

**CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE**

CURSO DE DIREITO

**A PRODUÇÃO DE PROVAS DIGITAIS NO PROCESSO JUDICIAL E A
ADAPTAÇÃO DO DIREITO À TECNOLOGIA**

MATEUS MANARIN KOBAYASHI

Presidente Prudente/SP

2025

**CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE**

CURSO DE DIREITO

**A PRODUÇÃO DE PROVAS DIGITAIS NO PROCESSO JUDICIAL E A
ADAPTAÇÃO DO DIREITO À TECNOLOGIA**

MATEUS MANARIN KOBAYASHI

Monografia apresentada como requisito parcial de conclusão do curso e obtenção do grau de Bacharel em Direito, sob a orientação do Prof. João Pedro Gindro Braz.

Presidente Prudente/SP

2025

A PRODUÇÃO DE PROVAS DIGITAIS NO PROCESSO JUDICIAL E A ADAPTAÇÃO DO DIREITO À TECNOLOGIA

Monografia apresentada como requisito
parcial para obtenção do grau de Bacharel
em Direito.

João Pedro Gindro Braz

Isabela Mendez Berni

Paulo Henrique Adomaitis

Presidente Prudente, _____.

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, por ser essencial em minha vida, autor de meu destino, meu guia, socorro presente na hora da angústia, aos meus pais, Walter e Rosélia, e a minha irmã, Alana, pelo carinho, apoio e incentivo que sempre me deram em todos os momentos da minha vida.

AGRADECIMENTOS

Agradeço a Deus por me permitir estar aqui, depois de tudo e tanto, por sempre ser meu guia, amparo e proteção.

Aos meus pais, Walter e Rosélia, pela base sólida que sempre me proporcionaram. Agradeço pelo apoio incondicional, pelos sacrifícios diários e, principalmente, por me ensinarem com o exemplo a nunca desistir dos meus objetivos. Tudo o que sou e conquistei até aqui devo à força e dedicação de vocês.

À minha irmã Alana e minha sobrinha Liz, cuja presença constante e afetuosa me impulsiona todos os dias a ser alguém melhor, não apenas por mim, mas por elas também.

À minha namorada Lara, por sua fé inabalável em mim, especialmente nos momentos em que até eu mesma duvidei das minhas capacidades. Seu apoio foi essencial em minha caminhada.

Aos amigos que a faculdade me deu, com quem tive a alegria de compartilhar experiências únicas, aprendizados e desafios ao longo dessa trajetória inesquecível.

Ao corpo docente da Toledo Prudente Centro Universitário, com destaque especial ao meu orientador, professor João Pedro Gindro Braz. Sua dedicação, atenção e comprometimento foram fundamentais para que eu pudesse concluir este trabalho com qualidade e confiança.

Ao Tribunal de Justiça do Estado de São Paulo, instituição onde tive a honra de estagiar durante a graduação, e que foi determinante para minha formação acadêmica e pessoal no curso de Direito.

Por fim, minha gratidão a todas as pessoas que contribuíram, direta ou indiretamente, para a minha trajetória. Cada encontro, ensinamento e experiência teve papel essencial no meu crescimento profissional e humano.

RESUMO

Esta pesquisa analisa a produção de provas digitais no processo judicial brasileiro, tendo como problemática a dificuldade de assegurar a validade, legalidade e eficácia dessas provas diante das inovações tecnológicas e da necessidade de proteção dos direitos fundamentais. O trabalho pretende discutir como o ordenamento jurídico pode adaptar-se para garantir a admissibilidade de elementos digitais como prova, considerando critérios técnicos como autenticidade, integridade e cadeia de custódia. A relevância do tema se justifica pelo crescimento do uso de meios eletrônicos nas interações sociais e jurídicas, o que demanda uma abordagem atualizada e multidisciplinar no âmbito jurídico, sobretudo para preservar princípios constitucionais como o contraditório, a ampla defesa e o devido processo legal. A pesquisa adota uma metodologia qualitativa, de natureza exploratória, com base em revisão bibliográfica, análise documental e estudo normativo-comparado, utilizando legislações como o Código de Processo Civil, o Marco Civil da Internet e a LGPD, além de normas técnicas como a ABNT NBR ISO/IEC 27037:2012. Conclui-se que, embora o Direito brasileiro reconheça a validade da prova digital, ainda são necessários avanços normativos e técnicos para garantir sua eficácia, sendo imprescindível a capacitação dos operadores do Direito e a criação de parâmetros claros e seguros para sua utilização no processo judicial.

Palavras-chave: Provas Digitais. Processo Judicial. Autenticidade. Cadeia de Custódia. Lei Geral de Proteção de Dados (LGPD).

ABSTRACT

This research analyzes the production of digital evidence in the Brazilian judicial process, addressing the challenge of ensuring the validity, legality, and effectiveness of such evidence in light of technological innovations and the need to protect fundamental rights. The study aims to discuss how the legal system can adapt to allow the admissibility of digital elements as evidence, considering technical criteria such as authenticity, integrity, and chain of custody. The relevance of the topic lies in the increasing use of electronic means in social and legal interactions, which demands a modern and multidisciplinary legal approach, especially to safeguard constitutional principles like the adversarial system, broad defense, and due process of law. The research employs a qualitative, exploratory methodology based on bibliographic review, document analysis, and comparative normative study, drawing from legislation such as the Code of Civil Procedure, the Brazilian Internet Civil Framework, the General Data Protection Law (LGPD), and technical standards like ABNT NBR ISO/IEC 27037:2012. It concludes that, although Brazilian law already recognizes the validity of digital evidence, further normative and technical developments are necessary to ensure its effectiveness, emphasizing the importance of training legal professionals and creating clear and secure parameters for its use in judicial proceedings.

Keywords: Digital Evidence. Judicial Process. Authenticity. Chain of Custody. General Data Protection Law (LGPD).

LISTA DE SIGLAS E ABREVIATURAS

ART – Artigo

ACs – Autoridades Certificadoras

AC-Raiz - Autoridade Certificadora Raiz

ANPD - Autoridade Nacional de Proteção de Dados

ARs - Autoridades de Registro

CC – Código Civil

CF – Constituição Federal

CPC – Código de Processo Civil

GDPR - Regulamento Geral sobre a Proteção de Dados

ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira

IP – Endereço de Protocolo da Internet

LGPD – Lei Geral de Proteção de Dados

MP – Medida Provisória

PJe - Processo Judicial Eletrônico

STF - Supremo Tribunal Federal

STJ - Superior Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO	10
2 CONCEITO E FUNÇÃO DA PROVA	12
2.1 Tipos De Prova.....	13
2.2 Classificação Das Provas.....	15
2.3 Prova Ilícita.....	17
2.4 Prova Digital	20
2.5 A Legalidade Da Prova Digital No Ordenamento Jurídico Brasileiro	23
3 A LEI GERAL DE PROTEÇÃO DE DADOS “LGPD” – LEI 13.709/18.....	26
3.1 Principais Características Da Lei Geral De Proteção De Dados e Sua Aplicação	27
3.2 Intersecção Entre Proteção De Dados e Direito Probatório	29
3.3 Ponderação Entre Direito à Prova e Direito à Privacidade.	31
4 REQUISITOS DA VALIDADE DA PROVA DIGITAL.....	34
4.1 Autenticidade, Integridade, Veracidade e Cadeia De Custódia.	35
4.2 Preservações Da Prova: Hash, Blockchain e Certificações Digitais.....	38
4.3 Desafios Práticos Na Produção e Valoração Da Prova Digital	41
5 CONCLUSÃO	44
REFERÊNCIAS.....	46

1 INTRODUÇÃO

O presente trabalho teve como objetivo analisar a crescente relevância da prova digital no processo judicial brasileiro, diante da profunda transformação tecnológica vivenciada pela sociedade nas últimas décadas. O trabalho concentrou-se na compreensão jurídica das provas digitais, investigando seus fundamentos, requisitos de validade, limites legais e desafios práticos, com especial atenção à compatibilização entre o uso dessas provas e os princípios constitucionais que regem o processo, como o contraditório, a ampla defesa e o devido processo legal.

A escolha do tema justificou-se pela crescente utilização de meios eletrônicos em relações sociais e comerciais, tornando frequente a apresentação de documentos digitais, mensagens, vídeos e registros de geolocalização como elementos de prova em juízo. Nesse cenário, surgiram diversas controvérsias envolvendo a licitude da coleta desses dados, a verificação de sua autenticidade, integridade e cadeia de custódia, além da necessidade de proteção dos direitos fundamentais dos envolvidos, especialmente à privacidade e à autodeterminação informativa. Tais questões exigiram um estudo aprofundado das novas exigências jurídicas impostas pela realidade digital.

A pesquisa teve como objetivo geral examinar a admissibilidade e os critérios de validade da prova digital no processo judicial brasileiro. Como objetivos específicos, buscou-se: (i) compreender o conceito e a função da prova no ordenamento jurídico; (ii) identificar os tipos e classificações das provas tradicionais e digitais; (iii) analisar os limites da prova ilícita e os critérios da cadeia de custódia; (iv) investigar a intersecção entre a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e o direito probatório; e (v) avaliar os principais desafios enfrentados na produção, preservação e valoração das provas digitais em juízo.

O estudo foi fundamentado em um referencial teórico de base doutrinária nacional, especialmente autores como Nucci, Didier Jr., Cambi, Sarmiento e Capez, além da legislação vigente, como o Código de Processo Civil, o Marco Civil da Internet, a Lei Geral de Proteção de Dados, a Medida Provisória nº 2.200-2/2001 e normas técnicas como a ABNT NBR ISO/IEC 27037:2012. O método utilizado foi o dedutivo, com abordagem qualitativa e exploratória. Foram utilizados como procedimentos a análise documental, revisão bibliográfica e estudo normativo-comparado. O problema central investigado foi: como assegurar a validade, legalidade e eficácia da prova

digital no processo judicial brasileiro diante das inovações tecnológicas e da proteção dos direitos fundamentais? Partiu-se da hipótese de que, embora o ordenamento jurídico já contenha normas que reconheçam a validade da prova digital, a ausência de regulamentações específicas e a dificuldade prática de garantir a autenticidade e a integridade dos dados ainda comprometem sua eficácia.

As limitações do trabalho residiram na delimitação temática voltada ao processo judicial civil e penal em território brasileiro, sem aprofundamento em contextos internacionais ou administrativos. Também se limitou à análise teórica e normativa, sem abordagem empírica ou jurisprudencial detalhada.

O texto foi organizado em sete capítulos. Inicialmente, apresentou-se o conceito e a função da prova no processo, passando pela classificação e análise das provas ilícitas. Em seguida, abordou-se a evolução e os fundamentos da prova digital no ordenamento jurídico brasileiro, com destaque para os impactos da LGPD. Posteriormente, trataram-se os requisitos técnicos da validade da prova digital, como a função hash, blockchain e certificações digitais, culminando em uma discussão crítica sobre os desafios práticos enfrentados na sua produção e valoração. Por fim, a conclusão sistematizou os principais achados e reafirmou a necessidade de adaptação ética, normativa e técnica do Direito à realidade digital contemporânea.

2 CONCEITO E FUNÇÃO DA PROVA

No processo judicial, a prova configura-se como um instrumento jurídico regulamentado por lei, utilizado para demonstrar a ocorrência ou não de um fato, delimitando suas características e circunstâncias. Através dela que se forma a convicção do juiz ou das partes interessadas, conferindo uma leitura jurídica sobre os fatos controvertidos. Neste sentido, dentro do Direito Processual Civil sintetiza Cambi (2001, p.41):

Juridicamente, o vocábulo “prova” é plurissignificante, já que pode ser referido a mais de um sentido, aludindo - se ao fato representado, à atividade probatória, ao meio ou fonte de prova, ao procedimento pelo qual os sujeitos processuais obtêm o meio de prova ou, ainda, ao resultado do procedimento, isto é, à representação que dele deriva (mais especificamente, à convicção do juiz)

Etimologicamente, conforme Nucci (2014, p. 338):

o termo em latim “probatio” significa ensaio, verificação, inspeção, exame, argumento, razão, aprovação ou confirmação, dele deriva o verbo “probare”, que significa ensaiar, verificar, examinar, reconhecer por experiência, aprovar, estar satisfeito com algo, persuadir alguém a alguma coisa ou demonstrar.

Na prática jurídica, a prova serve como ferramenta para o convencimento do magistrado quanto à veracidade dos fatos alegados, permitindo ao julgador aplicar o direito de maneira fundamentada.

Partindo desse ponto de vista, para a sustentação de uma decisão judicial justa e bem fundamentada, a função essencial da prova no direito processual torna-se possibilitar ao julgador um conhecimento preciso dos fatos, sobre os quais será aplicada a norma jurídica.

Além disso, a prova desempenha um papel relevante na proteção de direitos constitucionais, como o contraditório e a ampla defesa, garantidos no artigo 5º da Constituição Federal, pilares que asseguram a participação ativa das partes no processo, produzindo e questionando os elementos probatórios apresentados.

No âmbito jurídico, a prova pode ser compreendida sob dois aspectos principais: Objetivo: Como meio pelo qual os fatos relevantes são demonstrados, permitindo sua reconstrução histórica e Subjetivo: Relacionado à formação da convicção do julgador, a partir da análise das evidências apresentadas.

De acordo com Nucci (2009, p.15), a prova caracteriza-se como:

[...] a demonstração lógica da realidade, no processo, por meio dos instrumentos legalmente previstos, buscando gerar, no espírito do julgador, a certeza em relação aos fatos alegados e, por consequência, gerando a convicção objetivada para o deslinde da demanda

Essa definição ressalta o papel instrumental da prova para permitir o pleno exercício da função jurisdicional.

O artigo 369 do CPC reconhece que as partes podem empregar todos os meios legais e moralmente legítimos para demonstrar os fatos em que fundamentam suas alegações, ampliando as possibilidades probatórias para além dos meios tradicionalmente previstos na legislação.

Segundo Didier Júnior, a prova deve ser vista como o conjunto de meios que permitem demonstrar a veracidade ou falsidade de uma alegação, assim, se mostra fundamental para assegurar que as decisões judiciais sejam fundamentadas e próximas da realidade dos fatos.

2.1 Tipos De Prova

O Código Civil brasileiro, em seu art. 212, lista os meios de prova clássicos:

Art. 212. Salvo o negócio a que se impõe forma especial, o fato jurídico pode ser provado mediante:

- I - Confissão;
- II - Documento;
- III - Testemunha;
- IV - Presunção;
- V - Perícia.

Esses meios, amplamente reconhecidos, continuam a ser a espinha dorsal do direito probatório. Porém, o Código de Processo Civil (CPC), em seu art. 369, adota uma abordagem mais ampla e moderna, permitindo meios de prova atípicos, desde que sejam juridicamente idôneos, ou seja, lícitos e moralmente legítimos.

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.

Dentro dos meios típicos de prova, encontram-se a documental, amplamente valorizada por sua confiabilidade e estabilidade, e a testemunhal, essencial para a comprovação de fatos que não possam ser registrados em documentos, enquanto a prova pericial é utilizada para esclarecer questões técnicas ou científicas, sendo indispensável em litígios que exijam conhecimentos específicos. Além disso, a inspeção judicial permite que o juiz, pessoalmente, examine elementos materiais que influenciam a causa.

A evolução tecnológica trouxe novas possibilidades ao campo probatório, como as provas digitais, que abrangem mensagens de texto, e-mails, registros de localização e conteúdos extraídos de redes sociais, embora apresentem desafios como a necessidade de garantir autenticidade e integridade. Elementos digitais, como prints de tela, são amplamente utilizados, mas sua admissibilidade depende de cuidados específicos, como certificação por ata notarial ou perícia técnica que assegure sua veracidade, sendo o Marco Civil da Internet e a adoção de assinaturas digitais pelo CPC exemplos de medidas voltadas a assegurar a confiabilidade desses elementos.

As provas atípicas têm como objetivo permitir a apuração dos fatos por meios diversos daqueles expressamente previstos em lei como provas típicas. Sua produção exige do magistrado um cuidado redobrado quanto à observância dos princípios que regem o direito probatório, especialmente o princípio do contraditório (Didier Junior; Braga; Oliveira, 2018).

Assim, os meios atípicos de prova, como gravações, prints de telas ou vídeos, podem ser admitidos, desde que respeitem os princípios do contraditório e da ampla defesa, além de seguirem requisitos técnicos para atestar sua veracidade, logo, a partir dessa abertura do ordenamento jurídico faz-se possível evidenciar a flexibilidade necessária para acompanhar as mudanças sociais e tecnológicas, assegurando que o processo judicial se mantenha atualizado e eficaz, como Amaral (2015, p. 90) argumenta que:

De outro, diante do comando do art. 369 do CPC, que demonstra a evolução do nosso Direito em tema de produção de provas em juízo, é plenamente possível a utilização de outros meios de prova, além daqueles previstos no Código Civil, para a elucidação dos fatos em juízo. Admitem-se as chamadas

provas atípicas. Não se cogita, por isso, nenhuma repercussão, no particular, do Código Civil na legislação processual

Por fim, os tipos de prova no direito brasileiro refletem um sistema dinâmico, que busca equilibrar tradição e modernidade, garantindo que o processo judicial permaneça apto a lidar com as constantes transformações sociais e tecnológicas.

Destacam ainda Marinoni e Arenhart (2005, p. 354) que:

uma prova que não pode ser utilizada como típica porque na sua formação violou uma norma (ou porque na sua produção vai violá-la), certamente não pode ser admitida como prova atípica, sob pena de estar servindo para encobrir a desconsideração de uma regra

Em última análise, esses elementos são essenciais não apenas para reconstruir os fatos, mas também para assegurar que a decisão judicial seja fundamentada em critérios justos, objetivos e alinhados ao princípio do devido processo legal.

2.2 Classificação Das Provas

A classificação das provas é uma ferramenta essencial no estudo do direito probatório, pois permite compreender suas funções e características dentro do processo judicial. Essas classificações variam conforme critérios como objeto, fonte, momento de produção e forma, além de cada uma dessas divisões auxiliarem na identificação e no entendimento do papel de cada elemento probatório no contexto processual.

Neste sentido, Humberto Teodoro Júnior (2018, p. 933) argumenta:

Diante do exposto, é forçoso concluir que o novo Código, assim como o de 1973, foi bastante liberal em matéria de meios de prova, mostrando-se consentâneo com as tendências que dominam a ciência processual de nossos dias, nas quais, acima do formalismo, prevalece o anseio da justiça ideal, lastreada na busca da verdade material, na medida do possível

Sob o aspecto do objeto, as provas podem ser diretas ou indiretas, enquanto as provas diretas se referem diretamente ao fato que se deseja comprovar, não exigem raciocínios adicionais, como o depoimento de uma testemunha que presenciou um acidente, as provas indiretas não se relacionam diretamente ao fato

principal, mas fornecem indícios que permitem deduzir sua ocorrência, como um laudo pericial que aponta a provável causa de um dano, sugerindo uma conclusão com base em elementos técnicos.

Considerando a fonte, as provas podem ser reais ou pessoais, sendo as primeiras derivadas de objetos, documentos ou qualquer elemento material capaz de comprovar os fatos do processo, como documentos assinados, fotografias e gravações, que frequentemente fundamentam alegações. As provas pessoais, por sua vez, originam-se de declarações de pessoas, como depoimentos de testemunhas ou das próprias partes envolvidas no litígio, mas, apesar de sua relevância, exigem cautela, pois podem ser influenciadas por subjetividades ou lapsos de memória.

No que se refere ao momento de sua produção, as provas podem ser pré-constituídas ou causais, as pré-constituídas são aquelas elaboradas antes do início do processo judicial, com o objetivo de formalizar ou proteger direitos, como contratos ou certidões essas provas são frequentemente utilizadas para prevenir litígios ou assegurar elementos para eventual discussão judicial. Por outro lado, as provas causais são aquelas produzidas durante o curso do processo, como depoimentos coletados em audiência ou perícias determinadas pelo juiz, esse tipo de prova mostra-se fundamental para esclarecer fatos controversos que surgem no andamento da lide.

Outro critério relevante para a classificação das provas é sua forma, podendo-se identificar as documentais, orais e materiais. Sendo assim, as provas documentais incluem contratos, certidões, registros digitais e outros documentos com informações úteis para o processo, sendo amplamente utilizadas pela confiabilidade e facilidade de verificação, as provas orais abrangem os depoimentos das partes ou testemunhas, apresentados verbalmente durante o processo, enquanto as provas materiais referem-se a elementos físicos que podem ser analisados, como vestígios em cenas de crime ou objetos submetidos a exames periciais.

A classificação também pode levar em conta a legalidade da prova, ou seja, se ela foi obtida de forma lícita ou ilícita, ou seja, as provas lícitas respeitam os limites impostos pelo ordenamento jurídico e os direitos fundamentais, sendo plenamente admissíveis no processo judicial, em contraste, as provas ilícitas, obtidas em violação à lei ou a direitos constitucionais, são vedadas pelo artigo 5º, inciso LVI, da CF, e sua utilização é expressamente proibida. Na contemporaneidade, a doutrina ainda debate as nuances da admissibilidade de provas ilícitas por derivação,

conhecidas como "teoria dos frutos da árvore envenenada", que limita o uso de informações obtidas a partir de provas ilícitas originais.

Por fim, as provas também podem ser classificadas de acordo com sua natureza, sendo primárias ou secundárias, de modo que, as primárias estão diretamente relacionadas ao fato probando, como o contrato original em uma disputa contratual, já as secundárias referem-se a cópias ou reproduções, cuja autenticidade e integridade devem ser devidamente verificadas para que sejam aceitas.

Taruffo (2014, p. 58) descreve essa distinção entre prova direta e indireta da seguinte forma:

O elemento essencial dessa distinção é a conexão entre os fatos principais em litígio e o fato que constitui o objeto material imediato do elemento de prova. Quando os dois enunciados tratam do mesmo fato, a prova é direta, uma vez que se relacionam diretamente com um fato relevante ou principal: o enunciado acerca desse fato é o objeto imediato da prova. Quando, pelo contrário, a prova trata de um enunciado relativo a um fato diferente, a partir do qual se pode extrair uma conclusão acerca de um fato principal, então a prova é indireta ou circunstancial.

A análise das classificações apresentadas demonstra a complexidade e a relevância do direito probatório no sistema jurídico brasileiro, auxiliando na estruturação da atividade probatória e permitindo que o magistrado e as partes organizem e valorizem adequadamente os elementos apresentados, o que contribui para um julgamento mais justo e fundamentado. Em um contexto de constantes avanços tecnológicos, como o surgimento das provas digitais, essa organização se torna ainda mais indispensável, exigindo adaptação e rigor na aplicação dos critérios tradicionais.

2.3 Prova Ilícita

A prova ilícita ocupa um lugar central no debate jurídico, especialmente devido ao impacto que pode exercer sobre a legitimidade das decisões judiciais e a proteção dos direitos fundamentais, sendo sua inadmissibilidade consagrada pelo artigo 5º, inciso LVI, da Constituição Federal, que proíbe a utilização de elementos probatórios obtidos por meios ilícitos para fundamentar decisões judiciais, essa regra decorre da necessidade de preservar valores fundamentais, como a dignidade da

pessoa humana, a privacidade e a integridade do devido processo legal, que são pilares do Estado Democrático de Direito.

Para compreender a amplitude do conceito, a distinção das provas ilícitas das ilegítimas faz-se essencial, pois enquanto a ilicitude decorre da violação de normas de direito material durante a obtenção da prova, como em interceptações telefônicas não autorizadas ou invasões de privacidade, a ilegitimidade resulta do descumprimento de normas processuais, como a apresentação de uma prova fora do prazo legal ou sem respeito ao contraditório. Apesar da diferença conceitual, ambas podem comprometer a validade do elemento probatório e influenciar na decisão judicial.

Sobre o conceito de prova ilícita Didier (2018, p. 111) dispõe:

O conceito de prova ilícita é amplo, alcançando aquela prova que contraria qualquer norma do ordenamento jurídico. Assim, são exemplos de provas ilícitas a confissão obtida sob tortura, o depoimento de testemunha sob coação moral, a interceptação telefônica clandestina, a obtenção de prova documental mediante furto, a obtenção de prova mediante invasão de domicílio, a prova obtida pela quebra do dever de sigilo imposto ao mediador (art.3º, §2º, Lei n. 13.140/2015) etc. São também exemplos de provas ilícitas aquela colhida sem observância da participação em contraditório, o documento material ou ideologicamente falso, ou qualquer outra prova que se mostre em desconformidade com o ordenamento jurídico, pouco importando a natureza jurídica da norma violada

Já Avolio (2015, p. 50) argumenta que a prova ilícita está sempre atrelada a violação dos princípios de ordem material:

[...] é de se entender a prova colhida com infração a normas ou princípios de direito material - sobretudo de direito constitucional, porque como vimos, a problemática da prova ilícita prende-se sempre à questão das liberdades públicas, em que estão assegurados os direitos e garantias atinentes à intimidade, à liberdade, à dignidade humana; mas, também, de direito penal, civil, administrativo, nos quais já se encontram definidos na ordem infraconstitucional outros direitos ou cominações legais que podem se contrapor às exigências de segurança social, investigação criminal e accertamento da verdade, tais como os de propriedade, inviolabilidade do domicílio, sigilo da correspondência e outros

Sob esse viés, a teoria da inadmissibilidade das provas ilícitas identifica-se como fundamentada em princípios como o da proporcionalidade, pois avalia a tensão entre o interesse público na descoberta da verdade e a necessidade de proteção dos direitos fundamentais, admitindo, em situações excepcionais, a utilização de provas ilícitas quando sua exclusão implicaria em grave violação de

outros direitos fundamentais, como a proteção à vida ou à dignidade da pessoa humana, tal abordagem, conhecida como “teoria da proporcionalidade”, exige análise criteriosa caso a caso para evitar a banalização da ilicitude.

A respeito do princípio da proporcionalidade “pro societate”, Capez e Colnago (2015, p. 185) aduzem:

(...) consiste na admissibilidade das provas ilícitas, quando demonstrada a prevalência do interesse público na persecução penal, a tendência atual da jurisprudência dos Tribunais Superiores é a da não adoção. De acordo com esse entendimento, a não admissão de mecanismos de flexibilização das garantias constitucionais tem o objetivo de preservar o núcleo irredutível de direitos individuais inerentes ao devido processo legal, mantendo a atuação do Poder Público dentro dos limites legais. As medidas excepcionais de constrição de direitos não podem, assim, ser transformadas em práticas comuns de investigação

Outro aspecto relevante é a teoria dos frutos da árvore envenenada ou “fruits of the poisonous tree” ou teoria da prova ilícita por derivação amplamente aceita no Brasil através da jurisprudência do STF e encontra previsão no artigo 157 do Código de Processo Penal, a partir dessa doutrina, considera-se inadmissíveis não apenas as provas diretamente obtidas de forma ilícita, mas também todas as derivadas, devido à contaminação pela origem irregular. Segundo dispõe o artigo 157, § 3 do Código de Processo Penal, as provas ilícitas devem ser desentranhadas dos autos do processo e preclusa a decisão de desentranhamento, haverá a destruição da prova na presença facultativa das partes. Nestor Távora (2013, p. 396) diz que:

se a contaminação probatória for ampla, faltarão verdadeira justa causa para a deflagração da ação penal, de sorte que a inicial acusatória deve ser rejeitada caso os elementos informadores sejam contaminados pela extensão da prova ilícita, com arrimo no art. 395 em nova redação dada pela Lei nº 11.719/08.

Contudo, há exceções, como a teoria da fonte independente, que admite provas obtidas lícitamente e de forma autônoma, mesmo relacionadas a uma prova ilícita, e a teoria da descoberta inevitável, que permite o uso de provas que seriam inevitavelmente descobertas por outros meios lícitos.

No contexto das provas digitais, a questão da ilicitude torna-se ainda mais complexa, já que a facilidade de manipulação ou obtenção de informações sem autorização aumenta os riscos de violação de direitos fundamentais. Assim, situações envolvendo interceptações de mensagens em aplicativos, invasão de dispositivos

eletrônicos ou uso indevido de dados privados são exemplos que exigem análise rigorosa quanto à licitude, destacando a necessidade de os operadores do Direito acompanharem as inovações tecnológicas e utilizarem ferramentas adequadas para validação probatória.

A exclusão de provas ilícitas no processo não serve apenas como uma proteção aos direitos das partes, mas também um mecanismo de preservação da integridade do sistema judicial, pois o uso de elementos obtidos de maneira irregular compromete a imparcialidade do julgamento e pode gerar precedentes que incentivam práticas violadoras de direitos fundamentais. Nesse cenário, a doutrina e a jurisprudência brasileiras buscam equilibrar a busca pela verdade real com os limites impostos pela legalidade, assegurando que o processo judicial se mantenha um espaço de justiça e respeito às normas constitucionais.

Portanto, a prova ilícita não se limita a um tema técnico do Direito, mas reflete as tensões entre o poder investigativo e as garantias individuais, demandando uma análise criteriosa que leve em conta tanto os valores fundamentais do ordenamento jurídico quanto as especificidades de cada caso concreto. Ao estabelecer limites claros e respeitar os princípios constitucionais, o Direito reafirma seu compromisso com uma justiça que seja simultaneamente legítima e efetiva.

2.4 Prova Digital

Com o aumento exponencial do uso de dispositivos eletrônicos e da internet, tornou-se inevitável que informações geradas e armazenadas digitalmente passassem a desempenhar um papel crucial na atividade probatória no processo judicial, por isso, as provas digitais refletem diretamente a evolução tecnológica e a crescente digitalização das relações humanas e comerciais, além de ganharem destaque representando desafios e oportunidades para o direito probatório. Essas provas estão previstas no Marco Civil da Internet (Lei nº 12.965/14) e no CPC de 2015, que reconhecem a validade de documentos eletrônicos e assinaturas digitais, desde que respeitados os requisitos de autenticidade e integridade.

Nesse sentido, Alves (2016) argumenta que:

Com a instituição do Marco Civil da Internet foram criadas diretrizes para a utilização desta rede mundial de computadores, bem como estabelecidas as

garantias, os direitos e os deveres dos usuários em geral, cuja regulação está prevista na Lei 12.965/14.

Em decorrência, com a disseminação do uso da internet, especialmente como meio de comunicação e divulgação de dados, surgiram novas possibilidades de provas de fatos e negócios jurídicos envolvendo disputas que desagüam no poder Judiciário.

No entanto, nem tudo que está na internet pode ser utilizado como meio de prova de um direito em um processo judicial, tornando-se necessário definir quais seriam estas provas passíveis de utilização perante o Judiciário.

[...] Associado a esses fatores, o novo CPC passou a reforçar o uso e a validade dos documentos eletrônicos como prova em processo judicial, pois até então não havia expressa previsão normativa, dando margem à contestação ilegítima, ainda que a prova representasse fidedignamente a materialidade do direito objeto da demanda

A prova digital emerge como um elemento indispensável no contexto processual contemporâneo, refletindo as mudanças provocadas pelo avanço da tecnologia e sua profunda integração nas relações sociais e jurídicas, sendo definida como qualquer elemento probatório armazenado ou produzido em meio eletrônico, capaz de contribuir para a reconstrução de fatos no processo judicial. Com o aumento do uso de ferramentas digitais em diversos aspectos da vida cotidiana, os tribunais enfrentam novos desafios para incorporar essas inovações de forma a garantir julgamentos justos, respeitando os princípios do devido processo legal e a ampla defesa.

Outrossim, caracterizadas por uma ampla variedade de formas e origens, as provas digitais incluem documentos eletrônicos, e-mails, mensagens instantâneas, gravações de áudio e vídeo, registros de localização, entre outros, o que reflete o dinamismo da comunicação moderna, embora sua intangibilidade apresente desafios técnicos e jurídicos relacionados à obtenção, armazenamento e apresentação. Conforme Fredie Didier Jr. (2016, p. 693), a introdução do documento eletrônico pelo legislador foi acertada, reconhecendo-o como um meio de prova distinto, com características próprias que o diferenciam das provas tradicionais, como a testemunhal e a documental.

No Brasil, o uso de provas digitais encontra respaldo em legislações específicas, como a Lei nº 11.419/2006, que regulamenta a informatização do processo judicial, e o Código de Processo Civil, que inclui dispositivos para lidar com documentos eletrônicos, especificamente os artigos 411 e 425:

Art. 411. Considera-se autêntico o documento quando:

I - o tabelião reconhecer a firma do signatário;

II - a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei;

III - não houver impugnação da parte contra quem foi produzido o documento.

Art. 425. Fazem a mesma prova que os originais:

I - as certidões textuais de qualquer peça dos autos, do protocolo das audiências ou de outro livro a cargo do escrivão ou do chefe de secretaria, se extraídas por ele ou sob sua vigilância e por ele subscritas;

II - os traslados e as certidões extraídas por oficial público de instrumentos ou documentos lançados em suas notas;

III - as reproduções dos documentos públicos, desde que autenticadas por oficial público ou conferidas em cartório com os respectivos originais;

IV - as cópias reprográficas de peças do próprio processo judicial declaradas autênticas pelo advogado, sob sua responsabilidade pessoal, se não lhes for impugnada a autenticidade;

V - os extratos digitais de bancos de dados públicos e privados, desde que atestado pelo seu emitente, sob as penas da lei, que as informações conferem com o que consta na origem;

VI - as reproduções digitalizadas de qualquer documento público ou particular, quando juntadas aos autos pelos órgãos da justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pela Defensoria Pública e seus auxiliares, pelas procuradorias, pelas repartições públicas em geral e por advogados, ressalvada a alegação motivada e fundamentada de adulteração.

§ 1º Os originais dos documentos digitalizados mencionados no inciso VI deverão ser preservados pelo seu detentor até o final do prazo para propositura de ação rescisória.

§ 2º Tratando-se de cópia digital de título executivo extrajudicial ou de documento relevante à instrução do processo, o juiz poderá determinar seu depósito em cartório ou secretaria.

Além disso, a MP nº 2.200-2/2001, que instituiu a ICP-Brasil, garante a validade jurídica de assinaturas eletrônicas e certificações digitais, elementos fundamentais para atestar a veracidade de muitos documentos eletrônicos utilizados como prova. Esses instrumentos normativos não apenas validam o uso da tecnologia no contexto processual, mas também estabelecem um padrão mínimo de segurança para a manipulação de informações digitais.

A autenticidade refere-se à garantia de que a prova corresponde ao original, sem alterações, enquanto a integridade assegura que as características essenciais do documento permanecem intactas desde sua coleta até sua

apresentação em juízo, sendo a ICP-Brasil uma ferramenta essencial nesse processo. A produção da prova digital, entretanto, requer o cumprimento de requisitos técnicos e jurídicos que preservem o contraditório e a ampla defesa, como na coleta de dados, que deve respeitar a privacidade e garantir a legalidade, recorrendo-se, muitas vezes, a atas notariais em casos de mensagens e redes sociais, a fim de reduzir o risco de questionamentos quanto à autenticidade ou manipulação dos registros.

Apesar de representarem uma evolução significativa no âmbito probatório, as provas digitais enfrentam desafios, como a volatilidade dos meios digitais, que permite alterações rápidas e imperceptíveis, exigindo a atuação de peritos especializados e a capacitação técnica dos operadores do Direito. Ademais, o uso crescente de tecnologias avançadas, como a inteligência artificial, levanta questões sobre fraudes sofisticadas que desafiam os métodos tradicionais de validação, destacando a necessidade de constante adaptação às inovações tecnológicas.

Por outro lado, as provas digitais também trazem benefícios inegáveis, como a capacidade de armazenar e transmitir grandes volumes de informações de forma eficiente e a facilidade de acesso remoto a esses dados. Essas características não apenas tornam os processos mais céleres, mas também permitem uma abordagem mais abrangente e precisa na investigação dos fatos.

Em suma, a prova digital representa uma resposta às demandas de uma sociedade em transformação, marcada pela digitalização de suas interações e pela crescente dependência de tecnologias avançadas. Apesar de seus desafios, sua importância no contexto processual é inegável, e sua utilização continuará a crescer à medida que a sociedade se torna cada vez mais dependente de tecnologias digitais. Para garantir a efetividade e a justiça nos processos, é essencial que as normas jurídicas continuem a evoluir, acompanhando as inovações e proporcionando instrumentos eficazes para lidar com as complexidades desse novo cenário probatório.

2.5 A Legalidade Da Prova Digital No Ordenamento Jurídico Brasileiro

A legalidade da prova digital no ordenamento jurídico brasileiro configura-se como uma questão complexa e multidimensional, refletindo os desafios de incorporar inovações tecnológicas no Direito sem comprometer os princípios

fundamentais do sistema jurídico, já que a transformação digital impactou profundamente a forma como informações são produzidas, armazenadas e transmitidas, influenciando diretamente a atividade probatória e demandando adaptações progressivas para reconhecer, regulamentar e validar as provas digitais como elementos legítimos nos processos judiciais

O conceito de prova digital abrange uma vasta gama de elementos armazenados ou transmitidos em formato eletrônico, possuindo características como intangibilidade, alta replicabilidade e vulnerabilidade a alterações, o que exige critérios específicos para garantir admissibilidade, autenticidade e integridade, fundamentais para preservar a confiança no processo judicial. O Código de Processo Civil de 2015, ao tratar do tema, trouxe dispositivos relevantes, como o artigo 369, que permite às partes empregar todos os meios legais e moralmente legítimos para provar a verdade dos fatos, abrindo caminho para a utilização de elementos digitais na atividade probatória, além de estabelecer diretrizes para produção, conservação e avaliação dessas provas, sempre respeitando o contraditório, a ampla defesa e o devido processo legal.

Um dos principais desafios da prova digital está na sua obtenção, considerando que a proteção constitucional aos direitos à privacidade, intimidade e inviolabilidade das comunicações, prevista no artigo 5º, incisos X e XII da Constituição Federal, impõe limites claros ao acesso de dados digitais. A obtenção ilícita de provas, como por invasão de dispositivos ou interceptações não autorizadas, torna-se inadmissível pelo artigo 5º, inciso LVI, embora a jurisprudência admita exceções em situações extremas, aplicando os princípios da proporcionalidade e da proteção de direitos fundamentais superiores, como vida e segurança pública.

Ademais, a integridade e a autenticidade das provas digitais são aspectos essenciais, frequentemente comprometidos pela volatilidade e manipulabilidade dos dados eletrônicos, sendo garantidas por ferramentas como atas notariais, perícias técnicas e certificações digitais, que asseguram a veracidade das informações apresentadas, a atuação de especialistas em informática jurídica é indispensável para verificar se os dados atendem aos padrões legais e podem fundamentar decisões judiciais de forma confiável.

Apesar dos avanços legislativos, a prática forense revela desafios que vão além da regulamentação, pois a evolução tecnológica frequentemente ultrapassa a capacidade do Direito de acompanhar as mudanças, criando lacunas normativas e

deixando operadores do Direito sem diretrizes claras para lidar com questões complexas. Além disso, a resistência cultural à adoção de tecnologias e a falta de capacitação técnica de muitos profissionais do Direito comprometem a eficácia e a utilização adequada das provas digitais.

Por outro lado, as provas digitais oferecem benefícios significativos, como o registro e a preservação eficiente de informações, maior celeridade e economia processual, especialmente em disputas comerciais, crimes cibernéticos e casos envolvendo redes sociais, onde frequentemente se tornam os principais meios de reconstituir fatos e identificar responsabilidades. Dessa maneira, a facilidade de acesso a registros digitais, aliada à capacidade de armazenar grandes volumes de dados, torna essas provas ferramentas indispensáveis na busca pela verdade real.

A legalidade da prova digital no ordenamento jurídico brasileiro é um tema que exige uma abordagem equilibrada, que respeite os direitos fundamentais e, ao mesmo tempo, permita que a inovação tecnológica seja utilizada para aprimorar a justiça. O constante aprimoramento das leis, a capacitação dos profissionais e a adaptação do sistema jurídico às novas realidades são passos essenciais para que as provas digitais sejam plenamente integradas ao processo judicial, contribuindo para decisões mais justas, eficientes e alinhadas à dinâmica da sociedade contemporânea.

3 A LEI GERAL DE PROTEÇÃO DE DADOS “LGPD” – LEI 13.709/18

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, representou um marco na proteção dos direitos fundamentais à privacidade e à autodeterminação informativa no ordenamento jurídico brasileiro. Inspirada em legislações internacionais, como o GDPR da União Europeia, a LGPD visa regular o tratamento de dados pessoais por pessoas naturais e jurídicas, de direito público ou privado, a fim de assegurar os direitos dos titulares desses dados.

Sua relevância transcende a proteção da privacidade, influenciando diretamente o sistema probatório no âmbito processual, conforme evidenciado por estudos contemporâneos que discutem a validade e a produção de provas digitais.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, emerge como um instrumento jurídico fundamental em resposta à crescente complexidade das interações digitais e ao tratamento massivo de dados pessoais, configurando-se como norma de observância obrigatória também no âmbito do processo judicial.

Dessa maneira, a LGPD estabelece, de forma sistemática, princípios e regras que disciplinam o tratamento de dados pessoais, inclusive em meios digitais, resguardando os direitos fundamentais à liberdade, à intimidade e à privacidade. No que tange à produção de provas digitais, a LGPD introduz limites e responsabilidades específicas ao estabelecer que qualquer coleta e utilização de dados pessoais deve observar os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (art. 6º).

Assim, a prova digital não pode ser obtida ou utilizada de maneira genérica, desproporcional ou sem justificativa legal, sendo imprescindível a demonstração de que o dado pessoal é necessário e pertinente ao objeto do litígio.

A aplicação da LGPD no processo judicial impõe a adoção de mecanismos de proteção e controle, como a anonimização de dados quando possível, a limitação do acesso por terceiros não autorizados e o dever de informação ao titular dos dados, sobretudo quando tais dados forem coletados sem o seu conhecimento direto. Neste sentido:

Este cenário demanda, inclusive, a compatibilização entre a LGPD e o direito à prova, sendo necessária a ponderação entre os direitos fundamentais em

conflito — especialmente entre o direito à privacidade do titular dos dados e o direito à ampla defesa e contraditório da parte adversa, conforme o artigo 5º, incisos LIV e LV, da Constituição Federal. Nesse ponto, a doutrina destaca que a LGPD não se presta a impedir a produção de provas, mas a garantir que ela ocorra em conformidade com parâmetros éticos e jurídicos sólidos, evitando abusos e preservando o núcleo essencial dos direitos fundamentais. Neste sentido, Cortez (2023, p.96) argumenta:

A ausência de regulamentação específica sobre o uso de dados de localização como prova permite a violação de direitos fundamentais, exigindo-se, portanto, o desenvolvimento de um regime jurídico que concilie a eficiência investigativa com a salvaguarda da privacidade, pautado nos princípios da LGPD e em instrumentos internacionais como a Convenção de Budapeste

Além disso, no campo da valoração da prova digital, a LGPD impõe que se leve em consideração, também, a regularidade da obtenção dos dados e a integridade da cadeia de custódia, princípios igualmente essenciais para que o material digital tenha força probatória válida e eficaz. Nesse sentido, o art. 373 do CPC e o art.157 do Código de Processo Penal continuam sendo aplicáveis, mas agora devem ser interpretados à luz dos novos paradigmas introduzidos pela LGPD.

A LGPD reconfigura o processo judicial contemporâneo ao exigir uma nova cultura jurídica pautada pela proteção de dados, pela responsabilidade no uso das informações pessoais e pela construção de um processo judicial mais ético, eficiente e garantidor de direitos, reafirmando o compromisso do Estado com a dignidade da pessoa humana em uma sociedade digitalizada.

3.1 Principais Características Da Lei Geral De Proteção De Dados e Sua Aplicação

Essa legislação delinea um conjunto de princípios que funcionam como pilares para todo o seu conteúdo, como o princípio da finalidade, da adequação, da necessidade, da transparência, da segurança e da responsabilização. Diante disso, esses fundamentos não apenas orientam a atividade de tratamento de dados, mas também funcionam como critérios de controle e interpretação da própria norma, sendo essenciais para a verificação da legalidade dos atos que envolvam dados pessoais. Logo, é preciso exigir com rigor a verificação dos requisitos de autenticidade,

integridade e preservação da cadeia de custódia dos dados utilizados como prova digital, uma vez que tais exigências decorrem tanto do dever de probidade processual quanto da própria LGPD, que impõe padrões de segurança jurídica para o uso desses dados em juízo, isso significa que qualquer prova digital que envolva dados pessoais não pode ser produzida ou utilizada sem considerar os direitos do titular. Por exemplo, uma conversa privada obtida sem consentimento e sem ordem judicial pode ser considerada prova ilícita, não apenas pelo Código de Processo Civil ou Penal, mas também pela LGPD, que qualifica tal uso como tratamento irregular de dados.

Outra característica essencial da LGPD é a base legal para o tratamento de dados, que exige que toda atividade de coleta, uso, compartilhamento ou armazenamento de dados se fundamente em uma das bases previstas pela lei, como o consentimento do titular, cumprimento de obrigação legal ou regulatória, execução de contrato ou exercício regular de direitos em processo judicial. Tal exigência apresenta aplicação direta em processos judiciais, especialmente na atuação de advogados e peritos, que devem assegurar que os dados apresentados como prova tenham sido obtidos de forma lícita, sob pena de nulidade.

O impacto da LGPD no campo probatório mostra-se significativo, sobretudo no que diz respeito à produção e à validade das provas digitais. Nesse contexto, a legislação passa a funcionar como uma espécie de filtro normativo para a admissibilidade da prova digital, exigindo dos operadores do direito não apenas conhecimento técnico, mas também uma postura crítica e atenta aos direitos fundamentais dos envolvidos. Além disso, destaca-se a necessidade de alinhamento entre os dispositivos da LGPD e padrões técnicos, como a ABNT NBR ISO/IEC 27037:2012, especialmente em processos que envolvam dados sensíveis ou de localização, nos quais o risco de violação da intimidade e da privacidade é acentuado.

A ausência de normatização clara sobre o uso de certos dados digitais não pode justificar abusos na persecução penal. Torna-se possível compatibilizar a eficácia das investigações criminais com o respeito aos direitos fundamentais, desde que a produção probatória seja orientada por critérios técnicos e jurídicos adequados, como aqueles previstos na LGPD.

A aplicação da LGPD no Judiciário também encontra respaldo na doutrina ao tratar da prova documental eletrônica, mesmo com a evolução do Código de Processo Civil de 2015 e o reconhecimento do documento eletrônico como prova típica, ainda subsistem desafios quanto à sua validade e autenticidade. Nesse

contexto, a LGPD oferece critérios objetivos e rigorosos que contribuem para garantir a fidedignidade das informações e resguardar os direitos das partes envolvidas.

A LGPD também impõe a obrigação de registro das operações de tratamento, o que se desdobra em obrigações documentais e de transparência por parte dos agentes de tratamento. Em termos processuais, isso significa que qualquer entidade que apresente documentos digitais em juízo deve ter condições de comprovar a origem dos dados, a forma como foram tratados, e as medidas de segurança adotadas para sua proteção, o que faz-se especialmente relevante para órgãos públicos e empresas que atuam em litígios judiciais, pois a rastreabilidade das operações pode ser determinante para a aceitação ou não da prova.

Por fim, destaca-se a criação da Autoridade Nacional de Proteção de Dados (ANPD), encarregada de zelar pela aplicação da LGPD e de regulamentar aspectos técnicos da lei. A atuação da ANPD tem influência indireta sobre os processos judiciais ao definir parâmetros técnicos e boas práticas que podem ser utilizados como referência por magistrados ao avaliar a licitude e a confiabilidade de provas digitais, ainda que seu foco principal não seja o processo judicial, a regulamentação da ANPD contribui para a criação de um ambiente jurídico mais seguro e previsível.

A LGPD apresenta uma nova lógica acerca do tratamento jurídico das informações pessoais, exigindo uma revisão profunda das práticas forenses e administrativas. Sua eficácia depende não apenas da sua aplicação literal, mas da incorporação de seus valores nas rotinas institucionais, garantindo que os dados pessoais sejam tratados com o devido respeito à dignidade humana, à liberdade e à intimidade. Configura-se, portanto, como um instrumento que reafirma o compromisso do direito com a proteção dos mais essenciais atributos da personalidade, inclusive no âmbito processual, onde a prova digital, cada vez mais presente, deve ser compatibilizada com os princípios que a LGPD consagra.

3.2 Intersecção Entre Proteção De Dados e Direito Probatório

A intersecção entre proteção de dados e direito probatório é um campo jurídico emergente que tem despertado crescente atenção da doutrina e da jurisprudência, em razão da crescente digitalização das relações sociais, do aumento do volume de informações pessoais circulando nos processos judiciais e da entrada

em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD). Essa convergência revela tensões entre dois conjuntos de princípios fundamentais: de um lado, os direitos à privacidade, autodeterminação informativa e proteção de dados pessoais; de outro, os princípios do contraditório, da ampla defesa, do direito à prova e da busca pela verdade no processo judicial.

Do ponto de vista da proteção de dados, qualquer tratamento de informações pessoais no âmbito do processo judicial deve atender aos princípios da LGPD, especialmente os da necessidade, finalidade, transparência e adequação. Isso significa que a coleta, o armazenamento e o uso de dados pessoais devem ocorrer apenas quando estritamente necessários para o cumprimento de uma finalidade legítima, clara e compatível com os propósitos do processo judicial. Dados excessivos ou irrelevantes à controvérsia não devem ser incorporados aos autos, sob pena de violação à intimidade das partes ou de terceiros.

Por outro lado, o direito probatório, notadamente no processo civil, autoriza a parte a produzir toda prova lícita necessária para demonstrar seus direitos, com base no princípio do devido processo legal (art. 5º, inc. LV, da CF/88) e na liberdade de convencimento do magistrado (art. 371 do CPC). Quando essa produção envolve dados pessoais, especialmente dados sensíveis (como estado de saúde, filiação política ou religiosa, orientação sexual, entre outros), impõe-se um balanço entre o interesse público ou privado na produção da prova e os direitos fundamentais do titular dos dados.

Um dos principais desafios dessa intersecção está em definir limites ético-jurídicos para a obtenção e uso de provas digitais que contenham dados pessoais, como, por exemplo, o acesso a contas de e-mail, mensagens de aplicativos, prontuários médicos ou informações financeiras. O Superior Tribunal de Justiça já se posicionou no sentido de que a obtenção de provas envolvendo dados pessoais deve ser precedida de decisão judicial fundamentada, com indicação clara da pertinência do dado ao litígio e respeito à proporcionalidade.

Além disso, o encarregado pelo tratamento de dados (DPO) nas instituições públicas e privadas, incluindo os tribunais, deve assegurar que os dados pessoais inseridos nos processos sejam tratados com segurança, armazenados de forma adequada e protegidos contra acessos não autorizados, conforme os arts. 37 a 41 da LGPD. Isso se aplica também ao PJe (Processo Judicial Eletrônico), cujos

sistemas devem ser estruturados com base nos princípios da minimização de dados e da governança da informação.

A doutrina tem destacado que o novo paradigma exige uma releitura do direito probatório sob a ótica da proteção de dados, o que inclui desde a reformulação dos critérios de admissibilidade da prova até a responsabilização pelo uso indevido de dados obtidos em sede judicial.

A jurisprudência, por sua vez, caminha no sentido de reconhecer o direito ao esquecimento processual, ou seja, a limitação temporal da exposição de dados nos sistemas judiciais, bem como o direito à anonimização ou pseudonimização de partes e testemunhas em situações específicas. Isso implica uma mudança cultural no uso da informação processual, que deve deixar de ser vista como um recurso ilimitado e passar a ser tratada como um bem jurídico protegido por normas constitucionais e infraconstitucionais.

3.3 Ponderação Entre Direito à Prova e Direito à Privacidade.

A ponderação entre o direito à prova e o direito à privacidade trata-se de uma tensão clássica entre dois direitos fundamentais: de um lado, o direito à produção de provas para a defesa de interesses legítimos no processo judicial (art. 5º, inc. LV, da CF/88); de outro, o direito à privacidade, à intimidade e à proteção de dados pessoais (art. 5º, incs. X e LXXIX, CF/88; art. 6º, LGPD).

O direito à prova é um desdobramento do devido processo legal, do contraditório e da ampla defesa. A parte tem o direito de produzir todos os meios de prova admitidos em direito para demonstrar a veracidade dos fatos alegados. Tal prerrogativa é essencial para o exercício da defesa e para a busca da verdade no processo, sendo reconhecida pela jurisprudência como um direito fundamental de natureza instrumental. A negativa imotivada da produção de provas configura cerceamento de defesa e pode ensejar nulidade processual.

Por sua vez, o direito à privacidade protege a esfera íntima da pessoa, vedando intromissões indevidas em sua vida pessoal. Esse direito ganhou novos contornos com a entrada em vigor da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), que consagrou a autodeterminação informativa, impondo limites ao tratamento de dados pessoais, inclusive no âmbito judicial. A LGPD reconhece que o

tratamento de dados é possível quando necessário para o exercício regular de direitos em processo judicial, mas exige proporcionalidade, necessidade e minimização.

O art. 10 do Marco Civil da Internet protege a privacidade do conteúdo e das comunicações:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

A produção de determinadas provas pode envolver a exposição de aspectos íntimos de uma das partes ou de terceiros. A solução para essa colisão se dá pela aplicação do princípio da proporcionalidade, desdobrado em três subprincípios: i) adequação: a medida probatória deve ser idônea para alcançar a finalidade pretendida; ii) necessidade: não deve haver outro meio menos invasivo para atingir o mesmo fim; iii) proporcionalidade em sentido estrito: o sacrifício ao direito à privacidade deve ser justificado pela relevância da tutela judicial pretendida.

A ponderação exige uma análise concreta do caso, sopesando os interesses em conflito. O juiz deve fundamentar a autorização da prova invasiva com base em critérios objetivos, justificando por que ela é essencial à instrução do feito. O STF e o STJ têm reconhecido que o direito à prova não é absoluto e não pode justificar a violação desproporcional à privacidade.

De acordo com o Supremo Tribunal Federal (2020):

no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, [...], pois nenhum direito ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros

A jurisprudência tende a admitir provas invasivas apenas quando indispensáveis e obtidas por meios lícitos. A violação injustificada da intimidade pode levar ao reconhecimento da ilicitude da prova (CF, art. 5º, LVI).

A ponderação entre os dois direitos tem implicações diretas na produção, admissibilidade e valoração das provas digitais. Em pedidos de exibição de dados privados, o juiz deve verificar se os dados são essenciais ao deslinde da controvérsia, a parte requerente demonstrou interesse jurídico legítimo, os dados podem ser obtidos

de forma anonimizada ou parcial ou se existe risco de danos à intimidade que não justifique o acesso.

Daniel Sarmiento (2005, p. 85) diz que: “o direito à prova e o direito à intimidade devem ser ponderados de forma contextual, à luz da proporcionalidade, a fim de que nenhum seja eliminado, mas ambos sejam harmonizados na máxima medida possível”. Sarmiento defende que o direito à privacidade não pode ser reduzido a um obstáculo à verdade processual, mas tampouco deve ser sacrificado de forma automática.

Portanto, conclui-se que o equilíbrio entre o direito à prova e o direito à privacidade demanda análise criteriosa, pautada no princípio da proporcionalidade. Embora essencial ao contraditório e à ampla defesa, a produção de provas não pode violar indevidamente a intimidade ou os dados pessoais das partes. Assim, o Judiciário deve assegurar que tais provas sejam admitidas apenas quando indispensáveis, preservando os direitos fundamentais envolvidos, respeitando a legalidade, a necessidade e a adequação.

4 REQUISITOS DA VALIDADE DA PROVA DIGITAL

A validade da prova digital no processo judicial exige uma análise técnico-jurídica minuciosa, levando em conta as particularidades que a diferenciam das provas tradicionais. Em primeiro plano, faz-se necessário comprovar a autenticidade do material por meio de recursos técnicos que garantam que o documento eletrônico não foi adulterado ou forjado, entre esses recursos estão as assinaturas digitais, os certificados emitidos por autoridades da ICP-Brasil e o uso de funções hash, que geram uma espécie de "impressão digital" do arquivo e denunciam qualquer modificação em seu conteúdo original. A integridade da prova, por sua vez, está ligada à preservação do conteúdo desde a coleta até sua apresentação em juízo. A garantia da integridade depende da observância da cadeia de custódia, que consiste no registro cronológico e verificável de todas as etapas pelas quais a prova digital passa — como manuseio, armazenamento, análise e apresentação —, assegurando que o material permaneça fiel à sua forma original.

O cumprimento desses requisitos não é apenas uma exigência técnica, mas uma garantia processual que assegura às partes o exercício efetivo do contraditório e da ampla defesa. Isso porque a fragilidade da prova digital — suscetível à edição, supressão, ou fabricação — demanda a adoção de critérios rigorosos para evitar o risco de decisões judiciais baseadas em elementos duvidosos ou corrompidos. Em complemento, destaca-se que a jurisprudência brasileira vem evoluindo no sentido de exigir não apenas a apresentação da prova digital em formato inteligível, mas também a demonstração de sua origem, de sua integridade técnica e da idoneidade do meio utilizado para sua produção e armazenamento.

Conforme sustenta Silva (2022, p.200):

não basta a simples juntada de um print screen ou de uma mídia eletrônica ao processo para que se considere válida a prova digital; é imprescindível a verificação técnica dos elementos que garantem sua autenticidade e sua preservação ao longo do tempo

Os requisitos de validade da prova digital — autenticidade, integridade e preservação da cadeia de custódia — devem ser compreendidos como pressupostos inafastáveis de sua admissibilidade e eficácia probatória, sob pena de afronta direta

aos princípios constitucionais que estruturam o devido processo legal e à segurança jurídica.

4.1 Autenticidade, Integridade, Veracidade e Cadeia De Custódia.

A validade e eficácia das provas digitais no processo judicial estão condicionadas à observância de critérios técnicos rigorosos que assegurem sua confiabilidade, sendo os principais: a autenticidade, a integridade, a veracidade e a cadeia de custódia.

A autenticidade diz respeito à origem da prova, exigindo que se possa comprovar, de forma inequívoca, que o dado digital apresentado provém efetivamente da fonte que se alega e que não sofreu adulterações desde sua geração. Esse requisito impõe a utilização de mecanismos técnicos como a assinatura digital qualificada, o carimbo do tempo (timestamp) e a certificação digital no padrão ICP-Brasil.

Tais instrumentos conferem fé pública aos documentos eletrônicos, por meio de criptografia assimétrica e chaves de verificação, garantindo que o conteúdo foi efetivamente produzido por um agente identificável e que não houve modificação desde sua criação. Assim, Souza (2023, p.122) diz que:

a certificação digital não apenas autentica o documento, mas também estabelece um vínculo técnico-jurídico entre o conteúdo e o seu emissor, elemento essencial em qualquer processo que envolva responsabilidade civil, criminal ou administrativa

Já a integridade refere-se à manutenção do conteúdo original da prova digital ao longo do tempo e durante todas as etapas de seu manuseio, o que impede alterações, inclusões ou exclusões não autorizadas e garante que o material apresentado em juízo permanece idêntico ao originalmente coletado.

Esse atributo é garantido, sobretudo, pelo uso de funções hash, que são algoritmos matemáticos capazes de gerar um código único e inalterável para cada arquivo digital, de modo que, qualquer mínima alteração no conteúdo original, mesmo que imperceptível ao olho humano, modifica o hash e denuncia a violação da integridade do dado. Assim, o hash apresenta-se como uma ferramenta técnica

imprescindível para assegurar que a prova digital permaneça inviolada desde sua coleta até a apresentação em juízo.

A veracidade, por sua vez, envolve a correspondência entre o conteúdo probatório e os fatos da realidade, sendo indispensável para a formação da convicção judicial. Embora seja um conceito de natureza fática e muitas vezes subjetiva, a veracidade se relaciona diretamente com os requisitos anteriores, pois uma prova que é autêntica e íntegra possui maior presunção de veracidade, podendo, ainda assim, ser objeto de contradição pelas partes.

Acerca das provas digitais, a veracidade não é presumida e deve ser tecnicamente demonstrada, por meio de análises periciais, metadados, logs de acesso e registros de rede, entre outros elementos. Ocorre que a mera existência de um print screen, por exemplo, não atesta, por si só, a veracidade do fato que se pretende demonstrar, sendo necessário comprovar a autenticidade da fonte, a integridade do conteúdo e a idoneidade da forma de obtenção.

Entretanto, todos esses requisitos encontram seu suporte técnico e jurídico na cadeia de custódia, trata-se do conjunto de procedimentos destinados a preservar, documentar e registrar, de forma cronológica e segura, todas as etapas da manipulação de um vestígio digital desde a sua obtenção, passando pela guarda, análise, até a apresentação judicial.

Neste sentido, Guerra (2024, p. 113) argumenta que:

a cadeia de custódia da prova digital compreende etapas como o reconhecimento, a coleta, a preservação, a análise e a apresentação do vestígio digital, com registro detalhado de cada intervenção humana ou técnica sobre o dado, garantindo sua rastreabilidade e evitando a contaminação probatória

No contexto digital, a cadeia de custódia exige um controle ainda mais rigoroso, considerando a volatilidade e a vulnerabilidade dos dados eletrônicos.

Segundo a Lei nº 13.964/2019 (Pacote Anticrime), a cadeia de custódia é definida no artigo 158-A do Código de Processo Penal como:

Art. 185-A. 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 do seu reconhecimento até o descarte.

No campo processual civil, embora não haja previsão legal expressa, aplica-se por analogia, em especial nos casos que envolvem elementos digitais frágeis e suscetíveis à manipulação.

A prova digital, por sua natureza é intangível, reproduzível e modificável, exige um controle muito mais rígido de seu trajeto probatório. Assim, a cadeia de custódia revela-se como o principal instrumento de confiança e segurança jurídica. Sem uma cadeia de custódia bem documentada a prova pode ser considerada inidônea, o contraditório e a ampla defesa podem ser comprometidos e pode haver violação ao devido processo legal.

De acordo com a doutrina e normas técnicas (como a ABNT NBR ISO/IEC 27037:2012), a cadeia de custódia se estrutura nas seguintes fases: i) reconhecimento: identificação de que determinado dado, arquivo ou sistema contém potencial valor probatório; ii) isolamento: separação do dado original para evitar alterações ou contaminações; iii) coleta e aquisição: extração técnica dos dados com preservação dos metadados e geração de cópia forense (bit a bit); iv) acondicionamento e preservação: armazenamento em mídia segura e lacrada, com registro dos responsáveis por cada manuseio; v) documentação da manipulação: qualquer acesso ou movimentação do dado deve ser registrado (quem, quando, por quê, com que ferramenta); vi) exame e análise: a prova pode ser analisada por peritos ou técnicos, com emissão de laudo, sem que se altere o conteúdo original; vii) apresentação em juízo: utilização em audiência ou juntada aos autos, com referência clara ao processo de custódia; viii) descarte (se cabível): após o trânsito em julgado ou desnecessidade, o material pode ser inutilizado com registro formal.

Tal procedimento mostra-se essencial para afastar suspeitas de manipulação e conferir à prova digital um estatuto de credibilidade jurídica. A literatura especializada também destaca que a função hash, a criptografia e até soluções como blockchain são instrumentos tecnológicos fundamentais para garantir essas propriedades probatórias, pois registram matematicamente as características do arquivo, criando códigos únicos e invioláveis que permitem aferir qualquer modificação posterior. Nesse contexto, a ausência de comprovação adequada de qualquer um desses elementos pode acarretar a desconsideração da prova pelo magistrado, sob o fundamento de incerteza quanto à sua confiabilidade, violando, assim, os princípios do contraditório, da ampla defesa e da segurança jurídica. Dessa forma, a conjugação entre autenticidade, integridade, veracidade e cadeia de custódia é não apenas

desejável, mas obrigatória para a legitimação da prova digital no processo judicial brasileiro.

4.2 Preservações Da Prova: Hash, Blockchain e Certificações Digitais

A preservação da prova digital no processo judicial é um dos maiores desafios enfrentados pelo direito contemporâneo, dada a natureza volátil, imaterial e suscetível à alteração dos dados eletrônicos. Os instrumentos mais relevantes nesse contexto são a função *hash*, o uso de *blockchain* e a certificação digital, todos eles voltados a garantir a confiabilidade da prova e a preservação de sua cadeia de custódia.

A função *hash* (ou algoritmo *hash*) é um mecanismo matemático que transforma qualquer conjunto de dados como textos, imagens, vídeos ou arquivos digitais em uma sequência única de caracteres alfanuméricos de comprimento fixo, denominada valor *hash* ou *digest hash*. Essa sequência representa a “impressão digital” do conteúdo original. O *hash* é utilizado para preservar a integridade da prova digital ao longo de sua cadeia de custódia, pois, ao ser calculado no momento da coleta do dado, garante-se que o conteúdo original não será alterado. Qualquer modificação, ainda que mínima, gerará um novo *hash*, sinalizando que a integridade foi comprometida.

No processo judicial, especialmente nos casos que envolvem documentos eletrônicos, áudios, vídeos, e-mails ou mensagens de aplicativos, o *hash* é calculado no momento da extração da prova e reaplicado em cada etapa do manuseio, de modo que, se o valor continuar o mesmo, a integridade da prova está preservada.

A doutrina tem reconhecido o valor do *hash* como critério objetivo de validade probatória. Neste sentido, Souza (2023, p. 61) argumenta que: “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”

Essa afirmação reforça que, embora a função *hash* por si só não comprove a autoria da prova, ela é imprescindível para garantir a sua integridade, conferindo segurança jurídica e validade ao material apresentado em juízo. Ademais, a combinação do *hash* com outros mecanismos como certificação digital e registros

de *logs* fortalece a estrutura probatória e permite que o Judiciário atue com maior segurança.

Outro recurso importante para a preservação das provas digitais é o uso de tecnologias baseadas em *blockchain*, uma tecnologia originalmente desenvolvida como a base do funcionamento do *Bitcoin* (2008), mas rapidamente ganhou aplicações além das criptomoedas, sobretudo em áreas que exigem transparência, segurança e rastreabilidade de dados.

Blockchain trata-se de uma tecnologia de registro distribuído que armazena informações de forma imutável, sequencial e descentralizada. Em termos simples, consiste em uma cadeia de blocos (*block-chain*), onde cada bloco contém um conjunto de dados, um carimbo de tempo (*timestamp*) e uma referência criptográfica ao bloco anterior, criando um registro cronológico e inalterável das transações ou eventos registrados.

Cada bloco contém dados que podem variar conforme a aplicação (ex.: transações financeiras, registros judiciais, documentos etc.), *hash* do bloco (código gerado pelo conteúdo do próprio bloco) e *hash* do bloco anterior (elemento que encadeia os blocos de forma cronológica e lógica). A alteração de qualquer informação em um bloco modifica seu *hash*, o que quebra a cadeia e torna evidente a tentativa de fraude. Como a *blockchain* é replicada em milhares de computadores ao redor do mundo, para alterar um único dado seria necessário alterar simultaneamente todos os registros, o que é tecnicamente inviável em *blockchains* públicas.

Ademais, a cadeia de custódia digital exige que seja possível rastrear toda a trajetória da prova — desde sua obtenção até sua análise e apresentação. O *blockchain*, por seu caráter imutável e distribuído, é extremamente eficaz para isso: cada ação (*upload*, acesso, alteração, envio) pode ser registrada como um “bloco”, que permanecerá visível, auditável e inalterado. Isso garante a integridade dos dados (qualquer alteração quebra o *hash*), impossibilidade de fraude processual (não há como “fabricar” ou “editar” provas sem que isso fique evidente) e a validade como elemento probatório complementar. Assim, Guerra (2024, p. 133) diz que: “O *blockchain* gera a imutabilidade dos dados, não permitindo a modificação de conteúdo que lhe foi inserido, sendo um dos instrumentos mais promissores para a preservação da cadeia de custódia digital”

Apesar das vantagens, a adoção da *blockchain* ainda enfrenta a falta de regulamentação específica, desconhecimento técnico dos operadores do direito,

insegurança quanto à aceitação judicial como meio autônomo de prova e o risco de uso indevido ou entendimento errôneo das funções do sistema.

Por fim, a certificação digital é um mecanismo de autenticação que permite validar, com segurança, a identidade de uma pessoa física, jurídica ou de um sistema eletrônico em meios digitais. Trata-se de uma tecnologia baseada em criptografia que garante a autenticidade, a integridade e a não repudição de documentos eletrônicos, transações e assinaturas digitais. O seu principal instrumento é o certificado digital, que funciona como uma identidade eletrônica emitida por uma autoridade certificadora confiável.

A certificação digital utiliza a criptografia de chave pública (*PKI – Public Key Infrastructure*), que opera com um par de chaves: i) chave pública: usada para verificar a assinatura digital e criptografar dados; ii) chave privada: usada para assinar digitalmente e descriptografar dados.

Quando alguém assina digitalmente um documento usando sua chave privada, qualquer pessoa pode verificar a autenticidade da assinatura por meio da chave pública correspondente. Isso garante que o documento foi efetivamente assinado por quem detém a chave privada, e que não houve alteração do conteúdo desde a assinatura.

No Brasil, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) foi instituída pela Medida Provisória nº 2.200-2/2001, responsável por regulamentar a emissão e o uso dos certificados digitais. Os principais elementos da ICP-Brasil são: AC-Raiz: controlada pelo Instituto Nacional de Tecnologia da Informação (ITI); ACs: responsáveis por emitir os certificados digitais; ARs: realizam a interface com os usuários para validação da identidade.

Essa estrutura garante que os documentos assinados com certificado digital emitido pela ICP-Brasil tenham validade jurídica plena, conforme o artigo 10, §1º da Medida Provisória 2.200-2/2001.

A doutrina reconhece a eficácia da certificação digital como meio idôneo para garantir a validade jurídica de documentos eletrônicos. Segundo Souza, Munhoz e Carvalho (2023, p. 122):

A certificação digital não apenas autentica o documento, mas também estabelece um vínculo técnico-jurídico entre o conteúdo e o seu emissor, elemento essencial em qualquer processo que envolva responsabilidade civil, criminal ou administrativa.

Na produção de provas digitais, a certificação digital tem papel central na autenticação e verificação de autoria de documentos eletrônicos. Quando um documento é assinado digitalmente com certificado ICP-Brasil presume-se que foi assinado pela pessoa indicada no certificado, garante-se que o conteúdo não foi alterado após a assinatura e confere-se validade jurídica equivalente à de documentos físicos com firma reconhecida.

Além disso, em procedimentos de preservação de prova digital, como ata notarial, registros de e-mails, contratos eletrônicos ou prints de redes sociais, a certificação digital garante a autenticidade e a integridade do conteúdo coletado, reforçando a segurança probatória e facilitando sua admissibilidade judicial.

Assim, a certificação digital se consolida como uma ferramenta indispensável à legitimação da prova digital no processo judicial brasileiro, harmonizando o avanço tecnológico com os princípios constitucionais do devido processo legal e da segurança jurídica.

Ao garantir a autenticidade, a integridade e a não repudição, ela assegura que os documentos eletrônicos possam circular e produzir efeitos jurídicos com a mesma segurança dos documentos físicos, sendo, portanto, uma das bases mais sólidas para o fortalecimento da justiça digital no século XXI.

4.3 Desafios Práticos Na Produção e Valoração Da Prova Digital

A produção e valoração da prova digital no processo judicial enfrentam uma série de desafios práticos, que derivam tanto da complexidade técnica dos meios digitais quanto da necessidade de adaptação do Direito às novas realidades tecnológicas. Esses desafios se manifestam em diferentes etapas: desde a obtenção da prova, passando por sua preservação e apresentação em juízo, até a interpretação e valoração pelo magistrado, exigindo atuação conjunta de juristas, técnicos e peritos especializados. A seguir, apresento uma análise abrangente, profunda e sistemática sobre esses desafios.

Diferentemente das provas físicas tradicionais, cuja materialidade é diretamente perceptível, a prova digital é volátil, intangível e facilmente manipulável. Arquivos de texto, imagens, e-mails, mensagens de aplicativos e outros elementos digitais podem ser alterados com poucos comandos, tornando essencial a aplicação de mecanismos técnicos que assegurem sua autenticidade (autoria) e integridade

(imutabilidade). Na prática, entretanto, muitas partes apresentam capturas de tela (“*prints*”), documentos sem certificação digital ou metadados, o que dificulta a verificação de sua origem e pode comprometer sua admissibilidade judicial. A ausência de *hash*, assinatura digital ou registro confiável de extração compromete a credibilidade da prova e favorece sua impugnação.

O uso de ferramentas corriqueiras como capturas de tela, gravações informais e cópias de mensagens pode gerar insegurança jurídica, uma vez que são de fácil adulteração e geralmente não registram metadados essenciais como horários, endereços de IP, autores e dispositivos. Na prática, muitas vezes não há formalização da coleta por meio de ata notarial, nem perícia técnica, o que expõe a prova a críticas sobre sua veracidade.

Além disso, há uma natural resistência de empresas de tecnologia em fornecer dados mediante simples requerimento judicial, muitas vezes amparadas em legislações de proteção de dados estrangeiras, o que dificulta a obtenção de provas técnicas com respaldo institucional.

Um dos maiores obstáculos à adequada valoração da prova digital reside no descompasso entre o avanço tecnológico e o conhecimento técnico dos magistrados, advogados e membros do Ministério Público. Muitos operadores jurídicos ainda não dominam conceitos fundamentais como metadados, *hash*, *blockchain*, autenticação digital e criptografia.

Como resultado, podem conferir valor probatório a conteúdos tecnicamente frágeis, como mensagens sem origem verificada, ou desprezar elementos tecnicamente robustos, por não compreenderem sua relevância. Essa lacuna impõe a necessidade de capacitação técnica constante e da presença de peritos especializados nos processos que envolvem elementos digitais.

A jurisprudência tem oscilado diante dessa realidade, ora admitindo a flexibilização de formalidades, ora desconsiderando provas por ausência de rigor técnico. Conforme pontua Silva (2022, p. 200):

a verificação dos requisitos da autenticidade, integridade e preservação da cadeia de custódia deve ser estritamente exigida, sobretudo diante da vulnerabilidade da prova digital frente à adulteração e à fragilidade técnica dos meios comumente utilizados

Ademais, mesmo quando a prova digital é tecnicamente válida, surgem dificuldades quanto à sua valoração jurídica, especialmente nos casos em que o conteúdo é ambíguo, contextual ou obtido de forma potencialmente ilícita, o que suscita discussões sobre admissibilidade, proporcionalidade e respeito às garantias constitucionais, como o direito à intimidade e à ampla defesa. O Código de Processo Civil de 2015, embora avance no tratamento da prova documental eletrônica (art. 441), não contempla de forma específica os requisitos de admissibilidade e valoração da prova digital nem os protocolos técnicos que deveriam nortear sua coleta e apresentação.

Diante de tais desafios, é imperativo que o sistema jurídico se atualize para a nova realidade probatória imposta pela tecnologia. Isso inclui a elaboração de normativas específicas, a padronização dos procedimentos técnicos, a valorização da perícia e a formação continuada dos profissionais do direito. Apenas com essas medidas será possível assegurar que a prova digital seja tratada com o mesmo grau de segurança, confiabilidade e legitimidade das provas tradicionais, garantindo a efetividade do processo judicial

5 CONCLUSÃO

A incorporação de provas digitais ao processo judicial brasileiro reflete a necessidade de o Direito acompanhar as inovações tecnológicas e as mudanças sociais da atualidade. Desde os conceitos tradicionais sobre a função das provas, voltadas à reconstrução dos fatos e à formação do convencimento do juiz, até os desafios modernos relacionados à admissibilidade, autenticidade e integridade dos elementos digitais, observa-se um cenário de constantes transformações. O contexto apresentado demanda não apenas domínio técnico das novas tecnologias, mas também um esforço crítico para integrá-las ao sistema jurídico, sempre em harmonia com os valores e princípios constitucionais.

Assim, neste trabalho, analisou-se o conceito de prova e sua importância no processo, com ênfase nos diferentes tipos admitidos pelo ordenamento jurídico brasileiro, dedicou-se atenção especial às provas digitais, que ampliaram as possibilidades probatórias, mas trouxeram consigo questões sensíveis, como a licitude de sua obtenção, o direito à privacidade e a necessidade de garantir a segurança e confiabilidade desses elementos.

Embora o ordenamento jurídico brasileiro tenha avançado significativamente com normas como a Medida Provisória nº 2.200-2/2001, a Lei nº 11.419/2006, a Lei Geral de Proteção de Dados - Lei nº 13.709/18 e o Código de Processo Civil de 2015, que estruturam o uso de documentos e dados eletrônicos como provas, a ausência de regulamentações específicas e o ritmo acelerado das inovações tecnológicas mostram que ainda carece de uniformidade e especialização na regulamentação das provas digitais. As lacunas normativas, aliadas à insuficiência de capacitação dos operadores do Direito, geram insegurança jurídica e comprometem a efetividade da justiça, especialmente em casos em que a prova digital é o principal meio de demonstração dos fatos.

A questão das provas ilícitas também foi analisada, evidenciando os limites legais e éticos para a obtenção de provas e reforçando a inadmissibilidade de elementos que violem direitos fundamentais, tal regra é indispensável para preservar a integridade do processo judicial e evitar abusos que possam comprometer a justiça e a equidade das decisões. No contexto das provas digitais, essa discussão se intensifica, considerando a vulnerabilidade dos meios eletrônicos a manipulações e a complexidade de assegurar sua licitude e validade. Ademais, a análise realizada

demonstrou que a validade da prova digital não pode ser presumida, devendo ser construída por meio de procedimentos que garantam sua origem lícita, autenticidade, integridade e rastreabilidade. Esse cuidado técnico é fundamental para que a prova possa exercer seu papel de forma legítima, resguardando o devido processo legal e fortalecendo a função jurisdicional do Estado.

Por fim, a análise da legalidade das provas digitais reforça que sua admissibilidade depende de um equilíbrio entre inovação e respeito às garantias processuais, o papel dos operadores do Direito, peritos e legisladores torna-se crucial para assegurar que as tecnologias sejam utilizadas como ferramentas de apoio à justiça, e não como obstáculos ou fontes de insegurança jurídica.

Além disso, a constante capacitação técnica e a criação de mecanismos normativos mais robustos são fundamentais para acompanhar a velocidade das mudanças tecnológicas e garantir que o Direito continue a servir como um instrumento efetivo de pacificação social e proteção de direitos.

Contudo, a análise crítica apresentada nesta monografia reforça a importância de se pensar o Direito não apenas como um conjunto de normas, mas como um campo em constante evolução, que deve acompanhar os avanços sociais e tecnológicos sem abrir mão dos valores que sustentam o Estado Democrático de Direito.

Portanto, conclui-se que a integração das provas digitais no processo judicial brasileiro, além de uma adaptação técnica, representa uma transformação paradigmática que exige maturidade, inovação e comprometimento ético, a busca pela verdade no âmbito processual deve sempre respeitar os princípios constitucionais e considerar as peculiaridades de uma sociedade em constante mudança, garantindo que a tecnologia seja um meio de fortalecimento da justiça e não uma ameaça à sua realização.

REFERÊNCIAS

ALVES, Marcella Bizotto. **As provas eletrônicas no novo CPC associadas ao advento do Marco Civil da Internet**. 2016. Disponível em: <https://www.migalhas.com.br/depeso/247105/as-provas-eletronicas-no-novo-cpc-associadas-ao-advento-do-marco-civil-da-internet>. Acesso em: 07 de fevereiro de 2025.

AMARAL, Paulo Osternack. **Provas – atipicidade, liberdade e instrumentalidade**. São Paulo: RT, 2015.

AVOLIO, Luiz Francisco Torquato. **Provas ilícitas**. 6ªed. São Paulo, Ed. Revista dos Tribunais, 2015.

BARBOSA, Carolina Ap. Sales. **Teoria geral da Prova no Direito Processual Penal Brasileiro**. 2016. Disponível em: <https://www.jusbrasil.com.br/artigos/teoria-geral-da-prova-no-direito-processual-penal-brasileiro/337514638>. Acesso em: 20 de janeiro de 2025.

BRASIL. **Código Civil**. Lei nº 10.406, de 10 de janeiro de 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 22 de janeiro de 2025.

BRASIL. **Código de Processo Civil**. Lei n.º 13.105, de 16 de março de 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2015-2018/2015/lei/l13105.htm. Acesso em: 22 de janeiro de 2025.

BRASIL, Decreto de Lei nº3.689/1941. **Código de Processo Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em 22 de janeiro de 2025.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 de janeiro de 2025.

BRASIL. **Lei n.º 11.419, de 19 de dezembro de 2006**. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2004-2006/2006/lei/l11419.htm. Acesso em 07 de fevereiro de 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm. Acesso em 20 de fevereiro de 2025.

BRASIL. **Medida Provisória n.º 2.200-2, de 24 de agosto de 2001**. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em 25 de fevereiro de 2025.

BRASIL. Tribunal Superior do Trabalho. **Recurso Ordinário em Mandado de Segurança**. STF, MS 23.452, Rel. Min. Celso de Mello, Tribunal Pleno, 2020. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/tst/2554596264>. Acesso em: 01 de março de 2025.

CAMBI, Eduardo. **Direito Constitucional à prova no Processo Civil**. Revista dos Tribunais, v. 3, p 41, 2001.

CAMBI, Eduardo. **Direito Constitucional à prova**. São Paulo: RT, 1996, n.76.

CAPEZ, Fernando; COLNAGO, Rodrigo. **Código de processo penal comentado**. 1 ed. Ed. Saraiva, 2015.

CORTEZ, Raphaela Jéssica Reinaldo. **Prova digital no processo penal: o uso de dados de geolocalização na segurança pública e na investigação criminal**. Natal: UFRN, 2023.

DIDIER JUNIOR, Fredie; BRAGA, Paulo Sarno; OLIVEIRA, Rafael Alexandria de. **Curso de Direito Processual Civil**. 13. ed. Salvador: Juspodivm, 2018. 776 p. (Volume 2).

DIDIER JUNIOR, Fredie (Org.). **Direito Probatório**. 2. ed. Salvador: Juspodivm, 2016a. 1100 p. (5).

FREITAG, Leandro Ernani; MOTTA, Débora. **Provas digitais e o problema do print screen**. Revista da ESMESC, v. 30, n. 36, p. 24-50, 2023.

GUERRA, Maite Neves. **Regime democrático das provas digitais no processo penal: aquisição e qualificação**. Itajaí: UNIVALI, 2024, p. 113.

GUERRA, Maite Neves. **Regime democrático das provas digitais no processo penal: aquisição e qualificação**. Itajaí: UNIVALI, 2024, p. 133.

HARRISON, Klaus Neco Alves. **O uso das provas digitais no processo eletrônico**. Goiânia: Pontifícia Universidade Católica de Goiás, 2021.

MARCACINI, Augusto Tavares Rosa. Prova digital no processo: autenticidade e integridade. **Revista Brasileira de Direito Processual**, v. 14, p. 95-128, 2021.

MARINONI, Luiz Guilherme, ARENHART, Sérgio Cruz. **Comentários ao Código de Processo Civil**. 2ª ed. v.5, t.1. São Paulo: RT, 2005.

NUCCI, Guilherme de Souza. **Curso de Direito Processual Penal**. 20. ed. Rio de Janeiro: Forense, 2023.

NUCCI, Guilherme de Souza. **Manual de processo e execução penal**. 11. Ed. Rev., atual e ampl. Rio de Janeiro: Ed. Forense, 2014.

NUCCI, Guilherme de Souza. **Provas no Processo Penal**. 3. ed. Rio de Janeiro: Forense, 2015.

NUCCI, Guilherme de Souza. **Provas no processo penal**. São Paulo: Revista dos Tribunais, 2009.

PASTORE, Guilherme de Siqueira. **Considerações sobre a autenticidade e a integridade da prova digital**. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 63-79, janeiro-março de 2020.

SANTOS, Maria Clara Moura. **A validade das provas digitais no novo Código de Processo Civil**. Monografia (Bacharelado em Direito) – Universidade Federal Fluminense, Volta Redonda, RJ, 2019.

SARMENTO, Daniel. **Proporcionalidade e direito fundamentais: uma análise à luz da teoria dos direitos fundamentais de Robert Alexy**. Rio de Janeiro: Lumen Juris, 2005. p. 85.

SILVA, José Antônio Ribeiro de Oliveira. **A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova**. Rev. TST, São Paulo, vol. 88, n. 2, abr./jun. 2022, p. 200

SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 61.

SOUZA, Bernardo de Azevedo; MUNHOZ, Alexandre; CARVALHO, Romullo. **Manual prático de provas digitais**. São Paulo: Thomson Reuters Brasil, 2023. p. 122

TARUFFO, Michele. **A prova**. Tradução de: João Gabriel Couto. São Paulo: Marcial Pons, 2014.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal**. 8. Ed. Salvador: Ed. JusPODIVM, 2013.

TEODORO JÚNIOR, Humberto. **Curso de Direito Processual Civil**. Vol. 1. 59. ed. Rio de Janeiro: Forense, 2018.

THAMAY, Patrícia; TAMES, Ricardo. **Provas no processo civil: uma análise contemporânea**. 2. ed. São Paulo: Atlas, 2020.