIÇÃO E QUALIFICAÇÃO

MAITE NEVES GUERRA

Dissertação submetida ao Curso de Mestrado em Ciência Jurídica da Universidade do Vale do Itajaí – UNIVALI, como requisito parcial à obtenção do título de Mestre em Ciência Jurídica.

Orientador (a): Professor Doutor Alexandre Morais da Rosa

Itajaí (SC), junho de 2024.

AGRADECIMENTOS

Agradeço imensamente à minha família que sempre me proporcionou o melhor estudo e as melhores condições. Sem o apoio deles nada seria possível.
Ao meu namorado, Nito, que me incentiva, ajuda e apoia incondicionalmente. Sou sua grande fã.
Às minhas amigas que compreenderam minha ausência nos últimos dois anos e que, mesmo de longe, se mantiveram perto.
Aos meus professores da graduação e do mestrado, sem dúvidas carregado dentro de mim um pouco do conhecimento de vocês.
Ao dr. Paulo Cruz, pelo suporte, que sem ele não seria possível realizar um mestrado aos meus poucos 26 anos.
Por fim, ao meu orientador, Dr. Alexandre Morais da Rosa, que colocou meus pés no chão e me proporcionou grandes ensinamentos com toda sua sabedoria.

DEDICATÓRIA

Dedico este trabalho à minha família, às minhas amigas e em especial, ao Nito.

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a Coordenação do Curso de Mestrado em Ciência Jurídica, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Itajaí (SC), junho de 2024.

MAITE NEVES GUERRA

Assinado de forma digital por MAITE NEVES GUERRA
Dados: 2024.08.22 20:15:06 -03'00'

Maite Neves Guerra
Mestranda

P Á G I N A D E A P R O V A Ç Ã O

MESTRADO

Conforme Ata da Banca de defesa de mestrado, arquivada na Secretaria do Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica - PPCJ/ UNIVALI, em 28/06/2024, às 9h, a mestranda Maite Neves Guerra fez a apresentação e defesa da Dissertação, sob o título "REGIME DEMOCRÁTICO DAS PROVAS DIGITAIS: AQUISIÇÃO E QUALIFICAÇÃO".

A Banca Examinadora foi composta pelos seguintes professores: Doutor Alexandre Morais da Rosa (UNIVALI), como presidente e orientador, Doutor Leonardo Costa de Paula (Universidade Federal Fluminense), como membro, Doutor Airto Chaves Junior (UNIVALI), como membro e Doutora Maria Claudia da Silva Antunes de Souza (UNIVALI), como membro suplente. Conforme consta em Ata, após a avaliação dos membros da Banca, a Dissertação foi aprovada.

Por ser verdade, firmo a presente.

Itajaí (SC), 28 de junho de 2024.

PROF. DR. PAULO MÁRCIO DA CRUZ
Coordenador/PPCJ/UNIVALI

ROL DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AgRg	Agravo Regimental
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
CNH	Carteira Nacional de Habilitação
CPC	Código de Processo Civil
CPF	Cadastro de Pessoas Físicas
CPP	Código de Processo Penal
CRFB	Constituição da República Federativa do Brasil
DETRAN	Departamento de Trânsito
DNS	Domain Name System
ERB	Estações Rádio Base
GPS	Global Positioning System
ICP	Infraestrutura de Chaves Públicas
IEC	International Electrotechnical Commission
IML	Instituto Médico Legal
IP	Internet Protocol
IPED	Indexador e Processador de Evidências Digitais
ISO	Internet Protocol
MD	Message-Digest Algorithm
MP	Medida Provisória
MPF	Ministério Público Federal
NBR	Norma Brasileira
NCP	Network Control Protocol
NIST	National Institute of Standards and Technology
ONU	Organização das Nações Unidas
PDA	Personal Development Analysis
RE	Recurso Extraordinário
REsp	Recurso Especial
RG	Registro Geral
RMS	Recurso Ordinário em Mandado de Segurança

SHA	Secure Hash Algorithm
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCP	Transmission Control Protocol
TJ	Tribunal de Justiça
TRT	Tribunal Regional Trabalhista
TSE	Tribunal Superior Eleitoral
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
WI-FI	Wireless Fidelity
WWW	World Wide Web

ROL DE CATEGORIAS

Blockchain: Um programa de computador que realiza duas ações: verificação rápida de modificação nos dados e correção automática com base em replicadores desses dados. Com isso gera-se a imutabilidade dos dados, não permitindo a modificação de conteúdo que lhe foi inserido.[1]

Cadeia de custódia: 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.[2]

Conhecimento: O conhecimento vai além da informação, pois, enquanto a informação consiste em dados organizados e trabalhados, o conhecimento representa um nível superior de entendimento, envolvendo a aplicação e interpretação da informação de forma significativa. O conhecimento não se limita à posse de dados, mas reside na capacidade de abstrair ideias, compreender contextos e gerar novos saberes. A informação, por sua vez, é um recurso valioso para a construção do conhecimento, mas não é suficiente por si só para expandir o saber humano. É através do conhecimento que o indivíduo, dotado de capacidade cognitiva, identifica o que é relevante e transforma a informação em aprendizado e inovação[3]

Criptografia: A origem da palavra criptografia deriva das palavras gregas κρυπτός (kryptos), que significa escondido, e γράφειν (grafein), que significa escrever. Representava, inicialmente, uma forma diferente de escrita, que buscava impossibilitar a compreensão de mensagens trocadas, como uma espécie de “falar em códigos”, isto é, a forma não corresponde com a mensagem enviada, portanto,

---

[1] LAGO, Lucas. **Blockchain:** confiança através de algoritmos. Escola Politécnica do Estado de São Paulo, CEST – Boletim, v. 2, n. 4. out. 2017. p. 1.

[2] BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF; dez. 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm>. Acesso em: 06 mai 2024.

[3] SILVA, Heide Miranda da. **Qual a diferença entre dados, informação e conhecimento?** Disponível em: <https://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm>. Acesso em: 10 mar. 2024.

incompreendida, o que garantia a segurança das informações trocadas. Pela criptografia, uma mensagem simples é transformada numa mensagem cifrada, decifrada apenas por uma ou mais chaves. A criptografia é um método de codificação de dados que permite o acesso apenas de pessoas autorizadas, que possuem uma chave de acesso.[4]

Dados: São elementos brutos e isolados, ou seja, sem valor e conexão entre si[5]. São fatos soltos, sem contexto ou interpretação. Quando abordado no âmbito jurídico, os dados são evidências que poderão ser utilizados nos processos judiciais, mediante o devido e correto armazenamento e processamento. Em resumo os dados são a matéria-prima do caso a ser investigado e julgado. Os dados podem ser palavras, números, sons, imagens ou qualquer forma de representação simbólica de fatos.[6]

Dados digitais: Os dados (digitais) são coletados, processados, armazenados e transmitidos por meio de sistemas computacionais. Referem-se a informações que são armazenadas, processadas e transmitidas na forma de códigos binários, compostos por 0s e 1s. São representações digitais de diversos tipos de QEdados, como texto, imagens, vídeos, sons, entre outros. Esses dados digitais são utilizados em diversos contextos, desde arquivos armazenados em computadores até transmissões de dados pela internet.[7]

---

[4] EDGE, Charles; O'DONNELL, Daniel. ***Introduction to cryptography***. In: LOPES, Marcus Vinícius Pimenta. **A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de provas digitais.** Tese de Doutorado. 218 f. Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023. p. 73.

[5] BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF; nov. 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 09 mar. 2024.

[6] ROSA, Alexandre Morais da. **Lei de acesso à informação pode iluminar as sombras do processo penal**. Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2016-jan-01/limite-penal-lei-acesso-informacao-iluminar-sombras-processo-penal/>. Acesso em: 09 mar. 2024.

[7] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 99.

Documento eletrônico: O documento eletrônico é qualquer informação gerada, transmitida, acessada e armazenada em meios eletrônicos, que dispensa o papel físico. É ainda uma sequência de *bits* (representação decodificada) traduzida por algum programa ou *software* que representa algum fato ou informação. [8]

E-evidência: Em resumo, é a prova digital tratada**.** Trata-se da evidência digital que foi coletada, preservada, analisada e apresentada em processos judiciais. A E-Evidência é governada a partir da observação do meio a que se destina, da confiabilidade e da superação dos testes de verificação.[9]

Hash* ou função *hash: O código denominado *HASH* ou função *HASH,* é um algoritmo matemático que produz uma sequência numérica, única, específica e irreversível. É ele que garantirá que os dados contidos em determinado dispositivo não tenham sido corrompidos, adulterados, transmitidos ou armazenados. É a função *HASH* que servirá de parâmetro para identificação de quebra da cadeia de custódia digital, pois qualquer manipulação inadequada irá alterar esse código. São exemplos de aplicações comuns da função *HASH* o armazenamento seguro de senhas e assinaturas digitais. O código *HASH* através deste algoritmo matemático, gera chaves que representam de maneira quase unívoca um documento, registro, arquivo, etc. O *HASH* permite garantir que a evidência digital obtida não tenha sido manipulada nem alterada, já que o *HASH* gerado é inviolável. Em outras palavras, é uma função que representa dados de comprimento variável como um dado de comprimento fixo e onde pequenas diferenças nos dados de entrada geram uma grande diferença nos dados de saída. [10]

Informação: São dados organizados, processados, interpretados e analisados. Percebe-se que a informação não é possível sem o dado, mas o dado sem a devida qualificação, não tem valor interpretativo. É o resultado do processamento de

---

[8] ROSA, Alexandre Morais da; CANI, Luiz Eduardo. **Guia para Mitigação dos Erros Judiciários no Processo Penal**: as causas prováveis e as estratégias de enfrentamento. Florianópolis: Emais, 2021. p. 105.

[9] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-A. – 1. ed. – Florianópolis: Emais, 2021. p. 437.

[10] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 207.

dados, os quais, diferente dos dados, possuem um significado, contribuindo no processo de tomada de decisões.[11]

Internet: a Internet se refere à estrutura que conecta computadores e dispositivos em todo o mundo. Consiste em uma grande rede de dados digitais comportada de diversas outras redes que se interconectam e permitem a troca de dados entre cada um dos seus pontos de conexão. Em outras palavras, é a interligação de redes de computadores espalhadas pelo mundo, que passam a funcionar como uma só rede, possibilitando a transmissão de dados, sons e imagens de forma rápida.[12]

Metadados: São dados adicionais sobre determinada operação ou conteúdo digital que podem ajudar no processamento da informação pelos softwares, além de identificar recursos e manter históricos. Os metadados são informações estruturadas que facilitam a identificação, descoberta, seleção, uso, acesso e gerenciamento de objetos de informação, tanto físicos quanto digitais. [13]

Provas digitais: A prova digital, também conhecida como evidência digital (do inglês *digital evidence*) é o meio utilizado para demonstrar a evidência de um fato ou evento ocorrido em meio digital. As provas digitais são entidades imateriais, mas possuem sua própria materialidade, sendo definido conceitualmente, como impulsos elétricos que respondem a uma sequência numérica predefinida e que, quando canalizados em um suporte informático com memória, originam informações inteligíveis.[14]

Provas: O termo “prova” surge do verbo “provar”, cujo significado é o de demonstrar a veracidade de um enunciado sobre um fato tido por ocorrido no

---

[11] SILVA, Heide Miranda da. **Qual a diferença entre dados, informação e conhecimento?** Disponível em: <https://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm>. Acesso em: 10 mar. 2024.

[12] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p.7.

[13] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p.47.

[14] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 62.

mundo real. Tal palavra possui vários significados, sendo uma origem etimológica de probo (do latim, *probatio* e *probus*), traduzindo as ideias de verificação, inspeção, exame, aprovação ou confirmação. Juridicamente a prova são dados objetivos que confirmam ou negam uma asserção sobre determinado fato que interessa à decisão da causa. O conceito de prova é bastante extenso e diverso, isso porque a prova é ao mesmo tempo, meio, resultado e atividade. Por exemplo, a prova testemunhal é um meio, enquanto seu resultado, também é prova, de modo que revela a ocorrência ou não de fatos. Já a atividade é a própria realização da oitiva da testemunha pelas partes. A prova, busca a reconstituição (aproximativa e parcial) de um fato passado, histórico, para um juiz 'ignorante' (pois ignora os fatos). É a prova que permite a atividade recognitiva (e não cognitiva, pois indireta) do juiz em relação ao fato histórico (story of the case) narrado pela acusação. Ao mesmo tempo tem uma função persuasiva, pois é através dela que se permite a construção do convencimento, da decisão. Por isso, as provas servem para obter a captura psíquica do julgador, para formar sua convicção.[15]

Web: Enquanto a Internet se refere à estrutura que conecta computadores e dispositivos em todo o mundo, a Web é a rede (o sistema) em si pela qual é feita a navegação por hiperlinks, acessíveis através da internet. Em suma, a internet é a rede global de computadores, enquanto a web é um dos serviços que funcionam sobre essa rede, permitindo o acesso a informações e conteúdo.[16]

---

[15] LOPES JUNIOR, Aury; ROSA, Alexandre Morais da. **A importância da cadeia de custódia para a preservar a prova penal**. Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal/>. Acesso em: 25 mar 2024.

[16] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 7.

SUMÁRIO

RESUMO

A presente dissertação tem como intuito analisar as formas de aquisição e de qualificação de provas digitais no processo penal brasileiro. Com efeito, está inserida na linha de pesquisa “Direito, jurisdição e inteligência artificial” e projeto de pesquisa Democracia, processo e jurisdição. O objetivo da pesquisa é analisar os requisitos necessários para que as provas digitais sejam consideradas válidas nos processos penais, bem como os procedimentos adequados para sua coleta, preservação e apresentação em juízo, a fim de garantir maior segurança jurídica das decisões judiciais, com a devida preservação dos princípios constitucionais, da ampla defesa, do contraditório, do *in dubio pro reu*, da legalidade, presunção da inocência e a inadmissibilidade das provas ilícitas. Justifica-se a presente pesquisa, ante a evidente precariedade legislativa e jurídica brasileira na área, que enfrenta desafios significativos em acompanhar a rápida evolução tecnológica e se adequar a realidade moderna. A pesquisa está estruturada em três capítulos. O primeiro capítulo contextualiza o ambiente digital na contemporaneidade, abordando a sociedade da informação, a distinção entre dados, informação e conhecimento, e os conceitos de internet e web. Além disso, discute o papel dos dispositivos eletrônicos e a importância da privacidade e proteção de dados nesse cenário. O segundo capítulo explora a teoria geral da prova e sua aplicação às provas digitais, com ênfase nos direitos constitucionais à prova, contraditório e ampla defesa. Também são apresentados os conceitos de prova, suas finalidades, classificações e os meios de prova e de obtenção de prova. O capítulo introduz o conceito de prova digital, suas características e as principais espécies encontradas no contexto jurídico. Por fim, o terceiro capítulo concentra-se na qualificação e no tratamento das provas digitais, aprofundando a discussão sobre a cadeia de custódia, tanto no âmbito geral quanto no digital. São analisadas as etapas da cadeia de custódia, desde o reconhecimento e isolamento do vestígio até o seu descarte, com destaque para a importância da preservação da integridade e autenticidade das provas digitais. O capítulo também apresenta soluções tecnológicas que auxiliam na coleta, análise e preservação de provas digitais. A presente pesquisa está vinculada as ODS nº 9 e 16º. O 9º, pois fomenta a inovação, refletindo a importância de integrar tecnologias avançadas. Já o 16º, pois aborda a importância do acesso à justiça, eficácia das instituições legais, assegurando a proteção dos direitos fundamentais e a admissibilidade de provas legítimas e autênticas. Quanto a metodologia, registra-se que, na Fase de Investigação foi utilizado o Método Indutivo, na Fase de Tratamento de Dados o Método Cartesiano, e, o Relatório dos Resultados expresso na presente dissertação é composto na base lógica indutiva.

Palavras-chave: Provas digitais; Cadeia de Custódia; Blockchain; Dados; *Web*

ABSTRACT

This dissertation analyzes the methods of acquisition and qualification of digital evidence in the Brazilian criminal process. It is part of the line of research Law, Jurisdiction, and Artificial Intelligence, and of the research project Democracy, Process, and Jurisdiction. The research aims to examine the necessary requirements for digital evidence to be considered valid in criminal proceedings, and the appropriate procedures for its collection, preservation, and presentation in court, in order to ensure greater legal security of judicial decisions, while duly preserving constitutional principles such as ample defense, the adversarial process, the principle of in *dubio pro reo*, legality, the presumption of innocence, and the inadmissibility of illegal evidence. This research is justified by the evident legislative and legal precariousness in Brazil in this area, and the significant challenges it faces in keeping pace with rapid technological evolution and adapting to modern reality. The research is structured in three chapters. The first chapter contextualizes the digital environment in contemporary times, addressing the information society, the distinction between data, information and knowledge, and the concepts of the internet and the web. It also discusses the role of electronic devices and the importance of privacy and data protection in this scenario. The second chapter explores the general theory of evidence and its application to digital evidence, with an emphasis on the constitutional rights to evidence, the adversarial process, and ample defense. It presents the concepts of evidence, its purposes, classifications, and the means of evidence and obtaining evidence, and introduces the concept of digital evidence, its characteristics, and the main types found in the legal context. Finally, the third chapter focuses on the qualification and handling of digital evidence, discussing the chain of custody, both in general and in digital terms. The stages of the chain of custody are analyzed, from the recognition and isolation of the trace to its disposal, highlighting the importance of preserving the integrity and authenticity of digital evidence. The third chapter also presents technological solutions that can be used to assist in the collection, analysis, and preservation of digital evidence. This research is linked to Sustainable Development Goals (SDGs) 9 and 16. SDG 9 fosters innovation, reflecting the importance of integrating advanced technologies and SDG 16 addresses the importance of access to justice, the effectiveness of legal institutions, ensuring the protection of fundamental rights, and the admissibility of legitimate and authentic evidence. In terms of methodology, this research used the Inductive method in the Investigation Phase, the Cartesian method in the Data Processing Phase, and the inductive logical basis for the Report of the Results.

Keywords: Digital Evidence; Chain of Custody; Blockchain; Data; Web

INTRODUÇÃO

A pós-modernidade trouxe o que vem sendo chamado de revolução digital ou então a quarta revolução industrial[17], um novo normal da sociedade. Essa transformação modificou completamente a forma como o ser humano se relaciona.

A revolução digital é um fenômeno que fragmentou o conhecimento, alterou as formas de produção e distribuição do saber, e promoveu a diversidade e a pluralidade de vozes.[18]

O modelo de vida que se estabeleceu, descortinou tecnologias que proporcionam a automatização de inúmeras tarefas das mais simples às mais complexas. Pode-se dizer que na atualidade tarefas que demandariam mão-de obra e tempo humanos passam a ser efetuadas por meios tecnológicos que chama a atenção, principalmente, no mundo jurídico.

A partir das mudanças ocorridas, é possível perceber que a revolução digital está intimamente representada por velocidade e rapidez e a tecnologia colocada à disposição da humanidade dá a sensação de uma crescente busca por aceleração.

A medida em que as tarefas cotidianas e as interações pessoais foram inseridas no ambiente digital e informático, os conflitos dentro dos ambientes digitais aumentaram na mesma proporção.

A atualidade é marcada por uma sociedade conectada, fazendo com que boa parte das ações do dia a dia estejam documentadas e/ou armazenadas, seja por meio das redes sociais em trocas de mensagens, seja por meio de registros fotográficos e gravações de vídeos e áudios, compartilhamentos

---

[17] SCHAWAB, Klaus. **A quarta revolução industrial.** Tradução Daniel Moreira Miranda - São Paulo: Edipro, 2016. p. 18

[18] LYOTARD, Jean-François. **A condição pós-moderna: um relatório sobre o conhecimento**. Tradução de Ricardo Corrêa Barbosa. 7. ed. Rio de Janeiro: José Olympio, 1998.

com o público do cotidiano nas redes sociais, reuniões por videoconferência, tratativas e negociações por contratos digitais, compras e vendas de mercadorias digitais, dentre outras atividades diárias que estão ou podem estar armazenadas no ambiente digital ou eletrônico.

Toda a mudança que vem sendo ocasionada pelo desenvolvimento tecnológico, modifica também os meios de comprovação de fatos, tornando-se este um grande desafio para os juristas da pós-modernidade, que até então detinham possibilidades determinadas de meios de provas para a resolução dos conflitos.

A presente dissertação tem como intuito analisar as formas de aquisição e de qualificação de provas digitais no processo penal brasileiro. Com efeito, está inserida na linha de pesquisa “Direito, jurisdição e inteligência artificial” e projeto de pesquisa Democracia, processo e jurisdição. **O objetivo geral** da pesquisa é analisar os requisitos necessários para que as provas digitais sejam consideradas válidas nos processos penais, bem como os procedimentos adequados para sua coleta, preservação e apresentação em juízo, a fim de garantir maior segurança jurídica das decisões judiciais, com a devida preservação dos princípios constitucionais, da ampla defesa, do contraditório, do *in dubio pro reu*, da legalidade, presunção da inocência e a inadmissibilidade das provas ilícitas.

O **objetivo institucional** da presente Dissertação é a obtenção do título de Mestra em Ciência Jurídica pelo Curso de Mestrado em Ciência Jurídica da Univali.

Justifica-se a pesquisa, ante a evidente precariedade legislativa e jurídica brasileira na área, que enfrenta desafios significativos em acompanhar a rápida evolução tecnológica e se adequar a realidade moderna.

A evolução do direito é mais lenta que a evolução da sociedade, entretanto, é necessário atentar para questões que se colocam de forma tão definitiva como a produção de provas digitais e seu uso no judiciário, o estudo da presente matéria é imprescindível no cenário global e no ordenamento jurídico brasileiro, orientadas ao estabelecimento do regime jurídico correspondente.

Com efeito, a pesquisa está vinculada os ODS nº 9 e 16º. O 9º, pois fomenta a inovação, refletindo a importância de integrar tecnologias avançadas. Já o 16º, pois aborda a importância do acesso à justiça, eficácia das instituições legais, assegurando a proteção dos direitos fundamentais e a admissibilidade de provas legítimas e autênticas.

Os **objetivos específicos** da pesquisa são:

a) Explorar os fundamentos essenciais do ambiente digital na contemporaneidade, para fornecer uma compreensão abrangente dos principais elementos que o moldam;

b) Investigar a teoria geral da prova a fim de conceituar as provas digitais;

c) Analisar os meios de aquisição e qualificação de provas digitais no processo penal brasileiro que garantam validade jurídica.

O **problema de pesquisa** é analisar a seguinte questão: Quais elementos (ou requisitos) são necessários para que uma prova digital tenha validade jurídica nos processos penais?

Para o problema de pesquisa foi levantada a seguinte **hipótese**: Para que uma prova digital tenha validade, deve estar demonstrada a integridade da cadeia de custódia na aquisição e no tratamento da prova, certificando-se a observância dos requisitos de existência, validade e eficácia da prova.

Principia–se, no Capítulo 1, com a exploração dos fundamentos essenciais do ambiente digital na contemporaneidade, fornecendo uma compreensão abrangente dos principais elementos que moldam a interação humana com a tecnologia e a informação, abordando temas como a sociedade da informação, a distinção de dados, informação e conhecimento e, do mesmo modo, a distinção entre *Internet* e *Web*. Seguindo para o papel dos dispositivos e sistemas eletrônicos, buscando oferecer uma análise das dinâmicas e desafios enfrentados

neste contexto. Pretende-se, por meio dessa pesquisa, clarificar as complexidades do ambiente digital e seu impacto significativo na sociedade contemporânea.

O Capítulo 2 irá explorar a teoria geral da prova, evoluindo para a conceituação da prova digital, suas características e os desafios que ela representa para o sistema legal. Serão abordadas as diferentes formas de provas digitais, desde documentos eletrônicos e mensagens instantâneas até dados de geolocalização, e serão discutidas as implicações legais e éticas de seu uso. Ao compreender a importância e a complexidade das provas digitais, será possível construir uma justiça mais eficaz e justa na era digital.

Por fim, o Capítulo 3 dedica-se a esclarecer inicialmente sobre a cadeia de custódia como instrumento essencial para validade das provas de modo amplo, partindo para as especificidades da cadeia de custódia digital, que ficará evidente sua complexidade ante as provas tradicionais e, portanto, a ineficácia da aplicação isolada da Lei nº 13.694/2019, apelidada como pacote anticrime, que tratou da cadeia de custódia, que deixou de abordar de modo específico e apartado, sobre as provas digitais.

A pesquisa é finalizada com o objetivo principal, que é destrinchar não apenas a norma ABNT NBR ISO/IEC 27037:2013, mas também com o suporte de normas internacionais, para fins de identificar a(s) forma(s) correta(s) de tratamento da prova digital, de modo que preserve sua integridade. Ao final, pretende-se apresentar soluções tecnológicas para o tratamento das provas (evidências) digitais.

O presente Relatório de Pesquisa se encerra com as Considerações Finais, nas quais são apresentados aspectos destacados da Dissertação, seguidos de estimulação à continuidade dos estudos e das reflexões sobre a aquisição e qualificação das provas digitais.

Quanto à Metodologia empregada, registra-se que, na Fase de Investigação[19] foi utilizado o Método Indutivo[20], na Fase de Tratamento de Dados o Método Cartesiano[21], e, o Relatório dos Resultados expresso na presente dissertação é composto na base lógica indutiva.

Nas diversas fases da Pesquisa, foram acionadas as Técnicas do Referente[22], da Categoria[23], do Conceito Operacional[24] e da Pesquisa Bibliográfica[25].

Por fim, reitera-se a mais profunda gratidão à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro concedido por meio da bolsa de estudos. O suporte foi fundamental para a realização deste mestrado acadêmico, possibilitando a dedicação exclusiva à pesquisa e ao desenvolvimento acadêmico, sem os quais este estudo não teria sido possível. A CAPES desempenha um papel crucial no incentivo à pesquisa e à formação de recursos humanos qualificados no Brasil.

---

[19] "(...) momento no qual o Pesquisador busca e recolhe os dados, sob a moldura do Referente estabelecido (...)." PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica:** teoria e prática*.* 14 ed. ver., atual. e ampl. Florianópolis: Empório Modara, 2018. p. 112-113.

[20] "(...) pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral (...)". PASOLD, Cesar Luiz**. Metodologia da pesquisa jurídica:** teoria e prática*.* p. 114.

[21] Sobre as quatro regras do Método Cartesiano (evidência, dividir, ordenar e avaliar) veja LEITE, Eduardo de oliveira*.* **A monografia jurídica***.* 5 ed. São Paulo: Revista dos Tribunais, 2001. p. 22-26.

[22] "(...) explicitação prévia do(s) motivo(s), do(s) objetivo(s) e do produto desejado, delimitando o alcance temático e de abordagem para a atividade intelectual, especialmente para uma pesquisa." PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica:** teoria e prática*.* p. 69.

[23] "(...) palavra ou expressão estratégica à elaboração e/ou à expressão de uma ideia." PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica:** teoria e prática*.* p. 41.

[24] "(...) uma definição para uma palavra ou expressão, com o desejo de que tal definição seja aceita para os efeitos das ideias que expomos (...)". PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica:** teoria e prática*.* p. 58.

[25] "Técnica de investigação em livros, repertórios jurisprudenciais e coletâneas legais". PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica:** teoria e prática*.* p. 217.

Capítulo 1

AMBIENTE DIGITAL NA CONTEMPORANEIDADE

Revoluções denotam mudanças, mas não uma simples mudança, uma transformação total ou quase total de um determinado modelo de sociedade.

Historicamente, a humanidade atravessou algumas revoluções. Inicialmente, a primeira revolução industrial ocorreu entre 1760 e 1840, marcada pela invenção das máquinas a vapor e construção de ferrovias. Já a segunda, ocorreu entre o século XIX e XX, marcada pelo advento da eletricidade e linha de produção em massa. Por fim, a terceira revolução industrial, teve início em 1960, marcada pelo surgimento dos computadores e da internet, conhecida também como a revolução informática e das tecnologias de comunicação[26].

A globalização não tem exatamente um período delimitado na história, no entanto, o seu processo foi intensificado a partir da terceira revolução industrial, que contribui, a partir das novas tecnologias e novo modelo de produção, com o comércio internacional.[27] Apesar da resistência de boa parte do mundo durante este período de transição, não foi possível estagnar ou desacelerar o desenvolvimento tecnológico e a globalização, que se estabeleceu no mundo todo.

Fato é, que até os dias de hoje, a globalização econômica mundial é criticada e debatida por estudiosos do mundo todo. De todo modo, gostem ou não, a virtualidade é uma realidade incontestável.

---

[26] SCHAWAB, Klaus. **A quarta revolução industrial.** Tradução Daniel Moreira Miranda - São Paulo: Edipro, 2016. p. 18.

[27] SCHAWAB, Klaus. **A quarta revolução industrial.** Tradução Daniel Moreira Miranda - São Paulo: Edipro, 2016. p. 18

A ampla e diversificada adoção de tecnologias transformou profundamente as interações humanas, dando origem a um novo espaço: o ambiente virtual ou digital.

O ambiente digital é um espaço complexo, multifacetado e em constante evolução, com novas ferramentas e possibilidades surgindo a todo momento e em velocidades sem precedentes,[28] que possibilita uma ampla gama de atividades, desde o compartilhamento de informações e o comércio eletrônico à expansão das possibilidades de entretenimento e educação. Por meio de redes, plataformas e aplicativos, a humanidade é capaz se comunicar em tempo real, trocar informações, aprender novas habilidades e muito mais.[29]

Este capítulo, então, visa explorar os fundamentos essenciais do ambiente digital na contemporaneidade, para fornecer uma compreensão abrangente dos principais elementos que moldam a interação humana com a tecnologia e a informação.

O capítulo é iniciado pelo subtópico “sociedade da informação”, em que será abordado o contexto histórico da transformação social causada pela revolução tecnológica. No segundo subtópico, será realizada a distinção de dados, informação e conhecimento e, do mesmo modo, a distinção entre *Internet* e *Web*. Por fim, será analisado o papel dos dispositivos e sistemas eletrônicos, para fins de oferecer uma análise das dinâmicas e desafios enfrentados neste contexto. Pretende-se, por meio dessa pesquisa, clarificar as complexidades do ambiente digital e seu impacto significativo na sociedade contemporânea.

1.1 SOCIEDADE DA INFORMAÇÃO

Ao se abordar o ambiente digital na contemporaneidade, é essencial compreender acerca da sociedade da informação, fruto dessa constante evolução tecnológica. De acordo com VAZ[30], o mundo atual é marcado pelo

[28] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 31.

[29] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023 p. 31.

[30] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das

constante uso da tecnologia nos mais diversos âmbitos da atividade humana, na maior parte do mundo. Desde a antiguidade o homem vem constantemente se desenvolvendo e modificando o meio em que habita:

> Ao longo da História, o homem vem constantemente se desenvolvendo, modificando o meio em que habita e alterando as relações sociais. Da sociedade primitiva, ele passou à civilização, aprimorando-se no aproveitamento dos recursos naturais e no domínio das adversidades da natureza. Desde a Antiguidade, o homem desenvolve ferramentas e métodos para auxiliarem a realização de suas tarefas, bem como a comunicação, os cálculos e a sistematização de informações.[31]

Acerca da constante evolução da sociedade, ALVES[32] explica que a formação da sociedade da informação não ocorreu de repente, sendo proveniente de um longo processo evolutivo, iniciado na Revolução Industrial, na Inglaterra de meados do século XVIII, a qual consistiu em um conjunto de mudanças tecnológicas e estruturais com intenso reflexo na cadeia produtiva, seja em nível econômico ou social, alterando quase todos os aspectos da vida cotidiana da época ao espalhar-se pelo mundo a partir do século XX.

Desde os tempos primórdios o homem busca aplicar suas capacidades mentais com o intuito de transformas e adaptar o meio em que vive, adequando-se sempre às suas necessidades. A comunicação é uma dessas necessidades principais.[33]

---

características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 13.

[31] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 17.

[32] ALVES, Matheus de Araújo. **Crimes digitais:** análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova. Dissertação (Mestrado em Direito). 2018. 97 f. Faculdade de Ciências Humanas, Sociais e da Saúde, Universidade FUMEC, Belo Horizonte, 2018. p. 13.

[33] ALVES, Matheus de Araújo. **Crimes digitais:** análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova. Dissertação (Mestrado em Direito). 2018. 97 f. Faculdade de Ciências Humanas, Sociais e da Saúde, Universidade FUMEC, Belo Horizonte, 2018. p. 13.

Segundo VAZ[34], durante o século XX, o desenvolvimento tecnológico alcançou níveis impressionantes, com a criação e interligação dos computadores, diminuindo o tempo e a distância:

> A Segunda Guerra Mundial ensejou grandes avanços na área da ciência, permitindo, nesse contexto, a criação dos computadores, que se deu por volta de 1940. Eles funcionavam, inicialmente, com válvulas a vácuo e atendiam a propósitos militares.

Entre as décadas de 1950 e 1960, a substituição de válvulas por transistores impulsionou ainda mais o desenvolvimento dos computadores, aumentando sua velocidade e viabilizando seu uso comercial. Nas décadas seguintes, a utilização de circuitos integrados e microprocessadores possibilitou a redução do tamanho dos computadores, além de aprimorar sua velocidade e capacidade de armazenamento, o que expandiu ainda mais sua aplicação comercial.[35]

Na década de 1970, os Estados Unidos e o Japão, envolvidos em debates sobre a caracterização da sociedade pós-industrial, introduziram o termo Era/Sociedade da Informação, destacando o papel central da informação na vida econômica, política e social de indivíduos, empresas e nações.[36]

PINHEIRO[37] destaca em sua obra, que durante essa década, Alvin Tofler aponta o surgimento da sociedade da informação, citando que suas origens decorrem da expansão dos veículos de comunicação surgidos na primeira

---

[34] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 17.

[35] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 18.

[36] ALVES, Matheus de Araújo. **Crimes digitais:** análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova. Dissertação (Mestrado em Direito). 2018. 97 f. Faculdade de Ciências Humanas, Sociais e da Saúde, Universidade FUMEC, Belo Horizonte, 2018. p. 14.

[37] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 33.

metade do século XX, agrupados genericamente sob o nome de meios de comunicação de massa.

Baseado nos ensinamentos de Alvin Tofler, PINHEIRO[38] divide a evolução da humanidade em três ondas distintas. A primeira onda, a Era Agrícola, teve início com a transição do nomadismo para o cultivo da terra, estabelecendo a propriedade da terra como base da riqueza e do poder.

A segunda onda, a Era Industrial, emergiu com a Revolução Industrial, redefinindo a riqueza como uma combinação de propriedade, trabalho e capital, e atingiu seu ápice na Segunda Guerra Mundial, quando o modelo de produção em massa revelou seu lado mais sombrio.

A terceira onda, a Era da Informação, começou a se manifestar antes mesmo do apogeu da segunda onda, com a invenção de meios de comunicação como telefone, cinema, rádio e televisão, que disseminaram o elemento central da terceira onda: a informação. No entanto ressalta a autora que a consolidação da Era da Informação só ocorreu com o advento da tecnologia digital e da internet, que introduziram a velocidade e a descentralização da informação.[39]

A partir da década de 1980, a evolução dos computadores foi notável, com aumento significativo de capacidade e diversificação de funções. Essa evolução culminou na difusão do uso pessoal de computadores, consolidando sua presença em todas as esferas da sociedade.[40]

O computador se tornou parte integrante das diversas dimensões da vida humana, abrangendo os âmbitos familiar, profissional, comercial, educacional e de entretenimento. Paralelamente, diversos outros dispositivos eletrônicos foram criados e desenvolvidos, como celulares, palm tops,

---

[38] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 33-34.

[39] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 34.

[40] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 18.

smartphones, dispositivos de memória, tocadores de música e vídeos, minicomputadores, tablets, e-readers, câmeras digitais, gravadores digitais, GPS e jogos eletrônicos.[41]

A utilização desses dispositivos fomentou a criação, armazenamento e sistematização de informações em formato digital. Simultaneamente, o desenvolvimento da telefonia celular e da internet possibilitou a interligação abrangente e difusa dos dispositivos eletrônicos, proporcionando a transmissão de informações com maior rapidez e eficiência.[42]

A convergência desses fatores – a evolução dos computadores, a proliferação de dispositivos eletrônicos e o desenvolvimento da internet – culminou na emergência da sociedade da informação, na qual a produção, disseminação e utilização da informação se tornaram elementos centrais da atividade econômica e social.

Por sociedade da informação, pode-se compreendê-la como aquela que se vale da comunicação fácil, rápida e intensa, com grandes possibilidades de interatividade, constituindo-se de verdadeiras autoestradas da informação ou infovias. Nesse sentido, cumpre destacar as lições de BARRETO JR.[43]:

> A sociedade contemporânea atravessa uma verdadeira revolução digital em que são dissolvidas as fronteiras entre telecomunicações, meios de comunicação de massa e informática. Convencionou-se nomear esse novo ciclo histórico de sociedade da informação, cuja principal marca é o surgimento de complexas redes profissionais e tecnológicas voltadas à produção e ao uso da informação, que

---

[41] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 18.

[42] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 18.

[43] BARRETO JR., Irineu Francisco. **Atualidade do conceito de sociedade da informação para a pesquisa jurídica**. In: **O direito na sociedade da informação**. Coord. Liliana Minardi Paesani. São Paulo: Atlas, 2007, p. 61.

> alcançam ainda sua distribuição através do mercado, bem como as formas de utilização desse bem para gerar conhecimento e riqueza.

VAZ[44] explica que com a evolução tecnológica, houve uma substituição dos meios tradicionais de expressão por novos meios tecnológicos:

> Houve, assim, a substituição, em grande medida, de meios tradicionais de expressão por novos meios tecnológicos. Apenas como ilustração, pode-se citar que: os documentos anteriormente redigidos e arquivados em papel tornaram-se eletrônicos; as músicas foram transferidas do disco de vinil e da fita cassete para o formato digital; as fotografias deixaram de ser registradas em filme para também assumirem o formato digital; do mesmo modo, a captação de imagens em vídeos; e ainda a comunicação por cartas, bilhetes, telegrama, telefone, foi transmudada em mensagens eletrônicas de texto, e-mails, sistemas VoIP, dentre outros.

Tais transformações caracterizam uma revolução tecnológica, a "revolução informacional", comparável, por seus efeitos, à Revolução Industrial. Ela deu ensejo à denominada "sociedade da informação" ou "sociedade pós-industrial", formada na segunda metade do século XX.

Para trazer um significado de sociedade da informação, LISBOA[45] explica em sua obra que a expressão sociedade da informação ou então sociedade do conhecimento é uma forma de identificar o período histórico a partir da preponderância da informação sobre os meios de produção e distribuição dos bens na sociedade quando da vulgarização das programações de dados utilizados (sic) dos meios de comunicação existentes e dos dados obtidos sobre uma pessoa e/ou objeto, para a realização de atos e negócios jurídicos.

A sociedade da informação se define pela valorização e compartilhamento rápido e ilimitado da informação. Suas principais características

---

[44] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 17.

[45] LISBOA, Roberto Senise. **Direito na sociedade da informação**. Revista dos Tribunais, v. 95, n. 847, p. 78-95, mai. 2006. p. 78.

incluem a globalização e a transnacionalidade, as interações sociais, comerciais e políticas mediadas por meios eletrônicos, o valor econômico atribuído à informação e a onipresença do conhecimento em todos os produtos e serviços.

Diante da massiva utilização de dispositivos digitais nas atividades cotidianas, e da consequente importância da informação, os fatos concernentes ao Processo Penal também passaram a ocorrer no mundo virtual ou a serem registrados em formato digital. Dessa forma, cumpre a seguir explorar acerca dos dados e a informação existentes.

1.2 DADOS, INFORMAÇÃO E CONHECIMENTO

O avanço da tecnologia influenciou profundamente no comportamento da sociedade. Nos tempos atuais, é inimaginável conceber um mundo à margem do ambiente digital. A interconectividade, a velocidade na troca de informações e a presença constante da tecnologia tornaram-se elementos indissociáveis da existência humana, de modo que, não apenas permeou, mas também reconfigurou fundamentalmente a maneira como a sociedade vive, trabalha, se relaciona, se comunica e interage.

Verifica-se uma forte relação entre as ferramentas tecnológicas criadas pelo homem, através do aprimoramento de seu conhecimento, e a mudança de seu comportamento. De acordo com LIRA[46], a informação, enquanto instrumento de socialização, cumpre um papel importante na forma de aplicação, de entendimento, disseminação, interpretação e transformação de conhecimento, trazendo à tona a questão da influência da informação na competitividade, seja em nível empresarial ou nação.

É de extrema importância apresentar, ainda que de modo sucinto, os conceitos e distinções dos principais componentes desse meio ambiente digital, iniciando pela tríade: dados, informações e conhecimento, termos que se relacionam entre si, porém possuem conceitos distintos.

---

[46] LIRA, Waleska Silveira; CÂNDIDO, Gesinaldo Ataíde; ARAÚJO, Geraldo Maciel de; BARROS, Marcelo Alves de. **A busca e o uso da informação nas organizações**. Perspectivas em Ciência da Informação, v. 13, n. 1, p. 166-183, jan./abr. 2008. p. 169.

Os dados, são compreendidos como elementos brutos e isolados, ou seja, sem valor e conexão entre si[47]. São fatos soltos, sem contexto ou interpretação. Quando abordado no âmbito jurídico, os dados são evidências que poderão ser utilizados nos processos judiciais, mediante o devido e correto armazenamento e processamento. Em resumo os dados são a matéria-prima do caso a ser investigado e julgado.[48]

Os dados podem ser palavras, números, sons, imagens ou qualquer forma de representação simbólica de fatos. Nas palavras de SETZER[49]:

> Definimos *dado* como uma sequência de símbolos quantificados ou quantificáveis. Portanto, um texto é um dado. De fato, as letras são símbolos quantificados, já que o alfabeto por si só constitui uma base numérica. Também são dados imagens, sons e animação, pois todos podem ser quantificados a ponto de alguém que entra em contato com eles ter eventualmente dificuldade de distinguir a sua reprodução, a partir da representação quantificada, com o original.

SILVA[50] explica que os dados são a matéria prima da informação, ou seja, é a informação não tratada que ainda não apresenta relevância e representam um ou mais significados de um sistema que isoladamente não podem transmitir uma mensagem ou representar algum conhecimento.

---

[47] BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF; nov. 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 09 mar. 2024.

[48] ROSA, Alexandre Morais da. **Lei de acesso à informação pode iluminar as sombras do processo penal**. Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2016-jan-01/limite-penal-lei-acesso-informacao-iluminar-sombras-processo-penal/>. Acesso em: 09 mar. 2024.

[49] SETZER, Valdemar W. **Dado, informação, conhecimento e competência**. Disponível em: <https://www.ime.usp.br/~vwsetzer/datagrama>. Acesso em: 09 mar. 2024.

[50] SILVA, Heide Miranda da. **Qual a diferença entre dados, informação e conhecimento?** Disponível em: <https://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm>. Acesso em: 09 mar. 2024.

No sentido etimológico, SIDOU[51] apresenta a seguinte definição para a palavra “Dados”: “Registros sobre atos efetuados por uma pessoa, natural ou jurídica, ou sobre fatos a ela relacionados, e que servem de eventual informação sobre a conduta dessa pessoa.”

Ainda, de acordo com o dicionário de inglês Oxford[52], a palavra dados (pl.) possui as seguintes definições: “[Incontável, plural] Fatos ou informações, especialmente quando examinados e usados para descobrir coisas ou tomar decisões. [incontável] Informação que é armazenada por um computador.”

Por sua vez, o termo dado no singular (*Datum*) apresenta o significado de: “uma coisa dada ou concedida, algo conhecido ou assumido como fato, e tornado a base de raciocínio ou cálculo; uma suposição ou premissa da qual inferências são tiradas”.[53] (*tradução nossa*)

No contexto digital e informático, os dados (digitais) são coletados, processados, armazenados e transmitidos por meio de sistemas computacionais.

Segundo KENT[54], dados digitais referem-se a informações que são armazenadas, processadas e transmitidas na forma de códigos binários, compostos por 0s e 1s. São representações digitais de diversos tipos de dados, como texto, imagens, vídeos, sons, entre outros. Esses dados digitais são utilizados em diversos contextos, desde arquivos armazenados em computadores até transmissões de dados pela internet.

A respeito do tema, por meio do Decreto nº 11.491/2023[55], o Brasil aprovou a recepção da Convenção sobre o Crime Cibernético do Conselho

---

[51] SIDOU, José Maria Othon. **Dicionário jurídico:** Academia Brasileira de Letras Jurídicas. – 11. ed., rev. e atual. – Rio de Janeiro: Forense, 2016. p. 309.

[52] SIMPSON, J. A.; WEINER, E. S. C. ***The Oxford English Dictionary***. – 2. ed., v. 3 – Oxford/UK, Clarendon Press, 1989. p. 43.

[53] ***Datum:*** *A thing given ou granted; something known or assumed as fact, and made the basis of reasoning or calculation; an assumption or premiss from which inferences are drawn.*

[54] KENT, William. ***Data and reality:*** *a timeless perspective on perceiving and managing information in our imprecise world*. Bedford, MA: IBM Corporation, 1978. p. 7.

[55] BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime

da Europa (Convenção de Budapeste), a qual, em seu art. 1, *b*, define “dado de computador” da seguinte forma:

> **Artigo 1 – Definições**
>
> Para os fins desta Convenção:
>
> […] b. “dado de computador” é qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa;

Percebe-se que um documento eletrônico basicamente é um agrupamento de dados digitais gerados, transmitidos ou conservados por um sistema de computador.

No tocante à informação, ela é classificada como os dados organizados, processados, interpretados e analisados[56]. Percebe-se que a informação não é possível sem o dado, mas o dado sem a devida qualificação, não tem valor interpretativo.

SILVA[57] explica que a informação são os dados tratados, ou seja, são o resultado do processamento de dados, os quais, diferente dos dados, possuem um significado, contribuindo no processo de tomada de decisões.

Acerca do significado da palavra “informação”, LIRA[58] explica que tal palavra deriva do latim *informare*, significando dar forma ou aparência, criar,

---

Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm>.

[56] ROSA, Alexandre Morais da. **A questão digital**: o impacto da inteligência artificial no Direito. Revista de Direito da Faculdade Guanambi, v. 6, n. 2, jul./dez. 2019. Disponível em: <https://www.redalyc.org/journal/6080/608065718005/608065718005.pdf>. Acesso em: 09 mar. 2024.

[57] SILVA, Heide Miranda da. **Qual a diferença entre dados, informação e conhecimento?** Disponível em: <https://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm>. Acesso em: 09 mar. 2024.

[58] LIRA, Waleska Silveira; CÂNDIDO, Gesinaldo Ataíde; ARAÚJO, Geraldo Maciel de; BARROS, Marcelo Alves de. **A busca e o uso da informação nas organizações**. Perspectivas em Ciência da Informação, v. 13, n. 1, p. 166-183, jan./abr. 2008. p. 170.

representar uma ideia ou noção de algo que colocado em forma. A autora ressalta que ele pode ser um dado isolado ou um agrupamento organizado de dados, processado por algum tipo de tratamento coeso.

No contexto digital ou informático, VAZ[59] define os dados informáticos como elementos de informação representados no sistema binário, que em sua forma bruta, não permitem a compreensão de uma situação. Esses elementos básicos (caracteres, símbolos) de informação fornecidos ou produzidos por um computador, quando trabalhados e analisados em conjunto, dão origem à informação, que por sua vez, é capaz de transmitir significado e conhecimento sobre um determinado contexto.

Por sua vez, DONEDA[60] explica que, em relação à dos termos "dado" e "informação", é necessário notar preliminarmente que o conteúdo de ambos se sobrepõe em várias circunstâncias, o que, na ótica do autor, justifica uma certa promiscuidade na sua utilização. Nas palavras do autor:

> […] o "dado" apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de "pré-informação", anterior à interpretação e a um processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição. Mesmo sem aludir ao seu significado, na informação, já se pressupõe a depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza.

A respeito do conhecimento, SILVA[61], esclarece que o conhecimento vai além da informação, pois, enquanto a informação consiste em

---

[59] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 25.

[60] DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. – 2. ed. – São Paulo: Thomson Reuters Brasil, 2020. p. 139.

[61] SILVA, Heide Miranda da. **Qual a diferença entre dados, informação e conhecimento?** Disponível em:

dados organizados e trabalhados, o conhecimento representa um nível superior de entendimento, envolvendo a aplicação e interpretação da informação de forma significativa.

O conhecimento não se limita à posse de dados, mas reside na capacidade de abstrair ideias, compreender contextos e gerar novos saberes. A informação, por sua vez, é um recurso valioso para a construção do conhecimento, mas não é suficiente por si só para expandir o saber humano. É através do conhecimento que o indivíduo, dotado de capacidade cognitiva, identifica o que é relevante e transforma a informação em aprendizado e inovação.[62]

Para LIRA[63], para ser reconhecido o conhecimento como tal, é necessário a aprovação em termos de um critério de verdade socialmente aceito, como a avaliação formal de fatos ou apresentação de dados. Para a autora, o conhecimento é decorrente da interpretação da informação e de sua utilização para gerar novas ideias, resolver problemas ou tomar decisões, e existe quando uma informação é explicada e suficientemente compreendida por alguém, podendo ser ainda o resultado da aprendizagem.

Importante destacar que o conhecimento pode ser dividido em tácito e explícito, onde o conhecimento tácito é pessoal e difícil de normalizar, o que dificulta sua transmissão e compartilhamento, pois está profundamente enraizado nas ações e experiências de um indivíduo, bem como em suas emoções, valores, desejos ou ideais.[64]

<https://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm>. Acesso em: 10 mar. 2024.

[62] SILVA, Heide Miranda da. **Qual a diferença entre dados, informação e conhecimento?** Disponível em: <https://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm>. Acesso em: 10 mar. 2024.

[63] LIRA, Waleska Silveira; CÂNDIDO, Gesinaldo Ataíde; ARAÚJO, Geraldo Maciel de; BARROS, Marcelo Alves de. **A busca e o uso da informação nas organizações**. Perspectivas em Ciência da Informação, v. 13, n. 1, p. 166-183, jan./abr. 2008. p. 172.

[64] LIRA, Waleska Silveira; CÂNDIDO, Gesinaldo Ataíde; ARAÚJO, Geraldo Maciel de; BARROS, Marcelo Alves de. **A busca e o uso da informação nas organizações**. Perspectivas em Ciência da Informação, v. 13, n. 1, p. 166-183, jan./abr. 2008. p. 173.

Já o conhecimento explícito é expresso em palavras e números, facilmente comunicado e compartilhado sob a forma de dados brutos, fórmulas científicas, procedimentos codificados ou princípios universais, podendo ser facilmente processado por um computador, transmitido eletronicamente ou armazenado em banco de dados.[65]

Em suma, compreende-se que o conhecimento transcende a mera informação, pois envolve a aplicação e interpretação dos dados de forma significativa, demandando a capacidade de abstrair ideias e gerar novos saberes. Diante da importância do conhecimento na sociedade da informação, analisar a categoria de dados digitais se torna fundamental para compreender como a gera a informação, que é depois transformada em conhecimento, que será realizado no subtópico a seguir.

1.2.1 Categoria de Dados Digitais

Como explicado, os dados quando organizados geram uma informação, sendo que somente quando um dado é comunicado ele se torna uma informação e posteriormente um conhecimento.

Na sociedade da informação, a evolução tecnológica impulsionou o surgimento dos dados digitais, que são informações de natureza numérica e imaterial, processadas por sistemas computacionais. Esses dados, representados em diversos formatos como texto, imagem, áudio e vídeo, desempenham funções específicas e, quando agrupados, formam documentos eletrônicos, gerados, transmitidos ou armazenados por meio de computadores ou redes de comunicação.[66]

Em seus estudos, GUARDIA[67] categoriza os dados digitais em três modalidades distintas: dados sensíveis, dados pessoais em sentido estrito

---

[65] LIRA, Waleska Silveira; CÂNDIDO, Gesinaldo Ataíde; ARAÚJO, Geraldo Maciel de; BARROS, Marcelo Alves de. **A busca e o uso da informação nas organizações**. Perspectivas em Ciência da Informação, v. 13, n. 1, p. 166-183, jan./abr. 2008. p. 174.

[66] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal.** Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 99.

[67] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da

e dados públicos. Além disso, no contexto das tecnologias da informação, o autor identifica duas categorias adicionais: dados de conteúdo e dados de tráfego. Estes últimos podem ser subdivididos em dados indubitavelmente de tráfego, dados eventualmente de tráfego e dados afins.

Os dados pessoais podem ser compreendidos como toda informação que pode identificar um indivíduo, ainda que indiretamente. Podem ser incluídos na referida definição o número de identificação de funcionário dentro de uma empresa, e até mesmo características físicas.[68]

SOUZA e EDLER[69] definem que os dados pessoais são informações que possam levar à identificação de uma pessoa, de maneira direta ou indireta. Segundo os autores, os dados pessoais diretos não necessitam de nenhum processamento para identificação direta e eficaz do indivíduo, como o nome, o número do RG, ou do CPF.

Já os dados pessoais indiretos dependem da junção de várias informações, para que uma pessoa possa ser identificada, ou seja, a partir de um processamento, como o número da placa de um carro, por exemplo, com a junção dos dados cadastrais presentes no DETRAN, tornam possível a identificação da pessoa física a qual tem a posse do veículo cadastrado sobre o número da placa em questão.[70]

No mesmo sentido, GUARDIA[71] afirma que os dados pessoais correspondem a “a qualquer referência ou descrição objetiva que diga

---

Universidade de São Paulo, São Paulo, 2012. p. 100.

[68] MACIEL, Rafael Fernandes. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. – 1. ed. – Goiânia: RM Digital Education, 2019. p. 112.

[69] SOUZA, Kenny Maiana Silva Novais de; EDLER, Gabriel Octacílio Bohn. **A responsabilidade civil pelo vazamento digital de dados sob a ótica do direito brasileiro**. Revista Ibero Americana de Humanidades, Ciências e Educação. São Paulo, v.8.n.05. maio. 2022. p. 3127.

[70] SOUZA, Kenny Maiana Silva Novais de; EDLER, Gabriel Octacílio Bohn. **A responsabilidade civil pelo vazamento digital de dados sob a ótica do direito brasileiro**. Revista Ibero Americana de Humanidades, Ciências e Educação. São Paulo, v.8.n.05. maio. 2022. p. 3127.

[71] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 100.

respeito a uma pessoa singular e que submetidos a tratamento permitam alcançar informações acerca da sua vida". Ainda afirma o autor:

> Toda informação numérica, alfabética, gráfica, fotográfica ou acústica suscetível de apreciação por uma pessoa, e que seja capaz de identificar outra pessoa se consubstanciará em dado pessoal. A perfeita coincidência entre um dado e uma pessoa não é exigível, mas sim que a identificação possa ser alcançada a partir de esforços razoáveis. Como exemplos pense-se no nome, sobrenome, número de telefone, número do documento de identidade (RG), número do cadastro pessoal de pessoa física (CPF), domicílio, profissão, afiliação a grupos políticos ou associações e etc.[72]

Por sua vez, os dados pessoais relacionados à intimidade em sentido estrito de um indivíduo podem constituir dados sensíveis, pois de acordo com o autor, esses dados estão ligados ao núcleo mais íntimo e secreto da personalidade, como origem racial, opiniões políticas, preferências partidárias, convicções religiosas, saúde e orientação sexual.

Nesse sentido, POHLMANN[73] apresente a seguinte definição para dados pessoais sensíveis:

> Dado pessoal que possa relacionar uma pessoa natural com algum tipo de associação, movimento, sindicato, partido político, ou questões de ordem étnica, religiosas, políticas, filosóficas, vida sexual, etc. Estão incluídos nesta categoria, todos os dados médicos, biométricos e genéticos. Suas digitais são um dado sensível, assim como também são dados sensíveis, a sua preferência por algum time, sua preferência por um candidato em uma eleição (desde que você não o tenha feito público), etc.

Por sua vez, os dados pessoais em sentido estrito são considerados aqueles que se situam na esfera privada, delimitando as relações

---

[72] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 101.

[73] POHLMANN, Sérgio. **LGPD ninja:** entendendo e implementando a lei geral de proteção de dados nas empresas. Rio de Janeiro: Editora Fross, 2019. p. 36.

familiares e pessoais, contudo, diferentemente dos dados sensíveis, não estão ligados ao núcleo mais íntimo da personalidade.[74]

Os dados públicos são a expressão da esfera individual, afetando aspectos como honra e imagem da pessoa, elementos constitutivos da personalidade e vida social do indivíduo.[75]

No tocante aos dados de conteúdo, GUARDIA[76] os classifica como as informações que o emissor intencionalmente deseja transmitir ao receptor em uma comunicação eletrônica. São o objeto principal da comunicação e diferem dos dados de tráfego, que são acessórios e externos à mensagem em si.

Os dados de tráfego são elementos acessórios ou externos das comunicações eletrônicas, que permitem identificar a origem, destino, momento e duração da comunicação, independentemente do conteúdo transmitido. São essenciais para o funcionamento das redes de comunicação e podem incluir informações como número de telefone, endereço de IP, data e hora da comunicação. Tais dados podem ser indubitavelmente de tráfego quando constituem um constituem um artifício técnico essencial para o processo comunicativo, como os caracteres sobre origem, destino, rota, momento, duração, volume e modalidade da comunicação. Esses dados variam de acordo com a modalidade de comunicação eletrônica utilizada (telefonia, e-mail, VoIP, navegação na internet etc.).[77]

---

[74] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 101-102.

[75] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 102.

[76] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 104.

[77] GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal**. Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 105.

Também podem ser eventualmente de tráfego que, diferentemente dos indubitavelmente de tráfego, dependendo da intenção do emissor e do contexto da comunicação.

Dentro dos dados de tráfego pode haver os dados afins, que são uma categoria distinta de dados digitais, pois se trata de informações pessoais coletadas para a contratação de serviços, como dados de inscrição. Tais dados não são transmitidos em tempo real durante a comunicação, mas são necessários para o estabelecimento da prestação do serviço.

A categorização dos dados digitais, abrangendo dados sensíveis, pessoais e públicos, juntamente com a distinção entre dados de conteúdo e de tráfego, oferece um panorama abrangente do cenário digital. Compreender a natureza e as nuances de cada tipo de dado é fundamental para garantir a privacidade, a segurança e o uso ético das informações na era digital.

Cumpre a seguir explicar acerca dos metadados, aprofundando a compreensão sobre a organização e estruturação dos dados na era digital.

1.2.2 Metadados

Além das categorias de dados estudadas, existe ainda os chamados metadados, os quais, segundo lições de SOUZA[78], são dados adicionais sobre determinada operação ou conteúdo digital que podem ajudar no processamento da informação pelos softwares, além de identificar recursos e manter históricos.

Nesse sentido, ARAKAKI[79] desenvolve em sua pesquisa que os metadados são informações estruturadas que facilitam a identificação, descoberta, seleção, uso, acesso e gerenciamento de objetos de informação, tanto físicos quanto digitais. Em outras palavras, os metadados fornecem informações

[78] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 47.

[79] ARAKAKI, Ana Carolina Simionato; ARAKAKI, Felipe Augusto. **Dados e metadados:** conceitos e relações. Ci.Inf., Brasília/DF, n. 3, v. 49, p. 34-45, set./dez. 2020. p. 35-37.

contextuais e descritivas sobre um recurso, como um livro, um artigo, uma imagem ou um arquivo de computador.

POMERANTZ[80] explica que os metadados foram inicialmente identificados pela expressão “dados sobre dados”, cunhada na década de 1960 para se referir a um conjunto e declarações sobre os dados.

Acerca da função dos metadados, BUCKLAND[81] explica que os metadados podem ser usados para fornecer estruturas que suportam a pesquisa e a descoberta consistentes de informações em uma ampla variedade de documentos. Os metadados também podem, potencialmente, permitir distinções entre tipos ou documentos semelhantes.

Cumpre ressaltar que, na maioria das vezes, os metadados não estão aparentes ao usuário, não tendo grande utilidade no uso cotidiano da tecnologia, ainda que sejam efetivamente usados para diversas finalidades pelas aplicações. Para SOUZA[82], cada situação no meio digital pode eventualmente coletar e grava determinados metadados com base no seu objetivo, cabendo uma avaliação de cada caso. Dessa forma, percebe-se que os metadados podem ter variadas utilizações e, consequentemente, variadas definições.

Nesse sentido, ARAKAKI[83] explica haver vários tipos de metadados, podendo classificá-los em metadados: a) administrativos, que auxiliam na gestão e manutenção de coleções e recursos informacionais, fornecendo informações sobre sua origem e histórico de alterações; b) de autenticação, que permitem verificar a identidade, integridade e legitimidade de um recurso informacional; c) de preservação, que contêm informações sobre a preservação e conservação de recursos informacionais; d) de proveniência, que fornecem dados

---

[80] POMERANTZ, J. ***Metadata***. Cambridge: MIT Press, 2015. In: ARAKAKI, Ana Carolina Simionato; ARAKAKI, Felipe Augusto. **Dados e metadados:** conceitos e relações. Ci.Inf., Brasília/DF, n. 3, v. 49, p. 34-45, set./dez. 2020. p. 37.

[81] BUCKLAND, Michael. ***Information and Society***. Cambridge: MIT Press, 2017. p. 118.

[82] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 47.

[83] ARAKAKI, Ana Carolina Simionato; ARAKAKI, Felipe Augusto. **Dados e metadados:** conceitos e relações. Ci.Inf., Brasília/DF, n. 3, v. 49, p. 34-45, set./dez. 2020. p. 38.

sobre a origem, histórico de criação, modificações e relacionamentos de um recurso informacional; e) técnicos, que descrevem o funcionamento de um sistema e fornecem informações sobre o sistema ou recurso em si; f) meta-metadados, que são informações sobre o registro criado ou sobre a criação de um conjunto de dados; g) descritivos, que identificam e contextualizam recursos informacionais para fins de descoberta, identificação, seleção, aquisição e compreensão; h) de direitos, que informam sobre a propriedade intelectual e direitos autorais de um recurso informacional; i) de acesso e uso, que registram como um recurso informacional foi acessado e utilizado, incluindo restrições de acesso e circulação; j) estruturais, que descrevem a composição e organização de um recurso informacional.

Finalmente, no que diz respeito aos metadados na seara jurídica, SOUZA[84] explica que os metadados são importantes na medida em que podem revelar detalhes importantes sobre determinadas provas, permitindo novos argumentos sobre o material apresentando e viabilizando uma perícia mais conclusiva sobre o conteúdo. A título de exemplo, o autor apresenta o cenário de fotos capturadas pelo celular, que registram no arquivo de imagem as coordenadas GPS do momento em que foram captadas pela câmera.

Compreende-se que os metadados, apesar de invisíveis ao usuário comum, desempenham papel importante na organização e processamento de informações digitais, sendo especialmente relevante a seara jurídica. Sua capacidade de revelar detalhes ocultos, como localização e data de criação de arquivos demonstra-se fundamental para a análise de provas, reforçando argumentos e contribuindo para a elucidação de casos.

A análise dos metadados emerge como uma ferramenta poderosa para a compreensão completa de conteúdos digitais, revelando informações que vão além do que é imediatamente perceptível.

---

[84] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 47.

Isto posto, acerca dos dados, informação e conhecimento, torna-se importante explicar a seguir sobre a internet e web, elementos primordiais no desenvolvimento da sociedade da informação.

1.3 INTERNET E WEB

O mundo atual está cada vez mais conectado, onde a tecnologia se tornou parte essencial do dia a dia das pessoas. A internet revolucionou a forma como as pessoas se comunicam, trabalham, estudam e se divertem.

Ela está presente em praticamente todas as áreas da vida, desde o comércio e a educação até a saúde e o entretenimento. E, claro, o Direito, como regulador da sociedade, também não ficou indiferente a essa revolução digital.

Assim, para compreender o impacto da internet, é fundamental compreender de forma subdivida sua histórica, seu conceito e os demais aspectos, permitindo que se entenda como a internet se tornou o que é hoje e quais são os desafios que ela apresenta.

1.3.1 História da Internet

O que se conhece hoje como internet, assim como foi com o computador, surgiu inicialmente para fins militares. Sua origem vem dos Estados Unidos, no final da década de 1960, durante o período da Guerra Fria, com o nome de ARPANET. De acordo com ALVES[85], ela foi idealizada pela ARPA (*Advanced Research Projects Agency*), ligada ao Departamento de Defesa norte-americano.

PINHEIRO[86], descreve que a ARPANET foi criada com propósitos inicialmente militares, sendo um sistema que interligava as redes de computadores militares de forma descentralizada. A abordagem era tão inovadora

[85] ALVES, Matheus de Araújo. **Crimes digitais:** análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova. Dissertação (Mestrado em Direito). 2018. 97 f. Faculdade de Ciências Humanas, Sociais e da Saúde, Universidade FUMEC, Belo Horizonte, 2018. p. 14.

[86] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 40.

que garantia que, mesmo em caso de ataque a uma base militar, as informações não se perderiam, pois não havia uma central de dados única.

Acerca do contexto histórico, PAESANI[87] explica de forma mais aprofundada sobre o ARPANET:

> O projeto Arpanet da agência de projetos avançados (Arpa) do Departamento de Defesa norte-americano confiou, em 1969, a Rand Corporation a elaboração de um sistema de telecomunicações que garantisse que um ataque nuclear russo não interrompesse a corrente de comando dos Estados Unidos. A solução aventada foi a criação de pequenas redes locais CLAN), posiciona- das nos lugares estratégicos do país e coligadas por meio de redes de telecomunicação geográfica (WAN). Na eventualidade de urna cidade vira ser destruída por um ataque nuclear, essa rede de redes conexas - Internet, isto é, Inter Networking, literalmente, coligação entre redes locais distantes, garantiria a comunicação entre as remanescentes cidades coligadas.

Por sua vez, GUGLIARA[88] explica que a ARPANET, precursora da internet, foi concebida como uma estratégia militar americana. A rede era composta por computadores interligados, cada um funcionando como um "nó". Essa estrutura descentralizada garantia que, mesmo se um dos nós fosse destruído em um ataque, os demais permaneceriam operantes, assegurando a comunicação entre bases militares e o departamento de pesquisas do governo. Essa tática minimizava os riscos e mantinha a rede funcional em situações adversas.

SYDOW[89] explica em sua obra a ideia de difundir a informação em diversos centros estratégicos:

---

[87] PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. – 7. ed. – São Paulo: Atlas, 2014. p. 10.

[88] GUGLIARA, Rodrigo; FISCHER, Bianca Camargo. **Conceitos essenciais sobre a sociedade em rede.** Fundamentos do Direito Digital, Coordenadores: João Victor Rozatti Longhi; José Luiz de Moura Faleiros Júnior; Gabriel Oliveira de Aguiar Borges; Guilherme Reis. Uberlândia: LAECC, 2020. p. 138.

[89] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015. p. 31.

> Assim, a ideia foi a de difundir a informação sem que houvesse somente um centro estratégico frágil, que, atacado, levaria a um caos desenvolvimentista, permitindo-se que a informação trafegasse mesmo que tivesse havido a perda de um ou alguns núcleos tecnológicos. Pode-se dizer, portanto, que a importância inicial da rede informática foi estratégica.

Com o tempo, a ARPANET cresceu exponencialmente, sendo necessário substituir o protocolo de comutação de pacotes (unidade de transferência de informação), chamado *Network Control Protocol* (NCP) para os protocolos TCP/IP, que são, atualmente, as bases técnicas atuais de comunicação via Internet.[90]

Esse sistema passou a ser usado para fins civis, inicialmente em algumas universidades americanas, sendo utilizado pelos professores e alunos como um canal de divulgação, troca e propagação de conhecimento acadêmico-científico. Esse ambiente menos controlado possibilitou o desenvolvimento da internet nos moldes os quais a conhecemos atualmente.[91]

Esse primeiro acesso dos civis ao que seria conhecido futuramente como Internet ocorreu de forma gradual, sendo que os primeiros acessos civis ocorreram em universidades, conforme as lições de BRITO[92]:

> Durante toda a década de 1970, a ARPANET foi sendo aperfeiçoada com a ajuda de cientistas e disponibilizada inicialmente para as universidades, até que, em 1983, preocupados com possíveis falhas de segurança, o Departamento de Defesa opta por dividir os objetivos da rede e cria a MILNET, que possuía a mesma função, mas seu uso era reservado ao serviço militar, enquanto a primeira permanecia para uso acadêmico, transformando-se em ARPA-INTERNET.

---

[90] GUGLIARA, Rodrigo; FISCHER, Bianca Camargo. **Conceitos essenciais sobre a sociedade em rede.** Fundamentos do Direito Digital, Coordenadores: João Victor Rozatti Longhi; José Luiz de Moura Faleiros Júnior; Gabriel Oliveira de Aguiar Borges; Guilherme Reis. Uberlândia: LAECC, 2020. p. 138.

[91] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 40.

[92] BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013. p. 15.

O grande marco dessa tecnologia ocorreu em 1987, quando foi convencionada a possibilidade de seu uso para fins comerciais, passando-se a denominar “Internet”. Com o acesso público, durante a década de 1990, a Internet passou por um processo de expansão de expansão sem precedentes e seu rápido crescimento se deve a vários de seus recursos e facilidades de acesso e transmissão, tais como o correio eletrônico (e-mail) até o acesso a banco de dados e informação disponíveis na World Wide Web (WWW).[93]

Segundo as lições de SYDOW[94], em 1989, Tim Berners-Lee, um cientista inglês que trabalhava na *European Organization for Nuclear Research* na Suíça, criou um sistema inovador de documentos interligados. Essa tecnologia, lançada em 1992, permitia que os usuários navegassem por um ambiente virtual rico em texto, imagens, sons e mídias, através de links que os levavam a diferentes plataformas.

Conhecida como *World Wide Web* (ou simplesmente Web), essa invenção conquistou o mundo pela sua versatilidade e facilidade de uso, sendo popularmente reconhecida pelas letras "www".[95]

Vale destacar que no contexto histórico da Internet no Brasil, BRITO[96] explica que por volta de 1988 o país cedeu espaço para a nova tecnologia em centros universitários, iniciando pelo Laboratório Nacional de Computação Científica do Rio de Janeiro, que estabeleceu conexão com a Universidade de Maryland. Em seguida, foi a vez da Fapesp – Fundação de Amparo à Pesquisa de São Paulo, que se comunicou com um Laboratório de Chicago.

1.3.2 Conceito

Inicialmente, ao se conceituar a internet, por vezes encontram o uso da expressão Web como sinônimo, contudo, elas são coisas distintas. De

---

[93] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 40.

[94] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015. p. 32.

[95] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015. p. 33.

[96] BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013. p. 15.

forma resumida, utilizando das lições trazidas por SOUZA, MUNHOZ e CARVALHO[97], a Internet se refere à estrutura que conecta computadores e dispositivos em todo o mundo. Já a Web é a rede (o sistema) em si pela qual é feita a navegação por hiperlinks, acessíveis através da internet.

Em suma, a internet é a rede global de computadores, enquanto a web é um dos serviços que funcionam sobre essa rede, permitindo o acesso a informações e conteúdo.

No tocante ao seu conceito, a Lei nº 12.965/2014[98], também conhecida como o Marco Civil da Internet, apresenta em seu art. 5º, inciso I, a definição de internet:

> **Art. 5º** Para os efeitos desta Lei, considera-se:
>
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes; […].

Nas palavras de SOUZA, MUNHOZ e CARVALHO[99], a internet consiste em uma grande rede de dados digitais comporta de diversas outras redes que se interconectam e permitem a troca de dados entre cada um dos seus pontos de conexão.

Nesse sentido, TEIXEIRA[100] ensina que a internet é a "interligação de redes de computadores espalhadas pelo mundo, que passam a

---

[97] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 7.

[98] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF; abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 12 mar. 2024.

[99] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 36.

[100] TEIXEIRA, Tarcísio. **Direito digital e processo eletrônico**. – 6. Ed. – São Paulo: SaraivaJur, 2022. p. 42.

funcionar como uma só rede, possibilitando a transmissão de dados, sons e imagens de forma rápida".

PAESANI[101] explica em sua obra que a internet é o meio de comunicação que conecta milhões de pessoas ao redor do mundo:

> Hoje, a Internet é vista como um meio de comunicação que interliga dezenas de milhões de computadores no mundo inteiro e permite o acesso a urna quantidade de informações praticamente inesgotáveis, anulando toda distância de lugar e tempo.

Contudo, a autora ressalta que a definição de internet não possui uma resposta clara, nem completa:

> O que é a Internet? A resposta não é clara nem completa. Sob o ponto de vista técnico, a Internet é urna imensa rede que liga elevado número de computadores em todo o planeta. As ligações surgem de várias maneiras: redes telefônicas, cabos e satélites. Sua difusão é levemente semelhante à da rede telefônica. Existe, entretanto, urna radical diferença entre urna rede de computadores e urna rede telefónica: cada computador pode conter e fornecer, a pedido do usuário, urna infinidade de informações que dificilmente seriam obtidas por meio de telefonemas.[102]

Cumpre destacar que a internet, em seus primeiros anos, tinha seu acesso feito por computadores, que, por sua vez, utilizavam de modens. Atualmente, o acesso à internet é realizado pelos mais variados dispositivos tecnológicos, sobretudo por smartphones ligando-se à rede mundial de computadores via dados móveis ou Wi-Fi (*wireless fidelity*, ou "fidelidade sem fio").[103]

---

[101] PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. – 7. ed. – São Paulo: Atlas, 2014. p. 10-11.

[102] PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. – 7. ed. – São Paulo: Atlas, 2014. p. 13.

[103] TEIXEIRA, Tarcísio. **Direito digital e processo eletrônico**. – 6. Ed. – São Paulo: SaraivaJur, 2022. p. 42.

No tocante à identificação na internet, SOUZA, MUNHOZ e CARVALHO[104] ensina em sua obra que os pontos de conexão realizados para acesso à internet recebem uma identificação única, através de seu endereço IP, permitindo que a rede identifique a origem das requisições de dados e saiba para onde enviar as respostas. Só há troca de dados entre dois pontos da rede se ambos conseguirem se identificar de maneira objetiva (função desempenhada pelo sistema de endereços IP).

O endereço IP se trata de uma sequência de números ou caracteres únicos para determinada conexão, que permite a troca de dados em uma rede multiconectada com diversas outras.[105]

A partir da estrutura apresentada, existe a atuação conjunta de diversos elementos que ajudam a constituir o ambiente digital: os servidores e provedores. Para tanto, cumpre a seguir explicar acerca de referidos elementos.

1.3.3 Servidores e Provedores

Embora o processo de acesso à internet feito pelo usuário comum pareça simples, na verdade é complexo, pois funciona a partir dos códigos de endereço IP. Contudo, tal processo ainda é intermediado por outros elementos, conhecidos como Servidores (DNS, de dados e backbone) e Provedores de conexão.

Iniciando pelos Servidores DNS, SOUZA, MUNHOZ e CARVALHO[106] destacam em sua obra que a estrutura lógica da Internet funciona a partir dos códigos de endereço IP, que não são exatamente fáceis de lidar para usuários comuns. Diante desse cenário, criou-se uma identificação com nomes amigáveis, chamados de domínios, para facilitar a busca de determinados sites ou serviços on-line.

---

[104] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 36.

[105] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 37.

[106] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 38.

Esse serviço é prestado pelos conhecidos Servidores DNS, os quais permitem o uso de um nome amigável, como “www.google.com.br”, para identificar o endereço IP de um determinado servidor na internet, facilitando seu acesso.[107]

Nas palavras de VAZ[108], os Servidores DNS é “responsável pela conversão de endereços de sites em endereços IP, e vice-versa”.

Ainda, acerca do Servidor DNS e como é feito essa conexão, PINHEIRO[109] traz a seguinte lição:

> A tradução dos endereços IP, numéricos, para os seus correspondentes em palavras faz-se pelo protocolo DNS — Domain Name System. As terminações do endereço são feitas de acordo com os TLDs — Top Level Domains —, o primeiro grupo de caracteres após o último ponto de nome de domínio propriamente dito.

TAVARES[110] esclarece que a sigla DNS significa Sistema de Nomes de Domínio (*Domain Name System*), fazendo associação entre o domínio e o respectivo endereço IP a ele atribuído, permitindo a conexão. Em suma, cada equipamento hospeda um determinado website possui o seu endereço IP, que é alcançado pelo protocolo de conexão por meio dos Servidores DNS.

Por fim, SOUZA, MUNHOZ e CARVALHO[111] ressaltam que existe um controle sobre quem pode emitir esses domínios, o qual é dividido entre diversas organizações no mundo. Países gerenciam pós-fixos exclusivos como “.br” para o Brasil, “.ar” para argentina, “.uk” para Reino Unido, além de outros

---

[107] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 38.

[108] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 24.

[109] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 41.

[110] TAVARES, João Paulo Lodelo Guimarães. **O regime jurídico das provas digitais no direito brasileiro**. Civil Procedure Review, v. 12, n. 3, set./dez. 2020. p. 103.

[111] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 38.

criados por entidades privadas que criam seus próprios pós-fixos como “.info”, “.io” e “.app”. Cada entidade é autorizada a emitir nomes com os pós-fixos que gerencia.

Os Servidores de Dados são os computadores especializados para a função de processamento de dados de serviços digitais disponíveis através da internet. Geralmente eles são instalados em *datacenters*, que consistem em instalações preparadas para garantir sua continuidade utilizando-se de recursos de segurança, refrigeração, fontes alternativas de energia, múltiplas conexões de internet e outras medidas.[112]

SOUZA, MUNHOZ e CARVALHO[113] explicam que todos os dados da internet estão eventualmente guardados em um desses servidores. Quando se acessa um website na internet, na verdade está fazendo uma requisição a um servidor de dados, que lhe responde prontamente com as informações solicitadas, sejam páginas, imagens, vídeos e outros.

Vale destacar que há diversas finalidades para esses servidores, sendo a mais conhecida, a de manter os dados de websites, mas também existem servidores especializados na troca de mensagens de e-mail, servidores de suporte para aplicativos de celular, armazenamento de arquivos e muitos outros.

Geralmente esses servidores possuem um endereço IP fixo para facilitar o acesso de seus usuários e permitir a configuração de um domínio em servidores DNS. Salvo se o responsável pelo servidor alterar a configuração do endereço IP do servidor, a tendência é que ele se mantenha sempre o mesmo.[114]

Por sua vez, os Servidores Backbone são considerados os responsáveis por integrar diversas sub-redes da internet, oriundas de provedores de conexão, grandes datacenters e outros, interligando outros *backbones* ou

---

[112] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 39.

[113] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 39.

[114] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 39.

realizando o caminho de transferência de dados para outros países ou continentes. Eles são essenciais para a existência da internet e a maioria dos acessos de um usuário eventualmente passa por um desses servidores até chegar a seu destino.[115]

Os provedores de conexão são responsáveis por conectar residências e empresas à rede mundial, utilizando diferentes tecnologias como cabos, fibra óptica e rádio. Ao contratar um provedor, o usuário recebe um endereço IP, que funciona como um "número de identificação" na internet. No entanto, para facilitar o gerenciamento de muitos clientes, é comum que os provedores utilizem endereços IP dinâmicos, que mudam a cada nova conexão. Apesar dessa mudança constante, os provedores mantêm registros detalhados de qual cliente utilizou cada endereço IP em determinado momento, permitindo identificar o acesso, se necessário.[116]

Importante destacar que a Lei nº 12.965/2014[117] determina em seu art. 15 que todos os provedores de aplicações de internet constituído no Brasil devem manter os históricos de acessos de seus clientes pelo prazo de 6 (seis) meses.

Compreende-se que o acesso à internet, apesar de sua aparente simplicidade, é um processo intrincado que envolve uma rede complexa de servidores e provedores. A compreensão dessa estrutura subjacente é importante para entender o funcionamento da internet e seus diversos componentes.

---

[115] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 40.

[116] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 41.

[117] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF; abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 12 mar. 2024.

Cumpre a seguir explicar brevemente sobre os aparelhos eletrônicos que realizam a conexão com a internet e, consequentemente, transmitem dados digitais.

1.3.4 Dispositivos Móveis

No contexto da sociedade da informação, caracterizada pela transformação de aspectos da vida social e da personalidade humana em dados, a internet consolidou-se como um elemento central na comunicação. O acesso à rede mundial de computadores, inicialmente restrito aos computadores pessoais, expandiu-se significativamente com o advento dos dispositivos móveis, que proporcionam conexão imediata e ubíqua à internet.[118]

Os dispositivos móveis transcenderam sua função original de simples aparelhos de comunicação por voz, evoluindo para se tornarem ferramentas multifuncionais. Atualmente, os celulares agregam uma vasta gama de recursos e serviços, atendendo às diversas necessidades dos usuários em um único dispositivo.[119]

Convencionou-se adotar uma nova concepção para estes modernos aparelhos celulares, denominando-os de “smartphones”, os quais são caracterizados por THEOHARIDOU[120] como:

> […] um telefone celular com capacidades avançadas, que executa um sistema operacional identificável, permitindo aos usuários ampliar sua funcionalidade com aplicativos de terceiros que estão disponíveis em um repositório de aplicativos. De acordo com esta definição, os smartphones devem incluir hardware sofisticado com: a) capacidades de processamento avançadas (por exemplo, CPUs

[118] REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais:** o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado em Direito). 2020. 305 f. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020. p. 39.

[119] COUTINHO, Gustavo Leuzinger. **A Era dos ‘smartphones’:** um estudo exploratório sobre o uso dos ‘smartphones’ no Brasil. In: REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais:** o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado em Direito). 2020. 305 f. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020. p. 39.

[120] THEOHARIDOU, Marianthi; MYLONAS, Alexios; GRITZALIS, Dimitris. ***A risk assessment method for smartphones****. 27th Information Security and Privacy Conference* (*SEC*), jun. 2012, Heraklion, Crete, Greece. p. 444-445.

> modernas, sensores), b) capacidades de conectividade múltiplas e rápidas (por exemplo, Wi-Fi, HSDPA) e (opcionalmente) c) tela adequadamente limitada tamanhos. Além disso, o seu sistema operacional deve ser claramente identificável, por ex. Android, Blackberry, Windows Phone, iOS da Apple, etc. Finalmente, o sistema operacional deve permitir a instalação de aplicativos de terceiros a partir de repositórios de aplicativos ("mercados de aplicativos"), por exemplo. Android Market, BlackBerry App World, App Hub, App Store, etc.[121] (*Tradução nossa*)

Não bastasse, os smartphones ganharam ampla capacidade de memória, o que permitiu o armazenamento massivo de dados relacionados à personalidade dos seus titulares e de terceiros que com ele tenham interagido.[122]

Devido à sua natureza multifuncional, que combina comunicação e informática, o smartphone tem sido utilizado para a prática de delitos, tornando-se, consequentemente, uma importante fonte de provas. Contudo, a grande quantidade de dados pessoais armazenados nesses dispositivos exige que o acesso ao seu conteúdo seja realizado de forma criteriosa e proporcional, a fim de evitar violações à privacidade constitucionalmente garantida.[123]

Percebe-se que a evolução dos smartphones, de simples dispositivos de comunicação para ferramentas multifuncionais com grande

---

[121] **Texto Original:** smartphone is a cell phone with advanced capabilities, which executes an identifiable operating system allowing users to extend its functionality with third party applications that are available from an application repository. According to this definition, smartphones must include sophisticated hardware with: a) advanced processing capabilities (e.g. modern CPUs, sensors), b) multiple and fast connectivity capabilities (e.g. Wi-Fi, HSDPA), and (optionally) c) adequately limited screen sizes. Furthermore, their OS must be clearly identifiable, e.g. Android, Blackberry, Windows Pho ne, Apple's iOS, etc. Finally, the OS must allow third party application installation from application repositories ('app markets'), e.g. Android Market, BlackBerry App World, App Hub, App Store, etc.

[122] REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais:** o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado em Direito). 2020. 305 f. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020. p. 40.

[123] REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais:** o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado em Direito). 2020. 305 f. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020. p. 41.

capacidade de armazenamento, transformou-os em objetos centrais na sociedade da informação e em potenciais fontes de prova no âmbito jurídico.

A riqueza de dados pessoais contidos nesses aparelhos exige um delicado equilíbrio entre o acesso à informação e a proteção da privacidade e dos dados, o que demanda uma análise criteriosa e proporcional em cada caso, a fim de garantir o respeito aos direitos fundamentais dos indivíduos e a efetividade da investigação criminal.

Em razão dos dados existentes nesses dispositivos móveis, a seara jurídica possui uma nova fonte de prova, conhecida como prova digital. Contudo, deve haver cautela no acesso a referidos dados, ante a garantia do direito à privacidade e à proteção de dados, tema abordado na sequência.

1.4 A PRIVACIDADE E PROTEÇÃO DE DADOS

Inicialmente, para compreender o direito à privacidade e à proteção de dados, é necessário analisar brevemente o contexto histórico que moldou o desenvolvimento dessas garantias legais.

O ideal inicial de um direito à privacidade surgiu formalmente em 1890, com a publicação de um artigo de autoria de Samuel D. Warren e Louis D. Brandeis, intitulada “The Right to Privacy”. De acordo com MACIEL[124], referido artigo foi o precursor do direito à privacidade durante o século XIX:

> […] é considerado por muitos como o que mais influenciou o direito à privacidade. O interesse em divulgar fatos da vida privada de forma sensacionalista e fofocas cada vez mais sendo estampadas nos jornais (Yellow Jornalism) – que ganhavam ainda mais circulação (1000% entre 1850 e 1890) -, somados ao avanço tecnológico com o uso de câmeras fotográficas portáteis, motivou os advogados a levantar a necessidade de se pensar em um direito à privacidade mais amplo e não apenas sobre meios físicos, como o sigilo da carta ou a violação de domicílio. […] Era preciso, segundo os autores, que a lei assegurasse aos indivíduos em qual

[124] MACIEL, Rafael Fernandes. **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. – 1. ed. – Goiânia: RM Digital Education, 2019. p. 59.

> extensão desejassem comunicar seus pensamentos, sentimentos e emoções para outros.

Segundo o autor, esses direitos à época não eram baseados em propriedade, mas em um direito geral de o indivíduo ser deixado só, e sua violação configuraria um delito ao direito da personalidade, sujeito a medidas judiciais apropriadas.

Com o fim da Segunda Guerra Mundial, a Assembleia Geral da ONU apresenta no ano de 1948, a Declaração Universal dos Direitos Humanos[125], o qual alçou o direito de inviolabilidade à vida privada a um direito fundamental do homem, conforme disposto no art. 12 da Declaração:

> **Artigo 12.** Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Com a promulgação da Constituição da República Federativa do Brasil em 1988[126], foi garantido no ordenamento jurídico brasileiro o direito constitucional à privacidade, resguardando a vida privada e a intimidade, assegurando sua inviolabilidade, acompanhando a orientação internacional, conforme disposto no art. 5º, inciso X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

TEIXEIRA[127] conceitua a privacidade como o conjunto de informações pessoais que um indivíduo tem o direito de controlar, decidindo se as mantém restritas a si próprio ou se as compartilha com outros, e em quais condições. A privacidade, portanto, está relaciona ao que é privado, de

---

[125] ASSEMBLEIA GERAL DA ONU. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 12 mar. 2024.

[126] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Promulgada em 5 de out. de 1988. Brasília, DF; out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm>. Acesso em: 12 mar. 2024.

[127] TEIXEIRA, Tarcísio. **Direito digital e processo eletrônico**. – 6. Ed. – São Paulo: SaraivaJur, 2022. p. 72.

conhecimento limitado, em oposição ao que é público, de conhecimento geral, necessitando de atenção e proteção legal mais rigorosa.

Com base nos estudos realizados até o momento, percebe-se que entre a assinatura da Declaração Universal dos Direitos Humanos e a promulgação da CRFB/1988, a sociedade vivenciou uma revolução tecnológica com a computação e o surgimento da internet, que impulsionaram a globalização e o surgimento da sociedade da informação. Contudo, o mundo globalizado e as mudanças tecnológicas trouxeram novos desafios que antes passavam despercebidos.

Com o aumento da conectividade e da inclusão digital, o uso de tecnologias tornou-se onipresente. Todavia, a utilização segura e responsável dessas ferramentas requer cuidados que a população, em geral, negligência, seja por desconhecimento ou falta de preparo.[128]

De acordo com CALAZA[129], a privacidade tem se tornado um tema cada vez mais relevante na sociedade atual. O avanço tecnológico e a crescente utilização de ferramentas digitais têm levado à flexibilização do direito à privacidade. Em muitos casos, os indivíduos fornecem seus dados pessoais em troca de benefícios superficiais, como em jogos eletrônicos ou acesso a conteúdo online, sem considerar as implicações dessa troca.

A proteção de dados pessoais também exige atenção redobrada, pois, em uma sociedade impulsionada pela tecnologia, a coleta e o uso de dados são práticas comuns. Dessa forma, é crucial repensar as formas de garantir o direito constitucional à privacidade.[130]

---

[128] SANTANA, Priscila. **Do uso, tratamento e disponibilização de dados pessoais para fins processuais:** uma análise frente à Lei Geral de proteção de Dados. Estudos essenciais de Direito Digital, Coordenadores: João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior. Uberlândia: LAECC, 2019. p. 265-266.

[129] CALAZA, Tales. **O direito à privacidade: origem histórica e jurídica**. Fundamentos do Direito Digital, Coordenadores: João Victor Rozatti Longhi; José Luiz de Moura Faleiros Júnior; Gabriel Oliveira de Aguiar Borges; Guilherme Reis. Uberlândia: LAECC, 2020. p. 169.

[130] SANTANA, Priscila. **Do uso, tratamento e disponibilização de dados pessoais para fins processuais:** uma análise frente à Lei Geral de proteção de Dados. Estudos essenciais de Direito Digital, Coordenadores: João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior.

Embora intrinsecamente ligados, a privacidade e a proteção de dados pessoais são conceitos distintos. O direito à privacidade, em sua concepção tradicional, tem sido redefinido diante do avanço tecnológico e seus impactos na esfera privada.[131]

A revolução digital e a crescente necessidade de processamento massivo de dados para a sociedade hiper conectada e o desenvolvimento de tecnologias como inteligência artificial e aprendizado de máquina demandam uma nova perspectiva sobre o direito à privacidade. [132]

PAESANI[133] explica sua obra que o direito à privacidade vem assumindo relevância em razão das novas técnicas de comunicação:

> O direito à privacidade tem como fundamento a defesa da personalidade humana contra injunções ou intromissões alheias. Esse direito vem assumindo, aos poucos, maior relevo, com a expansão das novas técnicas de comunicação, que colocam o homem numa exposição permanente. Tem-se demonstrado particularmente delicada a operação para delimitar a esfera da privacidade, mas é evidente que o direito à privacidade constitui um limite natural ao direito a informação. Em contrapartida, está privada de tutela a divulgação da notícia, quando consentida pela pessoa. Admite-se, porém, o consentimento implícito, quando a pessoa demonstra interesse em divulgar aspectos da própria vida privada.

Percebe-se que a autora destaca em sua obra o papel crucial do direito à privacidade na proteção da personalidade humana, especialmente no contexto das novas tecnologias de comunicação. Também ressalta a complexidade

---

Uberlândia: LAECC, 2019. p. 265-266.

131 CARNEIRO, Aline Ferreira Costa; BRITO, Lucimeire Zago de; TAVARES, Viviane Ramone. **Compliance digital:** novas perspectivas sobre ética na sociedade da informação. Estudos essenciais de Direito Digital, Coordenadores: João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior. Uberlândia: LAECC, 2019. p. 215.

132 CARNEIRO, Aline Ferreira Costa; BRITO, Lucimeire Zago de; TAVARES, Viviane Ramone. **Compliance digital:** novas perspectivas sobre ética na sociedade da informação. Estudos essenciais de Direito Digital, Coordenadores: João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior. Uberlândia: LAECC, 2019. p. 215.

133 PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. – 7. ed. – São Paulo: Atlas, 2014. p. 34.

em definir os limites precisos da privacidade, mas enfatiza que este direito fundamental impõe limites ao direito à informação e equilibra a necessidade de proteção individual com o interesse público.

CALAZA[134] enfatiza que, ao passo em que a legislação relativa ao direito à privacidade evolui gradualmente, as tecnologias que permitem a invasão e a violação da intimidade evoluem de maneira exponencial, de modo que a tutela deste direito não deve apenas ser realizada em conformidade com a lei vigente, mas também com os princípios, os costumes e a analogia, devendo ser exploradas as demais fontes do direito, a fim de garantir a proteção mais completa possível a este direito constitucional.

A privacidade, compreendida como o direito de controlar a exposição da esfera íntima e dos dados pessoais, é um componente fundamental da liberdade individual. A Constituição garante ao cidadão a prerrogativa de preservar ou não sua intimidade e seus dados, cabendo ao Estado a proteção desse direito.[135]

No contexto da internet, a interceptação de comunicações e o acesso a dados por agentes públicos ou privados se tornam questões delicadas.

A crescente violência tem levado o Estado a utilizar tecnologias sofisticadas para obter informações e dados privados de acusados. Neste sentido, a doutrina tem admitido a interceptação e o acesso a dados em casos específicos, desde que haja provas contundentes, autorização judicial e observância aos princípios da proteção de dados, a fim de garantir o bem comum em detrimento de direitos individuais.[136]

---

[134] CALAZA, Tales. **O direito à privacidade: origem histórica e jurídica**. Fundamentos do Direito Digital, Coordenadores: João Victor Rozatti Longhi; José Luiz de Moura Faleiros Júnior; Gabriel Oliveira de Aguiar Borges; Guilherme Reis. Uberlândia: LAECC, 2020. p. 179.

[135] PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. – 7. ed. – São Paulo: Atlas, 2014. p. 40.

[136] PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. – 7. ed. – São Paulo: Atlas, 2014. p. 40.

É crucial ter cautela com o uso dessas tecnologias, pois o poder de vigilância estatal pode ter consequências imprevisíveis para a privacidade e a proteção de dados. A utilização de tais ferramentas devem ser restritas a situações excepcionais, com a devida autorização judicial e observância aos princípios da proteção de dados e responsabilidade por eventuais abusos.[137]

É preciso compreender que o direito à privacidade e à proteção de dados possuem no ordenamento jurídico brasileiro normas legais plicáveis ao tratamento indevido de dados, como como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).[138]

Uma vez abordados os principais aspectos do ambiente digital na contemporaneidade, abordar-se-á no capítulo seguinte acerca da Teoria Geral da Prova e as Provas Digitais, temas extrema relevância para a pesquisa.

[137] PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. – 7. ed. – São Paulo: Atlas, 2014. p. 40.

[138] CALAZA, Tales. **O direito à privacidade: origem histórica e jurídica**. Fundamentos do Direito Digital, Coordenadores: João Victor Rozatti Longhi; José Luiz de Moura Faleiros Júnior; Gabriel Oliveira de Aguiar Borges; Guilherme Reis. Uberlândia: LAECC, 2020. p. 169.

Capítulo 2

TEORIA GERAL DA PROVA E PROVAS DIGITAIS

A prova é um elemento fundamental na busca pela verdade e justiça no sistema legal, servindo como pilar para a tomada de decisões judiciais. Com o avanço da tecnologia, o conceito tradicional de prova se expandiu para incluir as provas digitais, que abrangem desde e-mails e mensagens de texto até registros de atividades online e dados de geolocalização.

A crescente presença de provas digitais em processos judiciais exige que o sistema legal se adapte e enfrente os desafios e oportunidades que elas apresentam. A natureza intangível e a facilidade de manipulação dos dados digitais exigem conhecimentos técnicos especializados e procedimentos rigorosos para garantir sua autenticidade e integridade, desde a coleta até a análise.

O uso de provas digitais levanta debates importantes sobre privacidade, segurança e a possibilidade de manipulação de dados. É crucial estabelecer limites claros e garantir a proteção dos direitos individuais ao mesmo tempo em que se aproveita o potencial dessas provas para fortalecer a busca pela verdade.

Este capítulo explorará o conceito de prova digital, suas características e os desafios que ela representa para o sistema legal. Abordaremos as diferentes formas de provas digitais, desde documentos eletrônicos e mensagens instantâneas até dados de geolocalização, e discutiremos as implicações legais e éticas de seu uso. Ao compreender a importância e a complexidade das provas digitais, poderemos construir um sistema legal mais justo e eficaz na era digital.

2.1 A TEORIA GERAL DA PROVA

Inicialmente, compreender a teoria da prova e sua aplicação na realidade contemporânea, é fundamental revisitar o direito constitucional à prova, que se configura como um direito fundamental e indispensável à efetivação da justiça.

A prova deve ser compreendida e produzida em consonância com as particularidades do caso concreto, adaptando-se às peculiaridades dos fatos a serem demonstrados.

A garantia constitucional desse direito impede que as partes sejam privadas da oportunidade de comprovar suas alegações, mesmo na ausência de meios de prova típicos, muitas vezes invocados como justificativa para a restrição do acesso à prova.[139] Portanto, cumpre esclarecer acerca dos aspectos constitucionais do direito à prova.

2.1.1 O Direito Constitucional à Prova

Não há justiça sem prova. Dentre os diversos princípios constitucionais que podem ser evocados, o mais evidente está previsto no art. 5º, inciso XXXV da CRFB/1988[140]: “a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito”.

Tal dispositivo constitucional visa expressar o princípio constitucional da inafastabilidade da jurisdição, garantindo o acesso à justiça, assegurando ao cidadão o direito de ter seu caso apreciado e solucionado pelo Poder Judiciário, quando houver lesão ou ameaça a direito. Essa garantia fundamental se traduz em uma prestação positiva do Estado, que deve atuar para solucionar conflitos de forma adequada.[141]

---

[139] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 17.

[140] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Promulgada em 5 de out. de 1988. Brasília, DF; out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm>. Acesso em: 28 mar. 2024.

[141] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 17.

É importante ressaltar que, embora fundamentais, os direitos não são absolutos. A subjetividade, inerente ao direito, justifica a diversidade de fontes e interpretações jurídicas. Nesse contexto, mesmo que todos os indivíduos tenham o direito de buscar amparo no sistema judiciário em caso de ameaça ou lesão a seus direitos, o acesso à justiça não é irrestrito. Existem procedimentos formais e requisitos específicos que devem ser observados para garantir a qualidade e a efetividade do processo judicial.

TAMER[142] leciona em sua obra sobre o princípio da inafastabilidade jurisdicional da seguinte forma:

> A inafastabilidade da jurisdição possui mesmo natureza principiológica. Essa conclusão deriva, especialmente, da compreensão de que a inafastabilidade preconiza um estado ideal das coisas a ser buscado representado pelo pleno acesso à jurisdição. **Sua aplicação não se justifica só pela subsunção do fato à descrição normativa, mas também pela verificação se os fatos e dispositivos contribuem para o acesso ou não**. Além disso, por delinear um fim a ser atingido, contribui diretamente e de forma complementar no raciocínio decisório. Do mesmo modo, a inafastabilidade se ajusta bem aos mais diversos conceitos de princípios desenvolvidos pela doutrina. Apresenta superioridade material ou valorativa sobre as regras, permite uma série indefinida de aplicações, pode ser compreendida como um mandado de otimização, como mandamento nuclear no contexto de resolução de conflitos e, ainda, como uma das normas mais fundamentais ou como uma verdade fundante desse sistema. Em síntese, a inafastabilidade da jurisdição possui um significado mais importante no Direito. O princípio da inafastabilidade é direito fundamental e nessa condição deve ser compreendido. Fundamentalmente, caracteriza-se como um direito a uma prestação positiva do Estado ou de quem estiver investido na função jurisdicional no sentido de solucionar adequadamente o conflito em caso de lesão ou ameaça a direito. **(grifo nosso)**

[142] TAMER, Maurício Antonio. **O princípio da inafastabilidade da jurisdição no direito processual civil brasileiro**. Rio de Janeiro: LMJ Mundo Jurídico, 2017. p. 118-119.

Depreende-se das lições acima que um acesso à justiça desqualificado compromete o propósito essencial do sistema jurídico, sobretudo, a ineficiência da devida aplicação da justiça e do direito.

A prova, é um meio (não um fim) de assegurar, a correta aplicação do princípio fundamental do livre acesso à justiça, embora sozinha, isto é, sem um procedimento adequado, não produza efetividade. Uma prova que não obedece aos procedimentos qualificados é capaz de comprometer não apenas um, mas diversos direitos fundamentais. Este tema será explorado em detalhes mais adiante nesta dissertação.[143]

Além do princípio da inafastabilidade jurisdicional, não há como dissertar sobre provas sem evocar o princípio do contraditório e da ampla defesa, previsto no art. 5, inciso LV, da CRFB/1988: “aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes;”.

Acerca do princípio do contraditório, LOPES JUNIOR[144] assevera que o contraditório poder ser tratado como um método de confrontação da prova:

> O contraditório pode ser inicialmente tratado como um método de confrontação da prova e comprovação da verdade, fundando-se não mais sobre um juízo potestativo, mas sobre o conflito, disciplinado e ritualizado, entre partes contrapostas: a acusação (expressão do interesse punitivo do Estado) e a defesa (expressão do interesse do acusado [e da sociedade] em ficar livre de acusações infundadas e imune a penas arbitrárias e desproporcionadas). É imprescindível para a própria existência da estrutura dialética do processo.

---

[143] TAMER, Maurício Antonio. **O princípio da inafastabilidade da jurisdição no direito processual civil brasileiro**. Rio de Janeiro: LMJ Mundo Jurídico, 2017. p. 159.

[144] LOPES JUNIOR, Aury. **Direito processual penal**. – 18. ed. – São Paulo, SaraivaJur, 2021. p. 237.

FAZZALARI[145] enfatiza que as decisões judiciais serão sempre construídas em contraditório, isto é, mediante efetiva e IGUALITÁRIA participação das partes no processo.

O princípio do contraditório é um dos mais importantes postulados no processo penal, pois trata do direito assegurado às partes de serem cientificados de todos os atos e fatos havidos no curso do processo, podendo manifestar-se e produzir as provas necessárias antes de ser proferida a decisão jurisdicional.[146]

NUCCI[147] explica que tal princípio significa dizer que a toda alegação fática ou apresentação de prova, feita no processo por uma das partes, tem a outra, adversária, o direito de se manifestar, havendo um perfeito equilíbrio na relação estabelecida pela pretensão punitiva do Estado em confronto com o direito à liberdade e à manutenção do estado de inocência do acusado.

A prova, em um processo justo e igualitário, é emanada pelo princípio do contraditório e da ampla defesa, que decorre da possibilidade de as partes utilizarem de meios amplos para influírem no convencimento do julgador.[148]

Neste sentido, THAMAY e TEMER[149] explica que os princípios constitucionais, tanto da inafastabilidade como do contraditório, sem o elemento essencial, a prova, não produzem eficácia plena. São princípios incompletos e vazios, desprovidos de materialização:

> Pergunta-se então: como exercer o poder de influência assegurado constitucionalmente sem a possibilidade de realizar a prova adequada e efetiva em relação ao fato alegado? Os princípios constitucionais da inafastabilidade e do contraditório, sem o

---

[145] FAZZALARI, Elio. ***Istituzioni di Diritto Processuale***. – 8. ed. – Padova: CEDAM, 1996. p. 86.

[146] AVENA, Norberto. **Processo Penal**. – 12. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020. p. 117.

[147] NUCCI, Guilherme de Souza. **Curso de direito processual penal**. – 17. ed. – Rio de Janeiro: Forense, 2020. p. 156.

[148] ALVIM, Arruda. **Manual de direito processual civil:** teoria geral do processo e o processo de conhecimento. – 17. ed. rev., atual. e ampl. – São Paulo: Revista dos Tribunais, 2019. p. 830.

[149] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 23.

> mecanismo da prova, seriam como almas errantes em busca de seus corpos que pudessem lhes dar vida concreta.

Finalmente, a CRFB/1988[150] prevê em seu art. 5º, inciso LVI outro princípio fundamental, a definir como inadmissível a produção ou provas obtidas por meios ilícitos: "**Art. 5º, LVI -** são inadmissíveis, no processo, as provas obtidas por meios ilícitos*"*

As provas obtidas por meios ilícitos constituem uma limitação de natureza constitucional ao sistema do livre convencimento estabelecido no art. 155 do CPP[151], segundo o qual o juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial.[152]

Neste sentido, NUCCI[153] destaca que o processo penal deve basear-se na produção de provas legais e legítimas, sendo inadmissível qualquer prova obtida por meios ilícitos. O autor ainda compara o art. 155 do CPP com o art. 369 do CPC, argumentando que a lei processual civil é mais rigorosa em relação à admissibilidade de provas do que a lei processual penal:

> No Código de Processo Penal, encontra-se o art. 155, parágrafo único, preceituando que "somente quanto ao estado das pessoas serão observadas as restrições à prova estabelecidas na lei civil". Por outro lado, no Código de Processo Civil, no art. 369, encontramos que "as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz". Aparentemente, o disposto na lei processual civil é mais rigoroso do que o estabelecido pela processual penal, embora todas as normas devam ser interpretadas em consonância

---

[150] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Promulgada em 5 de out. de 1988. Brasília, DF; out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm>. Acesso em: 28 mar. 2024.

[151] BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, RJ; out. 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 28 mar. 2024.

[152] AVENA, Norberto. **Processo Penal**. – 12. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020. p. 947.

[153] NUCCI, Guilherme de Souza. **Curso de direito processual penal**. – 17. ed. – Rio de Janeiro: Forense, 2020. p. 164.

> com o texto constitucional, além do que é admissível a interpretação analógica e a aplicação dos princípios gerais de direito em processo penal (art. 3.º, CPP).

De todo modo, assim como qualquer outro, não se trata de um princípio absoluto. Feito até aqui algumas considerações constitucionais acerca do direito à prova, cumpre abordar na sequência a conceituação de provas.

2.1.2 Conceito de Prova

O processo penal, como um instrumento de retrospecção, busca reconstruir um determinado fato histórico, instruindo o julgador por meio da reunião de provas. Essas provas, conforme lições de LOPES JUNIOR[154], são os meios pelos quais se reconstitui o crime, permitindo ao juiz formar sua convicção sobre o ocorrido

Acerca da terminologia da palavra, LIMA[155] explica que "prova" surge do verbo "provar", cujo significado é o de demonstrar a veracidade de um enunciado sobre um fato tido por ocorrido no mundo real. Tal palavra possui vários significados, sendo uma origem etimológica de probo (do latim, *probatio* e *probus*), traduzindo as ideias de verificação, inspeção, exame, aprovação ou confirmação.

Neste mesmo sentido, NUCCI[156] explica em sua obra acerca da origem do termo:

> O termo prova origina-se do latim – probatio –, que significa ensaio, verificação, inspeção, exame, argumento, razão, aprovação ou confirmação. Dele deriva o verbo provar – probare –, significando ensaiar, verificar, examinar, reconhecer por experiência, aprovar, estar satisfeito com algo, persuadir alguém a alguma coisa ou demonstrar.

---

[154] LOPES JUNIOR, Aury. **Direito processual penal**. – 18. ed. – São Paulo, SaraivaJur, 2021. p. 221.

[155] LIMA, Renato Brasileiro de. **Manual de Processo Penal:** volume único. – 8. ed. rev., ampl. e atual. – Salvador: JusPodivm, 2020. p. 655.

[156] NUCCI, Guilherme de Souza. **Curso de direito processual penal**. – 17. ed. – Rio de Janeiro: Forense, 2020. p. 683.

Por sua vez, GOMES FILHO[157] juridicamente define a prova como “dados objetivos que confirmam ou negam uma asserção sobre determinado fato que interessa à decisão da causa”.

O conceito de prova é bastante extenso e diverso, isso porque a prova é ao mesmo tempo, meio, resultado e atividade. Por exemplo, a prova testemunhal é um meio, enquanto seu resultado, também é prova, de modo que revela a ocorrência ou não de fatos. Já a atividade é a própria realização da oitiva da testemunha pelas partes.[158]

Ademais, LOPES JUNIOR e ROSA[159] definem a prova no processo penal da seguinte forma:

> [...] serve, a um só tempo, para buscar a reconstituição (aproximativa e parcial) de um fato passado, histórico, para um juiz ‘ignorante’ (pois ignora os fatos). É a prova que permite a atividade recognitiva (e não cognitiva, pois indireta) do juiz em relação ao fato histórico (story of the case) narrado pela acusação. Ao mesmo tempo tem uma função persuasiva, pois é através dela que se permite a construção do convencimento, da decisão. Por isso, as provas servem para obter a captura psíquica do julgador, para formar sua convicção.

AVENA[160] conceitua a prova como o “conjunto de elementos produzidos pelas partes ou determinados pelo juiz visando à formulação do convencimento quando a atos, fatos e circunstâncias”.

Para o autor, a produção da prova objetiva auxiliar na formação do convencimento do juiz quanto à veracidade das afirmações das partes

---

[157] GOMES FILHO, Antonio Magalhães. **Notas sobre a terminologia da prova** (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide (Coords.). Estudos em homenagem à Professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005.

[158] ALVIM, Arruda. **Manual de direito processual civil:** teoria geral do processo e o processo de conhecimento. – 17. ed. rev., atual. e ampl. – São Paulo: Revista dos Tribunais, 2019. p. 830.

[159] LOPES JUNIOR, Aury; ROSA, Alexandre Morais da. **A importância da cadeia de custódia para a preservar a prova penal**. Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal/>. Acesso em: 25 mar 2024.

[160] AVENA, Norberto. **Processo Penal**. – 12. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020. p. 917.

em juízo, não sendo destinada às partes que a produzem ou requerem, mas ao magistrado, possibilitando-o o julgamento de procedência ou improcedência da ação penal.[161]

Ademais, é importante destacar as diferenças entre provas e indícios. Conforme FERRAJOLI[162], as provas referem-se a fatos atuais e diretamente observados, que permitem inferências sobre eventos passados, como crimes. Elas são experimentadas no presente e geram conclusões baseadas na confiabilidade do meio ou da fonte, como testemunhas, documentos ou evidências materiais. A força indutiva das provas depende da confiabilidade subjetiva de suas fontes, como a sinceridade e autenticidade dos testemunhos e documentos, ou o rigor das perícias.

Por outro lado, os indícios são fatos do passado que sugerem uma hipótese explicativa sobre outro evento anterior. Eles possuem uma natureza mais indireta, pois não são experimentados diretamente, mas inferidos a partir de provas ou outros indícios. A força indutiva dos indícios depende de sua relevância objetiva, ou seja, de sua capacidade de gerar explicações plausíveis e verossímeis sobre o caso em questão.[163]

Em algumas situações, as provas podem ser confiáveis, mas os indícios delas derivados podem ser irrelevantes. Em outras, as provas podem ser questionáveis, enquanto os indícios se mostram significativos e decisivos.

Portanto, compreender essa distinção entre provas e indícios ajuda a esclarecer que, nos processos judiciais, as conclusões raramente se baseiam em provas diretas, mas geralmente em uma combinação de provas e indícios. Isso resulta em uma complexa cadeia de inferências que, quanto mais

---

[161] AVENA, Norberto. **Processo Penal**. – 12. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020. p. 918.

[162] FERRAJOLI, Luigi. **Direito e razão**: teoria do garantismo penal. – 4. ed., rev.; tradutores Ana Paula Zomer Zica ... [et al.] – São Paulo, Revista dos Tribunais, 2014. p. 106.

[163] FERRAJOLI, Luigi. **Direito e razão**: teoria do garantismo penal. – 4. ed., rev.; tradutores Ana Paula Zomer Zica ... [et al.] – São Paulo, Revista dos Tribunais, 2014. p. 107.

extensa for, menor será a probabilidade de se alcançar uma verdade inquestionável.[164]

Em síntese, a prova no processo penal visa auxiliar o juiz na formação de seu convencimento sobre a veracidade dos fatos alegados pelas partes. Essa atividade probatória, essencial para a busca da verdade, permite ao magistrado, que não possui conhecimento prévio dos acontecimentos, compreender a dinâmica do caso concreto e proferir uma decisão justa e fundamentada. Dito isso, cumpre a seguir explicar acerca da finalidade da prova.

2.1.2.1 Finalidade da Prova

A finalidade da prova, segundo LIMA[165], visa reconstruir os fatos investigados, buscando a maior fidelidade possível à realidade histórica, com o objetivo de formar a convicção do órgão julgador.

Para NUCCI[166], a finalidade da prova é convencer o juiz a respeito da verdade de um fato litigioso. Busca-se a verdade processual, ou seja, a verdade atingível ou possível. A verdade processual emerge durante a lide, podendo corresponder à realidade ou não, embora seja com base nela que o magistrado deve proferir sua decisão.

O objetivo da prova é convencer seu destinatário, o magistrado. Isso se deve em razão do magistrado não ter presenciado o fato a que é submetido sua apreciação, de modo que, é por meio das provas que o juiz poderá reconstruir o momento, a fim de decidir se o delito, de fato, ocorreu.[167]

Por fim, cumpre ressaltar que não é possível atingir com absoluta precisão a verdade histórica dos fatos, sendo possível dizer que se busca

---

[164] FERRAJOLI, Luigi. **Direito e razão**: teoria do garantismo penal. – 4. ed., rev.; tradutores Ana Paula Zomer Zica ... [et al.] – São Paulo, Revista dos Tribunais, 2014. p. 107.

[165] LIMA, Renato Brasileiro de. **Manual de Processo Penal:** volume único. – 8. ed. rev., ampl. e atual. – Salvador: JusPodivm, 2020. p. 658.

[166] NUCCI, Guilherme de Souza. **Curso de direito processual penal**. – 17. ed. – Rio de Janeiro: Forense, 2020. p. 691.

[167] REIS, Alexandre Cebrian Araújo. **Direito processual penal**. – 11. ed. – São Paulo: SaraivaJur, 2022. p. 535.

a verdade processual. Dito isso, cumpre a seguir explicar sobre a classificação da prova.

2.1.2.2 Classificação da Prova

As provas podem ser classificadas em quatro categorias: a) quanto ao objeto, b) quanto ao sujeito; c) quanto a forma; e d) quanto ao valor.[168]

A classificação da prova quanto ao objeto distingue entre provas diretas e indiretas. As provas diretas demonstram o fato em questão de forma imediata, como o testemunho ocular de um homicídio. Já as provas indiretas não comprovam diretamente o fato, mas permitem deduzi-lo por meio de um raciocínio lógico.[169]

Ademais, quanto ao sujeito da prova, AVENA[170] ensina que as provas podem ser classificadas em reais ou pessoais. As provas reais são aquelas que não se originam diretamente da pessoa, mas de elementos externos que comprovam a existência do fato, como um cadáver ou a arma do crime. Já as provas pessoais decorrem da manifestação de uma pessoa, como no caso do interrogatório, do testemunho ou dos laudos periciais.

A classificação da prova quanto à forma refere-se ao modo como ela é apresentada em juízo, podendo ser documental, que são documentos escritos que comprovam fatos ou atos; material, isto é, elementos físicos que demonstram a materialização de um fato; ou testemunhal, que se trata de manifestações pessoais orais, como depoimentos e esclarecimentos.[171]

Finalmente, quanto ao valor das provas, AVENA entende que elas podem ser consideradas em plenas ou não plenas. As provas plenas são aquelas que geram convicção sobre o fato investigado, podendo fundamentar a

---

[168] CAPEZ, Fernando. **Curso de processo penal**. – 30. ed. – São Paulo: SaraivaJur, 2023. p. 392.

[169] AVENA, Norberto. **Processo Penal**. – 12. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020. p. 920.

[170] AVENA, Norberto. **Processo Penal**. – 12. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020. p. 921.

[171] LIMA, Renato Brasileiro de. **Manual de Processo Penal:** volume único. – 8. ed. rev., ampl. e atual. – Salvador: JusPodivm, 2020. p. 659.

decisão judicial sobre a responsabilidade penal do acusado. Já as provas não plenas (ou circunstanciais), não possuem força para embasar isoladamente a decisão, mas podem corroborar outras evidências e fortalecer o convencimento do juiz.[172] Entretanto, a classificação das provas como plenas e não plenas é considerada controversa por parte da doutrina.

Isto posto, cumpre a seguir explicar sobre os meios de prova e meios e obtenção de provas.

2.1.3 Meios de Provas e Meios de Obtenção de Provas

No que diz respeito aos meios de provas, LOPES JUNIOR[173] ensina em sua obra que são os elementos necessários para constituir um fato. Por exemplo, documentos, testemunhas e perícias. São elementos que contam a história do fato concreto, fazendo com que o juízo “ligue os pontos”.

Já os meios de obtenção de provas, são instrumentos utilizados para se obter a prova. Não são as provas em si, mas sem os meios de obtenção de provas, as provas possivelmente não existiriam. São exemplos de obtenção de provas a delação premiada e buscas e apreensões. [174]

Em síntese, enquanto os meios de provas são destinados diretamente ao convencimento, os meios de obtenção são ferramentas que visam captar elementos que, no futuro, poderão ser utilizadas no processo, portanto, são indiretas ao convencimento e não diretas, como os meios de provas, pois produzirão efeitos de forma mediata.

Isto posto, cumpre ressaltar que a teoria geral da prova não se esgota por aqui. Contudo, para o foco da pesquisa, que são as provas digitais, a breve contextualização é suficiente para dar prosseguimento ao estudo.

---

[172] AVENA, Norberto. **Processo Penal**. – 12. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020. p. 921.

[173] LOPES JUNIOR, Aury. **Direito processual penal**. – 18. ed. – São Paulo, SaraivaJur, 2021. p. 425.

[174] LOPES JUNIOR, Aury. **Direito processual penal**. – 18. ed. – São Paulo, SaraivaJur, 2021. p. 425.

2.2 A PROVA DIGITAL

O crescimento acelerado das tecnologias tem impulsionado a quarta revolução industrial, integrando a internet e dispositivos digitais no cotidiano da sociedade. Embora esses avanços tenham proporcionado melhorias significativas na qualidade de vida, também possibilitaram a prática de crimes que ameaçam bens jurídicos individuais, coletivos e a própria estrutura social.

Diante da crescente utilização de tecnologias digitais e do aumento da criminalidade informática, faz-se necessário adaptar o ordenamento jurídico para acompanhar essa realidade. A regulamentação das provas digitais surge como um desafio fundamental, exigindo a criação de normas que permitam a utilização dessas provas no processo judicial, garantindo sua validade e eficácia na persecução penal e na proteção dos direitos fundamentais.[175]

Portanto, cumpre a seguir abordar sobre a prova digital, seu conceito, características e espécies de provas digitais, bem como as normas legais existentes no ordenamento jurídico brasileiro que tratam da produção, admissibilidade e valoração dessas provas, buscando uma compreensão abrangente do tema e suas implicações no âmbito jurídico.

2.2.1 Conceito

A busca pela conceituação das provas digitais ainda é um desafio para a doutrina, devido sua complexidade e constante evolução. Além de ser um tema contemporâneo, logo, seus estudos são recentes.

Em essência, a prova digital continua sendo prova, um instrumento jurídico destinado a comprovar a existência ou não de um fato, delineando suas características, circunstâncias e envolvidos, respondendo não apenas à questão da ocorrência, mas também ao modo como ocorreu e aos sujeitos a ele relacionados.

---

[175] HERMEIRO, Andreia Carina Cláudio. **A cadeia de custódia da prova digital:** o uso da tecnologia blockchain como forma de preservação. 2023. Dissertação (Mestrado em Ciências Jurídico-Forenses). 64 f. Faculdade de Direito da Universidade de Coimbra, Coimbra, 2023. p. 17-18.

Recapitulando a teoria da prova, pode-se dizer que a prova digital, também conhecida como evidência digital (do inglês *digital evidence*) é o meio utilizado para demonstrar a evidência de um fato ou evento ocorrido em meio digital.[176]

VAZ[177] conceitua a prova digital como “os dados em forma digital (no sistema binário) constantes de um suporte eletrônico ou transmitidos em rede de comunicação, os quais contêm a representação de fatos ou ideias”. A autora ainda faz uma relevante observação:

> Veja-se que é possível mencionar, sob a ideia de fonte real, prova eletrônica ou digital para designar os suportes físicos em que se encontram armazenados os dados – computadores, pen drives, CDs, DVDs, telefones celulares, aparelhos de MP3, as urnas eletrônicas, câmeras de vídeo ou fotográficas, etc.[178]

Ainda, a autora destaca que essa definição não compreende os meios de prova que se utilizam de sistemas informáticos para auxiliar na interpretação e análise dos dados contidos no processo.

As provas digitais são entidades imateriais, mas possuem sua própria materialidade, sendo definido conceitualmente, como impulsos elétricos que respondem a uma sequência numérica predefinida e que, quando canalizados em um suporte informático com memória, originam informações inteligíveis.[179]

O termo "digital", derivado da manipulação eletrônica, é autoexplicativo. Segundo KERR[180], a evidência digital consiste em sequências de

---

[176] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 32.

[177] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 61.

[178] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 62.

[179] **Texto Original:** *concettualmente si tratta di impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili.* In: DANIELE, Marcello. ***La prova digitale nel processo penale***. *Rivista di Diritto Processuale*, 2011. p. 283.

[180] KERR, O. S. ***Digital evidence and the new criminal procedure***. Columbia law review, v. 105,

zeros e uns, os sinais binários que compõem os dados digitais. O autor busca desmistificar a complexidade aparente das provas digitais, enfatizando que, em sua essência, são apenas sequências numéricas que podem ser interpretadas por meio de técnicas forenses apropriadas.

Por sua vez, NESSI[181] define a prova (evidência) digital, como qualquer informação extraída de qualquer meio eletrônico e que tecnicamente, é uma evidência física, que está constituída por campos magnéticos e pulsos eletrônicos que podem ser coletados e analisados com ferramentas técnicas especiais.

ROSA e CAN[182] explicam que, ainda que o fato, em si, não tenha ocorrido em um ambiente digital, a evidência pode ser encontrada em dispositivos eletrônicos, como celulares, computadores, câmeras de segurança, *smartwatches*[183]*,* câmeras digitais, dispositivos de armazenamento interno, *pendrive*, por exemplo, entre outros. A prova pode ser um arquivo de áudio, uma mensagem de texto, um vídeo, uma foto, registros de chamada, entre outros.

Nesse sentido, THAMAY e TEMER[184] ensina em sua obra que, embora os fatos possam ter ocorrido no meio físico, as provas podem existir no meio virtual:

> A resposta para todas essas perguntas parece possível a partir da própria semântica do termo digital agregado, o que induz a duas acepções de compreensão. Uma primeira, segundo a qual a prova digital pode ser entendida como a demonstração de um fato ocorrido nos meios digitais, isto é, um fato que tenha como suporte a utilização de um meio digital. E, uma segunda, em que, embora o

p. 279-318, 2005. p. 284.

[181] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p.

[182] ROSA, Alexandre Morais da; CANI, Luiz Eduardo. **Guia para Mitigação dos Erros Judiciários no Processo Penal**: as causas prováveis e as estratégias de enfrentamento. Florianópolis: Emais, 2021. p. 06.

[183] Smartwatch é um relógio inteligente, com funcionalidades de um smartphone.

[184] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 32.

> fato em si não tenha ocorrido em meio digital, a demonstração de sua ocorrência pode se dar por meios digitais.

ROSA e CANI[185] mencionam que a prova digital, uma categoria da prova eletrônica, é aquela obtida ou produzida em ambiente digital, onde os dados (de base, de tráfego e de conteúdo), geralmente vulneráveis, intangíveis e frágeis, necessitam de extração e tratamento em conformidade com normas técnicas e com a cadeia de custódia digital, sob pena de invalidade probatória. É aquela que se concentra em dados e evidências manipulados e transformados em formato digital, como mensagens de texto, mensagens de correio eletrônico, imagens, vídeos, registros de chamadas, dados de localização, informações sobre a conta em linha de um utilizador.

Por sua vez, KIST[186] compreende que a prova eletrônica é mais ampla do que a prova digital, pois engloba qualquer forma de dado, até mesmo aquele produzido por um dispositivo analógico. O autor salienta a importância de não confundir as nomenclaturas, pois cada uma deve observar procedimento específicos para sua correta produção.

Ademais, segundo lições de DANIELE[187], o número de provas ocultas dentro de sistemas eletrônicos está cada vez mais presente nos processos judiciais, provas que podem (e geralmente são) indispensáveis para uma correta e justa resolução do caso penal. Essas provas são mais precisamente denominadas como evidências digitais, uma vez que são originadas por uma manipulação eletrônica de números. Provas como essas, são uteis não apenas para demonstrar fatos ocorridos dentro dos sistemas ou dispositivos eletrônicos, mas também podem produzir conhecimentos relevantes para qualquer evento, portanto, têm um escopo operacional potencialmente ilimitado.

---

[185] ROSA, Alexandre Morais da. **O "*print screen*" é insuficiente à materialidade nos crimes digitais**. Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2022-jun-17/limite-penal-print-screen-materialidade-crimes-digitais/>. Acesso em: 19 abr. 2024.

[186] KIST, Dario José. **Prova digital no processo penal**. – 1. ed. – São Paulo: JH Minuzo, 2019. p. 108.

[187] DANIELE, Marcello. ***La prova digitale nel processo penale***. *Rivista di Diritto Processuale*, 2011. p. 283.

Portanto, compreende-se que a prova digital, apesar de sua complexidade e constante evolução, é um instrumento jurídico fundamental na era digital. Ela transcende o mero conceito de prova eletrônica, abrangendo qualquer informação extraída de meios eletrônicos, independentemente de o fato ter ocorrido no mundo digital ou físico.

Ressalte-se que a natureza intangível e frágil dos dados digitais exige cuidados especiais em sua coleta, armazenamento e análise, a fim de garantir sua validade e autenticidade no processo judicial. Assim, a prova digital se apresenta como um desafio e uma oportunidade para o Direito, que precisa se adaptar e desenvolver novas ferramentas para lidar com essa nova realidade.

2.2.2 Características da Prova Digital

As provas digitais, enquanto fontes de prova, representam uma nova realidade no âmbito jurídico, com peculiaridades que as diferenciam das demais categorias probatórias, especialmente no que tange ao seu registro, extração, preservação e apresentação em juízo.[188]

Conforme conceituado, as provas digitais se referem a qualquer informação ou dados eletrônicos que possam ser apresentados como evidência em um processo legal. Segundo THAMAY e TEMER[189], essas provas incluem uma ampla gama de elementos, como documentos eletrônicos, e-mails, mensagem de texto, registros de atividades digitais, imagens e vídeos digitais.

Dentre as características que compõem a prova digital, é possível classificá-las em: a) imaterialidade; b) volatidade; c) suscetibilidade de clonagem e facilidade de dispersão, d) necessidade de dispositivo para transmissão.

---

[188] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 66.

[189] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 23.

Segundo VAZ[190], a imaterialidade da prova digital, caracterizada pela ausência de representação física, facilita a sua transmissão e permite o armazenamento massivo de conteúdos em sistemas informáticos, dispensando a necessidade de movimentação física.

Já a volatilidade da prova digital refere-se à sua suscetibilidade a constantes mudanças. Por ser frágil, pode ser facilmente alterada ou desaparecer, bastando uma simples modificação na sequência numérica que a constitui.

Por sua vez, a suscetibilidade de clonagem e facilidade de dispersão da prova digital decorrem de sua imaterialidade. Essa característica a torna extremamente vulnerável ao processo de clonagem, podendo ser facilmente copiada e transmitida para outros dispositivos eletrônicos, o que representa um risco à preservação da originalidade do arquivo utilizado como prova.[191]

Por fim, a necessidade de um dispositivo para transmissão da prova digital reside no fato de que, apesar de ser imaterial e independente do meio físico de armazenamento, a prova digital necessita de um dispositivo físico para sua exposição, extração ou transmissão. Uma vez que a prova digital é constituída por combinações numéricas restritas ao ambiente digital, o dispositivo físico é o único meio pelo qual se pode acessar e processar o conteúdo probatório.[192]

Ademais, conforme lições de CARLIZZI[193], a imaterialidade e a dispersão, são as principais características da prova digital. Elas são imateriais pois não são físicas e palpáveis, como um documento impresso em papel. São dados

---

[190] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 68.

[191] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 69.

[192] VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012. p. 69-70.

[193] CARLIZZI, Gaetano. **La prova tecnológica nel processo penale.** In: LUPÁRIA, Luca; MARAFIOTI, Luca; PAOLOZZI, Giovanni (a cura di). Dimensione tecnologica e prova penale. G. Giappichelli Editore – Torino, 2019.

eletrônicos, transmitidos e armazenados em ambientes digitais. Também são dispersas, porque tendem estar em locais geograficamente distintos, sendo essa uma característica própria do ambiente digital. Por exemplo: um homicídio em que o local do fato foi na cidade de Balneário Camboriú/SC, mas que a prova mais importante para demonstrar o autor do fato está dentro um arquivo de mídia no celular de um cidadão que reside em Nova Iorque. Isso ocorre devido à natureza global das redes de computadores.

Tanto a imaterialidade como a dispersão, são desafios para o sistema judiciário. A primeira em razão da falta de conhecimento técnico dos servidores da justiça quanto a coleta, armazenamento, preservação e apresentação destas evidências. E a segunda, aumentam os desafios especialmente quanto a obtenção e admissibilidade em processos judiciais.

Finalmente, ROSA e CANI[194] ensinam que além das imaterialidade e da dispersão, as provas digitais também são: frágeis, pois são alteráveis e corrompidas facilmente, podendo ser duplicada e copiada de maneira exata, como se original fosse; rastreáveis, pois podem conter metadados, que levam a informação de origem, autoria, data e hora de criação, entre outros detalhes; recuperáveis, podendo ser recuperadas mesmo após terem sido excluídas ou ocultadas; e vastas e complexas, pois os dados podem ser volumosos e de difícil compreensão e análise.

É evidente que as provas digitais apresentam características únicas que as diferenciam significativamente das provas tradicionais. A imaterialidade, volatilidade, suscetibilidade de clonagem, facilidade de dispersão e a necessidade de dispositivos para sua transmissão impõem desafios e exigem conhecimentos técnicos especializados para sua correta manipulação e apresentação em juízo. No próximo tópico, serão abordadas as espécies de provas digitais, explorando suas particularidades e implicações jurídicas.

---

[194] ROSA, Alexandre Morais da; CANI, Luiz Eduardo. **Guia para Mitigação dos Erros Judiciários no Processo Penal**: as causas prováveis e as estratégias de enfrentamento. Florianópolis: Emais, 2021. p. 06.

2.3 ESPÉCIES DE PROVAS DIGITAIS

As possibilidades de evidências digitais são imensuráveis. No ordenamento jurídico brasileiro, são enquadradas em provas atípicas, isso porque, não possuem regramento específico. São algumas delas: mensagens instantâneas, páginas visitadas na internet, dados de geolocalização, documentos eletrônicos, correios eletrônicos, fotos, vídeos, áudios, endereço de IP, evidências em redes sociais, entre outros.

O número de evidências digitais, como dito, é imensurável. Logo, não seria possível elencar todas as possibilidades existentes neste estudo. Contudo, com a finalidade de posteriormente, especificar no terceiro capítulo, aprofundar a qualificação das provas digitais, serão abordadas aquelas que, atualmente, são mais utilizadas no cotidiano, e, consequentemente, são objetos de provas frequentes nos processos judiciais.

2.3.1 Documento Eletrônico

A prova documental é uma espécie clássica de prova, em qualquer área do direito. Legalmente, o conceito de documento está expresso no ordenamento jurídico da seguinte forma: *"**CPP - Art. 232.** Consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares."*[195]

Ressalte-se que o CPC prevê, na Seção VII, que a prova documental é qualquer escrito que possa servir de prova para os fatos alegados pelas partes em juízo e ainda, estabelece regras de admissibilidade da prova documental.

Embora o documento seja comumente interpretado como um sinônimo de prova documental, ele não existe para o fim de servir de prova, mas

[195] BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, RJ; out. 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 27 abr. 2024.

pode ser utilizado eventualmente como uma. Portanto, são distintos. O documento é o suporte e a prova documental é o resultado da utilização desse documento.[196]

CAPEZ[197], diferencia instrumento e documento, afirmando que o instrumento é produzido já com a finalidade de provar determinado fato. Já o documento, não é produzido com este fim determinado, mas, pode eventualmente vir a servir. O autor também conceitua os documentos na atual modernidade como:

> [...] não só os escritos, mas também qualquer forma corporificada de expressão do sentimento ou pensamento humano, tais como a fotografia, a filmagem, a gravação, a pintura, o desenho, o e-mail etc.

ROSA[198], complementa o conceito de prova documental afirmando que sua admissibilidade depende do atendimento aos requisitos de validade e da garantia de possibilidade de impugnação.

Quanto as espécies de documentos, é necessário distinguir os instrumentos públicos dos particulares. Aqueles são constituídos de fé-pública, que lhes garantem a presunção de veracidade ou presunção *juris tantum*. É como um selo do Estado de veracidade. Já os instrumentos particulares, são aqueles que não possuem fé-pública, portanto, desprovidos de qualquer intervenção do Estado. São exemplos de instrumentos públicos as procurações públicas e contratos de união estável público. Em ambos os exemplos, é possível que não sejam instrumentos públicos e sim particulares, entretanto, para a prática de determinados atos, a Lei exige que o instrumento seja público, justamente pela garantia dada à fé-pública.

A prova documental então abrange qualquer material, público ou privado, analógico ou digital, que represente um fato, um pensamento, uma expressão, uma ideia, uma foto, um vídeo, uma ordem, uma vontade, entre outros.

---

[196] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 112.

[197] CAPEZ, Fernando. **Curso de processo penal**. – 30. ed. – São Paulo: SaraivaJur, 2023. p. 892.

[198] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-A. – 1. ed. – Florianópolis: Emais, 2021. p. 437.

Pois bem, feitas as considerações referente aos documentos de modo amplo, pode-se afirmar que o documento eletrônico é qualquer informação gerada, transmitida, acessada e armazenada em meios eletrônicos, que dispensa o papel físico.[199]

Para MARQUES[200], o documento eletrônico é uma sequência de *bits* (representação decodificada) traduzida por algum programa ou *software* que representa algum fato ou informação. O autor explica que:

> [...] os documentos eletrônicos possuem os mesmos elementos que um documento escrito em suporte de papel, contendo, entretanto, os seguintes aspectos: a) constam em suporte material (disquete, circuitos, chips de memória, redes); b) contêm uma mensagem, em que está escrita em linguagem convencional de dígitos binários ou bits, entidades magnéticas que os sentidos humanos não podem perceber diretamente; c) estão escritos em um idioma ou código determinado; d) podem ser atribuídos a uma pessoa determinada com a qualidade de autor, mediante uma assinatura digital ou chave eletrônica.

Por sua vez, CLEMENTINO[201] define o documento eletrônico como “toda representação virtual que fornece informação ou prova, elaborado mediante o uso de computador, materializado pelo registro magnético ou similar”.

BORRUSSO, GIORGI, MATTIOLI e RAGONA[202], defendem que o documento eletrônico deve ser definido de forma mais ampla, importando apenas a representação jurídica do fato, pois a volatilidade da sociedade da informação prejudica essa definição, uma vez que sempre estaria ultrapassada.

---

[199] ROSA, Alexandre Morais da; CANI, Luiz Eduardo. **Guia para Mitigação dos Erros Judiciários no Processo Penal**: as causas prováveis e as estratégias de enfrentamento. Florianópolis: Emais, 2021. p. 105.

[200] MARQUES, Antônio Terêncio. **A prova documental na internet**. – 1. ed., 6. reimpr. - Curitiba: Juruá, 2011. p. 127.

[201] CLEMENTINO, Edilberto Barbosa. **Processo judicial eletrônico**. Curitiba: Juruá, 2007. p. 15.

[202] BORRUSO, Renato; DI GIORGI, Rosa Maria; MATTIOLI, Leonello; RAGONA, Mario. ***L´informatica del diritto****. Seconda edizione riveduta e aggiornata*. Milano: Dott. A. Giufrè, 2007. p. 77

É necessário ainda repisar que, assim como o termo “prova digital” trata-se de uma espécie da prova eletrônica, sendo este um termo mais amplo, o documento eletrônico e o digital também seguem a mesma linha.[203]

A título de exemplo prático, a CNH[204] digital e a CNH eletrônica. Enquanto a primeira é originada/criada exclusivamente e diretamente em formato digital a CNH eletrônica pode ser a CNH física em papel escaneada e digitalizada, ou seja, não foi originada por meio digital. Essa distinção é necessária pois para garantir a autenticidade desses documentos o procedimento é distinto.

No âmbito legislativo acerca do tema, a Lei nº 11.419/2006 [205] é considerada um grande marco na informatização judicial, entretanto, a Lei não expressa o conceito de documento eletrônico, cabendo apenas a doutrina definir e conceituá-lo.

A Lei do Processo Eletrônico trouxe regramentos sobre a informatização do processo judicial, alterando até mesmo o Código de Processo Civil de 1973. Em 2015, o novo Código de Processo Civil, trouxe consigo uma disposição separada e específica para os documentos eletrônicos, nos arts. 439 a 441. Entretanto, o CPC não abordou o conceito operacional do termo, limitando-se ao tratamento da utilização e apreciação dos documentos eletrônicos no processo civil. Além disso, as referidas normas são consideradas como de eficácia limitada, pois dependem de complementação normativa futura para produzirem todos os seus efeitos, vejamos:

> **Art. 439.** A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, **na forma da lei**.

---

[203] KIST, Dario José. **Prova digital no processo penal**. – 1. ed. – São Paulo: JH Minuzo, 2019. p. 108-109.

[204] **Definição da sigla:** Carteira Nacional de Habilitação.

[205] BRASIL. **Lei nº 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF; dez. 2006. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm>. Acesso em: 28 abr. 2024.

> **Art. 440.** O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor.
>
> **Art. 441**. Serão admitidos documentos eletrônicos produzidos e conservados **com a observância da legislação específica. (grifo nosso)**

De forma equivocada, a norma considera como meio eletrônico qualquer armazenamento de documentos e arquivos digitais. Entretanto, é necessário distinguir que todo documento eletrônico é um arquivo digital, mas nem todo arquivo digital é um documento eletrônico, necessariamente[206].

Para fundamentar essa informação, utiliza-se como exemplo a legislação italiana, que define o documento eletrônico como uma representação digital de dados, fatos ou atos juridicamente relevantes[207].

Denota-se, portanto, que arquivos digitais que não se propõe a demonstrar determinado fato, dado ou ato não são documentos, são apenas arquivos de sistemas, *drivers* ou protocolos.

É evidente que o processo judicial passou e continua em processo de informatização. A tecnologia e o direito tendem cada vez mais a se afunilarem, assim como a vida em comunidade. Apesar de algumas teorias como a do decrescimento, estudada por LATOUCH [208], que defende o retrocesso tecnológico, para uma vida mais feliz e próspera, no momento parece uma utopia. Não é possível, hoje, imaginar que a sociedade viverá algum dia sem os recursos tecnológicos. Portanto, cabe ao poder estatal regulamentar a utilização desses recursos, garantindo assim, a correta aplicação da justiça.

---

[206] POLL, Roberta Eggert. **Algoritmos decisionais e o poder judiciário:** limites à utilização da inteligência artificial, à luz dos direitos fundamentais. 2022. Tese (Doutorado em Direito). Programa de Pós-Graduação em Direito, Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022.

[207] GIOVANNI, Pascuzzi. ***Il diritto dell´era digitale****: tecnologie informatiche e regole privatistiche*. Bologna: Il Mulino, 2006. p. 77

[208] LATOUCHE, Serge. **Pequeno tratado do decrescimento sereno**. Tradução Claudia Berliner. São Paulo: Editora WMF Martins Fontes, 2009.

Sobre a importância do estabelecimento de requisitos criteriosos para garantir a validade jurídica do documento eletrônico, REINALDO FILHO[209] acrescenta que:

> [...] a informação em formato eletrônico é também dinâmica: o mero ato de ligar ou desligar um computador pode alterar a informação que ele armazena. Os computadores quando em funcionamento reescrevem e deletam informação, quase sempre sem o conhecimento específico do operador.

Nesse sentido, CHAVES JÚNIOR[210] defende o desenvolvimento tecnológico no ambiente judicial e de forma ainda mais específica, não meramente a digitalização de processos. Segundo o autor, esse desenvolvimento é importante “para uma nova racionalidade processual que possa tornar os direitos mais efetivos e as decisões mais justas”.

Depreende-se até aqui, que o documento eletrônico digital, como meio de prova, já faz parte da nova era tecnológica e da informatização dos processos judiciais. Entretanto, as normas brasileiras ainda são precárias e omissas em relação a correta produção desse tipo de prova.

Isto posto, aborda-se na sequência acerca das mensagens instantâneas.

2.3.2 Mensagens Instantâneas

Os serviços de mensagens instantâneas são amplamente usados em todo o mundo e oferecem uma variedade de recursos para tornar mais fácil e conveniente a comunicação entre amigos, familiares e colegas de trabalho. Ao viabilizar uma comunicação rápida e eficiente por meio de textos, áudios, fotos e

---

[209] REINALDO FILHO, Demócrito. **A exibição da prova eletrônica em juízo** – necessidade de alteração das regras do processo civil?. Disponível em: <https://www.migalhas.com.br/depeso/31031/a-exibicao-da-prova-eletronica-em-juizo---necessidade-de-alteracao-das-regras-do-processo-civil>. Acesso em: 01 mai. 2024.

[210] CHAVES JÚNIOR, José Eduardo de Resende. **Comentários à lei do processo eletrônico**. São Paulo: LTr, 2010. p. 24

vídeos, aplicativos de mensageria se tornaram parte das rotinas e, ao mesmo tempo, uma extensão da personalidade humana.[211]

É evidente que os aplicativos de mensagens instantâneas se tornaram parte onipresente na rotina de boa parte da humanidade, tanto em âmbito pessoal como profissional, em razão da facilidade de comunicação e conveniência que proporcionam. É possível, hoje, com esses aplicativos, se comunicar, com um colega ou familiar que esteja em qualquer lugar do mundo.

É por meio desses aplicativos que as pessoas compartilham sentimentos, opiniões, desabafos, até mesmo expressam sentimentos que pessoalmente não teriam coragem de compartilhar. Por essa razão, as mensagens instantâneas por serviços de aplicativos tornaram-se protagonistas nos processos judiciais, pode-se afirmar que é mais comum um processo judicial que utilize mensagens de aplicativos como prova, do que aqueles que não utilizam. Em razão disso, é de extrema importância o estudo deste meio de prova tão relevante na modernidade.[212]

A legalidade das mensagens instantâneas como meio de prova, está prevista no art. 369 do CPC[213]:

> **Art. 369.** As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.

Ademais, no tocante a validade das mensagens instantâneas como prova judicial, apesar da alta relevância das conversas de aplicativos de mensagens para fins de comprovação de fatos juridicamente relevantes, há ainda

---

[211] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 85.

[212] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 85.

[213] BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF; mar. 2015. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: 01 mai. 2024.

grande negligência entre os operadores do direito com a utilização dessas mensagens.

Não é incomum encontrar em processos judiciais a apuração de fatos com meras capturas de telas (*print screen*) de conversas, que nada mais são que arquivos de imagens, que podem ser facilmente manipuladas, alteradas ou forjadas. [214] Já existem aplicativos que inclusive criam diálogos falsos (*fakes),* como por exemplo o *Whatsfake, Fake chat; Whatsmochk Pro*, entre outros, que simulam a interface do *WhatsApp Messenger.* Existem também aplicativos que simulam conversas do *Instagram e Facebook,* como *Telefun e FunstaPro.* Além dos aplicativos que simulam mensagens que não são reais, as próprias capturas de tela podem ser alteradas facilmente com algum *software* de edição de imagens, isso porque, como dito, são apenas arquivos de imagens.[215]

Neste sentido, RUSAKOVA e ZAITSEV[216] abordam sobre a aceitação de capturas de tela nos processos judiciais russos, destacam a importância do estabelecimento de rigorosos critérios para sua admissibilidade, o que inclui, confirmar a identidade dos mensageiros, bem como a integridade do conteúdo. Discutem ainda a relevância da ordem e do contexto das mensagens, para garantir que sejam representativas e não manipuladas.

É saliente ainda destacar que na esfera cível, em regra, a prova quando não impugnada pela parte contrária, presume-se válida. Logo, caso uma das partes anexe aos autos capturas de tela como provas de eventuais diálogos e a outra parte não impugne a autenticidade dessa prova, estará consolidada sua validade[217].

---

[214] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-A. – 1. ed. – Florianópolis: Emais, 2021. p. 439.

[215] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 89.

[216] RUSAKOVA, E. P.; ZAITSEV, V. V*.* ***Messenger chats as evidenci in civil and arbitration proceedings*** – *Russian judicial practice. Russian Journal of Legal Studies (Moscow)*. v. 7, n. 3, p. 9-15, 2020.

[217] BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF; mar. 2015. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: 01 mai. 2024.

Por outro lado, no âmbito criminal, prevalecendo sempre a presunção de inocência[218] e sendo o ônus da prova da acusação, a qual deverá comprovar a validade e eficácia dessa prova. Deste modo, diferente do âmbito cível, cabe ao julgador verificar se a acusação cumpriu com o seu ônus probatório para formar sua convicção.

Neste sentido, o judiciário brasileiro já tem pautado suas decisões pelo indeferimento de acusações em que o *print screen* de conversas é utilizado como meio de prova.

No julgamento do Recurso Ordinário em Habeas Corpus nº 99.735/SC[219], de relatoria da Ministra Laurita Vaz, julgado em 27/11/2018, o STJ decidiu que o espelhamento de mensagens do WhatsApp Web, mesmo com autorização judicial, é ilegal e não pode ser equiparado à interceptação telefônica.

O STJ considerou que o espelhamento via WhatsApp Web permite acesso ilimitado a todas as conversas, passadas, presentes e futuras, possibilitando ao investigador atuar como participante e até mesmo excluir mensagens sem deixar rastros. Essa característica, aliada à criptografia de ponta a ponta do aplicativo, impede a contraposição do investigado e cria uma presunção absoluta de legitimidade dos atos dos investigadores.

Ainda, a Sexta Turma do STJ destacou a fragilidade da prova obtida por espelhamento, já que a exclusão de mensagens não deixa vestígios e a criptografia de ponta a ponta impede a recuperação do conteúdo. A decisão reforça a importância da proteção da privacidade e dos dados pessoais, limitando o uso de ferramentas invasivas na investigação criminal.

Ademais, durante o julgamento do Agravo Regimento no Recurso Ordinário em Habeas Corpus nº 133.430/PE[220], de relatoria do Ministro

---

[218] BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, RJ; out. 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 03 mai. 2024.

[219] BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Ordinário em Habeas Corpus nº 99.735/SC**. Relator(a): Ministra Laurita Vaz. Sexta Turma. Data do Julgamento: 27 nov. 2018. Publicado no DJe em: 12 dez. 2018.

[220] BRASIL. Superior Tribunal de Justiça (STJ). **Agravo Regimento no Recurso Ordinário em**

Nefi Cordeiro, julgado em 23/02/2021, o STJ decidiu pela validade da instauração de inquérito policial com base em notícia anônima acompanhada de capturas de tela de conversas do WhatsApp, desde que o interlocutor que forneceu as capturas seja integrante do grupo de conversas.

No entanto, a Sexta Turma do STJ considerou nulas as provas obtidas por meio do espelhamento das conversas via WhatsApp Web, por entender que essa ferramenta permite a manipulação e exclusão de mensagens, comprometendo a integridade da prova. As demais provas produzidas após as diligências preliminares da polícia, realizadas em razão da notícia anônima, foram mantidas.

Finalmente, deve-se destacar a recente decisão do STJ, no julgamento do Agravo Regimento no Habeas Corpus nº 828.054/RN[221], julgado em 23/04/2024, a Quinta Turma decidiu, por unanimidade, a necessidade de um processo rigoroso e bem documentado na coleta, armazenamento e análise de provas digitais, especialmente em casos criminais.

A jurisprudência estabelece um precedente importante ao enfatizar que a mera autorização judicial para a extração de dados não é suficiente para garantir a validade da prova. É crucial que as autoridades policiais sigam procedimentos rigorosos e utilizem ferramentas confiáveis para garantir que as provas digitais não sejam manipuladas ou alteradas de forma alguma.

Em síntese, o STJ consolidou o entendimento de que as provas digitais são admissíveis no processo penal, desde que sua coleta, armazenamento e análise sejam realizados com rigor e observância da cadeia de custódia, utilizando métodos e ferramentas confiáveis para garantir sua autenticidade e integridade, cumprindo à risca a metodologia de coleta de dados.

Habeas Corpus nº 133.430/PE. Sexta Turma. Relator(a): Ministro Nefi Cordeiro. Data do Julgamento: 23 fev. 2021. Publicado no DJe em: 26 fev. 2021.

[221] BRASIL. Superior Tribunal de Justiça (STJ). **Agravo Regimental no Habeas Corpus nº 828054/RN**. Quinta Turma. Relator(a): Ministro Joel Ilan Paciornik. Data do Julgamento: 24 abr. 2024. Publicado no DJe em: 29 abr. 2024.

Portanto, reitera-se que as mensagens instantâneas como meio de prova são válidas, porém, prescindem de comprovação da veracidade e autenticidade do conteúdo, para que se possa saber como essa prova foi coletada, por quem e de que modo.

Ressalte-se que muito se utiliza até os dias de hoje a ata notarial para demonstrar a autenticidade de diálogos oriundos de aplicativos de mensagens. Tal documento é um meio típico de prova, ou seja, seu regramento está previsto nas normas brasileiras. Originalmente está mencionada no art. 7º, III, da Lei nº 8.935/1994[222] (Lei dos Cartórios) e no art. 384 do CPC[223]: "**Art. 384.** A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião".

É evidente que a finalidade do artigo é garantir a demonstração da realidade de fatos observados eletronicamente pelo tabelião, que possui fé-pública, a partir de seus sentidos, de modo que registre documentalmente esses fatos.[224]

Ademais, DINIZ[225] define a ata notarial como um instrumento público elaborado por um tabelião de notas, com a finalidade de documentar a veracidade de atos, fatos e até percepções do notário. Assevera ainda que a ata notarial pode ser considerada como pré-constituída, isso porque em razão da função pública que lhe é conferida, contam com fé pública, o que lhe atribui a presunção de veracidade e autenticidade.

---

[222] BRASIL. **Lei nº 8.935, de 18 de novembro de 1994**. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro. (Lei dos cartórios). Brasília, DF; nov. 1994. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8935.htm>. Acesso em: 01 mai. 2024.

[223] BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF; mar. 2015. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: 01 mai. 2024.

[224] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 133.

[225] DINIZ, Maria Helena. **Curso de direito civil brasileiro:** teoria das obrigações contratuais e extracontratuais. – 40. ed., rev. e atual. de acordo com a Lei n. 14.195/2021 - São Paulo: Saraiva, 2023.

Por sua vez, ALVIM[226] esclarece que a ata notarial é um misto de documento público com testemunho oficial que pode conter apreensão de dados ou fatos, como arquivos de imagens, som, vídeos, conteúdo da internet, entre outros.

Entretanto, no que se refere as mensagens instantâneas de aplicativos de mensagens, tem sido questionada a confiabilidade da ata notarial, isso porque ela é elaborada a partir de um testemunho não especializado, além de estarem alocadas em um ambiente volátil e complexo. A ata notarial não produz uma prova com a garantia de que seu conteúdo seja original e não tenha sido forjado ou manipulado. Isso ocorre porque o conteúdo pode estar vulnerável a fraudes que não são imediatamente detectáveis pelo notário, além de fornecer limitado material para análise em situações de contestação, possibilitando contestações sobre a validade da evidência.

Neste sentido, ROSA[227] acrescenta que a produção da ata notarial necessita cumprir com alguns requisitos:

> A produção de Ata Notarial, para fins de validade, depende do preenchimento dos requisitos legais quanto a metodologia aplicável à extração de dados. O instrumento público por si, não é suficiente, porque será necessária a determinação dos indicadores capazes de atribuir integridade, autenticidade, auditabilidade, além de observar a cadeia de custódia. O conteúdo deve ser extraído da *web* e não de eventual *print* apresentado pelo requerente.

THAMAY e TEMER[228], por sua vez, afirmam que, apesar da ata notarial gozar de autenticidade e integridade, nada impede que sejam contestadas, pois sua presunção de veracidade não é absoluta, mas relativa.

Com isso, reafirma-se a necessidade da observância de critérios e regulamentos rigorosos para preservação das evidências oriundas de

---

[226] ALVIM, Eduardo Arruda; GRANADO, Daniel Willian; FERREIRA, Eduardo Aranha. **Direito processual civil**. – 6. ed. – São Paulo: SaraivaJur, 2019. p. 647.

[227] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-A. – 1. ed. – Florianópolis: Emais, 2021. p. 439.

[228] THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020. p. 135.

mensagens instantâneas de aplicativos de mensagens, para isso, mais adiante será abordada a definição da cadeia de custódia digital e sua importância para que a validade deste tipo de evidência digital seja garantida.

2.3.3 E-mails e Comunicações Eletrônicas

O correio eletrônico, conhecido como e-mail, é um dos serviços mais antigos da internet, com origens a década de 1970, antes mesmo da rede de computadores, sendo hoje um dos serviços digitais mais utilizados no mundo todo[229]. A finalidade do serviço é a transmissão de mensagens de forma rápida.

Neste sentido, SOUZA, MUNHOZ e CARVALHO[230] descrevem em sua obra o funcionamento do e-mail da seguinte forma:

> […] o serviço de e-mail usa servidores de dados específicos, como o uso de serviço SMTP para o envio dos e-mails, e o IMAP/POP3 para receber mensagens. […] Hoje, essa complexidade fica escondida da maioria dos usuários que, em sua maioria, usam serviços de webmails como Gmail, Hotmail e Outlook. Ao realizar o envio de uma mensagem, ocorre uma comunicação entre servidores, que trocam informações e mantêm LOGs sobre essa interação. O caminho tomado pelo e-mail, da sua origem até seu destino, fica gravado em seu cabeçalho técnico, permitindo rastrear sua existência a partir dos registros mantidos nos servidores envolvidos. A identificação do usuário ocorre através de um nome, seguido de um domínio de internet, como usuarioX@gmail.com. Nesse caso, o domínio gmail.com tem servidores de dados configurados com os serviços necessários para enviar ou receber mensagens e, provavelmente, possui um “usuarioX” autorizado em seu sistema para receber mensagens. Quando o usuário não existe, recebe-se uma mensagem do servidor informando erro no encaminhamento da mensagem.

O e-mail encontra sua definição na Lei nº 11.419/2006[231], conforme previsto no §2º, inciso II, do art. 1º da referida lei:

---

[229] ALVIM, Arruda. **Manual de direito processual civil:** teoria geral do processo e o processo de conhecimento. – 17. ed. rev., atual. e ampl. – São Paulo: Revista dos Tribunais, 2019. p. 133.

[230] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 133.

[231] BRASIL. **Lei nº 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo

> **Art. 1º […] § 2º** Para o disposto nesta Lei, considera-se:
>
> II - transmissão eletrônica toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;

Acerca da validade do e-mail como prova judicial, os tribunais brasileiros divergem sobre a validade do e-mail como prova judicial, mas o entendimento predominante da jurisprudência considera que as cópias de mensagens eletrônicas, por si só, não são suficientes para comprovar fatos e situações jurídicas, necessitando de outros elementos de convicção, como documentos, comprovantes.[232]

Neste sentido, o Superior Tribunal de Justiça (STJ) sedimentou a orientação de que o e-mail é capaz de fundamentar ações judiciais, desde que o juízo se convenças da verossimilhança das alegações e da idoneidade das declarações contidas nos autos:

> RECURSO ESPECIAL. AÇÃO MONITÓRIA. PROVA ESCRITA. JUÍZO DE PROBABILIDADE. CORRESPONDÊNCIA ELETRÔNICA. E-MAIL. DOCUMENTO HÁBIL A COMPROVAR A RELAÇÃO CONTRATUAL E A EXISTÊNCIA DE DÍVIDA. 1. A prova hábil a instruir a ação monitória, isto é, apta a ensejar a determinação da expedição do mandado monitório - a que alude os artigos 1.102-A do CPC/1.973 e 700 do CPC/2.015 -, precisa demonstrar a existência da obrigação, devendo o documento ser escrito e suficiente para, efetivamente, influir na convicção do magistrado acerca do direito alegado, não sendo necessário prova robusta, estreme de dúvida, mas sim documento idôneo que permita juízo de probabilidade do direito afirmado pelo autor. 2. **O correio eletrônico (e-mail) pode fundamentar a pretensão monitória, desde que o juízo se convença da verossimilhança das alegações e da idoneidade das declarações, possibilitando ao réu impugnar-lhe pela via processual adequada**. 3. O exame sobre a validade, ou não, da correspondência eletrônica (e-mail) deverá ser aferida no caso concreto, juntamente com os demais

judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF; dez. 2006. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm>. Acesso em: 01 mai. 2024.

[232] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 134.

> elementos de prova trazidos pela parte autora. 4. Recurso especial não provido. (REsp n. 1.381.603/MS, relator Ministro Luis Felipe Salomão, Quarta Turma, julgado em 6/10/2016, DJe de 11/11/2016.)[233] **(grifo nosso)**

No referido julgado, o relator, Ministro Luis Felipe Salomão, abordou a questão da validade do uso do e-mail como prova em ações monitórias. Ele destacou que a lei não exige que a prova seja robusta ou livre de dúvidas, mas sim que seja idônea e capaz de formar um juízo de probabilidade sobre o direito afirmado. O ministro reconhece que os e-mails podem ser questionados em relação à sua autenticidade, mas defende que essa avaliação deve ser feita caso a caso, juntamente com outras provas apresentadas.[234]

Ainda, acrescentou que “há mecanismos capazes de garantir a segurança e a confiabilidade da correspondência eletrônica e a identidade do emissor, permitindo a trocas de mensagens criptografadas entre os usuários”, citando como exemplo o e-mail assinado digitalmente com certificado digital.[235]

Portanto, compreende-se que, se a legislação brasileira não vedou a utilização de documentos eletrônicos como meio de prova, seria irrazoável dizer que uma relação negocial não possa ser comprovada por trocas de mensagens via e-mail. Isto posto, cumpre abordar acerca das provas de geolocalização.[236]

2.3.4 Provas de Geolocalização

A geolocalização utiliza dados de posição geográfica para determinar a localização de dispositivos ou indivíduos, podendo ser obtida por

---

[233] BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.381.603/MS**. Quarta Turma. Relator(a): Ministro Luis Felipe Salomão. Data do Julgamento: 06 out. 2016. Publicado no DJe em: 11 nov. 2016.

[234] BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.381.603/MS**. Quarta Turma. Relator(a): Ministro Luis Felipe Salomão. Data do Julgamento: 06 out. 2016. Publicado no DJe em: 11 nov. 2016.

[235] BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.381.603/MS**. Quarta Turma. Relator(a): Ministro Luis Felipe Salomão. Data do Julgamento: 06 out. 2016. Publicado no DJe em: 11 nov. 2016.

[236] BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.381.603/MS**. Quarta Turma. Relator(a): Ministro Luis Felipe Salomão. Data do Julgamento: 06 out. 2016. Publicado no DJe em: 11 nov. 2016.

diversas tecnologias, como internet, GPS e radiofrequência. Presente em dispositivos móveis como *smartphones* e *smartwatches*, a geolocalização é fundamental para aplicativos de navegação e tem sido cada vez mais utilizada como prova em processos judiciais, devido à sua ampla aplicação e ao grande volume de dados gerados.[237]

Nas palavras de SOUZA, MUNHOZ e CARVALHO[238], o uso de dados de geolocalização como prova digital decorre, principalmente, da carência da prova testemunhal no direito brasileiro, muitas vezes incapaz de contribuir para esclarecer os fatos. Até recentemente, era comum o arrolamento de testemunhas para provar a presença de determinada pessoa em uma localidade, mas existem muitos problemas nesse caminho. Acerca das testemunhas, os autores complementam da seguinte forma:

> As testemunhas podem se lembrar de fatos de forma imprecisa ou distorcida; mentir ou omitir; mudar suas histórias ao longo do tempo; fornecer informações diversas em depoimentos diferentes; exagerar propositalmente ao relatar um acontecimento ou mesmo se confundir ao descrever detalhes importantes. Há ainda a possibilidade de se deixar levar por seus interesses, opiniões e crenças, o que afeta a confiabilidade daquilo que relatam em juízo.[239]

No tocante à validade da prova judicial nos tribunais, é preciso compreender que possui entendimento distintos em três áreas do direito, são elas: civil, penal e do trabalho.

No âmbito civil, a geolocalização é utilizada para determinar a localização de bens e pessoas, identificar fraudes em contratos e delimitar propriedades rurais. As Câmaras Cíveis têm autorizado o uso desses dados em processos judiciais, especialmente em litígios bancários, para comprovar a

---

[237] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 149.

[238] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 149.

[239] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 149-150.

solicitação de empréstimos, muitas vezes em conjunto com a biometria facial. A ausência de perícia na geolocalização não é considerada, em algumas Câmaras, como cerceamento de defesa.[240]

No âmbito penal, por sua vez, a geolocalização auxilia órgãos de persecução penal na investigação e comprovação de crimes, identificação de envolvidos, localização de testemunhas e vítimas, e reconstrução de rotas. A defesa pode utilizar esses dados para apresentar álibis, refutar depoimentos e fortalecer a linha de defesa. A admissibilidade da geolocalização como prova em casos penais tem sido objeto de decisões recentes do STJ[241] e STF[242], com diferentes entendimentos sobre a necessidade de quebra de sigilo e a proporcionalidade da medida.[243]

Já no âmbito trabalhista, a geolocalização é utilizada para comprovar a presença do empregado no local de trabalho, o cumprimento da jornada de trabalho e a observância de regras de segurança. Há divergência entre os Tribunais Regionais do Trabalho sobre a extração de dados de geolocalização de dispositivos dos reclamantes, sendo admitida apenas em casos excepcionais, quando outras provas são insuficientes para esclarecer os fatos.[244]

Isto posto, vale destacar as lições de REBELLATO[245], o qual explica que a utilização de instrumentos investigativos para a geolocalização de

---

[240] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 149-150.

[241] O STJ compreende que a a quebra do sigilo de dados de geolocalização é adequada, necessária e proporcional em casos nos quais inexiste outra medida cabível para desvendar o delito (AgRg no RMS 68487/PE), sendo considerada menos invasiva que a interceptação telefônica, modalidade que dá acesso ao fluxo de comunicações de dados e o conhecimento do conteúdo integral da conversa (AgRg no RMS 67093/MT).

[242] Para o STF, a quebra de sigilo de dados de geolocalização é objeto de discussão no RE 1.301.250 RG/RJ, sob a relatoria da Ministra Rosa Weber, que teve repercussão geral reconhecida (tema 1.148) em junho de 2021. O leading case até o momento não foi submetido a julgamento.

[243] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 151.

[244] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 151-152.

[245] REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais:** o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado em Direito). 2020. 305 f. Faculdade de Direito, Universidade de São Paulo, São Paulo,

pessoas vem sendo alvo de intensos debates no cenário jurisprudencial norte-americano:

> Em United States vs. Jones 565 U.S. 400 (2012), a Suprema Corte julgou que a instalação de um dispositivo de Global Positioning System (GPS) em um veículo de um suspeito, a fim de monitorar seus deslocamentos, constituiria uma modalidade de “search and seizure” protegida pela Fourth Amendment, o que exigiria uma prévia autorização judicial para a utilização do referido meio de produção de prova. […] a Suprema Corte reconheceu, por apertada maioria, a necessidade de ordem judicial lastreado em “probable cause”, para a aquisição de dados digitais atinentes à movimentação das pessoas, através dos registros das torres de chamadas dos aparelhos celulares, não sendo aplicável a extensão da “third party doctrine” quanto aos registros mantidos pela operadora de telefonia celular.

Portanto, compreende-se que os dados de geolocalização são uteis para o esclarecimento de fatos que não puderam ser demonstrados pela prova testemunhal e podem ser obtidos através de outros bancos de dados (ERBs).

2.4 NORMAS LEGAIS SOBRE PROVAS DIGITAIS

Encerrando o presente capítulo, cumpre apresentar brevemente algumas das normas legais presentes no ordenamento jurídico brasileiro de grande importância para as provas digitais. Vale frisar que a legislação sobre provas digitais no Brasil é relativamente nova e ainda está em desenvolvimento.

Dentre as normas legais que possuem conexão ou relevância nas provas digitais, pode-se destacar as seguintes: a) MP nº 2.200-2/2001; b) Lei n° 11.419/2006; c) Lei n° 12.682/2012; d) Lei n° 12. 965/2014; e) Lei n° 13.694/2019. Assim, cumpre abordar brevemente as referidas normas.

Iniciando pela MP nº 2.220-2/2001, que regulamenta a utilização de certificados digitais e a Infraestrutura de Chaves Públicas Brasileira

---

2020. p. 125-126.

(ICP-Brasil). De acordo com SOUZA, MUNHOZ e CARVALHO[246], a medida estabelece os requisitos técnicos e de segurança para a emissão, uso e validação de certificados digitais, e dispõe também sobre chaves criptográficas.

PINHEIRO[247] ensina em sua obra que a MP nº 2.200-2/2001 foi responsável pela instituição da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), cuja finalidade é descrita em seu art. 1º: "para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras".[248]

ARAUJO[249] ensina que a MP nº 2.200-2/2001 é a legislação que trata do trânsito de documentos em forma eletrônica, sendo a responsável pela criação da Infraestrutura de Chaves Públicas (ICP-Brasil), visando garantir a "a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras".

Outra norma importante para o instituto da prova digital é a Lei nº 11.419/2006[250], também conhecida como Lei do Processo Eletrônico, a qual regulamenta o emprego de meios eletrônicos no processo judicial, dispondo sobre a realização de atividades processuais eletrônicas e definindo as regras para a validade jurídica das informações eletrônicas.[251]

---

[246] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 221-222.

[247] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 154.

[248] BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF; ago. 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em: 01 jun. 2024.

[249] ARAÚJO, Marcelo Barreto de. **Comércio eletrônico, Marco Civil da internet, Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviços e Turismo, 2017. p. 149.

[250] BRASIL. **Lei nº 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF; dez. 2006. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm>. Acesso em: 01 jun. 2024.

[251] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de**

Essa lei representa um marco na modernização do sistema judiciário brasileiro, pois, ao regulamentar o uso de meios eletrônicos no processo judicial, a lei viabilizou a prática de atos processuais de forma digital, como a distribuição de petições por meio eletrônico.

Em 2012, surge a Lei nº 12.682/2012[252], a qual estabelece as regras para a elaboração e arquivamento de documentos em meios eletrônicos, determinando que documentos elaborados e armazenados eletronicamente possuem a mesma validade jurídica de documentos em papel, desde que cumpram certas exigências técnicas.[253]

Essa equiparação jurídica contribui para a desmaterialização dos processos, promovendo a eficiência e a celeridade na administração pública e privada, além de reduzir custos e o impacto ambiental.

Ressalte-se que essa lei exige a utilização de tecnologias como a assinatura digital e o certificado digital, a fim de garantir a autenticidade, integridade e, quando necessário, a confidencialidade dos documentos eletrônicos, assegurando a segurança jurídica das relações estabelecidas nesse formato (art. 3º).

Ademais, a norma legal que merece destaque é a Lei nº 12.965/2014[254], também conhecida como o Marco Civil da Internet. Esta lei é considerada uma espécie de “Constituição da Internet no Brasil”, regulamentando,

---

provas digitais. São Paulo: Thomson Reuters Brasil, 2023. p. 221-222.

[252] BRASIL. **Lei nº 12.682, de 9 de julho de 2012**. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Brasília, DF; jul. 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm>. Acesso em: 01 jun. 2024.

[253] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 221-222.

[254] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF; abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 jun. 2024.

entre outras, questões como a liberdade de expressão, a privacidade, a responsabilidade civil e a neutralidade da rede.[255]

De acordo com as lições de ARAUJO[256], A internet, outrora considerada um "território livre", tem sido progressivamente regulamentada, transformando-se em um espaço de "liberdade vigiada". Essa mudança decorre da constatação de que o ambiente virtual é palco de diversas atividades, incluindo a prática de crimes, o que exige a aplicação de regras e a garantia de segurança jurídica.

Para o autor, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, surgiu para preencher essa lacuna, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no Brasil. A lei também define diretrizes para a atuação do Poder Público, visando garantir o acesso universal à rede.

Assim, percebe-se que o Marco Civil da Internet proporcionou uma base legal para o Poder Judiciário, permitindo a resolução de conflitos entre provedores de internet e usuários de forma mais consistente e fundamentada, em contraste com as decisões anteriores, muitas vezes contraditórias, baseadas em interpretações do Código Civil e do Código de Defesa do Consumidor.

De acordo com REBELLATO[257], o Marco Civil da Internet, buscou disciplinar os princípios, garantias, direitos e deveres no ambiente virtual, sendo pioneira como forma de se regulamentar as diretrizes para atuação do Estado, as relações em ambiente virtual e a disciplina da internet no Brasil.

---

[255] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 221-222.

[256] ARAÚJO, Marcelo Barreto de. **Comércio eletrônico, Marco Civil da internet, Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviços e Turismo, 2017. p. 83-85.

[257] REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais:** o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado em Direito). 2020. 305 f. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020. p. 120.

Após o Marco Civil da Internet, surge o Decreto nº 8.771/2016[258], o qual regulamenta o Marco Civil para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

Finalmente, cabe destacar a Lei nº 13.694/2019, conhecida como o Pacote Anticrime. Embora não seja uma lei específica sobre provas digitais, o Pacote Anticrime é relevante porque trata da cadeia de custódia, elencando as etapas que devem ser cumpridas para manter e documentar a história cronológica dos vestígios.[259]

Abordados os principais aspectos da teoria da prova e das provas digitais, cumpre abordar no próximo capítulo sobre a qualificação e tratamento das provas digitais, cujo enfoque será sobre a cadeia de custódia.

---

[258] BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF; mai. 2016. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 01 jun. 2024.

[259] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 221-222.

Capítulo 3

AQUISIÇÃO E QUALIFICAÇÃO DE PROVAS DIGITAIS

A prova digital válida (E-Evidencia) é governada a partir da observação do meio a que se destina, da confiabilidade e da superação dos testes de verificação. Já o tratamento da E-Evidencia, consiste na aquisição adequada da prova e observação criteriosa dos requisitos técnicos estabelecidos pela ABNT NBR ISO/IEC 27037:2013[260]: auditabilidade, reprodutibilidade, repetibilidade, justificabilidade e da cadeia de custódia digital, isto é, todos os processos utilizados nas etapas de qualificação de provas digitais devem ser auditáveis, repetíveis, justificáveis e reprodutíveis e seguir os critérios da cadeia de custódia, evitando assim, sua quebra.[261]

Dito isso, este capítulo pretende esclarecer inicialmente sobre a cadeia de custódia como instrumento essencial para validade das provas de modo amplo, partindo para as especificidades da cadeia de custódia digital, que ficará evidente sua complexidade ante as provas tradicionais e, portanto, a ineficácia da aplicação isolada da Lei nº 13.694/2019, apelidada como pacote anticrime, que tratou da cadeia de custódia, que deixou de abordar de modo específico e apartado, sobre as provas digitais.

Seguindo então para o objetivo principal desta dissertação, que é destrinchar não apenas a norma ABNT NBR ISO/IEC 27037:2013, mas também com o suporte de normas internacionais, para fins de identificar a(s) forma(s) correta(s) de tratamento da prova digital, de modo que preserve sua

---

[260] BRASIL. Associação Brasileira de Normas Técnicas. **ABNT ISO/IEC 27037:2013**. Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. São Paulo: ABNT, 2013.

[261] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-A. – 1. ed. – Florianópolis: Emais, 2021. p. 437.

integridade. Ao final, pretende-se apresentar soluções tecnológicas para o tratamento das provas (evidências) digitais.

3.1 CADEIA DE CUSTÓDIA

A cadeia de custódia é um procedimento fundamental para garantir a integridade e a confiabilidade das provas digitais, assegurando sua validade no processo judicial. Em um Estado Democrático de Direito, a busca pela verdade não pode justificar a utilização de meios ilícitos, especialmente em investigações criminais. É dever do servidor da justiça buscar a verdade por meios legais e legítimos, preservando a integridade das provas e respeitando os direitos e garantias fundamentais dos envolvidos.

Neste sentido, GRINOVER[262] assevera que “a investigação criminal e a luta contra a criminalidade devem ser conduzidas de acordo com um rito probatório legalmente predeterminado”.

O conceito de cadeia de custódia surpreendeu ao vir introduzido na Lei nº 13.964/2019[263], conhecida como o “Pacote Anticrime”, que incluiu ao Código de Processo Penal os arts. 158-A a 158-F:

> 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 referida introdução da cadeia de custódia, de forma expressa, determinada e detalhada no Código de Processo Penal, MATIDA[264] esclarece que:

---

[262] FERNANDES, Antônio Scarance.; GRINOVER, Ada Pelegrini; FILHO, Antônio Magalhães Gomes. **As nulidades no processo penal**. São Paulo: Revista dos Tribunais, 2011. p. 58.

[263] BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF; dez. 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm>. Acesso em: 06 mai 2024.

[264] MATIDA, Janaina. **A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes**. Boletim IBDCRIM, Ano 28, n. 331, p. 6-9, jun. 2020, p. 7.

> No dia 24 de dezembro de 2019 fomos surpreendidos pela sanção presidencial da Lei 13.964, apelidada pelo então Ministro da Justiça como “Pacote Anticrime”. Ainda que não seja possível ignorar a presença de contundentes retrocessos na legislação em questão, a surpresa a que me refiro foi sobre alguns aspectos positivos: de certo modo, a chegada do juiz das garantias, a eficaz blindagem ao *pleabargaining* e, finalmente, a previsão legislativa da cadeia de custódia das provas renovaram o fôlego dos que anseiam por um sistema de justiça genuinamente acusatório. Enquanto não podemos festejar a integral substituição de um sistema com flagrante raiz inquisitorial por um sistema de justiça verdadeiramente sintonizado com a Carta Constitucional de 1988, resta-nos dirigir esforços a otimizar os efeitos destas mudanças que chegam a conta-gotas.

Apesar do conceito ser expressamente introduzido no Brasil em lei, apenas em 2019 com o Pacote Anticrime, a cadeia de custódia é um instituto de proteção e preservação abordado há muitos anos pela doutrina nacional e internacional. Seu destaque nos surge nos anos 90, após um ex-jogador de futebol americano ser absolvido da acusação de homicídio contra sua ex-esposa e outro homem.[265]

No Brasil, Geraldo Prado e o julgamento do Habeas Corpus nº 160.662/RJ[266] do STJ, são destaques do início da abordagem da importância da cadeia de custódia das provas. Em 2014, a Portaria nº 82 do Ministério da Justiça já definiu a cadeia de custódia como o “conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte”. [267]

---

[265] Em 1994, o ex-jogador de futebol americano O.J. Simpson foi investigado, acusado e processado por duplo homicídio, sendo absolvido das acusações em função da forte argumentação da defesa de que a preservação do local do crime e os procedimentos de coleta de vestígios foram realizados de forma incorreta e inadequada, evidenciando uma falha na cadeia de custódia das provas. In: FONSECA, Gabriel Ciríaco. **O delegado de polícia e a cadeia de custódia**. Consultor Jurídico (ConJur), 27 jun. 2022. Disponível em: <https://www.conjur.com.br/2022-jun-27/gabriel-ciriaco-delegado-cadeia-custodia/>. Acesso em: 04 jun. 2024.

[266] BRASIL. Superior Tribunal de Justiça (STJ). **Habeas Corpus nº 160.662/RJ**. Sexta Turma. Relator(a): Ministra Assusete Magalhães. Data do Julgamento: 18 fev. 2014. Publicado no DJe em: 17 mar. 2014.

[267] BRASIL. Ministério da Justiça. **Portaria nº 82, de 25 de março de 2014**. Estabelece normas e procedimentos para a cadeia de custódia de vestígios. Diário Oficial da União, Brasília, DF, 26

Depreende-se desde já que a cadeia de custódia não é um instituto exclusivo das provas digitais ou da informatização processual, faz parte da teoria geral da prova como elemento essencial para a validação de provas no sentido amplo.[268]

MATIDA[269] conceitua a cadeia de custódia como a documentação cronológica do vestígio, que assegurará que a evidência ou o vestígio chegue à instrução probatória revestidos de confiabilidade.

ROSA e CANI[270] define a cadeia de custódia como o conjunto de medidas que asseguram a rastreabilidade, integridade e autenticidade das evidências, as quais garantem que essas evidências não sejam adulteradas, contaminadas ou substituídas desde sua coleta até a produção em juízo, cuja inobservância pode mitigar ou quebrar a eficácia probatória.[271]

Por sua vez, EDINGER[272] leciona que a cadeia de custódia é composta de elos:

> […] a cadeia de custódia é composta de elos, que dizem respeito a um vestígio que, por sua vez, eventualmente, será considerado uma prova. Um elo é qualquer pessoa que tenha manejado esse vestígio. É dever do Estado – e, também, direito do acusado, identificar, de maneira coerente e concreta, cada elo, a partir do momento no qual o vestígio foi encontrado. Assim, fala-se em cadeia de custódia íntegra quando se fala em uma sucessão de elos provados.

---

mar. 2014. Seção 1. p. 3.

[268] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 208.

[269] MATIDA, Janaina. **A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes**. Boletim IBDCRIM, Ano 28, n. 331, p. 6-9, jun. 2020, p. 7.

[270] ROSA, Alexandre Morais da; CANI, Luiz Eduardo. **Guia para Mitigação dos Erros Judiciários no Processo Penal**: as causas prováveis e as estratégias de enfrentamento. Florianópolis: Emais, 2021. p. 2.

[271] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-A. – 1. ed. – Florianópolis: Emais, 2021. p. 400.

[272] EDINGER, Carlos. **Cadeira de custódia, rastreabilidade probatória**. Revista brasileira de ciências criminais, v. 24, n. 120, p. 237-257, mai./jun., 2016. p. 252-254.

É fundamental a preservação das fontes de prova, especialmente com aquelas produzidas fora do processo, como por exemplo, a coleta de DNA e a intercepção telefônica. A preservação das evidências é a verdadeira condição de validade probatória.[273]

PRADO[274], ensina que qualquer modificação na fonte da evidência, contamina seus meios. A falta de cuidado com a preservação dessas fontes, descredibiliza a confiabilidade desses meios. E o “livre convencimento motivado” não pode servir como muleta para que provas contaminadas possam servir como fundamento de uma condenação, isso porque existem critérios de validade que limitam o poder decisório, a fim de evitar eventuais discricionaridades.

LOPES JUNIOR[275], defende a importância da cadeia de custódia para os processos criminais como um mecanismo que minimiza a subjetividade e a discricionariedade das decisões. Isso porque, depender simplesmente da boa-fé ou má-fé dos agentes policiais/estatais fragiliza as decisões, deixando aberto o campo da injustiça. Portanto, a cadeia de custódia, ao determinar regras claras e objetivas, protege o decisionismo.

Os princípios que envolvem a cadeia de custódia são: a) princípio da mesmidade (e não mesmice); e b) princípio da desconfiança. O primeiro se refere à garantia de que a prova valorada nos autos do processo é exatamente a mesma que foi coletada, ou seja, sem nenhuma alteração. A manipulação inadequada da prova coletada e original, pode violar a mesmidade, quebrando a cadeia de custódia. [276]

---

[273] LOPES JUNIOR, Aury. **Direito processual penal**. – 18. ed. – São Paulo, SaraivaJur, 2021. p. 490.

[274] PRADO, Geraldo. **Prova penal e sistema de controles epistémicos:** a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2024. p. 94.

[275] LOPES JUNIOR, Aury. **Direito processual penal**. – 18. ed. – São Paulo, SaraivaJur, 2021. p. 491.

[276] PRADO, Geraldo. **Prova penal e sistema de controles epistémicos:** a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2024. p. 94.

Já o segundo princípio, da desconfiança, é a exigência de que toda prova deve ser “acreditada”, isto é, que a prova somente possa ser valorada caso tenha passado por procedimentos que demonstrem que de fato aquela prova corresponde ao que a parte alega ser.[277]

É possível então concluir até aqui, que garantir a integridade e a mesmidade da prova é o principal objetivo da cadeia de custódia.

Para compreender de fato os procedimentos da cadeia de custódia, cabe aqui destrinchar os artigos introduzidos no Código de Processo Penal, pela Lei nº 13.964/2019 que formalizou e consolidou este instrumento de grande relevância para a justiça, trazendo os requisitos de validade das evidências produzidas.

Inicialmente, o §1º do art. 158-A do CPP[278] apresenta que “O início da cadeia de custódia dá-se com a preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio”. Na sequência, o §3º do mesmo dispositivo define que “vestígio é todo material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal”.

Cabe aqui uma ressalva, a definição de vestígio (dados de realidade) veio introduzida na norma de forma estreita, quando na verdade, deve ser analisada de forma mais ampla.

Ao definir que o vestígio é "todo material bruto, visível ou latente" implica que o vestígio é algo físico e tangível, ainda os que são latentes, que não são imediatamente visíveis a olho nu, após técnicas específicas, são componentes físicos. Entretanto, nem todo vestígio é palpável, como por exemplo as mensagens de aplicativos de mensagens, e-mails, interceptações telefônicas

---

[277] PRADO, Geraldo. **Prova penal e sistema de controles epistémicos:** a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2024. p. 94.

[278] BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, RJ; out. 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 18 mai. 2024.

etc. Não há razão para deixar de reconhecê-los como vestígios.[279] Portanto, aqui serão alcançados todos os tipos de vestígios inclusive (e especialmente) os imateriais e intangíveis (dados digitais).

Os vestígios são definidos então, como qualquer dado de realidade, como por exemplo, digitais, DNA, instrumentos, mídias, arquivos de vídeo, etc. Quando esses vestígios são analisados, tornam-se uma informação (evidência).[280]

A partir disso, o conjunto de atos da cadeia de custódia, segundo o artigo 158-B do CPP [281]consiste em: 1. Reconhecimento; 2. Isolamento;

---

[279] MATIDA, Janaina. **A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes**. Boletim IBDCRIM, Ano 28, n. 331, p. 6-9, jun. 2020, p. 7.

[280] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-A. – 1. ed. – Florianópolis: Emais, 2021. p. 400.

[281] **Art. 158-B.** A cadeia de custódia compreende o rastreamento do vestígio nas seguintes etapas:

I - reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;

II - isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;

III - fixação: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;

IV - coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza;

V - acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;

VI - transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;

VII - recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;

VIII - processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;

IX - armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;

X - descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e,

3. Fixação; 4. Coleta; 5. Acondicionamento; 6. Transporte; 7. Recebimento; 8. Processamento; 9. Armazenamento; 10. Descarte: [282]

Segundo as lições de LIMA[283], o reconhecimento é o rastreamento do elemento, para fins de distinguir aquilo que é e o que não é relevante para a produção da prova. Por exemplo, a arma, o sangue ou o celular.

O isolamento, por sua vez, é a preservação do ambiente de forma imediata, para deixá-lo imaculado/puro. Já a fixação é a descrição detalhada de como o vestígio se encontra, podendo ser registrada por fotos, filmagens ou croquis, por exemplo, o perito fotografa a faca e faz um desenho demostrando sua posição exata no local do crime, tudo pormenorizado no laudo pericial.

Ademais, a coleta é considerada como o ato de recolher o vestígio, que deve ser, preferencialmente, realizada por um perito. Após o processo de coleta, passa-se ao acondicionamento, que é o ato de embalar o vestígio de forma adequada, ou seja, de acordo com as características da sua natureza, devendo constar a anotação de data e nome de quem acondicionou.

Quando a prova estiver devidamente acondicionada, passa-se para o transporte, isto é, a transferência do vestígio, em condições adequadas, que assegurem sua imutabilidade até o órgão responsável, IML, por exemplo.

Após, é feito o recebimento da prova, ato formal da transferência para o órgão responsável pela análise do vestígio com as seguintes informações: número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu.

---

quando pertinente, mediante autorização judicial.

[282] BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal**.** Acesso em: 18 mai. 2024.

[283] LIMA, Renato Brasileiro de. **Manual de Processo Penal:** volume único. – 8. ed. rev., ampl. e atual. – Salvador: JusPodivm, 2020. p. 723-725.

As últimas etapas são o processamento, que é a análise em si do vestígio, geralmente o exame pericial; seguida pelo armazenamento, isto é, a guarda em condições adequadas para eventual contraperícia. E, por fim, o descarte, é a liberação do vestígio.[284]

É evidente que o vestígio durante toda essa trajetória pode passar por mãos e profissionais diferentes, no entanto, a mera alternância de profissionais que tiveram acesso aos vestígios não viola o procedimento, tampouco a ausência de menção no relatório dessa alternância.[285]

Todas as etapas devem ser documentadas de forma cronológica, respeitando-se as características físicas e biológicas de cada vestígios, tendo sempre como máxima, a garantia da sua integridade. Além de todas as etapas, a documentação deve detalhar as circunstâncias pelas quais os vestígios foram colhidos, a identidade de todos os profissionais que manipularam o vestígio, a data e a hora de cada etapa, determinando-se a duração, a segurança do armazenamento e a forma de transporte aos curadores sucessivos.[286]

O protocolo documental da cadeia de custódia, deve registrar os seguintes indicadores: "*a) quem; b) quando; c) como; d) onde; e) por que; f) para que; g) o que; h) com que motivação."* [287] A conferência desses indicadores irá garantir a existência, eficácia e validade da cadeia de custódia.

Acerca das consequências da quebra da cadeia de custódia, a Lei nº 13.964/2019 é silente, apesar da consolidação importantíssima de todos os procedimentos e etapas. Sobre esse prisma, existem vertentes dogmáticas que divergem entre si. Para os chamados "juristas garantistas" como é o caso de Aury

---

[284] LIMA, Renato Brasileiro de. **Manual de Processo Penal:** volume único. – 8. ed. rev., ampl. e atual. – Salvador: JusPodivm, 2020. p. 723-725.

[285] BADARÓ, Gustavo Henrique. **Processo Penal**. – 9. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2021. p. 703.

[286] BADARÓ, Gustavo. **A cadeia de custódia e sua relevância para a prova penal**. In: SIDI, Ricardo; LOPES, Anderson Bezerra. **Temas atuais da investigação preliminar no processo penal**. – 1. reimpr. – Belo Horizonte: D'Plácido, 2018. p. 517-538.

[287] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-C. p. 401.

Lopes Junior e Alexandre Morais da Rosa, entendem que qualquer ruptura das etapas previstas em Lei, consiste na declaração de ilicitude ou ilegitimidade da prova e consequente imediata e inafastável exclusão (desentranhamento dos autos, se for o caso) e dos que dele decorrem, a conhecida teoria da árvore dos frutos envenenados. Já para os chamados juristas mais punitivistas, entendem que caberá ao julgador, de acordo com o caso concreto, valorar e decidir sobre a prova obtida com irregularidades na cadeia de custódia.[288]

Entretanto, é importante destacar que nem toda irregularidade da custódia, automaticamente, quebra a cadeia de custódia. Nos casos em que, apesar da inobservância de determinado critério legal, esteja mantida a mesmidade, a credibilidade e a confiabilidade, poderá ser validada.

No mesmo sentido dos efeitos da quebra da cadeia de custódia, a confirmação dessa quebra, diverge entre os processualistas. Os garantistas, entendem que, na dúvida sobre a extensão do efeito, prevalece a presunção de inocência, ou seja, na dúvida, o imputado deve ser favorecido. Já para os punitivistas, a inobservância dos critérios legais, somente irá quebrar a cadeia de custódia caso seja demonstrado o prejuízo da confiabilidade, mesmidade e credibilidade.

Neste sentido, CHAVES JUNIOR, DE PAULA e PÁDUA[289] abordam sobre o art. 563 do CPP, onde está presente o princípio do prejuízo, que define que não há que se falar em ineficácia do ato ou do processo sem prejuízo (*pas de nullité sans grief*). Segundo os autores, o referido postulado tem servido no Brasil para que juízes e tribunais estabeleçam dúvidas sobre a existência de nulidades relativas ou absolutas, valendo-se da prova do prejuízo que, nestes casos, transfere o ônus ao acusado, o que fragiliza a necessária imparcialidade do julgador e viola o devido processo legal:

---

[288] MATIDA, Janaina. **A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes**. Boletim IBDCRIM, Ano 28, n. 331, p. 6-9, jun. 2020, p. 8.

[289] CHAVES JUNIOR, Airto; DE PAULA, Leonardo Costa; PÁDUA, Thiago Aguiar de. **O prejuízo da "regra do prejuízo"**: a não recepção constitucional do art. 563 do Código de Processo Penal (*pas de nullité sans grief*). Revista Brasileiro de Ciências Criminais, Ano 29, v. 182, p. 163-190, ago. 2021.

> Se a Constituição é a norma que mais vale; se é ela quem deve determinar e conduzir a interpretação do ordenamento jurídico infraconstitucional; e, se o devido processo legal substancial determina que a forma é garantida do acusado, especialmente quanto aos vetores relacionados ao Código de Processo Penal, e não havendo preponderância de um suposto postulado principiológico (como o *pas de nulitté sans grief*) então o artigo 563 do CPP deve ser interpretado no sentido de se presumi o prejuízo ao acusado. Deve-se, a partir disso, decretar-se a nulidade sempre que se verifique a violação do rito/forma em temas ligados à "medula óssea" ou "espinha dorsal" do Processo Penal: competência, quebra da parcialidade, cerceamento de defesa, constrição da liberdade pessoal ou de direito patrimonial, prova, julgamento e fundamentação das decisões judiciais.

Essa regra da prova do prejuízo afasta até mesmo a presunção de inocência, pois obriga o acusado a produzir uma prova impossível, já que o "prejuízo" é cláusula genérica de extrema indeterminação. Tanto que doutrina jurisprudência brasileiras não conceituam essa categoria, apenas se ocupam em dizer que não é prejuízo. Exige-se, dessa forma, que o acusado demonstre coisa que não se sabe, bem ao certo, o que é realmente.[290]

Dessa forma, percebe-se que, num sistema que tem por objetivo precípuo a proteção das garantias do imputado, não se pode obrigar que a parte mais frágil dessa relação seja obrigada a produzir prova de tal prejuízo. Até mesmo porque, conforme afirmam os autores, sabe bem ao certo o que esse prejuízo significa.[291]

Nesse sentido, REIS e GONÇALVES [292] ressaltam acerca da inobservância das recomendações legais:

---

[290] CHAVES JUNIOR, Airto; DE PAULA, Leonardo Costa; PÁDUA, Thiago Aguiar de. **O prejuízo da "regra do prejuízo"**: a não recepção constitucional do art. 563 do Código de Processo Penal (*pas de nullité sans grief*). Revista Brasileiro de Ciências Criminais, Ano 29, v. 182, p. 163-190, ago. 2021.

[291] CHAVES JUNIOR, Airto; DE PAULA, Leonardo Costa; PÁDUA, Thiago Aguiar de. **O prejuízo da "regra do prejuízo"**: a não recepção constitucional do art. 563 do Código de Processo Penal (*pas de nullité sans grief*). Revista Brasileiro de Ciências Criminais, Ano 29, v. 182, p. 163-190, ago. 2021.

[292] REIS, Alexandre Cebrian Araújo. **Direito processual penal**. – 11. ed. – São Paulo: SaraivaJur,

> É extremamente importante ressaltar que a inobservância das recomendações legais relativas à cadeia de custódia do vestígio 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.

A autora que esta subscreve, em razão da ausência de norma concreta sobre o tema, pugna pela declaração imediata de ilicitude ou ilegitimidade, com a consequente exclusão dos autos, tanto das provas ilícitas ou ilegítimas em si, como das dela decorrentes.

E, no mesmo sentido, sob a lente de um Estado Democrático de Direito, a presunção de inocência sempre deverá prevalecer, de modo que, atitudes relapsas, negligentes, imprudentes ou imperitas dos agentes policiais/estatais que acarretem defeito na cadeia de custódia, na dúvida dos efeitos, devem beneficiar o imputado e não o prejudicar, isso porque, seria como dar suporte a uma hipótese possivelmente inverídica, dando ensejo ao risco de condenação de inocentes. É dever do Estado garantir a integridade da cadeia de custódia das provas e tomar atitudes que mitiguem eventual quebra dos elos.

Feitas até aqui, as principais ponderações acerca do instrumento da cadeia de custódia das provas em âmbito geral, a seguir, adentrar-se-á ao centro da pesquisa, a cadeia de custódia das provas digitais.

3.2 CADEIA DE CUSTÓDIA DA PROVA DIGITAL

Apesar de abordar com clareza a cadeia de custódia dos vestígios tradicionais, a Lei nº 13.964/2019 pecou ao não dedicar um espaço específico para os vestígios digitais, tendo em vista que na época em que foi publicada (2019), as provas digitais já eram protagonistas nos processos judiciais. Segundo dados estatísticos da Convenção de Budapeste de 2018[293], em média 85% das investigações criminais dependem de provas digitais.

2022. p. 600.

[293] CONVENÇÃO DE BUDAPESTE**. Convenção sobre o Cibercrime**. Budapeste, 2018. Disponível em: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>. Acesso em: 19 mai.

Como dito anteriormente, a introdução dos novos artigos inicia de forma errônea ao restringir o conceito de vestígio como objetos materiais e tangíveis, praticamente excluindo as provas digitais, sendo que, diante da complexidade e alto grau de vulnerabilidade das provas digitais, exigem uma cadeia de custódia ainda mais detalhada.[294]

O isolamento da cadeia de custódia determina que o vestígio seja isolado e reservado, entretanto, a plurissubjetividade dos materiais informáticos é bastante comum, ainda que quanto menor a quantidade de pessoas que tenham contato com o vestígio menor é o risco de uma contaminação.

Quanto ao reconhecimento e fixação dos vestígios digitais, também não estão de acordo com os novos artigos. O modo de registro de uma prova digital é lógico, o que significa dizer que a linguagem utilizada para guardar esse dado ou informação é incompreensível por um ser humano, em razão de sua complexidade, entretanto, com o auxílio de um dispositivo eletrônico programado, essa linguagem pode ser rapidamente traduzida para um ser humano. Portanto, apenas um profissional capacitado e especializado é capaz de reconhecer e fixar adequadamente um vestígio digital.[295]

Um dispositivo eletrônico, via de regra, não apaga definitivamente dados, a não ser que todo um procedimento lógico seja seguido, não simplesmente “deletar”. Exemplificando, imagine-se um computador que possua espaço de memória para 1000 arquivos. Cada arquivo salvo corresponde a um espaço de forma linear e progressiva. Se por acaso um dos arquivos for deletado, o próximo arquivo não ocupará o lugar deste que foi deletado, apenas seguirá a sequência lógica. Ao final, quando não houver mais espaço na sequência

2024.

[294] BADARÓ, Gustavo. **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. p. 8.

[295] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 205.

de 1000, o processador passará a salvar os próximos arquivos nestes espaços que foram deletados e em sequência linear e sucessiva. [296]

Portanto, a prova digital não é objetiva e clara como uma prova comum, a análise requer uma profunda varredura complexa de todos os instrumentos.

O artigo 158-D do CPP[297] prevê que a escolha do recipiente em que a prova será colocada, deve ser criteriosa, observando-se as características da natureza do vestígio. No caso das provas digitais, o "recipiente" é irrelevante, isso porque, em razão de sua pluralidade, cópias da mesma fonte são idênticas as originais (clones).[298]

Quando a totalidade de um dispositivo eletrônico composto de dados/fatos importantes sobre determinado caso é copiado para outro dispositivo, totalmente novo, limpo e neutro essa cópia (clone) é legítima e idêntica ao material original. Isso ocorre porque o clone recebe um código denominado *HASH,* que é único, específico e irreversível, que irá garantir que os dados ali contidos não foram corrompidos, adulterados, transmitidos ou armazenados.

É a função *HASH* que servirá de parâmetro para identificação de quebra da cadeia de custódia digital, pois qualquer manipulação inadequada irá alterar esse código.[299] São exemplos de aplicações comuns da função *HASH* o armazenamento seguro de senhas e assinaturas digitais.

Portanto, diferente das provas tradicionais que exigem uma preservação no sentido de serem intocáveis porque só existe a prova original, e qualquer "cópia" não seria autêntica. No âmbito digital, isso é irrelevante, pelas

---

[296] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 206.

[297] BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, RJ; out. 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 19 mai. 2024.

[298] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 207.

[299] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 61.

razões expostas, em especial, graças a função *HASH*. Entretanto, não significa que a preservação das evidências digitais seja mais fácil, muito pelo contrário, qualquer mudança na sequência lógica de algum algoritmo, símbolo, numeral de arquivos podem quebrar a cadeia de custódia e os efeitos, nesse caso, seriam os mesmos da cadeia de custódia tradicional já discutidos no tópico anterior.

Nesse sentida, VIEIRA[300] explica que:

> O princípio da mesmidade contempla a integridade da evidência, mas com esta não ser confunde. A integridade do dado implica que ele não seja modificado intencionalmente ou acidentalmente sem autorização. A ordem dos bits importa!

Visto isso, é importante esclarecer que as especificações sobre este algoritmo (*HASH*) serão aprofundadas em breve. No momento atual, a ideia é abordar a complexidade da cadeia de custódia das provas digitais em relação as tradicionais.

Cabe ainda aqui uma reflexão importante. A legislação que regulamentou a cadeia de custódia (Lei nº 13.964/2019), como já explanado, não estabeleceu sobre as consequências da quebra da cadeia de custódia, tampouco critérios objetivos de como e quando deve ser declarada esta quebra. Logo, caberá ao julgador, de acordo com o caso concreto, valorar e decidir sobre a prova obtida com irregularidades na cadeia de custódia, se deve ou não ser declarada a quebra. No âmbito das evidências digitais, essa valoração pelo julgador é substancialmente mais complexa, pois muitas vezes exigirá conhecimentos técnicos avançados de computação forense e segurança da informação que pouquíssimos juízes são capazes de compreender, afinal, não possuem nenhum tipo de treinamento ou capacitação.

STEPHENSON e GILBERT[301] consideram como os cinco principais elementos da cadeia de custódia digital: a) As fontes que incluem os

---

[300] VIEIRA, Thiago. **Processo penal e novas tecnologias**. In: CONGRESSO IBCCRIM, 22., 2022, Florianópolis. Anais [...]. Florianópolis: IBCCRIM, 2022.

[301] SADIKU, Matthew; SHADARE, Adebowale; MUSA, Sarhan. ***Digital Forensic Chain of Custody***. *International Journal of Advanced Research in Computer Science and Software Engineering*, v. 7,

dispositivos eletrônicos, nuvens e o PC; b) As pessoas envolvidas, o autor, o réu, os investigadores forenses, peritos e qualquer outro agente que tenha envolvimento com os fatos; c) Os fatores, que respondem questões como, Onde estão as evidências?; Quem as gerencia?; Por que faze-lo?; Quando serão tratadas?; Como serão tratadas?; d) As instituições (ex.: autoridades policiais); e) Técnicas que irão garantir a integridade das evidências digitais.[302]

O tratamento das provas digitais (e-evidence) merece uma análise mais minuciosa e específica do que as tradicionais, devendo-se ir além dos critérios estabelecidos na Lei nº 13.964/2019.

Dito tudo isso, abordar sobre a cadeia de custódia digital é um desafio, cabendo adotar o suporte de doutrinas, normas e regulamentos esparsos, tanto brasileiros, como internacionais. Até o momento de elaboração desta dissertação, a principal norma que embasa a cadeia de custódia digital, é ABNT ISO 27037:2013[303], editada pela Organização Internacional de Padronização (ISO). A Norma estabelece critérios de tratamento das evidências digitais para garantir a integridade e autenticidade das evidências digitais.

---

n. 7, p. 117-118, 2017. p. 117.

[302] **Texto Original:** *There are five important elements in a digital chain of custody (DCoC) process:*

- *Characteristics: These include the sources such as PC, digital devices, and cloud.*
- *Dynamics: These include people who are involved in the process, i.e. suspect, victim, law professionals, forensic investigators. Chain of custody has always been a people process.*
- *Factors: These answer the following questions: What is the digital evidence? Where are the digital evidence? Who manage with digital evidence? Why do it? When digital evidence is handled? How is handled with digital evidence? These questions can be answered using fingerprints, biometrics, time stamp, GPS locators, set of procedures, and best practices.*
- *Institutions: These will include law enforcement, military, security agencies, bank, insurance, corporate institutions, and individuals.*
- *Integrity: Techniques for ensuring integrity of digital evidence include CRC (Checksum Redundancy Check), digital signature, encryption, timestamp, and watermarking.*

[303] BRASIL. Associação Brasileira de Normas Técnicas. **ABNT ISO/IEC 27037:2013.** Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. São Paulo: ABNT, 2013.

3.2.1 Primeiro Passo: Reconhecimento, Identificação, Preparação e Isolamento

Antes de iniciar a abordagem sobre os critérios de coleta e aquisição das evidências digitais, o reconhecimento e identificação das fases que antecedem estes passos merecem atenção.

Neste ponto, é importante reiterar alguns conceitos dispostos no primeiro capítulo. O conceito de informação, resumidamente, é a interpretação de dados isolados, que juntos e interpretados, formam uma informação. A informação, gerada por dados digitais, pode ser encontrada em diversas fontes e a correta análise e compreensão das especificidades de cada fonte é de suma importância para garantir que aquisição dessa prova seja adequada.

AZEVEDO[304], entende que existem dois tipos de fontes de informação, as fontes abertas e as fontes fechadas. As abertas são aquelas cujo acesso é permitido sem restrições de segurança, por exemplo, *YouTube*, *sites*, *blogs*, redes sociais, informações públicas do governo, *podcasts*, dentre outros. Já as fontes fechadas são derivadas de informações privadas, de acesso restrito, públicas ou privadas. Essas fontes podem necessitar ou não de autorização judicial. São exemplos de fontes fechadas, dados de geolocalização, IP de acessos a plataformas digitais, trocas de mensagens privadas, dentre outros.

Já NESSI[305] classifica as fontes das provas digitais em três tipos, são elas: a) Sistemas de computação aberta; b) Sistemas de comunicação; c) Sistemas de computação convergentes.

Os sistemas de computação aberta são derivados de computadores pessoais e servidores. Os sistemas de comunicação, derivam-se de telecomunicações, internet e comunicação sem fio. Já os convergentes, derivam de *Smartphones*, cartões inteligentes, assistentes pessoais e PDAs.

---

[304] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 54.

[305] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 16.

O hardware é composto por todos os componentes físicos de um sistema de computador, enquanto a informação é dados, programas armazenados e mensagens de dados.

As evidências digitais podem ser encontradas em diversos tipos de dispositivos eletrônicos, compreender as individualidades de cada objeto é importante para o reconhecimento e identificação da evidência.[306]

Dispositivos de armazenamento, como os discos rígidos, internos e externos, USB (pendrive), cartões de memória, armazenamento em nuvens, podem ser objetos de evidências como correios eletrônicos, histórico de navegação de websites, arquivos em diversos formatos, documentos, chaves de memória, etc.

Dispositivos portáveis, como relógios inteligentes (*Smartwatches),* celulares inteligentes *(Smartphones), tablets,* sistema de posicionamento global (GPS), câmeras digitais, câmeras de segurança, sistemas em veículos, PDAs, podem ser objetos de evidências como lista de chamadas, mensagens instantâneas, páginas visitadas da *internet,* fotos, vídeos, documentos, imagens, vídeos e mensagens de redes sociais, etc.[307]

Dispositivos periféricos, como fax, telefone, teclado, mouse, scanners, impressoras, podem conter evidências físicas que permitem a transformação para um dispositivo informático, como por exemplo, documentos impressos.

Redes de computadores consiste em dois ou mais dispositivos conectados entre si, podendo conter evidências como softwares e dados de armazenamento externo.

A fase de reconhecimento, nada mais é do que a preparação para a coleta. Este é o momento de estabelecer os processos e prioridades dos

---

[306] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 21.

[307] INTERPOL. **Global guidelines for digital forensics laboratory**. 2023.

trabalhos. É com a organização dos processos, após o reconhecimento e identificação dos objetos, que se estabelecerá se a evidência será coletada e transportada ou se será processada no local por servidores. Por óbvio, o processo de identificação e reconhecimento deve ser realizado por agentes especializados e capacitados em computação forense.[308]

Definir as prioridades é essencial. As evidências mais voláteis devem ser priorizadas, tanto com relação as digitais quanto as tradicionais (por exemplo, DNA, impressões digitais). A ordem de coleta, aquisição e análise de cada um deve ser planejada para mitigar a destruição dos outros.[309]

Nesta fase é importante seguir algumas recomendações como: identificar e separar pessoas que estavam tendo contato com os dispositivos (administradores, gestores, trabalhadores, usuários, etc.) e restringir/proibir o acesso. Recomenda-se também que todos os objetos sejam fotografados antes de serem desconectados ou transportados.

A identificação de outros dispositivos como consoles que armazenem informações em formato digital (videogames e smart TVs) também é necessária. Utilização de luvas descartáveis para manusear todos os equipamentos. Não manipular/alterar o estado em que os dispositivos se encontram, se estiverem desligados, por exemplo, não devem ser ligados.

Caso os equipamentos estejam desligados, devem ser desconectados da tomada ou removidas as pilhas ou bateria, se possível, ainda, recomenda-se o uso de dispositivos de bloqueio, como a bolsa de Faraday[310] ou o uso de máquinas recém-formatada, sem nenhuma atividade ou até conexões seguras de *internet,* entre outros.[311]

---

[308] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 21.

[309] *SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE)*. ***Best practices for computer forensic acquisitions (17-F-002-2.0)***. Disponível em: < https://www.swgde.org/17-f-002/>. Acesso em: 25 mai. 2024.

[310] FARADAY, Michael. ***Experimental researches in electricity***. In: NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 26.

[311] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de**

No caso de linhas telefônicas, é essencial que o número e nome do titular conste na ata de busca e apreensão. Por fim, recomenda-se que os dispositivos sejam lacrados e imobilizados, proibindo qualquer manipulação ou até mesmo visualizações, pois poderá alterar ou destruir a evidência.[312]

É evidente que, existem limitações inevitáveis de cada método, por isso, é necessário que cada agente/perito/examinador tome medidas que mitiguem os efeitos adversos o máximo possível. Técnicas não tradicionais podem ser necessárias para a aquisição de dados de dispositivos que usam tecnologias novas.[313]

Em suma, a primeira etapa é definida pela seleção dos dispositivos com evidência digital, a garantia de utilidade processual, o estabelecimento de prioridades e procedimentos, o emprego de técnicas adequadas e o registro de cada ato realizado, isto é, a documentação e descrição das características da evidência, como sua origem, localização, formato e conteúdo. Passada então, a primeira etapa de reconhecimento, identificação, preparação e isolamento de forma organizada e metódica, a próxima etapa é a coleta, a aquisição e preservação dos vestígios.

3.2.2 Segundo Passo: Coleta, Aquisição, Acondicionamento e Preservação

A norma ABNT NBR ISO/IEC 27037:2013 distingue o ato de coleta e aquisição, embora em boa parte das pesquisas os dois termos são utilizados como sinônimos.

Segundo a ABNT NBR ISO/IEC 27037:2013[314], a coleta consiste no ato de recolher o dispositivo para análise em ambiente apropriado, geralmente um laboratório. O ambiente deve ser seguro e controlado, no mínimo,

---

provas digitais. São Paulo: Thomson Reuters Brasil, 2023. p. 58.

312 NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 24

313 *SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE)*. ***Best practices for computer forensic acquisitions (17-F-002-2.0)***. Disponível em: < https://www.swgde.org/17-f-002/>. Acesso em: 25 mai. 2024

314 BRASIL. Associação Brasileira de Normas Técnicas. **ABNT ISO/IEC 27037:2013**. Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. São Paulo: ABNT, 2013.

com energia elétrica estável e o acesso deve ser limitado apenas para pessoas essenciais nos processos. Essa etapa também inclui o acondicionamento correto destes dispositivos.[315]

Para AZEVEDO[316], que adota a coleta e a aquisição como sinônimos, a coleta consiste: “no registro sistemático das informações relativas ao fato, respeitando seu estado original, bem como anotando detalhes sobre sua origem e sobre o método empregado durante a extração”.

A fase de coleta é caracterizada também pela adoção/seleção de métodos que não alterem o estado original do conteúdo, pela documentação de todos os atos, com registro detalhado e fotografado.[317]

A documentação de todas as etapas, manipulações, extrações, alterações é formalização da cadeia de custódia, é com este relatório que as partes do processo poderão se certificar ou se necessário impugnar, se a cadeia de custódia foi seguida corretamente.

Ainda na etapa de coleta, faz parte do procedimento a embalagem e rotulagem de tudo que foi identificado como elemento relevante de prova. A etiquetagem/rotulagem deve conter informações como o número do processo, autor da etapa, data e hora, número de série, fabricante, modelo, espécie, quantidade e a identificação se é possível a cópia/regravamento. Já para o armazenamento, devem ser utilizados sacos tipo polietileno ou similar.[318]

Já a etapa da aquisição, segundo a norma, consiste na produção de cópia integral e idêntica da evidência digital. Recomenda-se para

---

[315] *SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE)*. ***Best practices for computer forensic acquisitions (17-F-002-2.0)***. Disponível em: < https://www.swgde.org/17-f-002/>. Acesso em: 25 mai. 2024

[316] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 60.

[317] BRASIL. Associação Brasileira de Normas Técnicas. **ABNT ISO/IEC 27037:2013**. Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. São Paulo: ABNT, 2013.

[318] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 28.

garantir a integridade da cópia, a utilização de tecnologias como código *Hash*, que já é um método de preservação das evidências, as quais serão descriminadas em breve.

Neste sentido, CARVALHO[319] assinala a importância de que os dispositivos de armazenamento estejam limpos:

> É de suma importância que os dispositivos de armazenamento que irão receber a cópia forense da evidência estejam "forensemente" limpos. Não devem contar um bit sequer que não devesse estar ali, caso contrário poderão contaminar a cópia da evidência e gerar um resultado inverídico.

Nesta fase, é essencial identificar se o dispositivo está ligado ou desligado, isso porque caso esteja ligado, não deve ser desligado e caso esteja desligado não pode ser ligado, isso em razão da premissa anteriormente citada de que, o estado original do objeto não deve ser alterado. Além disso, recomenda-se que nos dispositivos desligados devem ser realizadas as cópias dos dados não voláteis apenas. Já nos dispositivos ligados, recomenda-se a identificação de criptografia, armadilhas e os dados voláteis, devendo-se realizar a cópia desses dados.[320]

Então as principais diferenças entre a coleta e a aquisição são que, a primeira, consiste na reunião de potenciais evidências em ambiente adequado, garantindo que, a cadeia de custódia permaneça íntegra. Enquanto a aquisição é a segunda etapa, é a cópia integral e idêntica dos dados relevantes ou do dispositivo inteiro, é a extração dos dados.

É importante observar que materiais volumosos ou que afetem direitos de terceiros ou que por algum motivo, necessitem de conhecimento urgente, sugere-se a utilização de ferramentas de amostragem rápida, como a

---

[319] CARVALHO, Romullo Wheryko Rodrigues de. **A importância da cadeia de custódia na computação forense**. Revista Brasileira de Criminalística, v. 9, n. 2, p. 134-138, jul. 2020. p. 136.

[320] BRASIL. Polícia Federal. **Diretrizes para a coleta e preservação de evidências digitais –** NC nº 21**.** Disponível em: **<**https://www.gov.br/ctir/pt-br/centrais-de-conteudo/palestras-em-pdf/coloquios/9o-coloquio-ctir-gov-2013-2015/1coloquio2015_palestra03_dpf_flaviosilveira.pdf/view>. Acesso em: 30 de mai. 2024.

triagem, que consiste, na busca rápida, sem se aprofundar em todo o material, é uma busca dinâmica e pontual. Apesar de eficiente, é uma técnica que potencializa o risco de informações serem deixadas de lado.[321]

A aquisição também pode ser realizada por meio de imagem forense, o que requer uma expertise ainda maior dos agentes responsáveis. A imagem forense, realizada por programas de computador ou um dispositivo autônomo duplicador forense, consiste em uma cópia bloco a bloco – bit a bit – do conteúdo, autenticada pelo código *Hash* ou por resumo matemático. No caso da cópia, para não contaminar a prova, o acesso ao dispositivo deve ser feito por outro dispositivo que bloqueie a escrita ou que não escreva sobre o conteúdo. Já o duplicador forense, por si só, bloqueia a escrita, sem a necessidade de um segundo dispositivo, e ainda tem a capacidade de produzir múltiplas cópias, caso seja um hardware.[322]

BADARÓ[323] assevera em sua obra que o método empregado garanta a integridade do dado digital:

> É imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força probandi do conteúdo probatório por ele representado. Normalmente, é necessário fazer uma cópia ou "espelhamento", obtendo o bitstream da imagem do disco rígido ou suporte de memória em que o dado digital está registrado. Além disso, por meio de um cálculo de algoritmo de hash, é possível verificar a perfeita identidade da cópia com o arquivo original. Com isso, de um lado, se preserva o material original e, de outro, se garante a autenticidade e integridade do material que foi examinado pelos peritos.

A aquisição deve ser realizada em ordem de volatilidade, ou seja, da mais volátil para a menos volátil[324], são elas: a) conteúdo de registros, b)

---

[321] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 26.

[322] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 26.

[323] BADARÓ, Gustavo. **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. p. 8.

[324] BRASIL. Associação Brasileira de Normas Técnicas. **ABNT ISO/IEC 27037:2013**. Tecnologia da

tabelas de roteamento e memória cache, c) processos em execução, d) memória RAM, e) dispositivos de armazenamento massivo, f) contêineres de armazenamento remoto, g) armazenamento de backup e respaldo.[325]

Já no que consiste na preservação das evidências, que são técnicas que devem ser aplicadas para fins de garantir a integridade, imutabilidade e autenticidade do conteúdo. A preservação deve ser praticada desde o primeiro contato com as possíveis provas, ainda na etapa de identificação e reconhecimento até a valoração em juízo. Todas as recomendações de todas as etapas, são métodos de preservação. Atualmente existem soluções tecnológicas que serão abordadas a seguir, que asseguram a preservação e integridade das provas digitais.

VACIAGO[326], resume bem as etapas da seguinte forma:

> Para tanto, é necessário: (i) individualizar o suporte informático que contém o dado digital útil à investigação; (ii) obter o dado digital através de técnica de interceptação, no caso de fluxo de comunicação, ou mediante o sequestro e cópia ou espelhamento do suporte em que está registrado o arquivo de dados; (iii) conservar os dados digitais obtidos e copiados em local seguro e adequado; (iv) realizar a análise dos dados obtidos – examinando exclusivamente a cópia do suporte informático – que sejam relevantes para o objeto da investigação; (v) apresentar os resultados da investigação em juízo, mediante a produção de prova pericial e eventuais esclarecimentos verbais dos peritos em audiência.

O *National Institute for Standard and Technology* (*NIST*) [327] distingue quatro fases do tratamento das evidências digitais:

---

informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. São Paulo: ABNT, 2013.

[325] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 27.

[326] VACIAGO, Giuseppe. ***Digital Evidence****. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*. Torino: Giappichelli, 2012. p. 23.

[327] KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. ***Guide to integrating forensic techniques into incident response****: recommendations of the National Institute of Standards and Technology (NIST)*, ago. 2006. Disponível em:

Durante a coleta, os dados relacionados a um evento específico são identificados, rotulados, registrados e coletados, e sua integridade é preservada. Na segunda fase, de exame, ferramentas e técnicas forenses adequadas aos tipos de dados que foram coletados são executados para identificar e extrair as informações relevantes dos dados coletados protegendo sua integridade.

O exame pode usar uma combinação de ferramentas automatizadas e processos manuais. A próxima fase, a análise, envolve a análise dos resultados do exame para obter informações úteis que abordem as questões que foram o ímpeto para a realização da coleta e do exame. A fase final envolve relatar os resultados da análise, que podem incluir a descrição das ações executadas e recomendar melhorias para políticas, diretrizes, procedimentos, ferramentas e outros aspectos do processo forense.

3.2.3 Terceiro Passo: Exame, Análise e Resultados

A etapa de exame, consiste na identificação e filtro de tudo aquilo que foi coletado, preservado e etiquetado.[328] Identificar o que é importante para a perícia ou não, é essencial neste momento, visto que, ainda que exista indícios de ilegalidade, nem tudo é relevante para o objetivo da perícia.

Após a identificação, deve ser realizada a extração de informações relevantes com o suporte de ferramentas forenses, como a recuperação de dados perdidos ou excluídos, extração de metadados e indexação. A indexação pode ser realizada por softwares como Autopsy[329], IPED[330] e outros.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>. Acesso em: 26 mai. 2024.

[328] BRASIL. Polícia Federal. **Diretrizes para a coleta e preservação de evidências digitais –** NC nº 21**.** Disponível em: **<**https://www.gov.br/ctir/pt-br/centrais-de-conteudo/palestras-em-pdf/coloquios/9o-coloquio-ctir-gov-2013-2015/1coloquio2015_palestra03_dpf_flaviosilveira.pdf/view>. Acesso em: 30 mai. 2024.

[329] Autopsy é um software de análise forense digital de código aberto utilizado para investigar e analisar computadores e dispositivos móveis. Ele é amplamente usado por investigadores, analistas de segurança e profissionais de TI para realizar investigações forenses em sistemas comprometidos ou em dispositivos suspeitos de conter evidências digitais. Disponível em: <https://www.autopsy.com/about/>. Acesso em: 30 mai. 2024.

[330] É um sistema para indexação e processamento de evidências digitais, que busca e organiza dados de interesse em arquivos visíveis, ocultos, apagados e fragmentados que estejam em

A filtragem é realizada após a identificação e indexação, que tornará fácil a separação daqui que servirá para o laudo/relatório e o que não servirá. Por fim, finalizada a etapa do exame, todos os passos devem ser documentados. [331]

A análise é a fase de inspecionar os resultados coletados no exame, para fins de gerar respostas úteis para as questões apresentadas nas fases anteriores. A análise então, é a produção da informação, isto é, a transformação dos dados em informação. Nesse sentido, recapitulando o conceito de informação, como: “Os dados com interpretação e sentido atribuídos em face de Hipótese”. [332]

Na análise também é realizada a identificação de pessoas, data, horários, locais, eventos, metadados de arquivos, login e senha. Após a identificação, deve ser realizada a identificação dos fatos de forma lógica, como uma espécie de linha do tempo. Em seguida, deve ser realizada a reconstrução da cena, ou seja, apresentar o passo a passo do objeto que está sendo investigado.

Por fim, novamente, documentar todos os passos de forma técnica, com embasamentos científicos, para garantir a reprodutibilidade, e não, ainda, para uma compreensão jurídica.[333]

O relatório final ou laudo pericial, é então a etapa em que será redigido o resultado obtido de todas as etapas, desde a descrição de cada passo até a conclusão final. É neste momento, após todas as etapas, que se obtém a evidência digital.

---

dispositivos como discos rígidos, pendrives, cartões de memória, SSDs, CDs, DVDs e outros tipos de mídias de armazenamento. Disponível em: <https://github.com/sepinf-inc/IPED>. Acesso em: 30 mai. 2024.

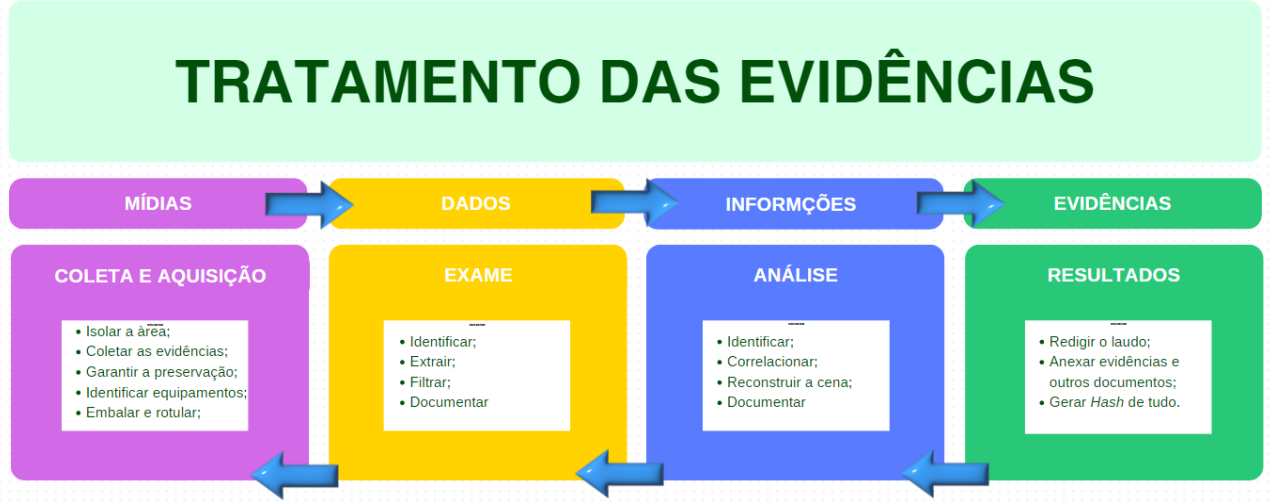
[331] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 61.

[332] ROSA, Alexandre Morais da. **Guia do processo penal estratégico:** de acordo com a teoria dos jogos e MCDA-A.

[333] SOUZA, Adriano Gomes. **Etapas do processo de computação forense:** uma revisão. Acta de Ciências e Saúde, n. 5, v2, 2016. Disponível em: **<**https://www2.ls.edu.br/actacs/index.php/ACTA/article/download/138/128>. Acesso em: 30 mai. 2024.

A conclusão dos resultados deve ser descrita e fundamentada com embasamentos técnico científicos, demonstrando-se todo o percurso da cadeia de custódia da evidência e de forma compreensiva juridicamente. Além de redigir o laudo, devem ser anexadas todas as evidências e demais documentos.[334]

Em resumo, as etapas são definidas da seguinte forma:



Fonte: BRASIL. Polícia Federal. **Diretrizes para a coleta e preservação de evidências digitais – NC nº 21.** Acesso em: 30 mai. 2024.

3.3 SOLUÇÕES TECNOLÓGICAS

No contexto técnico, diversas ferramentas auxiliam na preservação e no acondicionamento seguro de materiais digitais, garantindo a integridade e a autenticidade das provas. Essas tecnologias, cada vez mais sofisticadas, oferecem recursos que automatizam o processo, simplificando a gestão e o manuseio de evidências digitais.

Para facilitar a compreensão e aplicação dessas ferramentas, é essencial explorar suas funcionalidades e potencialidades. A seguir, serão apresentadas algumas das principais soluções tecnológicas utilizadas na área forense digital, com foco em suas características e aplicações práticas na coleta, análise e preservação de provas digitais.

---

[334] BRASIL. Polícia Federal. **Diretrizes para a coleta e preservação de evidências digitais** –NC nº 21**.** Acesso em: 30 mai. 2024.

3.3.1 Função *Hash*

O código denominado *HASH* ou função *HASH,* é um algoritmo matemático que produz uma sequência numérica, única, específica e irreversível. É ele que garantirá que os dados contidos em determinado dispositivo não tenham sido corrompidos, adulterados, transmitidos ou armazenados.

É a função *HASH* que servirá de parâmetro para identificação de quebra da cadeia de custódia digital, pois qualquer manipulação inadequada irá alterar esse código. São exemplos de aplicações comuns da função *HASH* o armazenamento seguro de senhas e assinaturas digitais.[335]

O código *HASH* através deste algoritmo matemático, gera chaves que representam de maneira quase unívoca um documento, registro, arquivo, etc. O *HASH* permite garantir que a evidência digital obtida não tenha sido manipulada nem alterada, já que o *HASH* gerado é inviolável.[336]

Em outras palavras, é uma função que representa dados de comprimento variável como um dado de comprimento fixo e onde pequenas diferenças nos dados de entrada geram uma grande diferença nos dados de saída.[337]

Alguns exemplos de função *HASH*, são MD5, SHA-1, SHA-256, SHA-512, sendo que os dois primeiros são considerados inseguros para preservação de provas digitais caso sejam utilizados de forma isolada, enquanto, os dois últimos, de forma isolada, são suficientes para quase todas as aplicações.[338]

É por essa tecnologia que a aquisição das evidências digitais deve ser realizada por meio de cópia, porque, quando a totalidade de um dispositivo

---

[335] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 207.

[336] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 43.

[337] NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017. p. 43.

[338] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 61.

eletrônico composto de dados/fatos importantes sobre determinado caso é copiado para outro dispositivo, totalmente novo, limpo e neutro essa cópia (clone) é legítima e idêntica ao material original. Isso ocorre porque o clone recebe um código *HASH.*[339] Deste modo, caso seja realizada qualquer alteração, esse código sofrerá também alteração.

3.3.2 Criptografia

A origem da palavra criptografia deriva das palavras gregas κρυπτός (kryptos), que significa escondido, e γράφειν (grafein), que significa escrever. Representava, inicialmente, uma forma diferente de escrita, que buscava impossibilitar a compreensão de mensagens trocadas, como uma espécie de "falar em códigos", isto é, a forma não corresponde com a mensagem enviada, portanto, incompreendida, o que garantia a segurança das informações trocadas. Pela criptografia, uma mensagem simples é transformada numa mensagem cifrada, decifrada apenas por uma ou mais chaves.[340]

Conforme lições de PINHEIRO[341], as criptografia é um método de codificação de dados que permite o acesso apenas de pessoas autorizadas, que possuem uma chave de acesso:

> Método de codificação de dados que permite o acesso apenas de pessoas autorizadas, possuidoras de chave de acesso. Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, entre outras finalidades, para autenticar a identidade de usuários e autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos e proteger o sigilo de comunicações pessoais e comerciais

A técnica, inicialmente, consistia em escrever em cifras de transposição, em que apenas a posição dos símbolos era alterada de modo que o

---

[339] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 207

[340] EDGE, Charles; O'DONNELL, Daniel. ***Introduction to cryptography***. In: LOPES, Marcus Vinícius Pimenta. **A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de provas digitais.** Tese de Doutorado. 218 f. Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023. p. 73.

[341] PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021. p. 364.

receptor deveria organizar as posições de cada símbolo para poder compreender a mensagem. Por exemplo, uma tira de papel, possuía letras aleatórias espalhadas, que em primeiro momento não representavam nada legível, mas que quando enroladas em um cilindro, entregava uma mensagem legível. [342]

A técnica de comunicação em cifras, ou comunicação secreta, foi evoluindo à medida que eram descobertas as fragilidades de cada uma. Afinal, se a técnica é criada por um humano, também pode ser quebrada por um. A base foi e é a cumplicidade do emissor e do receptor. [343]

Com a evolução da tecnologia e dos meios de comunicação, a criptografia tomou uma relevância ainda maior. As mensagens por meio de dispositivos eletrônicos, denominadas como mensagens via ondas abertas, sem a criptografia, são facilmente interceptadas. Isso ocorre porque, em regra, comunicações informáticas, desde e-mails, cadastros, mensagens instantâneas, pagamentos são realizados em redes públicas, a internet é uma rede pública, tornando sua interceptação de certa forma frágil e facilitada. [344]

A criptografia hoje em dia é utilizada tanto pelo governo como por empresas privadas e especialmente por bancos, para fins de proteção, segurança, autenticação, confiabilidade e integridade das comunicações. [345]

A utilização atualmente é por meio de chaves que contém criptografias únicas. Essa chave criptografada pode ser a senha de acesso a conta de banco de um cidadão, por exemplo. Além das mensagens, textos, imagens, sons, e outros arquivos podem também ser criptografados.

---

[342] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 211.

[343] ANDRADE, Rafael Santos; SILVA, Fernando dos Santos. **Algoritmo de criptografia RSA:** análise entre a segurança e velocidade. Revista Eventos Pedagógicos, v. 3, n. 3, p. 438-457, ago. – dez. 2012. p. 439.

[344] SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022. p. 212.

[345] ANDRADE, Rafael Santos; SILVA, Fernando dos Santos. **Algoritmo de criptografia RSA:** análise entre a segurança e velocidade. Revista Eventos Pedagógicos, v. 3, n. 3, p. 438-457, ago. – dez. 2012. p. 439.

SCHENIER[346] especifica as diversas finalidades da criptografia, como a proteção de dados financeiros, proteção de conversas de telefone, protege os dados do computador, protege a identidade dos dissidentes em todo o mundo, protege o governo e os sistemas governamentais, protege a rede de comunicações, a rede elétrica nacional, e infraestrutura de transporte, carros interconectados, termostatos e dispositivos médicos, odos os quais podem destruir vidas e propriedades se hackeados e mal utilizados. A criptografia se tornará ainda mais crítica para a segurança pessoal e nacional. [347]

Nos dias de hoje, existem dois tipos de chaves criptográficas, as simétricas e as assimétricas. O que as diferencias é que as chaves simétricas ou privadas, tanto codificam como descodificam, isto é, a mesma chave é utilizada para criptografar e descriptografar. Já as assimétricas são utilizadas duas chaves, uma para criptografar e outra para descriptografar e são correspondentes/vinculadas entre si. [348]

É comumente utilizada atualmente, para transações financeiras, compras na *internet*, proteção de segurança para dispositivos, nas mensagens do aplicativo *whatsapp,* nos e-mails, nas assinaturas digitais e

---

[346] SCHNEIER, Bruce, ***The value of encryption***. The Ripon Forum, abr. 2016. Disponível em: <https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.html>. Acesso em: 27 mai. 2024.

[347] **Texto Original:** *Encryption protects your financial details and passwords when you bank online. It protects your cell phone conversations from eavesdroppers. If you encrypt your laptop—and I hope you do—it protects your data if your computer is stolen. It protects your money and your privacy. Encryption protects the identity of dissidents all over the world. It's a vital tool to allow journalists to communicate securely with their sources, NGOs to protect their work in repressive countries, and attorneys to communicate privately with their clients. Encryption protects our government. It protects our government systems, our lawmakers, and our law enforcement officers. Encryption protects our officials working at home and abroad. During the whole Apple vs. FBI debate, I wondered if Director James Comey realized how many of his own agents used iPhones and relied on Apple's security features to protect them. Encryption protects our critical infrastructure: our communications network, the national power grid, our transportation infrastructure, and everything else we rely on in our society. And as we move to the Internet of Things with its interconnected cars and thermostats and medical devices, all of which can destroy life and property if hacked and misused, encryption will become even more critical to our personal and national security*.

[348] ANDRADE, Rafael Santos; SILVA, Fernando dos Santos. **Algoritmo de criptografia RSA:** análise entre a segurança e velocidade.

certificados digitais, para recuperações de dados perdidos ou excluídos. Em suma, a criptografia é uma segurança virtual de proteção de dados.

A criptografia impõe desafios ainda maiores para a qualificação das provas digitais, especialmente para a investigação criminal. O desconhecimento desta tecnologia, gera, muitas vezes, requisições impossíveis de serem concretizadas, isso porque, a criptografia impede a interceptação de mensagens criptografas[349], e bem sabemos que o *whatsapp* é hoje um dos maiores meios de comunicação do cidadão brasileiro.

A compreensão acerca da criptografia, é fundamental, pois desempenha funções cruciais na integridade e autenticidade das provas digitais.

Como anteriormente esclarecido, a função *HASH* tradicional/simples, é essencial para garantir que um arquivo ou dado não tenha sido alterado, para isso, transforma dados de comprimento variável em comprimento fixo. Já o *HASH* criptografado, realiza essa transformação de maneira unidirecional, isto é, com uma propriedade adicional de segurança, tornando quase impossível a reversão do código *HASH*. [350]

Com tudo isso, é possível afirmar que a criptografia, além impor desafios, também desempenha um papel fundamental na qualificação das evidências digitais, auxiliando na verificação de integridade de dados digitais, para documentar e proteger a cadeia de custódia e na proteção e segurança, evitando manipulações.

3.3.3 Blockchain

Essa tecnologia consiste em um programa de computador que realiza duas ações: verificação rápida de modificação nos dados e correção automática com base em replicadores desses dados. Com isso gera-se a

[349] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-C. p. 420.

[350] LAGO, Lucas. **Blockchain:** confiança através de algoritmos. Escola Politécnica do Estado de São Paulo, CEST – Boletim, v. 2, n. 4. out. 2017. p. 1.

imutabilidade dos dados, não permitindo a modificação de conteúdo que lhe foi inserido. Nas palavras de SOUZA, MUNHOZ e CARVALHO[351]:

> Em outros termos, a cada novo bloco de dados gera-se uma "impressão digital" (código HASH) do bloco anterior e grava-se junto do novo bloco, fazendo um "encadeamento de blocos" (origem do termo blockchain). Isso facilita a verificação de modificações no seu conjunto de dados, onde se mudar um, o resto não "se encaixa".

Dificilmente, nos dias de hoje, alguém nunca tenha ouvido falar em *blockchain*. Essa tecnologia foi proposta em 1991, mas apenas em 2008 tornou-se conhecida, sendo criada para viabilizar a utilização segura das criptomoedas, desenvolvida como um livro-razão, que registrava todas as transações financeiras em forma de blocos encadeados.[352]

Alguns especialistas consideram que a blockchain é a maior revolução digital até os dias de hoje desde a criação da *Word Wide Web* (www). Apesar da tecnologia ter nascido para as criptomoedas, atualmente já é utilizada para diversas finalidades, saúde, negócios, setor público e privado, e também para a preservação das provas digitais.[353]

A principal finalidade da tecnologia é garantir a imutabilidade dos dados. São como pedaços de códigos gerados virtualmente que carregam informações conectadas como blocos de dados que formam uma corrente. Portanto, é um grande banco de dados, não rastreável. [354]

---

[351] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 65.

[352] LAGO, Lucas. **Blockchain:** confiança através de algoritmos. Escola Politécnica do Estado de São Paulo, CEST – Boletim, v. 2, n. 4. out. 2017. p. 1.

[353] ROSA, Alexandre Morais da; PRÓSPERO, Felipe Navas. **Qual a validade jurídica dos documentos pela rede blockchain?** Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2019-jan-11/limite-penal-qual-validade-juridica-documentos-rede-blockchain/>. Acesso em: 28 mai. 2024.

[354] ROSA, Alexandre Morais da; PRÓSPERO, Felipe Navas. **Qual a validade jurídica dos documentos pela rede blockchain?** Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2019-jan-11/limite-penal-qual-validade-juridica-documentos-rede-blockchain/>. Acesso em: 28 mai. 2024.

De forma simples, a blockchain:

> [..] pode ser entendido como um banco de dados online, público e descentralizado, criado para tornar a distribuição de informação transparente e confiável, sem precisar de um agente externo e centralizador que valide o processo.

Segundo Nakamoto,[355] a blockchain é “uma rede que marca o tempo das transações, colocando-se em uma cadeia contínua no “Hash”, formando um registro que não pode ser alterado sem refazer todo o trabalho”.

As características mais fortes da blockchain são: descentralização, sua natureza aberta/pública, auditabilidade e transparência. Pública, porque qualquer um pode vê-la, tendo em vista que está na própria rede e descentralizada, pois não pertence a nenhum órgão ou instituição exclusiva, como bancos ou notários.

Para as provas digitais, a blockchain fornece um ambiente seguro e autêntico de preservação de provas, que irá garantir que a cadeia de custódia não seja quebrada e que nenhuma prova sofra nenhuma alteração. Para o registro de provas digitais em alguma blockchain, é necessária a criação de um código *HASH* criptografado, isto é, uma assinatura digital e inseri-la na plataforma.[356]

SOUZA, MUNHOZ e CARVALHO[357], por sua vez, apresenta em sua obra a seguinte aplicação dessa tecnologia nas provas digitais:

> Há diversas aplicações para essa tecnologia, porém, no que se refere às provas digitais, ela pode ser usada na etapa de preservação das informações contra manipulação posterior. Isso porque, após calcular-se os códigos HASH, pode-se inseri-los em

---

[355] NAKAMOTO, Satoshi. ***Bitcoin:*** *a peer-to-peer electronic cash system*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 28 mai. 2024.

[356] HERMEIRO, Andreia Carina Cláudio. **A cadeia de custódia da prova digital:** o uso da tecnologia blockchain como forma de preservação. 2023. Dissertação (Mestrado em Ciências Jurídico-Forenses). 64 f. Faculdade de Direito da Universidade de Coimbra, Coimbra, 2023. p. 50.

[357] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 66.

> uma rede confiável de blockchain, preservando a integridade digital dos arquivos e gerando uma referência de anterioridade dos dados.

Cita-se aqui, uma solução baseada em *blockchain* para preservação das provas digitais: a plataforma DataCertify.[358], desenvolvida para identificar, coletar e preservar fatos que ocorrem no ambiente digital. Além da tecnologia *blockchain*, a plataforma também utiliza carimbo de tempo:

> O sistema da DataCertify utiliza tecnologias avançadas de criptografia e carimbo de tempo, combinadas com um código que impossibilita a adulteração do conteúdo visualizado. Essa combinação, além de garantir a segurança das provas registradas, as protege contra adulterações e falsificações **após a captura**. Cada registro recebe um carimbo de tempo confiável, atestando o momento da captura e registro.

A plataforma fornece a possibilidade de registro de provas como mensagens de aplicativos como o WhatsApp, postagens de redes sociais como o Facebook e *Instagram*, e-mails e conteúdo de sites.

A plataforma DataCertify, realiza o processo da seguinte forma:

> A DataCertify permite que qualquer pessoa (usuário) colete, registre e armazene situações ocorridas na internet, por meio de um sistema que evita a adulteração do conteúdo. A coleta ocorre a partir de um programa instalado na máquina do usuário, que bloqueia qualquer botão e/ou comando que permitiria a adulteração das informações visualizadas, garantindo, assim, que o conteúdo acessado corresponde à informação presente na web e que qualquer pessoa que tenha percorrido o mesmo caminho do usuário naquele momento teria como resultado a informação presente na tela. Durante a navegação, um arquivo que contém as saídas gráficas e áudios reproduzidos é gerado, contendo os comandos do usuário e links acessados. Após a navegação, para que seja possível garantir a imutabilidade do arquivo capturado, uma cópia do arquivo gerado é salva em uma nuvem criptografada, na qual ela será mantida pelo período de 20 anos, e é feito o cálculo

[358] DATACERTIFY. **Como a DataCertify garante a segurança das provas registradas?** Disponível em: <https://www.datacertify.com.br/>. Acesso em: 28 mai. 2024.

> do código HASH do arquivo. Com o HASH, é realizada uma transação em uma Blockchain pública e, a partir desse registro em Blockchain, é impossível que qualquer adulteração no conteúdo registrado passe despercebida. O uso da Blockchain, aliado ao método de captura desenvolvido pela DataCertify se dá em razão do entendimento recorrente por parte de diversos Tribunais, de acordo com os quais, a segurança intrínseca à tecnologia e das informações nela registradas são uma forma válida de prova, garantindo tanta segurança ao julgador quanto uma Ata Notarial. A exemplo, citam-se os seguintes julgados: TSE- Al em Recurso Especial Eleitoral nº 0600126-54.2020.6.06.0121 TJ - SP - Apelação Cível nº 1009061-63.2017.8.26.0100 TRT da 12ºRegião - Processo nº 0000621-92.2021.5.12.0004. Nosso sistema garante a preservação das cinco primeiras etapas da cadeia de custódia previstas no art. 158-A até 158-F do Código de Processo Penal. Ademais, o art. 369 do Código de Processo Civil permite que qualquer meio de prova moralmente legítimos possam ser utilizados como prova, enquanto o art. 411, também do Código de Processo Civil, dispõe que um documento será considerado autêntico quando for possível identificar a sua autoria. A DataCertify combina diversas tecnologias consideradas suficientes para garantir captura adequada e a imutabilidade do conteúdo registrado, a partir de um protocolo que impossibilita a edição do conteúdo visualizado durante a captura, o que garante maior segurança e confiança quanto à imutabilidade do fato preservado por meio de nosso sistema. Este relatório contempla as informações referentes à captura e o registro realizado a partir de nosso sistema, contendo a identificação do usuário, metadados do arquivo gerado a partir da captura e outras informações que permitem a análise aprofundada do conteúdo preservado. Caso haja interesse, todas as informações presentes neste relatório e a sua integridade podem ser checadas a partir do link disponibilizado na capa do relatório, sendo necessário informar apenas o código de acesso ao registro. Na página de checagem, é possível conferir, além das informações do registro e dos metadados do arquivo, os dados do registro em Blockchain e a íntegra da gravação realizada, a qual sempre aconselhamos que nossos usuários juntem ao processo.

Em suma, ao ser instalado o programa pelo usuário, o sistema bloqueia comandos que poderiam adulterar as informações visualizadas, assegurando que o conteúdo acessado corresponda exatamente à informação

presente na web. Durante a navegação, um arquivo contendo saídas gráficas e áudios é gerado, registrando comandos do usuário e links acessados. Esse arquivo é então salvo em uma nuvem criptografada por 20 anos e tem seu código *HASH* calculado. O *HASH* é registrado em uma Blockchain pública, tornando impossível adulterações no conteúdo sem serem detectadas.

Entretanto, é importante destacar que a plataforma DataCertify e outras soluções que utilizam a tecnologia Blockchain, fornecem uma segurança de preservação apenas após coletado, mas não durante, portanto, não garantem a origem ou confiança da informação.

3.3.4 Verifact

A Verifact[359] é uma plataforma on-line de verificação de provas digitais, como conversas de WhatsApp, e-mails, conversas do Telegram, blogs, sites, notícias, lojas virtuais, vídeos do Youtube etc. A partir da coleta dessas provas que deve ser realizada pelos usuários da plataforma, resulta na emissão de um relatório técnico certificado, com telas registradas, dados e metadados técnicos auditáveis.

Além do relatório, tem também os vídeos de registro de toda a navegação. O relatório possui assinatura digital certificada e carimbo de tempo ICP-BRASIL, esse carimbo é o que garante a imutabilidade dos dados, até mesmo se o conteúdo por apagado futuramente, com os dados e metadados coletados é possível realizar ampla perícia técnica das informações, para comprovar que o material é aquilo que diz ser e vem de onde diz ter vindo.

SOUZA, MUNHOZ e CARVALHO[360] explicam em sua obra acerca dessa plataforma, a qual se enquadra nos requisitos apontados pelas normas internacionais e os princípios da cadeia de custódia:

> Essa solução enquadra-se nos requisitos apontados por normas internacionais e os princípios da cadeia de custódia apresentados

[359] VERIFACT. **Validade jurídica**: alta confiança para registro de fatos na internet. Disponível em: <https://www.verifact.com.br/validadejuridica/>. Acesso em: 28 mai. 2024.

[360] SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 79.

> anteriormente, além de ser facilmente acessível a qualquer pessoa devido à sua disponibilidade em qualquer momento e custos mais atrativos. A empresa afirma que seu procedimento permite embasar argumentos de conteúdos disponíveis na internet quanto à sua integridade, anterioridade, origem, contexto e ausência de adulteração durante e após o processo de coleta. Ou seja, permite afirmar que determinado conteúdo estava publicado em determinado site, em determinado momento, tal qual se apresenta nos conteúdos captados, havendo meio eficaz de se evitar interferências indevidas.

Ademais, a plataforma garante que preserva todas as etapas da cadeia de custódia e todas as recomendações da ISSO 27037:2013. Justifica a preservação da cadeia de custódia da seguinte forma:

> • **Reconhecimento:** em conjunto com o usuário, que direciona os conteúdos a serem registrados, enquanto a ferramenta busca dados técnicos sobre a situação;
>
> • **Isolamento:** coleta em ambiente controlado e isolado de interferências de outras atividades, com medidas efetivas para evitar a intervenção e uso de ponto de acesso seguro à internet;
>
> • **Fixação:** descrição dos dados com origem, data de registro em horário local e UTC, códigos hash individuais para cada arquivo e outros
>
> • **Coleta:** registro de imagens, vídeos, áudios e arquivos, com a coleta de metadados técnicos. O resultado é gravado em formatos abertos e facilmente acessíveis;
>
> • **Acondicionamento:** armazenamento dos dados com selo que garante a integridade posterior do material, realizado com o recurso da Certificação Digital ICP/Brasil (Assinatura Verifact + Carimbo de Tempo). **(grifo nosso).**

Para embasar sua capacidade, a empresa disponibiliza em seu site diversos laudos emitidos por empresas de cibersegurança, afirmando sua capacidade de evitar a manipulação do conteúdo durante e após coleta e preservação do material, tendo sua capacidade técnica atestada por órgãos

públicos como o Ministério Público Federal[361] e Tribunal Superior Eleitoral[362], Polícia Civil de Santa Catarina[363], Ministério Público do Mato Grosso do Sul[364], Polícia Civil do Paraná[365], Ministério Público da Bahia[366], Ministério Público de São Paulo[367], Ministério Público da Paraíba[368] e empresas de Cibersegurança como a eSecurity, SWT Brasil[369], EarlySec[370] e Sipercon[371].

---

[361] BRASIL. Ministério Público Federal (MPF). **Atestado de capacidade técnica PGR nº 00011690/2024**. jan. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/01/atestado_MPF_verifact_jan2024.pdf>. Acesso em: 28 mai. 2024.

[362] BRASIL. Tribunal Superior Eleitoral (TSE). **Atestado nº 48/2023**. jul. 2023. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2023/08/Atestado_de_Capacidade_Tecnica_n_48_TSE-Verifact.pdf>. Acesso em: 28 mai. 2024.

[363] SANTA CATARINA. Polícia Civil de Santa Catarina; Delegacia-Geral; Gerência de Tecnologia da Informação. **Atestado de capacidade técnica**. jan. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/01/atestado_PCSC_verifact_jan2024.pdf>. Acesso em: 28 mai. 2024.

[364] MATO GROSSO DO SUL. Ministério Público do Mato Grosso do Sul. **Atestado de capacidade técnica**. mar. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/05/atestado_ministerio_publico_ms_verifact.pdf>. Acesso em: 28 mai. 2024.

[365] PARANÁ. Secretaria de Estado da Segurança Pública; Polícia Civil do Paraná. **Atestado de capacidade técnica**. nov. 2022. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2022/11/2022_atestado_de_capacidade_tecnica-Verifact-PCPR.pdf>. Acesso em: 28 mai. 2024.

[366] BAHIA. Ministério Público do Estado da Bahia. **Atestado:** parecer jurídico 409/2020. out. 2021. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2021/10/Atestado_SEI_19.09.01970.0016798_2021_65.pdf>. Acesso em: 28 mai. 2024.

[367] SÃO PAULO. Ministério Público do Estado de São Paulo. **Atestado de capacidade técnica**. jun. 2022. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2022/10/Atestado_Capacidade_Tecnica_Verifact_Tecnologia_Ltda_CAEX_MPSP.pdf>. Acesso em: 28 mai. 2024.

[368] PARAÍBA. Ministério Público da Paraíba; Núcleo de Gestão do Conhecimento (NGC); Grupo de Atuação Especial contra o Crime Organizado (GAECO). **Atestado de capacidade técnica**. jan. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/01/atestado_MPPB_verifact_jan2024.pdf>. Acesso em: 28 mai. 2024.

[369] NAGY, Marcelo; STEFANO, Leandro Morales Baier. **Auditoria baseada nos requisitos dispostos na ABNT NBR ISSO/IEC 27037:2013 e no Código de Processo Penal**. STW Brasil – Segurança em Tecnologia Ltda. 28 mar. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/03/laudo_verifact_iso27037_cadeia-de-custodia.pdf>. Acesso em: 28 mai. 2024.

[370] MONTEVERDE, Wagner Ap. **Parecer técnico de auditoria de infraestrutura de aplicação**. EarlySec. 29 nov. 2019. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2020/03/Parecer_auditoria_aplicacao_Verifact-manifesto2019Ax.pdf>. Acesso em: 28 mai. 2024.

[371] SANTOS, Uelinton B. dos. **Parecer técnico:** plataforma Verifact. Sipercon. 02 set. 2019. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2021/11/parecer-perito-v2.0-

A jurisprudência também já tem reconhecido a plataforma como um método seguro de qualificação da prova digital:

> Representação. Eleições 2022. Propaganda eleitoral irregular. Veiculação no story do facebook e instagram. Validação por mecanismo legal de autenticidade de prova digital. Ausência. Representação improcedente. I – A veiculação de propaganda irregular através do story do facebook e instagram exige a validação por mecanismo legal de autenticidade de prova digital **(verifact**, originalmy, ata notarial, etc.), a fim de demonstrar a legitimidade da prova, mormente o dia, horário e local de extração do conteúdo. II – Representação improcedente.[372]

Em síntese, a plataforma Verifact se destaca por seu sistema que respeita minuciosamente as etapas aplicáveis da cadeia de custódia estipuladas pelo Código de Processo Penal. A plataforma Verifact se diferencia da blockchain por garantir a integridade da prova digital desde a coleta, e não apenas na etapa de preservação. Enquanto a blockchain impede manipulações posteriores ao registro, a Verifact cria um ambiente virtualizado e isolado para cada coleta, sem atividades anteriores, com conexão independente e acesso limitado, garantindo a não manipulação dos dados durante todo o processo.

Em concluso, percebe-se que a crescente importância das provas digitais no sistema judiciário exige uma compreensão abrangente das tecnologias e dos procedimentos adequados para garantir a sua validade e autenticidade.

A cadeia de custódia desempenha um papel crucial na preservação da integridade das provas, desde a sua coleta até a apresentação em juízo. Ainda, a utilização de soluções tecnológicas, como a função *hash*, a criptografia, blockchain e Verifact, tem se mostrado fundamental para garantir a

final-assinado.pdf>. Acesso em: 28 mai. 2024.

[372] RONDÔNIA. Tribunal Regional Eleitoral de Rondônia. **Representação nº 0601791-65.2022.6.22.0000**, de Cacoal/RO. Relator: Desembargador Marcelo Stival. Data de Julgamento: 17 out. 2022.

confiabilidade e a segurança das provas digitais, contribuindo para a efetividade da justiça na era digital.

Assim, compreende-se que a busca pela verdade dos fatos no processo judicial deve sempre se pautar pela observância dos direitos e garantias fundamentais, especialmente no que diz respeito à privacidade e à proteção de dados pessoais, afinal, a justiça digital deve ser construída sobre bases sólidas, que garantam a confiabilidade das provas e a proteção dos direitos individuais.

CONSIDERAÇÕES FINAIS

A revolução digital é um fenômeno que fragmentou o conhecimento, alterou as formas de produção e distribuição do saber, e promoveu a diversidade e a pluralidade de vozes.[373]

O modelo de vida que se estabeleceu, descortinou tecnologias que proporcionam a automatização de inúmeras tarefas das mais simples às mais complexas. Pode-se dizer que na atualidade tarefas que demandariam mão-de obra e tempo humanos passam a ser efetuadas por meios tecnológicos que chama a atenção, principalmente, no mundo jurídico.

A partir das mudanças ocorridas, é possível perceber que a revolução digital está intimamente representada por velocidade e rapidez e a tecnologia colocada à disposição da humanidade dá a sensação de uma crescente busca por aceleração.

A medida em que as tarefas cotidianas e as interações pessoais foram inseridas no ambiente digital e informático, os conflitos dentro dos ambientes digitais aumentaram na mesma proporção.

A atualidade é marcada por uma sociedade conectada, fazendo com que boa parte das ações do dia a dia estejam documentadas e/ou armazenadas, seja por meio das redes sociais em trocas de mensagens, seja por meio de registros fotográficos e gravações de vídeos e áudios, compartilhamentos com o público do cotidiano nas redes sociais, reuniões por videoconferência, tratativas e negociações por contratos digitais, compras e vendas de mercadorias digitais, dentre outras atividades diárias que estão ou podem estar armazenadas no ambiente digital ou eletrônico.

Toda a mudança que vem sendo ocasionada pelo desenvolvimento tecnológico, modifica também os meios de comprovação de fatos,

---

[373] LYOTARD, Jean-François. **A condição pós-moderna: um relatório sobre o conhecimento**. Tradução de Ricardo Corrêa Barbosa. 7. ed. Rio de Janeiro: José Olympio, 1998.

tornando-se este um grande desafio para os juristas da pós-modernidade, que até então detinham possibilidades determinadas de meios de provas para a resolução dos conflitos.

A presente dissertação teve então como intuito analisar as formas de aquisição e de qualificação de provas digitais no processo penal brasileiro. Com efeito, foi inserida na linha de pesquisa “Direito, jurisdição e inteligência artificial” e projeto de pesquisa Democracia, processo e jurisdição. O objetivo geral da pesquisa foi analisar os requisitos necessários para que as provas digitais sejam consideradas válidas nos processos penais, bem como os procedimentos adequados para sua coleta, preservação e apresentação em juízo, a fim de garantir maior segurança jurídica das decisões judiciais, com a devida preservação dos princípios constitucionais, da ampla defesa, do contraditório, do *in dubio pro reu*, da legalidade, presunção da inocência e a inadmissibilidade das provas ilícitas.

Ante a evidente precariedade legislativa e jurídica brasileira na área, que enfrenta desafios significativos em acompanhar a rápida evolução tecnológica e se adequar a realidade moderna, é de suma importância compreender os aspectos que envolvem todo este ambiente digital.

A evolução do direito é mais lenta que a evolução da sociedade, entretanto, é necessário atentar para questões que se colocam de forma tão definitiva como a produção de provas digitais e seu uso no judiciário, o estudo da presente matéria é imprescindível no cenário global e no ordenamento jurídico brasileiro, orientadas ao estabelecimento do regime jurídico correspondente.

Com efeito, a pesquisa vinculou-se aos ODS nº 9 e 16º. O 9º, pois fomenta a inovação, refletindo a importância de integrar tecnologias avançadas. Já o 16º, pois aborda a importância do acesso à justiça, eficácia das instituições legais, assegurando a proteção dos direitos fundamentais e a admissibilidade de provas legítimas e autênticas.

Para o desenvolvimento lógico da pesquisa, esta foi dividida em três capítulos.

No **Capítulo 1** inicialmente foram explorados os fundamentos essenciais do ambiente digital na contemporaneidade, fornecendo uma compreensão abrangente dos principais elementos que moldam a interação humana com a tecnologia e a informação. Ao abordar temas como a distinção de dados, informação e conhecimento, do mesmo modo, a distinção entre *Internet* e *Web* e, ainda, a definição de metadados. Seguindo para o papel dos dispositivos e sistemas eletrônicos, buscou-se oferecer uma análise das dinâmicas e desafios enfrentados neste contexto. Pretendeu-se, por meio dessa exploração, clarificar as complexidades do ambiente digital e seu impacto significativo na sociedade contemporânea.

Como disposto naquele Capítulo, a sociedade da informação, surgiu a partir da Revolução Industrial até sua consolidação com a era digital. Desde tempos antigos, a humanidade desenvolveu tecnologias para facilitar a comunicação e sistematização de informações. Com o advento dos computadores na Segunda Guerra Mundial e a subsequente evolução tecnológica, especialmente a internet, a sociedade da informação emergiu, transformando profundamente aspectos econômicos, sociais e políticos. Esta era é marcada pela rápida disseminação e valorização da informação, com implicações significativas no campo do direito processual, agora também digitalizado.

Acerca da diferenciação entre dados, informação e conhecimento, notou-se que os dados são elementos brutos e isolados, como palavras, números ou imagens, que não possuem valor interpretativo por si só. Eles são a matéria-prima inicial e potencialmente informativa, necessitando de processamento para se tornarem significativos. No contexto jurídico, dados são evidências que podem ser utilizadas em processos judiciais após serem corretamente armazenados e processados.

A informação surge quando os dados são organizados, interpretados e processados de maneira que adquirem significado e relevância contextual. É o resultado do tratamento dos dados, capaz de contribuir para processos decisórios e compreensão de situações específicas. Enquanto os dados são elementos individuais, a informação representa um nível de organização e interpretação que facilita a compreensão.

O conhecimento vai além da informação ao envolver a aplicação significativa e interpretação dos dados para gerar novos entendimentos e inovações. É um nível superior de compreensão que inclui a capacidade de abstração e contextualização, permitindo a transformação da informação em aprendizado e criação de novos saberes. O conhecimento pode ser tácito, pessoal e difícil de formalizar, ou explícito, facilmente comunicável e compartilhado sob formas codificadas ou universais.

No mesmo contexto, foi possível compreender a definição de dados digitais, que são informações de natureza numérica e imaterial, processadas por sistemas computacionais. Esses dados, representados em diversos formatos como texto, imagem, áudio e vídeo, desempenham funções específicas e, quando agrupados, formam documentos eletrônicos, gerados, transmitidos ou armazenados por meio de computadores ou redes de comunicação. Quanto a categorização dos dados digitais, subdivide-se em: dados sensíveis, pessoais e públicos e dados de conteúdo e de tráfego.

Os dados sensíveis são informações ligadas ao núcleo íntimo da personalidade, como origem racial, opiniões políticas, saúde e orientação sexual. Os dados pessoais em sentido estrito referem-se a informações na esfera privada que delimitam relações familiares e pessoais, mas não estão ligadas ao núcleo íntimo da personalidade. Os dados públicos são informações que afetam aspectos como honra, imagem e vida social do indivíduo. Os dados de conteúdo são as informações principais transmitidas intencionalmente em uma comunicação eletrônica. Os dados de tráfego são informações acessórias que identificam a origem, destino, momento e duração da comunicação eletrônica, sem incluir o conteúdo da mensagem.

Dando continuidade, buscou-se definir os metadados, que são dados adicionais sobre determinada operação ou conteúdo digital que podem ajudar no processamento da informação pelos softwares, além de identificar recursos e manter históricos.

Observou-se que existem várias categorias de metadados: **Administrativos**, que auxiliam na gestão e manutenção de coleções e recursos, fornecendo informações sobre origem e histórico de alterações. De **autenticação**: Permitem verificar a

identidade, integridade e legitimidade de um recurso informacional. De **preservação**: Contêm informações sobre a preservação e conservação de recursos informacionais ao longo do tempo. De **proveniência**: Fornecem dados sobre a origem, histórico de criação, modificações e relacionamentos de um recurso informacional. **Técnicos**, que descrevem o funcionamento de um sistema ou recurso informacional, incluindo especificações técnicas. **Meta-metadados**, que são informações sobre o próprio registro ou sobre a criação de um conjunto de dados. **Descritivos**, que identificam e contextualizam recursos informacionais para fins de descoberta, identificação, seleção, aquisição e compreensão. **Direitos**, que informam sobre a propriedade intelectual e direitos autorais de um recurso informacional. **Acesso e Uso**, que registram como um recurso informacional foi acessado e utilizado, incluindo restrições de acesso. **Estruturais**, que descrevem a composição e organização de um recurso informacional, indicando sua estrutura interna.

Foi abordada também a distinção de *internet* e *web*, que não raras as vezes são utilizados como sinônimos. A Internet se refere à estrutura que conecta computadores e dispositivos em todo o mundo. Já a Web é a rede (o sistema) em si pela qual é feita a navegação por hiperlinks, acessíveis através da internet.

Notou-se ainda que o processo de acesso à internet funciona a partir dos códigos de endereço IP. Contudo, tal processo ainda é intermediado por outros elementos, conhecidos como Servidores (DNS, de dados e backbone) e Provedores de conexão. Os servidores DNS Servidores são os que permitem o uso de um nome amigável, como “www.google.com.br”, para identificar o endereço IP de um determinado servidor na internet, facilitando seu acesso. Os servidores de dados são os computadores especializados para a função de processamento de dados de serviços digitais disponíveis através da internet. Geralmente eles são instalados em *datacenters*, que consistem em instalações preparadas para garantir sua continuidade utilizando-se de recursos de segurança, refrigeração, fontes alternativas de energia, múltiplas conexões de internet e outras medidas. Os servidores backbone são considerados os responsáveis por integrar diversas sub-redes da internet, oriundas de provedores de conexão, grandes datacenters e outros, interligando outros *backbones* ou realizando o caminho de transferência de dados para outros países ou continentes. Já os provedores de conexão são responsáveis por conectar residências e empresas à rede mundial, utilizando diferentes tecnologias como cabos, fibra óptica e rádio. compreende-se que o acesso à internet, apesar de sua aparente simplicidade,

é um processo intrincado que envolve uma rede complexa de servidores e provedores. Portanto, a compreensão dessa estrutura subjacente é importante para entender o funcionamento da internet e seus diversos componentes.

Sobre os dispositivos móveis, observou-se que evoluíram de simples aparelhos de comunicação por voz para ferramentas multifuncionais, conhecidos como "smartphones" que são telefones celulares com capacidades avançadas, executando sistemas operacionais identificáveis como Android, iOS, entre outros, e permitindo a instalação de aplicativos de terceiros e possuem hardware sofisticado, como CPUs modernas e múltiplas capacidades de conectividade (Wi-Fi, HSDPA). Estes dispositivos têm grande capacidade de memória, permitindo o armazenamento massivo de dados pessoais e de terceiros. A multifuncionalidade dos smartphones e sua capacidade de armazenamento de dados pessoais tornaram-nos ferramentas centrais na sociedade da informação e potenciais fontes de prova no âmbito jurídico.

O desafio é o acesso ao conteúdo dos smartphones que deve ser realizado de forma criteriosa e proporcional para evitar violações à privacidade, que é constitucionalmente garantida. A grande quantidade de dados pessoais armazenados nesses dispositivos exige um equilíbrio entre o acesso à informação e a proteção da privacidade e dos dados.

Por fim, compreendeu-se a privacidade como o direito de controlar a exposição da esfera íntima e dos dados pessoais, como um componente fundamental da liberdade individual.

No **Capítulo 2**, explorou-se a teoria geral da prova, evoluindo para a conceituação da prova digital, suas características e os desafios que ela representa para o sistema legal. Abordou-se as diferentes formas de provas digitais, desde documentos eletrônicos e mensagens instantâneas até dados de geolocalização, e discutiu-se as implicações legais e éticas de seu uso. Ao compreender a importância e a complexidade das provas digitais, é possível construir um sistema legal mais justo e eficaz na era digital.

Como disposto naquele Capítulo, juridicamente, as provas são dados objetivos que confirmam ou negam uma asserção sobre determinado fato que interessa à decisão da causa. Já a prova digital, também conhecida como evidência digital (do inglês *digital evidence*) é o meio utilizado para demonstrar a evidência de um fato ou evento ocorrido em meio digital. As provas digitais são entidades imateriais, mas possuem sua própria materialidade, sendo definido conceitualmente, como impulsos elétricos que respondem a uma sequência numérica predefinida e que, quando canalizados em um suporte informático com memória, originam informações inteligíveis.

Acerca das características das provas digitais, notou-se que são: imateriais, frágeis, voláteis, rastreáveis, recuperáveis, vastas, dispersas e complexas.

Imateriais, pois não possui representação física, facilitando sua transmissão e permitindo o armazenamento massivo de conteúdos em sistemas informáticos. Voláteis, pois são suscetíveis a constantes mudanças e pode ser facilmente alterada ou desaparecer com simples modificações na sequência numérica que a constitui. Suscetíveis a clonagem e dispersíveis, devido à sua imaterialidade, a prova digital pode ser facilmente clonada e transmitida para outros dispositivos eletrônicos, o que representa um risco à preservação da originalidade do arquivo.

Além disso, são frágeis (facilmente alteráveis e corrompidas), rastreáveis (contêm metadados sobre origem e autoria), recuperáveis (podem ser recuperadas após exclusão) e vastas e complexas (envolvem dados volumosos e de difícil análise).

Abordou-se ainda as especificidades de alguns tipos de provas digitais, mais comumente utilizados atualmente, como os documentos eletrônicos, mensagens instantâneas, provas de geolocalização e comunicações eletrônicas (e-mails). Destacando a evidente invalidade jurídica dos *print screens* (captura de telas) como meios de prova.

A prova documental é uma espécie clássica de prova e está prevista de maneira expressa no CPC e sua admissibilidade depende do atendimento aos requisitos de validade e da garantia de possibilidade de impugnação. A prova

documental então abrange qualquer material, público ou privado, analógico ou digital, que represente um fato, um pensamento, uma expressão, uma ideia, uma foto, um vídeo, uma ordem, uma vontade, entre outros. Já o documento eletrônico pode ser definido como qualquer informação gerada, transmitida, acessada e armazenada em meios eletrônicos, que dispensa o papel físico ou então como uma sequência de *bits* (representação decodificada) traduzida por algum programa ou *software* que representa algum fato ou informação.

É necessário ainda repisar que, assim como o termo “prova digital” trata-se de uma espécie da prova eletrônica, sendo este um termo mais amplo, o documento eletrônico e o digital também seguem a mesma linha.

A título de exemplo prático, a CNH digital e a CNH eletrônica. Enquanto a primeira é originada/criada exclusivamente e diretamente em formato digital a CNH eletrônica pode ser a CNH física em papel escaneada e digitalizada, ou seja, não foi originada por meio digital. Essa distinção é necessária pois para garantir a autenticidade desses documentos o procedimento é distinto.

É evidente que os aplicativos de mensagens instantâneas se tornaram parte onipresente na rotina de boa parte da humanidade, tanto em âmbito pessoal como profissional, em razão da facilidade de comunicação e conveniência que proporcionam**.** apesar da alta relevância das conversas de aplicativos de mensagens para fins de comprovação de fatos juridicamente relevantes, há ainda grande negligência entre os operadores do direito com a utilização dessas mensagens. Não é incomum encontrar em processos judiciais a apuração de fatos com meras capturas de telas (*print screen*) de conversas, que nada mais são que arquivos de imagens, que podem ser facilmente manipuladas, alteradas ou forjadas. Já existem aplicativos que inclusive criam diálogos falsos (*fakes),* como por exemplo o *Whatsfake, Fake chat; Whatsmochk Pro*, entre outros, que simulam a interface do *WhatsApp Messenger.* Existem também aplicativos que simulam conversas do *Instagram e Facebook,* como *Telefun e FunstaPro.* Além dos aplicativos que simulam mensagens que não são reais, as próprias capturas de tela podem ser alteradas facilmente com algum *software* de edição de imagens, isso porque, como dito, são apenas arquivos de imagens. Neste sentido, o judiciário brasileiro já tem pautado suas

decisões pelo indeferimento de acusações em que o *print screen* de conversas é utilizado como meio de prova.

Outra consideração importante sobre as mensagens instantâneas como meios de prova, é que o STJ decidiu que o espelhamento de mensagens de whatsapp como meio de prova é ilegal e não pode ser equiparado a interceptação telefônica, isso porque o espelhamento via WhatsApp Web permite acesso ilimitado a todas as conversas, passadas, presentes e futuras, possibilitando ao investigador atuar como participante e até mesmo excluir mensagens sem deixar rastros.

Quanto a confiabilidade da ata notarial, é questionável, isso porque ela é elaborada a partir de um testemunho não especializado, além de estarem alocadas em um ambiente volátil e complexo. A ata notarial não produz uma prova com a garantia de que seu conteúdo seja original e não tenha sido forjado ou manipulado.

Acerca da validade do e-mail como prova judicial, notou-se que os tribunais brasileiros divergem sobre a validade do e-mail como prova judicial, mas o entendimento predominante da jurisprudência considera que as cópias de mensagens eletrônicas, por si só, não são suficientes para comprovar fatos e situações jurídicas, necessitando de outros elementos de convicção, como documentos, comprovantes.

Já a geolocalização utiliza dados de posição geográfica para determinar a localização de dispositivos ou indivíduos, sendo essencial para aplicativos de navegação. Esses dados são cada vez mais utilizados como prova em processos judiciais, devido à precisão e ao volume de informações que podem fornecer. A carência da prova testemunhal no direito brasileiro leva ao uso crescente de provas de geolocalização para esclarecer fatos.

Encerrando o segundo capítulo com a menção das normas legais que possuem conexão ou relevância nas provas digitais, destacando as seguintes: a) MP nº 2.200-2/2001; b) Lei n° 11.419/2006; c) Lei n° 12.682/2012; d) Lei

n° 12. 965/2014; e) Lei n° 13.694/2019. Assim, cumpre abordar brevemente as referidas normas.

Por fim, o **Capítulo 3** esclareceu inicialmente sobre a cadeia de custódia como instrumento essencial para validade das provas de modo amplo, partindo para as especificidades da cadeia de custódia digital, ficando evidente sua complexidade ante as provas tradicionais e, portanto, a ineficácia da aplicação isolada da Lei nº 13.694/2019, apelidada como pacote anticrime, que tratou da cadeia de custódia, mas deixou de abordar de modo específico e apartado, sobre as provas digitais. Seguindo então para o objetivo principal desta dissertação, que foi destrinchar não apenas a norma ABNT NBR ISO/IEC 27037:2013, mas também com o suporte de normas internacionais, para fins de identificar a(s) forma(s) correta(s) de tratamento da prova digital, de modo que preserve sua integridade. Ao final, pretendeu-se apresentar soluções tecnológicas para o tratamento das provas (evidências) digitais.

O conceito da cadeia de custódia foi introduzido no código de processo penal pelo pacote anticrime, apesar disso esse instituto de proteção e preservação já é abordado há muitos anos pela doutrina nacional e internacional. A cadeia de custódia veio conceituada em lei 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.

A partir disso, o conjunto de atos da cadeia de custódia, segundo o artigo 158-B do CPP consiste em: 1. Reconhecimento; 2. Isolamento; 3. Fixação; 4. Coleta; 5. Acondicionamento; 6. Transporte; 7. Recebimento; 8. Processamento; 9. Armazenamento; 10. Descarte.

O protocolo documental da cadeia de custódia, deve registrar os seguintes indicadores: "*a) quem; b) quando; c) como; d) onde; e) por que; f) para que; g) o que; h) com que motivação."* [374] A conferência desses indicadores irá garantir a existência, eficácia e validade da cadeia de custódia.

[374] ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-C. p. 401.

Acerca das consequências da quebra da cadeia de custódia, a Lei nº 13.964/2019 é silente, apesar da consolidação importantíssima de todos os procedimentos e etapas. Sobre esse prisma, existem vertentes dogmáticas que divergem entre si. Garantistas entendem que qualquer ruptura das etapas previstas em Lei, consiste na declaração de ilicitude ou ilegitimidade da prova e consequente imediata e inafastável exclusão (desentranhamento dos autos, se for o caso) e dos que dele decorrem, a conhecida teoria da árvore dos frutos envenenados. Já os punitivistas, entendem que caberá ao julgador, de acordo com o caso concreto, valorar e decidir sobre a prova obtida com irregularidades na cadeia de custódia.

Apesar de abordar com clareza a cadeia de custódia dos vestígios tradicionais, a Lei nº 13.964/2019 pecou ao não dedicar um espaço específico para os vestígios digitais, tendo em vista que na época em que foi publicada (2019), as provas digitais já eram protagonistas nos processos judiciais. Segundo dados estatísticos da Convenção de Budapeste de 2018, em média 85% das investigações criminais dependem de provas digitais.

A lei restringe erroneamente o conceito de vestígio a objetos materiais e tangíveis, praticamente excluindo as provas digitais. Devido à complexidade e vulnerabilidade dessas provas, elas exigem uma cadeia de custódia mais detalhada. O isolamento da cadeia de custódia visa minimizar a contaminação, mas a plurissubjetividade dos materiais informáticos é comum.

O reconhecimento e a fixação de vestígios digitais diferem das provas tradicionais, pois a linguagem digital é incompreensível sem um dispositivo eletrônico programado para tradução. Apenas profissionais capacitados podem reconhecer e fixar vestígios digitais adequadamente.

Dados em dispositivos eletrônicos não são apagados definitivamente sem um procedimento lógico específico. A exclusão de um arquivo deixa espaço disponível, que será utilizado sequencialmente para novos arquivos. Portanto, a prova digital requer uma análise complexa e detalhada.

O artigo 158-D do CPP prevê que o recipiente para armazenar a prova deve observar suas características. No caso das provas digitais, o “recipiente”

é irrelevante, pois cópias digitais são idênticas ao original, garantidas pelo código HASH, que assegura a integridade dos dados.

Então é evidente que o tratamento das provas digitais exige uma análise mais específica do que as tradicionais, indo além dos critérios estabelecidos na Lei nº 13.964/2019.

Primeiro Passo: Reconhecimento, Identificação, Preparação e Isolamento

Reconhecimento e Identificação: A fase inicial envolve a identificação e reconhecimento das evidências digitais, considerando as características únicas de cada fonte de informação. As fontes podem ser abertas (acesso livre) ou fechadas (acesso restrito, necessitando ou não de autorização judicial).

Preparação: Após a identificação, a preparação envolve estabelecer processos e prioridades para o trabalho, decidindo se a evidência será coletada no local ou transportada para análise.

Isolamento: Medidas para isolar e preservar a integridade das evidências incluem fotografar os dispositivos, usar luvas descartáveis, evitar ligar ou desligar dispositivos, desconectar da tomada ou remover baterias, e usar dispositivos de bloqueio como bolsas de Faraday.

Documentação: Detalhes como identificação do titular da linha telefônica e rotulagem de dispositivos são documentados, assegurando que não sejam manipulados ou visualizados indevidamente.

Segundo Passo: Coleta, Aquisição, Acondicionamento e Preservação

Coleta: Envolve recolher dispositivos para análise em ambiente apropriado e seguro, com documentação detalhada de todas as etapas, fotografando e rotulando as evidências. A embalagem correta, usando sacos de polietileno, é fundamental.

Aquisição: Produção de uma cópia integral e idêntica da evidência digital, garantindo a integridade com tecnologias como o código Hash. A cópia deve ser realizada de dispositivos limpos para evitar contaminação.

Ordem de Volatilidade: A coleta deve seguir a ordem de volatilidade dos dados, começando com os mais voláteis.

Preservação: Aplicação de técnicas desde o primeiro contato para garantir a integridade, imutabilidade e autenticidade das evidências, assegurando a cadeia de custódia.

Terceiro Passo: Exame, Análise e Resultados

Exame: Identificação e filtro das evidências coletadas para determinar o que é relevante para a perícia. Ferramentas forenses são usadas para extrair e indexar informações.

Análise: Inspeção dos resultados para gerar respostas úteis. Inclui identificação de pessoas, datas, locais e eventos, criando uma linha do tempo e reconstruindo a cena.

Documentação e Relatório Final: Todos os passos são documentados de forma técnica e científica. O relatório final inclui uma descrição detalhada do percurso da cadeia de custódia e as conclusões finais, com embasamento técnico-científico compreensível juridicamente.

No contexto técnico, já existem diversas ferramentas que ajudam a preservar e armazenar com segurança materiais digitais, assegurando a integridade e autenticidade das provas. Estas tecnologias, cada vez mais avançadas, automatizam processos, simplificando a gestão e manuseio de evidências digitais.

Função *Hash*: Um algoritmo matemático que gera uma sequência numérica única e irreversível para verificar se os dados de um dispositivo foram alterados. A função hash é crucial para garantir que evidências digitais não sejam manipuladas, assegurando a legitimidade de cópias de dispositivos eletrônicos.

Criptografia: Transformação de uma mensagem simples em uma mensagem cifrada, acessível apenas por pessoas autorizadas com uma chave de acesso. Utilizada para proteger dados financeiros, comunicações e a identidade de usuários. Existem chaves simétricas (mesma chave para codificar e decodificar) e assimétricas (duas chaves diferentes, uma para cada função). A criptografia é essencial para proteger a integridade e autenticidade das provas digitais.

Blockchain: é uma tecnologia que verifica e corrige automaticamente dados modificados, gerando imutabilidade. É um banco de dados online, público e descentralizado, usado para garantir a preservação de provas digitais. Um exemplo é a plataforma DataCertify, que utiliza blockchain e carimbo de tempo para garantir a imutabilidade dos dados coletados da internet, entretanto, é importante destacar que a plataforma DataCertify e outras soluções que utilizam a tecnologia Blockchain, fornecem uma segurança de preservação apenas após coletado, mas não durante, portanto, não garantem a origem ou confiança da informação.

Verifact: Plataforma online para verificação de provas digitais, emitindo relatórios técnicos certificados com assinatura digital e carimbo de tempo ICP-BRASIL. Preserva todas as etapas da cadeia de custódia e é reconhecida por diversos órgãos públicos e jurisprudências como método seguro para qualificação de provas digitais. A plataforma Verifact se diferencia da blockchain por garantir a integridade da prova digital desde a coleta, e não apenas na etapa de preservação. Enquanto a blockchain impede manipulações posteriores ao registro, a Verifact cria um ambiente virtualizado e isolado para cada coleta, sem atividades anteriores, com conexão independente e acesso limitado, garantindo a não manipulação dos dados durante todo o processo.

Em concluso, percebe-se que a crescente importância das provas digitais no sistema judiciário exige uma compreensão abrangente das tecnologias e dos procedimentos adequados para garantir a sua validade e autenticidade.

A busca pela verdade no processo judicial deve sempre se pautar pela observância dos direitos e garantias fundamentais, especialmente no que diz respeito à privacidade e à proteção de dados pessoais, afinal, a justiça digital deve ser construída sobre bases sólidas, que garantam a confiabilidade das provas e a proteção dos direitos individuais.

Por fim, retoma-se o problema e a hipótese básica da pesquisa:

Quais elementos (ou requisitos) são necessários para que uma prova digital tenha validade jurídica nos processos penais?

Para o problema de pesquisa foi levantada a seguinte hipótese: Para que uma prova digital tenha validade, deve estar demonstrada a integridade da cadeia de custódia na aquisição e no tratamento da prova, certificando-se a observância dos requisitos de existência, validade e eficácia da prova.

Verificou-se que de fato, a ausência de demonstração da integridade da cadeia de custódia, poderá resultar a quebra da cadeia de custódia, que acarreta a ilicitude ou ilegitimidade da prova, com a consequente exclusão dos autos, tanto das provas ilícitas ou ilegítimas em si, como das dela decorrentes. Em resumo, a cadeia de custódia deve demonstrar: a) As fontes que incluem os dispositivos eletrônicos, nuvens e o PC; b) As pessoas envolvidas, o autor, o réu, os investigadores forenses, peritos e qualquer outro agente que tenha envolvimento com os fatos; c) Os fatores, que respondem questões como, Onde estão as evidências?; Quem as gerencia?; Por que faze-lo?; Quando serão tratadas?; Como serão tratadas?; d) As instituições (ex: autoridades policiais); e) Técnicas que irão garantir a integridade das evidências digitais.

A Existência corresponde ao dever de a evidência ser corretamente identificada e registrada no momento da coleta, assegurando que o dispositivo ou dado digital seja preservado em seu estado original. A Validade corresponde a aquisição, que a integridade dos dados deve ser garantida por meio de técnicas como a utilização de código *Hash*, que assegura que a cópia seja idêntica ao original sem qualquer alteração. Já a Eficácia significa que o procedimento deve ser documentado detalhadamente, incluindo a embalagem, rotulagem e preservação das

evidências, de forma que a cadeia de custódia permaneça intacta e a prova possa ser apresentada em juízo com total confiança em sua autenticidade.

A utilização de soluções tecnológicas, como a função *hash*, a criptografia, blockchain e Verifact, tem se mostrado fundamental para garantir a confiabilidade e a segurança das provas digitais, contribuindo para a efetividade da justiça na era digital.

Desta forma, resta finalizado o trabalho de pesquisa sobre o regime democrático as provas digitais no processo penal: aquisição e qualificação.

REFERÊNCIA DAS FONTES CITADAS

ALVES, Matheus de Araújo. **Crimes digitais:** análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova. Dissertação (Mestrado em Direito). 2018. 97 f. Faculdade de Ciências Humanas, Sociais e da Saúde, Universidade FUMEC, Belo Horizonte, 2018.

ALVIM, Arruda. **Manual de direito processual civil:** teoria geral do processo e o processo de conhecimento. – 17. ed. rev., atual. e ampl. – São Paulo: Revista dos Tribunais, 2019.

ALVIM, Eduardo Arruda; GRANADO, Daniel Willian; FERREIRA, Eduardo Aranha. **Direito processual civil**. – 6. ed. – São Paulo: SaraivaJur, 2019.

ANDRADE, Rafael Santos; SILVA, Fernando dos Santos. **Algoritmo de criptografia RSA:** análise entre a segurança e velocidade. Revista Eventos Pedagógicos, v. 3, n. 3, p. 438-457, ago. – dez. 2012.

ARAKAKI, Ana Carolina Simionato; ARAKAKI, Felipe Augusto. **Dados e metadados:** conceitos e relações. Ci.Inf., Brasília/DF, n. 3, v. 49, p. 34-45, set./dez. 2020.

ARAÚJO, Marcelo Barreto de. **Comércio eletrônico, Marco Civil da internet, Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviços e Turismo, 2017.

ASSEMBLEIA GERAL DA ONU. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>.

AVENA, Norberto. **Processo Penal**. – 12. ed. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020.

BADARÓ, Gustavo Henrique. **Processo Penal**. – 9. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2021.

BADARÓ, Gustavo. **A cadeia de custódia e sua relevância para a prova penal**. In: SIDI, Ricardo; LOPES, Anderson Bezerra. Temas atuais da investigação preliminar no processo penal. – 1. reimpr. – Belo Horizonte: D'Plácido, 2018.

BADARÓ, Gustavo. **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.

BAHIA. Ministério Público do Estado da Bahia. **Atestado:** parecer jurídico 409/2020. out. 2021. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2021/10/Atestado_SEI_19.09.01970.0016798_2021_65.pdf>.

BARRETO JR., Irineu Francisco. **Atualidade do conceito de sociedade da informação para a pesquisa jurídica**. In: O direito na sociedade da informação. Coord. Liliana Minardi Paesani. São Paulo: Atlas, 2007.

BORRUSO, Renato; DI GIORGI, Rosa Maria; MATTIOLI, Leonello; RAGONA, Mario. ***L´informatica del diritto****. Seconda edizione riveduta e aggiornata*. Milano: Dott. A. Giufrè, 2007.

BRASIL. Associação Brasileira de Normas Técnicas. **ABNT ISO/IEC 27037:2013**. Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. São Paulo: ABNT, 2013.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Promulgada em 5 de out. de 1988. Brasília, DF; out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm>.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm>.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF; mai. 2016. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, RJ; out. 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>.

BRASIL. **Lei nº 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF; dez. 2006. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm>.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF; nov. 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>.

BRASIL. **Lei nº 12.682, de 9 de julho de 2012**. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Brasília, DF; jul. 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm>.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF; abr. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF; mar. 2015. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF; dez. 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm>.

BRASIL. **Lei nº 8.935, de 18 de novembro de 1994**. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro. (Lei dos cartórios). Brasília, DF; nov. 1994. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8935.htm>.

BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF; ago. 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>.

BRASIL. Ministério da Justiça. **Portaria nº 82, de 25 de março de 2014**. Estabelece normas e procedimentos para a cadeia de custódia de vestígios. Diário Oficial da União, Brasília, DF, 26 mar. 2014. Seção 1.

BRASIL. Ministério Público Federal (MPF). **Atestado de capacidade técnica PGR nº 00011690/2024**. jan. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/01/atestado_MPF_verifact_jan2024.pdf>.

BRASIL. Polícia Federal. **Diretrizes para a coleta e preservação de evidências digitais –** NC nº 21**.** Disponível em: **<**https://www.gov.br/ctir/pt-br/centrais-de-conteudo/palestras-em-pdf/coloquios/9o-coloquio-ctir-gov-2013-2015/1coloquio2015_palestra03_dpf_flaviosilveira.pdf/view>.

BRASIL. Superior Tribunal de Justiça (STJ). **Agravo Regimental no Habeas Corpus nº 828054/RN**. Quinta Turma. Relator(a): Ministro Joel Ilan Paciornik. Data do Julgamento: 24 abr. 2024. Publicado no DJe em: 29 abr. 2024.

BRASIL. Superior Tribunal de Justiça (STJ). **Agravo Regimento no Recurso Ordinário em Habeas Corpus nº 133.430/PE**. Sexta Turma. Relator(a): Ministro Nefi Cordeiro. Data do Julgamento: 23 fev. 2021. Publicado no DJe em: 26 fev. 2021.

BRASIL. Superior Tribunal de Justiça (STJ). **Habeas Corpus nº 160.662/RJ**. Sexta Turma. Relator(a): Ministra Assusete Magalhães. Data do Julgamento: 18 fev. 2014. Publicado no DJe em: 17 mar. 2014.

BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Especial nº 1.381.603/MS**. Quarta Turma. Relator(a): Ministro Luis Felipe Salomão. Data do Julgamento: 06 out. 2016. Publicado no DJe em: 11 nov. 2016.

BRASIL. Superior Tribunal de Justiça (STJ). **Recurso Ordinário em Habeas Corpus nº 99.735/SC**. Sexta Turma. Relator(a): Ministra Laurita Vaz. Data do Julgamento: 27 nov. 2018. Publicado no DJe em: 12 dez. 2018.

BRASIL. Tribunal Superior Eleitoral (TSE). **Atestado nº 48/2023**. jul. 2023. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2023/08/Atestado_de_Capacidade_Tecnica_n_48_TSE-Verifact.pdf>.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013.

BUCKLAND, Michael. ***Information and Society***. Cambridge: MIT Press, 2017.

CALAZA, Tales. **O direito à privacidade: origem histórica e jurídica**. Fundamentos do Direito Digital, Coordenadores: João Victor Rozatti Longhi; José Luiz de Moura Faleiros Júnior; Gabriel Oliveira de Aguiar Borges; Guilherme Reis. Uberlândia: LAECC, 2020.

CAPEZ, Fernando. **Curso de processo penal**. – 30. ed. – São Paulo: SaraivaJur, 2023.

CARLIZZI, Gaetano. **La prova tecnológica nel processo penale.** In: LUPÁRIA, Luca; MARAFIOTI, Luca; PAOLOZZI, Giovanni (a cura di). Dimensione tecnologica e prova penale. G. Giappichelli Editore – Torino, 2019.

CARNEIRO, Aline Ferreira Costa; BRITO, Lucimeire Zago de; TAVARES, Viviane Ramone. **Compliance digital:** novas perspectivas sobre ética na sociedade da informação. Estudos essenciais de Direito Digital, Coordenadores: João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior. Uberlândia: LAECC, 2019.

CARVALHO, Romullo Wheryko Rodrigues de. **A importância da cadeia de custódia na computação forense**. Revista Brasileira de Criminalística, v. 9, n. 2, p. 134-138, jul. 2020.

CHAVES JUNIOR, Airto; DE PAULA, Leonardo Costa; PÁDUA, Thiago Aguiar de. **O prejuízo da "regra do prejuízo"**: a não recepção constitucional do art. 563 do Código de Processo Penal (*pas de nullité sans grief*). Revista Brasileiro de Ciências Criminais, Ano 29, v. 182, p. 163-190, ago. 2021.

CHAVES JÚNIOR, José Eduardo de Resende. **Comentários à lei do processo eletrônico**. São Paulo: LTr, 2010.

CLEMENTINO, Edilberto Barbosa. **Processo judicial eletrônico**. Curitiba: Juruá, 2007.

CONVENÇÃO DE BUDAPESTE**. Convenção sobre o Cibercrime**. Budapeste, 2018. Disponível em: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

COUTINHO, Gustavo Leuzinger. **A Era dos 'smartphones':** um estudo exploratório sobre o uso dos 'smartphones' no Brasil. In: REBELLATO, Luiz Fernando Bugiga. **A**

análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares.

DANIELE, Marcello. **La prova digitale nel processo penale**. Rivista di Diritto Processuale, 2011.

DATACERTIFY. **Como a DataCertify garante a segurança das provas registradas?** Disponível em: <https://www.datacertify.com.br/>.

DINIZ, Maria Helena. **Curso de direito civil brasileiro:** teoria das obrigações contratuais e extracontratuais. – 40. ed., rev. e atual. de acordo com a Lei n. 14.195/2021 - São Paulo: Saraiva, 2023.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. – 2. ed. – São Paulo: Thomson Reuters Brasil, 2020.

EDGE, Charles; O'DONNELL, Daniel. *Introduction to cryptography*. In: LOPES, Marcus Vinícius Pimenta. A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de provas digitais. Tese de Doutorado. 218 f. Pontíficia Universidade Católica de Minas Gerais, Belo Horizonte, 2023.

EDINGER, Carlos. **Cadeira de custódia, rastreabilidade probatória**. Revista brasileira de ciências criminais, v. 24, n. 120, p. 237-257, mai./jun., 2016.

FARADAY, Michael. Experimental researches in electricity. In: NESSI, Alan Martin. Manual de evidencia digital.

FAZZALARI, Elio. ***Istituzioni di Diritto Processuale***. – 8. ed. – Padova: CEDAM, 1996.

FERNANDES, Antônio Scarance.; GRINOVER, Ada Pelegrini; FILHO, Antônio Magalhães Gomes. **As nulidades no processo penal**. São Paulo: Revista dos Tribunais, 2011.

FERRAJOLI, Luigi. **Direito e razão**: teoria do garantismo penal. – 4. ed., rev.; tradutores Ana Paula Zomer Zica ... [et al.] – São Paulo, Revista dos Tribunais, 2014.

FONSECA, Gabriel Ciríaco. **O delegado de polícia e a cadeia de custódia**. Consultor Jurídico (ConJur), 27 jun. 2022. Disponível em: <https://www.conjur.com.br/2022-jun-27/gabriel-ciriaco-delegado-cadeia-custodia/>.

GIOVANNI, Pascuzzi. **Il diritto dell´era digitale**: tecnologie informatiche e regole privatistiche. Bologna: Il Mulino, 2006.

GOMES FILHO, Antonio Magalhães. **Notas sobre a terminologia da prova** (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide (Coords.). Estudos em homenagem à Professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005.

GUARDIA, Gregório Edoardo Raphael Selingardi. **Comunicações eletrônicas e dados digitais no processo penal.** Dissertação (Mestrado em Direito). 2012. 256 f. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012.

GUGLIARA, Rodrigo; FISCHER, Bianca Camargo. **Conceitos essenciais sobre a sociedade em rede.** Fundamentos do Direito Digital, Coordenadores: João Victor Rozatti Longhi; José Luiz de Moura Faleiros Júnior; Gabriel Oliveira de Aguiar Borges; Guilherme Reis. Uberlândia: LAECC, 2020.

HERMEIRO, Andreia Carina Cláudio. **A cadeira de custódia da prova digital:** o uso da tecnologia blockchain como forma de preservação. 2023. Dissertação (Mestrado em Ciências Jurídico-Forenses). 64 f. Faculdade de Direito da Universidade de Coimbra, Coimbra, 2023.

INTERPOL. Global guidelines for digital forensics laboratory. 2023.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. **Guide to integrating forensic techniques into incident response**: recommendations of the National Institute of Standards and Technology (NIST), ago. 2006. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>.

KENT, William. **Data and reality:** a timeless perspective on perceiving and managing information in our imprecise world. Bedford, MA: IBM Corporation, 1978.

KERR, O. S. ***Digital evidence and the new criminal procedure***. Columbia law review, v. 105, p. 279-318, 2005.

KIST, Dario José. **Prova digital no processo penal**. – 1. ed. – São Paulo: JH Minuzo, 2019.

LAGO, Lucas. **Blockchain:** confiança através de algoritmos. Escola Politécnica do Estado de São Paulo, CEST – Boletim, v. 2, n. 4. out. 2017.

LATOUCHE, Serge. **Pequeno tratado do decrescimento sereno**. Tradução Claudia Berliner. São Paulo: Editora WMF Martins Fontes, 2009.

LIMA, Renato Brasileiro de. **Manual de Processo Penal:** volume único. – 8. ed. rev., ampl. e atual. – Salvador: JusPodivm, 2020.

LIRA, Waleska Silveira; CÂNDIDO, Gesinaldo Ataíde; ARAÚJO, Geraldo Maciel de; BARROS, Marcelo Alves de. **A busca e o uso da informação nas organizações**. Perspectivas em Ciência da Informação, v. 13, n. 1, p. 166-183, jan./abr. 2008.

LISBOA, Roberto Senise. **Direito na sociedade da informação**. Revista dos Tribunais, v. 95, n. 847, p. 78-95, mai. 2006.

LOPES JUNIOR, Aury; ROSA, Alexandre Morais da. **A importância da cadeia de custódia para a preservar a prova penal**. Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal/>.

LOPES JUNIOR., Aury. **Direito processual penal**. – 18. ed. – São Paulo: Saraiva Educação, 2021.

LYOTARD, Jean-François. **A condição pós-moderna: um relatório sobre o conhecimento**. Tradução de Ricardo Corrêa Barbosa. 7. ed. Rio de Janeiro: José Olympio, 1998.

MACIEL, Rafael Fernandes. Manual prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18). – 1. ed. – Goiânia: RM Digital Education, 2019.

MARQUES, Antônio Terêncio. **A prova documental na internet**. – 1. ed., 6. reimpr. - Curitiba: Juruá, 2011.

MATIDA, Janaina. A cadeia de custódia é condição necessária para a redução dos riscos de condenações de inocentes. Boletim IBDCRIM, Ano 28, n. 331, p. 6-9, jun. 2020.

MATO GROSSO DO SUL. Ministério Público do Mato Grosso do Sul. **Atestado de capacidade técnica**. mar. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/05/atestado_ministerio_publico_ms_verifact.pdf>.

MONTEVERDE, Wagner Ap. **Parecer técnico de auditoria de infraestrutura de aplicação**. EarlySec. 29 nov. 2019. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2020/03/Parecer_auditoria_aplicacao_Verifact-manifesto2019Ax.pdf>.

NAGY, Marcelo; STEFANO, Leandro Morales Baier. **Auditoria baseada nos requisitos dispostos na ABNT NBR ISSO/IEC 27037:2013 e no Código de Processo Penal**. STW Brasil – Segurança em Tecnologia Ltda. 28 mar. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/03/laudo_verifact_iso27037_cadeia-de-custodia.pdf>.

NAKAMOTO, Satoshi. ***Bitcoin:*** *a peer-to-peer electronic cash system*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>.

NESSI, Alan Martin. ***Manual de evidencia digital***. – 1. ed. – Lima: American Bar Association, 2017.

NUCCI, Guilherme de Souza. **Curso de direito processual penal**. – 17. ed. – Rio de Janeiro: Forense, 2020.

PAESANI, Liliana Minardi. **Direito e internet:** liberdade de informação, privacidade e responsabilidade civil. – 7. ed. – São Paulo: Atlas, 2014.

PARAÍBA. Ministério Público da Paraíba; Núcleo de Gestão do Conhecimento (NGC); Grupo de Atuação Especial contra o Crime Organizado (GAECO). **Atestado de capacidade técnica**. jan. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/01/atestado_MPPB_verifact_jan2024.pdf>.

PARANÁ. Secretaria de Estado da Segurança Pública; Polícia Civil do Paraná. **Atestado de capacidade técnica**. nov. 2022. Disponível em:

<https://www.verifact.com.br/wp-content/uploads/2022/11/2022_atestado_de_capacidade_tecnica-Verifact-PCPR.pdf>.

PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica:** teoria e prática.

PINHEIRO, Patricia Peck. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021.

POHLMANN, Sérgio. **LGPD ninja:** entendendo e implementando a lei geral de proteção de dados nas empresas. Rio de Janeiro: Editora Fross, 2019.

POLL, Roberta Eggert. **Algoritmos decisionais e o poder judiciário:** limites à utilização da inteligência artificial, à luz dos direitos fundamentais. 2022. Tese (Doutorado em Direito). Programa de Pós-Graduação em Direito, Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022.

POMERANTZ, J. ***Metadata***. Cambridge: MIT Press, 2015. In: ARAKAKI, Ana Carolina Simionato; ARAKAKI, Felipe Augusto. **Dados e metadados:** conceitos e relações.

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

REBELLATO, Luiz Fernando Bugiga. **A análise constitucional do sigilo e da privacidade nas investigações criminais:** o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado em Direito). 2020. 305 f. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2020.

REINALDO FILHO, Demócrito. **A exibição da prova eletrônica em juízo** – necessidade de alteração das regras do processo civil?. Disponível em: <https://www.migalhas.com.br/depeso/31031/a-exibicao-da-prova-eletronica-em-juizo---necessidade-de-alteracao-das-regras-do-processo-civil>.

REIS, Alexandre Cebrian Araújo. **Direito processual penal**. – 11. ed. – São Paulo: SaraivaJur, 2022.

RONDÔNIA. Tribunal Regional Eleitoral de Rondônia. **Representação nº 0601791-65.2022.6.22.0000**, de Cacoal/RO. Relator: Desembargador Marcelo Stival. Data de Julgamento: 17 out. 2022.

ROSA, Alexandre Morais da. **A questão digital**: o impacto da inteligência artificial no Direito. Revista de Direito da Faculdade Guanambi, v. 6, n. 2, jul./dez. 2019. Disponível em: <https://www.redalyc.org/journal/6080/608065718005/608065718005.pdf>.

ROSA, Alexandre Morais da. **Guia do processo penal estratégico**: de acordo com a teoria dos jogos e MCDA-A. – 1. ed. – Florianópolis: Emais, 2021.

ROSA, Alexandre Morais da. **Lei de acesso à informação pode iluminar as sombras do processo penal**. Consultor Jurídico (ConJur). Disponível em:

<https://www.conjur.com.br/2016-jan-01/limite-penal-lei-acesso-informacao-iluminar-sombras-processo-penal/>.

ROSA, Alexandre Morais da. **O "*print screen*" é insuficiente à materialidade nos crimes digitais**. Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2022-jun-17/limite-penal-print-screen-materialidade-crimes-digitais/>.

ROSA, Alexandre Morais da; CANI, Luiz Eduardo. **Guia para Mitigação dos Erros Judiciários no Processo Penal**: as causas prováveis e as estratégias de enfrentamento. Florianópolis: Emais, 2021.

ROSA, Alexandre Morais da; PRÓSPERO, Felipe Navas. **Qual a validade jurídica dos documentos pela rede blockchain?** Consultor Jurídico (ConJur). Disponível em: <https://www.conjur.com.br/2019-jan-11/limite-penal-qual-validade-juridica-documentos-rede-blockchain/>.

RUSAKOVA, E. P.; ZAITSEV, V. V. **Messenger chats as evidenci in civil and arbitration proceedings** – Russian judicial practice. Russian Journal of Legal Studies (Moscow). v. 7, n. 3, p. 9-15, 2020.

SADIKU, Matthew; SHADARE, Adebowale; MUSA, Sarhan. **Digital Forensic Chain of Custody**. International Journal of Advanced Research in Computer Science and Software Engineering, v. 7, n. 7, p. 117-118, 2017.

SANTA CATARINA. Polícia Civil de Santa Catarina; Delegacia-Geral; Gerência de Tecnologia da Informação. **Atestado de capacidade técnica**. jan. 2024. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2024/01/atestado_PCSC_verifact_jan2024.pdf>.

SANTANA, Priscila. **Do uso, tratamento e disponibilização de dados pessoais para fins processuais:** uma análise frente à Lei Geral de proteção de Dados. Estudos essenciais de Direito Digital, Coordenadores: João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior. Uberlândia: LAECC, 2019.

SANTOS, Uelinton B. dos. **Parecer técnico:** plataforma Verifact. Sipercon. 02 set. 2019. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2021/11/parecer-perito-v2.0-final-assinado.pdf>.

SÃO PAULO. Ministério Público do Estado de São Paulo. **Atestado de capacidade técnica**. jun. 2022. Disponível em: <https://www.verifact.com.br/wp-content/uploads/2022/10/Atestado_Capacidade_Tecnica_Verifact_Tecnologia_Ltda_CAEX_MPSP.pdf>.

SCHNEIER, Bruce, ***The value of encryption***. The Ripon Forum, abr. 2016. Disponível em: <https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.html>.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução Daniel Moreira Miranda. São Paulo: Edipro, 2018.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE). **Best practices for computer forensic acquisitions (17-F-002-2.0)**. Disponível em: < https://www.swgde.org/17-f-002/>.

SETZER, Valdemar W. **Dado, informação, conhecimento e competência**. Disponível em: <https://www.ime.usp.br/~vwsetzer/datagrama>.

SIDOU, José Maria Othon. **Dicionário jurídico:** Academia Brasileira de Letras Jurídicas. – 11. ed., rev. e atual. – Rio de Janeiro: Forense, 2016.

SILVA, Heide Miranda da. **Qual a diferença entre dados, informação e conhecimento?** Disponível em: <https://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm>.

SIMPSON, J. A.; WEINER, E. S. C. ***The Oxford English Dictionary***. – 2. ed., v. 3 – Oxford/UK, Clarendon Press, 1989.

SOUZA, Adriano Gomes. **Etapas do processo de computação forense:** uma revisão. Acta de Ciências e Saúde, n. 5, v2, 2016. Disponível em: **<**https://www2.ls.edu.br/actacs/index.php/ACTA/article/download/138/128>.

SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023.

SOUZA, Kenny Maiana Silva Novais de; EDLER, Gabriel Octacílio Bohn. **A responsabilidade civil pelo vazamento digital de dados sob a ótica do direito brasileiro**. Revista Ibero Americana de Humanidades, Ciências e Educação. São Paulo, v.8.n.05. maio. 2022.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015.

SYDOW, Spencer Toth. **Curso de direito penal informático**: parte geral e especial. – 3. ed. – Salvador: JusPODIVM, 2022.

TAMER, Maurício Antonio. **O princípio da inafastabilidade da jurisdição no direito processual civil brasileiro**. Rio de Janeiro: LMJ Mundo Jurídico, 2017.

TAVARES, João Paulo Lodelo Guimarães. **O regime jurídico das provas digitais no direito brasileiro**. Civil Procedure Review, v. 12, n. 3, set./dez. 2020.

TEIXEIRA, Tarcísio. **Direito digital e processo eletrônico**. – 6. Ed. – São Paulo: SaraivaJur, 2022.

THAMAY, Rennan; TEMER, Maurício. **Provas no direito digital:** conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020.

THEOHARIDOU, Marianthi; MYLONAS, Alexios; GRITZALIS, Dimitris. ***A risk assessment method for smartphones***. *27th Information Security and Privacy Conference* (*SEC*), jun. 2012, Heraklion, Crete, Greece.

VACIAGO, Giuseppe. **Digital Evidence**. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato. Torino: Giappichelli, 2012.

VAZ, Denise Provasi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de Doutorado. 198 f. Faculdade de Direito da Universidade de São Paulo, São Paul, 2012.

VERIFACT. **Validade jurídica**: alta confiança para registro de fatos na internet. Disponível em: <https://www.verifact.com.br/validadejuridica/>.

VIEIRA, Thiago. **Processo penal e novas tecnologias**. In: CONGRESSO IBCCRIM, 22., 2022, Florianópolis. Anais [...]. Florianópolis: IBCCRIM, 2022.

.