

DIGITALIZAÇÃO E TEORIA DA PROVA: UMA ANÁLISE CONTEMPORÂNEA

DIGITALIZATION AND THEORY OF EVIDENCE: A CONTEMPORARY ANALYSIS

Edielma Rocha Dutra¹; Tiago Cappi Janini²

Resumo: A sociedade da informação trouxe mudanças significativas em diversos campos do conhecimento, incluindo o direito. Este artigo investiga o impacto da digitalização sobre a teoria da prova, considerando as profundas transformações ocasionadas pela sociedade da informação. O problema de pesquisa gira em torno de como a digitalização, combinada com a ampla disponibilidade de dados digitais, altera os fundamentos tradicionais da prova jurídica, especialmente no que se refere à autenticidade, integridade e preservação das evidências, com destaque para a relevância da cadeia de custódia. O objetivo principal é identificar e analisar as novas dinâmicas impostas à prática jurídica, ressaltando os desafios e oportunidades que emergem na coleta, preservação e apresentação de provas digitais. A metodologia empregada consiste na análise de bibliografia especializada, incluindo doutrinas, artigos acadêmicos, teses de mestrado e doutorado, legislações aplicáveis e a jurisprudência sobre o tema. Além disso, foram consideradas discussões contemporâneas acerca da privacidade e da segurança no manejo de dados digitais. Conclui-se que, no contexto jurídico atual, a digitalização impõe a necessidade de novas abordagens teóricas e práticas, de modo a garantir tanto a efetividade quanto a segurança jurídica na utilização das provas digitais, reafirmando a importância de uma robusta cadeia de custódia.

Palavras-chave: Sociedade da Informação; ecossistema digital; segurança dos dados pessoais; teoria da prova; provas digitais.

Abstract: The information society has brought significant changes across various fields of knowledge, including law. This article investigates the impact of digitalization on proof theory, considering the profound transformations caused by the information society. The research problem revolves around how digitalization, combined with the wide availability of digital data, changes the traditional foundations of legal evidence, especially with regard to authenticity, integrity and preservation of evidence, with emphasis on the relevance of the chain of custody. The main objective is to identify and analyze the new dynamics imposed on legal practice, highlighting the challenges and opportunities that emerge in the collection, preservation and presentation of digital evidence. The methodology used consists of the analysis of specialized

¹ Oficial de Promotoria no Ministério Público do Estado de São Paulo (MPSP). Graduada pela Universidade Católica de Santos (UNISANTOS). Pós-graduada em Direito Processual Penal pela Instituto Damásio de Direito/IBMEC. Pós-graduanda em Direito Penal e Criminologia na PUC - Rio Grande do Sul. Mestranda em Direito da Sociedade da Informação nas Faculdades Metropolitanas Unidas.

² Doutor em Direito pela Pontifícia Universidade Católica de São Paulo. Professor do Programa de Mestrado em Direito na Sociedade da Informação e da graduação da FMU. Estágio de Pós-Doutorado na Universidade Estadual do Norte do Paraná (UENP), bolsista PNPd-CAPES.

bibliography, including doctrines, academic articles, master's and doctoral theses, applicable legislation and jurisprudence on the subject. Furthermore, contemporary discussions about privacy and security in the handling of digital data were considered. It is concluded that, in the current legal context, digitalization imposes the need for new theoretical and practical approaches, in order to guarantee both effectiveness and legal security in the use of digital evidence, reaffirming the importance of a robust chain of custody.

Keywords: Information Society; digital ecosystem; personal data security; theory of evidence; digital evidence.

INTRODUÇÃO

A Era Digital, impulsionada pela difusão de algoritmos e pela crescente digitalização das atividades humanas, trouxe mudanças substanciais para diversos campos do saber, incluindo o Direito. As interações sociais, o trabalho e as formas de comunicação foram profundamente modificados, exigindo uma reavaliação dos alicerces sobre os quais se constrói o sistema jurídico. Nesse cenário, a Teoria do Direito precisa se adaptar às novas dinâmicas, e, em especial, a Teoria da Prova, essencial no direito processual para a busca da verdade, é diretamente impactada pelas inovações tecnológicas e pela proliferação de dados digitais.

O problema de pesquisa aqui abordado é como a digitalização e a sociedade da informação afetam os conceitos tradicionais da Teoria da Prova, com ênfase na autenticidade, integridade e cadeia de custódia das provas digitais. As rápidas transformações tecnológicas exigem uma releitura dos mecanismos tradicionais de produção e valoração de provas, questionando-se até que ponto os paradigmas processuais vigentes são capazes de responder adequadamente a essas mudanças.

O objetivo deste artigo é analisar os desafios e oportunidades trazidos pela digitalização no campo da prova processual. Questões como a volatilidade dos dados digitais, a integridade e autenticidade das provas, e a adaptação das normas processuais ao ambiente digital serão discutidas à luz de doutrinas e jurisprudências. Além disso, o artigo também explora as potencialidades das tecnologias emergentes, como a inteligência artificial, na coleta e análise de evidências, buscando formas mais eficientes e seguras de garantir a verdade processual.

A metodologia aplicada é a análise crítica de bibliografia especializada, englobando estudos acadêmicos, doutrinas, legislações e jurisprudências, de forma a oferecer uma visão ampla sobre as mudanças na Teoria da Prova na era digital. Em suma, o artigo busca fomentar a reflexão sobre o futuro da Teoria da Prova em um mundo cada vez mais digital, incentivando

o debate sobre como o sistema jurídico pode se adaptar a essa nova realidade de forma justa e eficaz.

1. A SOCIEDADE DA INFORMAÇÃO E O DIREITO

A sociedade da informação é marcada pela predominância das tecnologias de informação e comunicação (TICs) e pela digitalização dos dados. Segundo Manuel Castells (1999, p. 119), essa sociedade é caracterizada pela capacidade de gerar, processar e transmitir informações de maneira eficiente. No contexto jurídico, isso significa que as provas digitais, como e-mails, mensagens de texto e registros de redes sociais, tornaram-se cada vez mais comuns.

A sociedade da informação representa uma transformação profunda na maneira como a informação é gerada, processada e disseminada. Este conceito, amplamente discutido por estudiosos como Manuel Castells, refere-se a uma era em que as tecnologias de informação e comunicação (TICs) desempenham um papel central na estruturação das sociedades modernas. A digitalização e a conectividade global são características marcantes dessa sociedade, influenciando diversos aspectos da vida cotidiana, incluindo o campo jurídico.

A sociedade da informação é definida por várias características distintivas. Dário José Kist (2024, p. 29) assim a descreve:

a sociedade da informação e da comunicação é um “mundo” com intenso fluxo de informações, que está em veloz e permanente mudança e em que o conhecimento é flexível, fluido e sempre em expansão; as noções existentes sobre território foram relativizadas, pois superadas as barreiras que o espaço, assim como o tempo, impunham à comunicação entre as pessoas, notadamente as ausentes.

Nesse contexto, tem-se a digitalização (a conversão de informações analógicas em formato digital permite um armazenamento, processamento e transmissão mais eficientes. Isso inclui desde documentos e registros até comunicações pessoais e transações financeiras), conectividade global (a internet e outras redes de comunicação conectam indivíduos e organizações em escala global, permitindo a troca instantânea de informações), abundância de dados (a produção e o armazenamento de grandes volumes de dados, muitas vezes referidos como "big data", criam novas possibilidades para análise e tomada de decisão), velocidade de informação (a rapidez com que a informação pode ser transmitida e acessada transforma a maneira como as decisões são tomadas e como as interações sociais e comerciais ocorrem).

A introdução dessas características no contexto jurídico traz uma série de implicações. A digitalização resulta em novas formas de provas digitais, evidências digitais, como e-mails, mensagens de texto, registros de redes sociais e dados de localização. Esses tipos de provas requerem novas abordagens para autenticação e verificação. A facilidade com que dados digitais podem ser manipulados levanta questões sobre a autenticidade e a integridade das provas. Ferramentas tecnológicas e protocolos de segurança são necessários para garantir que as provas digitais sejam confiáveis.

Ademais, a conectividade global e a abundância de dados oferecem aos advogados e juízes acesso a uma quantidade sem precedentes de informações, potencialmente enriquecendo a análise de casos e a tomada de decisões. A coleta e o uso de dados digitais levantam preocupações sobre privacidade e segurança, exigindo um equilíbrio entre o uso de informações para fins legais e a proteção dos direitos individuais.

A sociedade da informação, portanto, não apenas redefine a maneira como a informação é tratada, mas também desafia e enriquece o campo jurídico, exigindo uma adaptação contínua para lidar com as novas realidades tecnológicas.

A crescente adoção de recursos digitais e o consequente armazenamento massivo de informações através do tráfego contínuo na web, impulsionado por tecnologias que são constantemente desenvolvidas, resulta no registro de grande parte das atividades diárias da sociedade. Nesse cenário, as provas digitais ganham destaque, pois essa realidade demanda um sistema que ofereça aos cidadãos todos os meios legítimos para satisfação pessoal e corporativa, utilizando tecnologias, mas sempre com atenção à segurança da informação. É importante destacar que, até pouco tempo atrás, as provas em processos judiciais eram majoritariamente físicas, com raras exceções de provas em formatos como áudio em CD ou disquete. Atualmente, no entanto, as provas digitais dominam as investigações criminais e são fundamentais na produção de evidências em processos jurídicos, que também se tornaram majoritariamente eletrônicos. As provas digitais que sustentam processos judiciais ou investigações criminais incluem desde documentos digitais, como contratos virtuais e capturas de tela de conversas em aplicativos, até vídeos e áudios anexados por meio de mídias digitais. A computação forense, por sua vez, é o ramo da criminalística focado na análise de vestígios cibernéticos, ou seja, informações armazenadas ou transmitidas digitalmente, abrangendo todos os elementos relacionados a elas.

2. A TEORIA DA PROVA NA ERA DIGITAL

A era digital trouxe uma revolução na forma como as provas são coletadas, apresentadas e analisadas nos processos judiciais. A teoria da prova, que tradicionalmente se baseava em evidências físicas e testemunhais, agora deve se adaptar a um ambiente onde as provas digitais desempenham um papel cada vez mais central.

Fazendo uma análise histórica deste fenômeno contemporâneo, Tiago Cappi Janini (2010, p. 35-36) aduz que a cibernética provocou uma verdadeira revolução, dada a evolução da internet e dos meios de transmissão de informação. Surge um ambiente onde pessoas de todos os países, pertencentes às mais diversas culturas e linguagens, encontram-se trocando informações processadas digitalmente em uma rede de computadores interconectada. Essas informações não possuem uma forma material estável no tempo e no espaço, e transcendem qualquer tipo de fronteira. Assim, emerge um novo meio social: a internet (JANINI, 2010, p. 35).

2.1. Conceitualização de “prova”

No âmbito jurídico, a prova é um elemento fundamental para a resolução de conflitos e a tomada de decisões judiciais. Em linhas gerais, a prova consiste em qualquer meio ou recurso utilizado para demonstrar a veracidade de fatos alegados pelas partes em um processo. O objetivo da prova é servir de suporte fático com o fim de convencer o juiz ou tribunal sobre a ocorrência ou não de determinados eventos, influenciando diretamente o resultado do julgamento.

Este entendimento vai ao encontro da doutrina de Cássio Scarpinella Bueno (2010, p. 261), que explica que a prova seria “tudo que puder influenciar, de alguma maneira, na formação da convicção do magistrado para decidir de uma forma ou de outra, acolhendo no todo ou em parte, ou rejeitando o pedido do autor”. Da mesma forma, Luiz Guilherme Marinoni e Daniel Mitidiero (2011, p. 334) definem a prova como “meio retórico, regulado pela legislação, destinado a convencer o Estado da validade de proposições controversas no processo, dentro de parâmetros fixados pelo direito e de critérios racionais”.

Tiago Cappi Janini (2010, p. 36), explicando o termo “prova” num contexto prático, aduz que:

A “prova” como enunciação consiste nos atos produzidos para construir o fato alegado, ou seja, como ação de provar. Tomada como enunciado, “prova” seria o resultado da atividade realizada. É importante ressaltar que o vocábulo ainda é comumente usado no sentido no suporte físico. Exemplificando, usa-se a *prova* testemunhal. O processo de elaboração de uma prova testemunhal. O processo de elaboração de uma *prova testemunhal* consiste inicialmente na oitiva da testemunha, que somente ingressará nos autos quando levada a termo. Esse ato de oitiva é a *prova* na sua acepção de enunciação, como procedimento utilizado para a elaboração de um enunciado. Esse enunciado será a prova testemunhal, que consiste nas informações prestadas pela testemunha em relação ao fato alegado. Salienta-se que o enunciado está vertido em documento (suporte físico), também chamado de prova. Percebe-se, portanto, que o problema surge porque todas as etapas têm a mesma denominação: *prova*.

Modernamente, o conceito de prova ganhou novas conotações. O avanço da tecnologia trouxe novos suportes para o documento denominado prova. Tais suportes são comumente denominados de provas digitais. Trata-se de um leque amplo, que inclui e-mails, mensagens de texto, registros de chamadas telefônicas, dentre outros.

Nesse contexto, Lucien (2023, p. 39-40) define a prova digital do seguinte modo:

Prova digital não é nada mais nada menos que todo e qualquer dado que esteja armazenado ou que seja transmitido via computador e sirva para apoiar ou para rejeitar alguma teoria sobre como um crime específico aconteceu e que contenha elementos críticos desse crime, como intenção ou alibi.

De forma mais detalhada, Alexandre Morais da Rosa (2022, n.p):

Prova Digital (*e-evidence*). A prova digital (espécie da prova eletrônica) é a obtida e/ou produzida em ambiente eletrônico digital, em que os dados (de base, de tráfego e de conteúdo), em geral, vulneráveis, intangíveis e frágeis, devem ser extraídos e tratados em observância às normas técnicas, observada a cadeia de custódia digital, sob pena de ineficácia probatória. A tendência contemporânea é a do uso futuro da tecnologia blockchain. Definição de “e-evidence”. A definição de “e-evidence” orienta-se pela: (a) relevância (meio de prova adequado ao fim que se destina); (b) confiabilidade (equivalência entre o verificado e o representado); e, (c) suficiência (deve congrega os elementos necessários de superação aos testes de verificação).

Como se vê, o conceito de prova jurídica é dinâmico e adaptável às mudanças sociais e tecnológicas, sempre buscando garantir um julgamento justo e equitativo.

Com isso, percebe-se que a prova, antes advinda de um movimento centrípeto, seja materializada num documento físico (ex.: oitiva reduzida a termo) seja materializada num documento digital (ex.: CD-ROM, pen-drive); hoje se encontra em movimento inverso, ou seja, centrífugo, cuja produção se inicia no ecossistema digital (redes sociais – Facebook, Tic Toc, Youtube, X etc.; jornais digitais; etc.). Dessa forma, importante analisar o conceito de documento eletrônico (ou digital).

2.2. Conceitualização de documento eletrônico (ou digital)

Para Rennan Thamay e Maurício Tamer (2022, n.p.), a prova, de modo geral, é o instrumento que forma a convicção de alguém em relação a um fato específico. No ecossistema digital (dispositivos, dados, usuários, plataformas, serviços online), explicam que a expressão "prova digital" pode ser interpretada de duas maneiras. A primeira interpretação considera a prova digital como a evidência de um evento que ocorreu em ambientes digitais, ou seja, um fato que depende do uso de um meio digital. A segunda interpretação sugere que, mesmo que o evento não tenha acontecido em um ambiente digital, sua comprovação pode ser feita através de meios digitais.

Os fatos ocorridos em meios digitais, para os quais a prova é necessária (prova digital), incluem situações como o envio de e-mails, mensagens por aplicativos como WhatsApp e Telegram, cópia ou desvio de bases de dados, cópia de *software*, e a publicação de vídeos na internet, sejam eles de conteúdo íntimo ou difamatório, entre outros. Além disso, o meio digital pode ser utilizado como ferramenta para comprovar a existência de um fato ocorrido fora do ambiente digital. Um exemplo seria uma ata notarial feita a partir da observação de uma foto em uma rede social, onde um funcionário de uma empresa aparece junto com um diretor de uma concorrente, demonstrando um possível conluio entre eles. No contexto criminal, o monitoramento judicialmente autorizado de conversas no WhatsApp pode fornecer provas de crimes como tráfico de drogas. Nesses casos, os fatos não são digitais por natureza, mas os meios digitais servem como um mecanismo de comprovação (THAMAY; TAMER; 2022, n.p.).

Nesse contexto, Rennan Thamay e Maurício Tamer (2022, n.p.) conceituam prova digital da seguinte forma:

o instrumento jurídico vocacionado a demonstrar a ocorrência ou não de determinado fato e suas circunstâncias, tendo ele ocorrido total ou parcialmente em meios digitais ou, se fora deles, esses sirvam como instrumento para sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo.

Assim, documento eletrônico (ou digital) caracteriza-se por ser produzido, autenticado, armazenado e transmitido em formato eletrônico, mantendo sua forma original. Diversos exemplos ilustram essa categoria, como: (i) arquivos em formato PDF ou DOC, com ou sem assinatura eletrônica; (ii) vídeos criados integralmente em ambiente digital ou disponibilizados em plataformas online, como o YouTube, acessíveis por meio de QR Code; (iii) mensagens trocadas em aplicativos de mensageria instantânea, a exemplo de WhatsApp e

Telegram; (iv) e-mails; (v) arquivos de áudio em MP3 ou outros formatos, gravados inclusive em dispositivos móveis, entre outros (THAMAY; TAMER; 2022, n.p.).

Nesse contexto, alertam Rennan Tamay e Maurício Tamer (2022, n.p) que é fundamental distinguir o documento digital do digitalizado. Este último, representando um terceiro tipo documental, consiste na versão digital de um documento originalmente físico. A conversão para o meio eletrônico ocorre por meio de processos de digitalização, como fotografia, uso de aplicativos específicos ou *scanners*.

Partindo dessa premissa (documento digitalizado ≠ documento digital), no Brasil tem-se a Lei do Processo Judicial Eletrônico (Lei n. 11.419/2006), que dispõe sobre a informatização do processo judicial. Essa lei buscou principalmente promover a emancipação do indivíduo em uma sociedade digital. Conforme explicam Carmen Elisângela Dias Moreira de Resende e outros (2023, p. 145-186), esta lei define como meio eletrônico qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais (inciso I, art. 2º); como transmissão eletrônica, toda forma de comunicação à distância utilizando redes de comunicação, preferencialmente a internet (inciso II, art. 2º); e como assinatura eletrônica, a identificação inequívoca do signatário, seja por certificado digital emitido por Autoridade Certificadora credenciada, conforme legislação específica, ou por cadastro de usuário no Poder Judiciário, conforme regulamentação dos órgãos competentes (inciso III, art. 2º).

Os autores salientam também que o artigo 11 da referida lei estabelece que "os documentos produzidos eletronicamente e anexados aos processos eletrônicos, com garantia de origem e de seu signatário, conforme estabelecido nesta lei, serão considerados originais para todos os efeitos legais" (BRASIL, 2006). Nesse contexto, as provas digitais anexadas aos processos eletrônicos serão consideradas originais para todos os efeitos legais, desde que seja possível verificar sua fonte (RESENDE; BERKENBROCK; RIBEIRO; GOMES; 2023, p. 145-186).

De acordo com o § 3º do artigo 11 da mencionada lei, "os originais dos documentos digitalizados [...] devem ser preservados pelo detentor até o trânsito em julgado da sentença ou, quando permitido, até o final do prazo para interposição de ação rescisória" (BRASIL, 2006) para possibilitar a verificação de sua legitimidade caso haja contestação pela parte adversa. Essa regra é bastante semelhante ao que existia no artigo 225 do Código Civil e no Código de Processo Civil. Assim, a inovação reside em atribuir à parte contrária o ônus da prova quanto à

alegação de falsidade da prova apresentada nos autos, verificando sua autenticidade (RESENDE; BERKENBROCK; RIBEIRO; GOMES; 2023, p. 145-186).

2.3. Autenticidade e integridade da prova e a importância da cadeia de custódia

2.3.1. Autenticidade e integridade da prova

A teoria da prova na era digital enfrenta desafios únicos. A autenticidade e a integridade das provas digitais são questões centrais. Como garantir que um e-mail apresentado como prova não foi adulterado? Como assegurar que uma mensagem de texto é genuína? Essas questões exigem novas abordagens e ferramentas tecnológicas.

A proteção contra ameaças cibernéticas é essencial para garantir a autenticidade e a integridade das provas digitais. Isso inclui a implementação de medidas de segurança robustas, como criptografia e autenticação multifatorial, para proteger dados sensíveis. Isso porque, diferentemente das provas físicas, que podem ser examinadas diretamente, as provas digitais são suscetíveis a manipulações e adulterações. Isso levanta questões críticas sobre como assegurar que um e-mail, uma mensagem de texto ou um arquivo digital não foram alterados desde sua criação.

Isso porque “o documento produzido em meio eletrônico pode, em regra, ser alterado sem esforço, em meios de armazenamento suscetíveis de regravação”. Isso se dá porque o “fluxo de dados em uma rede de computadores, como a internet” é muito denso e intenso, fazendo com que “a informação armazenada em meio eletrônico” seja apenas temporária, podendo ser substituída, diante de sua “grande volatilidade” (PASTORE, 2020, p. 64).

Nesse sentido, para que a prova digital alcance o mesmo nível de confiabilidade que a prova documental obtida de um suporte físico, é crucial que ela ofereça a mesma segurança jurídica. Isso só será garantido se forem cumpridas duas condições fundamentais: (i) a origem do documento digital deve ser claramente identificável, assegurando sua autenticidade, o que significa que não deve haver dúvidas sobre quem o produziu; e (ii) deve ser possível verificar a integridade das informações contidas no documento digital, independentemente do formato em que se apresentem, seja texto, áudio, vídeo, entre outros.

Ademais, Guilherme de Siqueira Pastore (2020, p. 68-69) alerta que:

Vale destacar que tais parâmetros – autenticidade e integridade – são expressamente previstos pela legislação processual para o registro de atos processuais eletrônicos (art. 195 do Código de Processo Civil) e podem ser estendidos, seja por analogia, seja pela própria finalidade da prova, a todo e qualquer registro eletrônico que se pretenda utilizar com força probante no processo.

Nesse sentido, autenticidade refere-se à verificação de que a prova é genuína e não foi falsificada. Isso pode envolver o uso de assinaturas digitais, certificados de autenticidade e registros de metadados. Já a integridade trata da diz respeito à garantia de que a prova não foi modificada. Ferramentas como *hashes* criptográficos e registros de auditoria são frequentemente utilizados para verificar a integridade dos dados digitais.

Na realidade, a doutrina tem destacado que existem três requisitos essenciais — ou pressupostos de validade — para que a prova digital possa ser utilizada com segurança em um processo judicial: (i) a autenticidade; (ii) a integridade; e (iii) a preservação da cadeia de custódia. Assim, é importante compreender o que cada um desses requisitos envolve. Isso porque "A falha em qualquer um desses aspectos resultará na fragilidade da própria prova, tornando-a fraca e, em alguns casos, até mesmo incapaz de produzir efeitos no caso concreto" (THAMAY; TAMER, 2020, p. 39-40).

Dessa forma, Rennan Thamay e Maurício Tamer (2020, p. 40) definem a autenticidade como "a qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital", ou seja, "a qualidade que assegura que o autor aparente do fato é, com efeito, seu autor real" (THAMAY; TAMER, 2020, p. 40).

No que diz respeito à integridade, os mesmos autores esclarecem que é "a característica da prova digital que garante a certeza quanto à sua completude e ausência de adulteração". Assim, a prova digital será considerada íntegra quando se apresentar "livre de qualquer modificação ou adulteração desde o momento da ocorrência do fato até a apresentação do resultado da prova", estando apta a "demonstrar a reprodução do fato em sua totalidade e integridade" (THAMAY; TAMER, 2020, p. 45).

2.3.2. A importância da Cadeia de Custódia

Em relação à cadeia de custódia, trata-se de ponto nevrálgico quanto à validação de provas digitais. Isso porque, conforme destacam Alexandre Moraes da Rosa e Aury Lopes Jr. (2015, n.p.), a prova constitui o elemento central do processo penal. É através da prova que se

busca reconhecer um fato ocorrido no passado, permitindo ao juiz tomar, no presente, uma decisão que terá repercussões no futuro.

Dada essa complexidade, e considerando o próprio procedimento de coleta e preservação das provas digitais, torna-se evidente que a observância rigorosa da cadeia de custódia é essencial ao lidarmos com provas digitais (BADARÓ, 2021).

Ademais, conforme destaca Gustavo Badaró (2021, p. 8), “A necessidade de documentação da cadeia de custódia é fundamental para assegurar o potencial epistêmico das fontes de prova reais.”

Atualmente, alguns mecanismos são utilizados na cadeia de custódia. Conforme explica Gustavo Badaró (2021, p. 4):

É imprescindível que o método empregado garanta a integridade do dado digital e, com isso, a força *probandi* do conteúdo probatório por ele representado. Normalmente, faz-se uma cópia ou “espelhamento”, obtendo o *bitstream* da imagem do disco rígido ou suporte de memória em que o dado digital está registrado. Além disso, por meio de um cálculo de algoritmo de *hash*, é possível verificar a perfeita identidade da cópia com o arquivo original. Com isso, de um lado, se preserva o material original, e, de outro, se garante a autenticidade e integridade do material que foi examinado pelos peritos.

O autor também pondera que, para assegurar a autenticidade e evitar a contaminação das provas digitais, seria ideal que o legislador definisse uma técnica específica para a individualização e apreensão dessas provas, sob risco de sua inutilização. No entanto, considerando que a informática é uma ciência relativamente jovem, sem métodos e técnicas uniformemente aceitos, e que as técnicas computacionais estão em rápida evolução, essa solução se revela inviável (BADARÓ, 2021, p. 2).

No Brasil, a cadeia de custódia passou a ser legalmente tutelado no Brasil com o advento do pacote anticrime, e se encontra prevista nos artigos 158-A a 158-F, do Código de Processo Penal. Trata-se do mecanismo garantidor de um mínimo de confiabilidade, que documenta o caminho que percorreu a prova, desde a sua coleta, até sua análise pelo juiz competente.

Quando um computador, celular ou qualquer dispositivo similar é submetido a perícia, é fundamental, de acordo com a exigência legal da cadeia de custódia, demonstrar que o objeto analisado é o mesmo que, após a perícia, é apresentado ao juiz. Este é o atual entendimento do Superior Tribunal de Justiça (STJ). Assim, no RHC 143.169/RJ, julgado em 07/02/2023, de relatoria do Min. Messod Azulay Neto, decidiu que “São inadmissíveis as provas digitais, sem

o registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos.” (BRASIL, 2023)

Da mesma forma, no julgamento do HC 828.054-RN, julgado em 23/04/2024 e relatado pelo Min. Joel Ilan Paciornik, por unanimidade fixou que “Mostra-se indispensável que todas as fases do processo de obtenção das provas digitais sejam documentadas, cabendo à polícia, além da adequação de metodologias tecnológicas que garantam a integridade dos elementos extraídos, o devido registro das etapas da cadeia de custódia, de modo que sejam asseguradas a autenticidade e a integralidade dos dados.” (BRASIL, 2024)

Como se vê, somente com a adequada documentação da cadeia de custódia da prova conseguir-se-á assegurar sua autenticidade e integralidade, possibilitando o escrutínio da mesma em sede judicial, de modo a preservar a ampla defesa e o contraditório.

3. PRIVACIDADE E SEGURANÇA NA COLETA E NO USO DOS DADOS DIGITAIS

A coleta e o uso de dados digitais levantam preocupações significativas sobre privacidade e segurança. Os operadores do direito devem equilibrar a necessidade de acessar informações relevantes com a proteção dos direitos individuais.

A coleta e o uso de dados digitais são temas que têm ganhado destaque na sociedade contemporânea, principalmente devido ao avanço tecnológico e à crescente digitalização das atividades humanas. Assim, no ambiente digital, é fácil perceber que privacidade e a segurança são pontos sensíveis que merecem destaque. Com a proliferação de dispositivos conectados à internet e a capacidade de armazenar grandes volumes de informações, surgem preocupações significativas sobre como esses dados são coletados, armazenados e utilizados. A privacidade dos indivíduos está em risco quando informações pessoais são capturadas sem consentimento explícito ou quando são utilizadas para fins que os usuários não autorizaram. Além disso, a segurança dos dados é uma questão crítica, pois violações e vazamentos podem expor informações sensíveis, resultando em consequências graves para os indivíduos afetados.

Nesse contexto, enfrenta-se o desafio de equilibrar a necessidade de acessar informações digitais relevantes para investigações e processos judiciais com a proteção dos direitos individuais à privacidade. Este equilíbrio é delicado, pois, por um lado, o acesso a dados pode ser crucial para a resolução de crimes e a administração da justiça. Por outro lado, a coleta

indiscriminada ou excessiva de dados pode levar a abusos e à violação dos direitos fundamentais dos cidadãos.

Em contraste com o mundo digital que experimentamos hoje, Anderson Schreiber (2014, p. 138-139) afirma que o direito à privacidade se expandiu para incluir muito mais do que apenas a proteção de dados pessoais ou o simples direito à intimidade. Daí porque Schreiber define o direito à privacidade como "o direito ao controle da coleta e da utilização dos próprios dados pessoais".

Barreto Junior e Venturini Junior (2020, p. 11-12) fazem análise a privacidade no contexto do ecossistema digital:

A privacidade torna-se cada vez mais inatingível na Sociedade da Informação. Perdeu-se, com a tecnologia, a possibilidade de assegurar a diferença entre pessoa identificada e identificável. A dicotomia entre dados anônimos (sigilosos) e dados pessoais, identificáveis não é mais viável em decorrência do aparato tecnológico e das técnicas de *linkage* de bancos de dados, além do georreferenciamento. Inaugura-se um tempo em que os dados pessoais são insumos, uma sociedade movida e orientada por dados.

Na sociedade da informação, os dados pessoais são frequentemente considerados um dos ativos mais valiosos. Eles são utilizados para personalizar serviços, direcionar publicidade e até mesmo para a tomada de decisões automatizadas. No entanto, essa valorização dos dados também os torna alvos atraentes para cibercriminosos, que podem explorar vulnerabilidades em sistemas de segurança para roubar informações sensíveis. Ataques cibernéticos, como *phishing*, *ransomware* e violações de dados, são ameaças constantes que podem ter consequências devastadoras para indivíduos e organizações. Nesse contexto, sobressai a importância de se garantir a segurança dos dados pessoais.

Analisando essa questão, Denise Francoski e Fernando Tasso (2021, n.p.) aduzem que “a segurança da informação é indissociável da proteção de dados pessoais.”. Explicam, ainda, que embora a garantia da segurança da informação não seja sinônimo do direito à proteção de dados pessoais, como frequentemente se presume, existe uma relação inegável entre ambos. A segurança da informação atua como um pré-requisito essencial, uma condição necessária para que os direitos dos titulares dos dados pessoais sejam efetivamente protegidos (FRANCOSKI, TASSO, 2021, n.p.).

Percebe-se, portanto, que é crucial que existam regulamentações claras e rigorosas que orientem a coleta e o uso de dados digitais, garantindo que os direitos dos indivíduos sejam respeitados e que a segurança das informações seja mantida.

No Brasil, a privacidade, como um exemplo dos direitos da personalidade, recebeu atenção especial na Constituição Federal de 1988. No artigo 5º, inciso X, a Constituição declara como invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (BRASIL, 2024).

Normativos jurídicos têm buscado enfrentar tal problemática. Leis e regulamentos, como o Regulamento Geral sobre a Proteção de Dados [GDPR - Regulamento (EU) 2018/1725] na União Europeia e a Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709/2018) no Brasil, estabelecem diretrizes sobre como os dados pessoais devem ser coletados, armazenados e utilizados. O cumprimento dessas regulamentações é crucial para evitar violações de privacidade (BRASIL, 2024; UNIÃO EUROPEIA, 2018).

Assim, o GDPR da União Europeia unifica e padroniza as regras de tratamento de dados pessoais, ditando como empresas devem coletar, armazenar, proteger e compartilhar informações de cidadãos da UE. A legislação tem alcance extraterritorial, aplicando-se também a empresas fora da UE que ofereçam produtos ou serviços a residentes da União Europeia.

O GDPR tem como objetivo primordial fortalecer a proteção, o controle e a privacidade dos dados pessoais, combatendo sua divulgação indevida. Para se adequarem a essa nova realidade, as empresas precisam realizar uma análise crítica de seus processos e, em muitos casos, implementar mudanças significativas. Ademais, prevê a elaboração de um Plano de Adaptação, que deve ser embasado em um diagnóstico preciso do modelo operacional atual da empresa, mapeando os pontos de atenção e definindo ações concretas a serem implementadas para alcançar a conformidade com o regulamento.

A LGPD, por sua vez, regula o tratamento de dados pessoais, abrangendo informações armazenadas em formato físico ou digital, por entidades públicas ou privadas, independentemente do porte. Essa regulamentação se aplica a uma ampla gama de operações realizadas com os dados, seja por meios manuais ou digitais. O tratamento de dados, ponto central da Lei, engloba qualquer atividade que utilize dados pessoais, desde a coleta até a eliminação. Isso inclui: coleta, produção e recepção (obtenção dos dados, seja diretamente da pessoa ou de outras fontes), classificação, utilização e acesso (organização, uso e consulta das informações), reprodução, transmissão e distribuição (cópia, envio e compartilhamento dos dados), processamento, arquivamento e armazenamento (tratamento, organização e guarda das informações), eliminação, avaliação e controle (exclusão, análise e gestão dos dados),

modificação, comunicação, transferência, difusão ou extração (alteração, compartilhamento, movimentação e divulgação das informações).

Além disso, a transparência e a responsabilidade são princípios fundamentais que devem guiar a atuação dos operadores do direito no contexto digital. As instituições devem adotar práticas que assegurem que os dados sejam coletados de maneira ética e que os indivíduos sejam informados sobre como suas informações estão sendo utilizadas. A implementação de tecnologias de proteção de dados, como criptografia e anonimização, pode ajudar a mitigar riscos e proteger a privacidade dos usuários. Ademais, a educação e a conscientização sobre direitos digitais são essenciais para que os cidadãos possam exercer controle sobre suas informações pessoais e exigir responsabilidade das entidades que as manipulam.

4. EFICIÊNCIA PROCESSUAL E O ACESSO ÀS NOVAS FORMAS DE EVIDÊNCIA

A digitalização das provas e a automação de processos no âmbito jurídico têm o potencial de transformar a eficiência processual. A inserção de tecnologias que automatizam a triagem e a organização de documentos libera os profissionais do direito para concentrarem seus esforços em tarefas mais complexas e estratégicas. Ferramentas digitais, como softwares de gerenciamento de processos e plataformas de armazenamento de dados, permitem que as informações sejam facilmente acessadas e manipuladas, agilizando a coleta e análise de provas. O tempo de resposta, que antes era comprometido por longos processos de busca e organização de documentos físicos, é reduzido. Além disso, a automação minimiza a ocorrência de erros humanos em tarefas repetitivas e aumenta a produtividade.

O professor e magistrado Bruno Alves Rodrigues (2021, p. 183) explica que um dos grandes problemas do poder judiciário fica situado na ocorrência de “gargalos” que prejudicam o impulsionamento dos processos judiciais, o que impacta diretamente no ajuste da tramitação processual com o princípio da duração razoável do processo (art. 5º, LXXVIII, da CF/1988). O autor ainda salienta que atualmente, qualquer empresa moderna possui sistemas operacionais que otimizam o fluxo de processos, enquanto o CPC manteve um sistema que “depende da operação humana, desempenhada pelo escrivão ou chefe de secretaria, para: a) guarda de processos (art. 152, IV, do CPC); b) conclusões (art. 152, IV “a”, do CPC) (...)” (RODRIGUES,

2021, p. 184), sendo que esses sistema analógico com diversas etapas ocasiona a demora no impulsionamento processual, justamente pela necessidade de operação manual.

Assim, utilizando a tecnologia de *analytics*, bem como uma melhor organização e classificação dos processos, influenciaria em uma racionalização maior e sistematização da gestão processual (Rodrigues, 2021, p. 184). Rodrigues (2021, p. 184) ainda traz uma conclusão relevante sobre a questão da identificação dos processos com a sistematização da gestão processual, ainda traz dados importantes sobre os prejuízos sofridos por conta da ausência do monitoramento efetivo dos processos judiciais, confira-se por oportuno:

Exemplificativamente, poderiam ser identificados processos indevidamente mantidos em 'arquivo', quando pertinente conclusão para análise de hipótese de prescrição intercorrente, ou mesmo para liberação de depósitos judiciais indevidamente mantidos em processos que já contaram com a extinção da execução. Para se ter uma dimensão, por exemplo, do prejuízo causado pela ausência de um monitoramento sistêmico dos depósitos judiciais, apenas na Justiça do Trabalho, no ano de 2020, após o TRT 21 desenvolver o 'Sistema Garimpo', uma ferramenta eletrônica que 'localiza depósitos recursais, honorários periciais e alvarás não sacados por empresas, advogados ou peritos em processos antigos' (LA-GR-PR, 2019), foi identificado 'cerca de R\$ 2 bilhões em contas judiciais de empresas e de trabalhadores 'esquecidas' no Banco do Brasil e na Caixa Econômica Federal. Aproximadamente R\$ 183 milhões foram liberados após a identificação de seus donos' (NOTÍCIAS DO TST, 2020).

Inegável que o avanço tecnológico com a correta implementação das tecnologias no âmbito jurídico seria capaz de agilizar a tramitação de processos judiciais, resolvendo parte dos problemas com morosidade dentro do poder judiciário como um todo, sendo certo que a “principal baliza ética a ser verificada no desenvolvimento e na implantação de IA no Poder Judiciário é a de jamais permitir que aquilo que necessariamente deva representar expressão de consciência humana seja reduzido à mera manifestação de um ato de inteligência artificial” (RODRIGUES, 2021, p. 186).

É importante ressaltar que a validade jurídica dos documentos eletrônicos não se limita apenas à sua autenticidade e integridade, mas também à sua admissibilidade como prova em processos judiciais. Inclusive, nesse contexto a professora Fernanda Rosa de Vasconcelos Oliveira (2019, p. 19), ressalta que “o meio de armazenamento e a forma de transmissão da informação devem seguir procedimentos seguros capazes de garantir o armazenamento livre de ataques cibernéticos, documentos salvaguardados em repositórios digitais confiáveis – RDC-Arq –, com a segurança de manutenção da cadeia de custódia, assuntos ainda pouco discutidos e com reduzida implementação no país”.

Um dos grandes desafios enfrentados pelos operadores do direito na era digital é justamente essa admissibilidade das provas digitais nos tribunais. A volatilidade das provas digitais, que podem ser facilmente manipuladas, levanta dúvidas quanto à sua confiabilidade e integridade. Inicialmente as normas processuais não foram concebidas para lidar com essas características, o que muitas vezes resulta em incertezas sobre a validade das provas apresentadas. Para garantir que as provas digitais sejam admissíveis, as regras precisam ser atualizadas para refletir as particularidades desse novo tipo de prova. Isso inclui, por exemplo, a criação de diretrizes que definam claramente os procedimentos necessários para a coleta, preservação e apresentação de provas digitais.

A questão da coleta, preservação e apresentação das provas digitais, ou seja, a cadeia de custódia da prova é tão relevante, que o Superior Tribunal de Justiça noticiou em 2023 que a quinta turma reconheceu que “são inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, da autenticidade e da confiabilidade dos elementos informáticos” (STJ, 2023, online). No caso concreto, o Ministro Ribeiro Dantas, destacou que “antes mesmo de ser periciado pela polícia, o conteúdo extraído dos equipamentos foi analisado pela própria instituição financeira vítima” (STJ, 2023, online).

Além da questão da admissibilidade, a relevância das provas digitais é outro ponto importante, as provas digitais precisam ser analisadas no contexto em que foram criadas e coletadas para determinar sua importância no processo. A facilidade de modificação de provas digitais exige que os advogados realizem uma avaliação da sua relevância e impacto no resultado do caso. Em âmbito penal, a cadeia de custódia, que documenta todos os acessos e movimentações das provas, torna-se o elemento essencial para garantir sua integridade e valor probatório.

Uma solução para essa questão é a utilização de assinaturas digitais e certificados digitais que não apenas fortalece a segurança e confiabilidade dos documentos, mas também facilita sua aceitação como evidência em tribunais e procedimentos legais. Esses mecanismos fornecem uma trilha digital confiável que pode ser auditada e verificada, aumentando a credibilidade dos documentos eletrônicos perante as autoridades judiciárias (OLIVEIRA, 2019, p. 18).

Outro aspecto relevante a considerar quanto ao tema das provas digitais é o desenvolvimento de legislação e regulamentação específica que apoie e valide o uso de documentos eletrônicos na prática jurídica. Em muitos países, foram promulgadas leis e normas que reconhecem a validade legal da assinatura digital e certificação digital, proporcionando um arcabouço jurídico sólido para o uso dessas tecnologias no contexto judicial. Esse reconhecimento legal é fundamental para garantir a segurança jurídica e a eficácia dos documentos eletrônicos em ambientes judiciais.

As leis que reconhecem a validade legal da assinatura digital e certificação digital podem variar de acordo com o país. Nos Estados Unidos, a Lei de Assinaturas Eletrônicas (*E-Sign Act*) e a Lei Uniforme de Transações Eletrônicas (UETA) estabelecem o reconhecimento legal das assinaturas eletrônicas em transações comerciais e legais. No Brasil, a Lei n. 14.063/2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos, também reconhece a validade jurídica da assinatura digital e a classifica como simples, avançada e qualificada, conforme é possível extrair do art. 4º do referido diploma legal³.

A utilização de técnicas avançadas de criptografia e segurança da informação, por exemplo, permitem a proteção dos documentos eletrônicos contra adulterações e fraudes. A criptografia permite que os dados sejam protegidos contra acessos não autorizados e alterações

³ Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:

I - assinatura eletrônica simples:

a) a que permite identificar o seu signatário;

b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;

II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características:

a) está associada ao signatário de maneira unívoca;

b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;

c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;

III - assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

§ 1º Os 3 (três) tipos de assinatura referidos nos incisos I, II e III do caput deste artigo caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular, e a assinatura eletrônica qualificada é a que possui nível mais elevado de confiabilidade a partir de suas normas, de seus padrões e de seus procedimentos específicos.

§ 2º Devem ser asseguradas formas de revogação ou de cancelamento definitivo do meio utilizado para as assinaturas previstas nesta Lei, sobretudo em casos de comprometimento de sua segurança ou de vazamento de dados.

não autorizadas, garantindo a confidencialidade e integridade das informações contidas nos documentos eletrônicos. Essas medidas de segurança são importantes para mitigar os riscos associados ao uso de documentos eletrônicos na prática jurídica e aumentar a confiança nas tecnologias digitais (INTERNET SOCIETY, 2016, p. 1).

No âmbito da modernização do processo judicial, um escritório de advocacia envolvido em uma disputa civil de propriedade, por exemplo, pode inserir uma variedade de documentos eletrônicos no processo. Isso inclui contratos digitalizados, escrituras públicas e certidões de registro de imóveis pertinentes ao caso. Além disso, e-mails trocados entre as partes ou advogados, contendo acordos prévios ou negociações, podem ser anexados como evidências eletrônicas. Relatórios de avaliação de peritos, transcrições de audiências virtuais e manifestações orais das partes também podem ser documentados eletronicamente para registro no processo. Para garantir a autenticidade e integridade desses documentos, assinaturas digitais e certificados digitais devem ser utilizados, reforçando sua validade jurídica (MENDES; MARQUES, 2021, p. 10).

Nesse contexto, sistemas de inteligência artificial e algoritmos complexos podem ser empregados para auxiliar na tomada de decisões judiciais, promovendo a eficiência processual. Essa abordagem inovadora tem o potencial de revolucionar o sistema judiciário, oferecendo uma alternativa eficiente e ágil para lidar com a crescente demanda por resolução de litígios, o que, conforme mencionado anteriormente, é amplamente ressaltado pelo professor e magistrado Bruno Alves Rodrigues em sua obra, de 2021, “A inteligência Artificial no Poder Judiciário e a Convergência com a consciência humana para a efetividade da justiça”.

Nesse sentido, os professores Juliano Souza de Albuquerque Maranhão, Juliana Abrusio Florêncio e Marco Almada (2021, p. 166), ressaltam que:

Sistemas baseados em conhecimento são sistemas inteligentes que realizam inferências a partir de representações internas de conhecimento (...). Essas representações do conhecimento são construídas de antemão, durante o projeto de um sistema computacional, mas, uma vez que elas sejam feitas, o sistema pode atualizar sua base de conhecimento a partir das informações que adquire do ambiente, aplicando as mesmas regras de inferência para lidar com situações percebidas.

Assim, é possível concluir que o uso de inteligência artificial (IA) e aprendizado de máquina também é uma inovação que contribui para o aumento da eficiência no âmbito processual. A análise de grandes volumes de dados digitais, realizada por algoritmos avançados, pode identificar padrões, prever resultados e auxiliar advogados e juízes na tomada de decisões mais fundamentadas. A eficiência processual não se resume apenas à redução de tempo, mas

também à melhoria da qualidade das decisões judiciais. As provas digitais, quando integradas a sistemas tecnológicos eficientes, proporcionam uma visão mais abrangente do caso, permitindo a construção de argumentos mais robustos e embasados. No entanto, a eficiência gerada por essas inovações exige um ambiente jurídico adaptado e uma infraestrutura tecnológica robusta, para garantir que as informações sejam manuseadas de forma segura e ágil.

CONCLUSÃO

Os desafios e oportunidades apresentados pela era digital exigem uma adaptação contínua do sistema jurídico. Ao desenvolver novas competências técnicas, garantir a privacidade e a segurança dos dados e aproveitar as tecnologias avançadas, os operadores do direito podem transformar a prática jurídica e melhorar a busca pela justiça. A colaboração entre o direito e a tecnologia será fundamental para enfrentar os desafios e aproveitar as oportunidades que a era digital oferece.

Ao longo deste artigo, ficou evidente que a digitalização dos processos e a proliferação de dados digitais desafiam os conceitos tradicionais de autenticidade, integridade e cadeia de custódia das evidências. Esses desafios exigem do sistema jurídico uma adaptação profunda para garantir que a busca pela verdade processual continue sendo efetiva e justa.

A autenticidade e a integridade das provas digitais emergem como questões centrais neste novo contexto. A facilidade com que dados digitais podem ser alterados ou manipulados demanda a implementação de medidas robustas de segurança cibernética. A utilização de criptografia, autenticação multifatorial e outras tecnologias de proteção torna-se essencial para assegurar que as evidências apresentadas em juízo sejam confiáveis e legítimas.

A importância da cadeia de custódia é reforçada na era digital, pois ela garante a rastreabilidade e a confiabilidade das provas desde a sua coleta até a apresentação. Sem um controle rigoroso dessa cadeia, a admissibilidade das provas digitais pode ser comprometida, afetando diretamente a tomada de decisões judiciais. Portanto, protocolos claros e padronizados para o manuseio de evidências digitais são indispensáveis.

A privacidade e a segurança na coleta e uso de dados digitais também se apresentam como preocupações, tornando necessário equilibrar o acesso a informações relevantes para a justiça com a proteção dos direitos individuais. A legislação e as práticas jurídicas precisam

evoluir para garantir que a coleta de dados não infrinja direitos fundamentais, mantendo a integridade do processo legal.

A digitalização traz, ainda, oportunidades significativas para a eficiência processual. A automação de tarefas e o uso de inteligência artificial podem agilizar procedimentos, reduzir erros e aprimorar a análise de grandes volumes de dados. No entanto, a adoção dessas tecnologias requer investimentos em infraestrutura e formação adequada dos profissionais do direito, garantindo que estejam aptos a lidar com as novas ferramentas.

Assim, destaca-se a necessidade de uma formação interdisciplinar para os operadores do direito. A colaboração com especialistas em tecnologia torna-se cada vez mais relevante, e a educação jurídica deve incorporar conhecimentos técnicos em seus currículos. Somente assim será possível enfrentar os desafios da era digital e aproveitar plenamente as oportunidades que ela oferece.

Em suma, a digitalização impõe uma reconfiguração da Teoria da Prova e das práticas processuais. Cabe ao sistema jurídico adaptar-se de maneira proativa, promovendo mudanças que assegurem a efetividade, a segurança jurídica e a proteção dos direitos fundamentais na era da informação, sendo certo que o futuro da justiça depende da capacidade de integrar a tecnologia de forma ética e eficiente em seus procedimentos.

REFERÊNCIAS

BADARÓ, Gustavo. A cadeia de custódia da prova digital. Artigo elaborado para apresentação de palestra, como mesmo tema, no **Congresso Internacional de Direito Probatório**, realizado nos dias 18 e 19 de novembro de 2021, em Porto Alegre-RS, pela Pontifícia Universidade Católica do Rio Grande do Sul e pela Universidade Alberto Hurtado, com apoio do IBDP e da Procnet. Disponível em: https://edisciplinas.usp.br/pluginfile.php/7833426/mod_resource/content/1/U8%20-%20BADARO%20-%20A%20cadeia%20de%20custo%CC%81dia%20da%20prova%20digital%20PUCRS%20-%20co%CC%81pia.pdf. Acesso em: 19 out.2024.

BARRETO JUNIOR, Irineu Francisco; VENTURINI JUNIOR, Gustavo. Inteligência Artificial e seus efeitos na Sociedade da Informação. *In: LISBOA, Roberto Senise (Org.). O Direito na Sociedade da Informação*. v.4, 2020. São Paulo (SP): Almedina, 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 out.2024.

BRASIL. Decreto-lei n. 3.689, de 3 de outubro de 1941. **Código de Processo Penal (CPP)**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 19 out.2024.

BRASIL. Lei 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 out. 2024.

BRASIL. Lei n. 11.419, de 19 de dezembro de 2006. **Lei do Processo Eletrônico**. Dispõe sobre a informatização do processo judicial. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/L11419.htm. Acesso em: 19 out. 2024.

BRASIL. **Superior Tribunal de Justiça**. AgRg no HABEAS CORPUS Nº 828054 - RN (2023/0189615-0). Ministro Relator Joel Ilan Paciornik. Quinta Turma. Julgado em 23/04/2024. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301896150&dt_publicacao=29/04/2024. Acesso em 19 out.24.

BRASIL. **Superior Tribunal de Justiça**. AgRg no RECURSO EM HABEAS CORPUS Nº 143.169 - RJ (2021/0057395-6). Ministro Relator Jesuíno Rissato (Desembargador Convocado do TJDFT). Julgado em 07/02/2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202100573956&dt_publicacao=02/03/2023. Acesso em: 19 out.2024.

BRASIL. Superior Tribunal de Justiça. **A cadeia de custódia no processo penal: do Pacote Anticrime à jurisprudência do STJ**. Publicado em 23 de abril de 2023. Online. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-A-cadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-do-STJ.aspx>. Acesso em: 21 out.2024.

BRASIL. Lei n. 11.419, de 19 de dezembro de 2006. **Lei do Processo Eletrônico**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 09 dez. 2024.

BRASIL. Lei n. 14.063, de 23 de setembro de 2020. **Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm. Acesso em: 09 dez. 2024.

BUENO, Cassio Scarpinella. **Curso sistematizado de direito processual civil**. v. 02, tomo I, 3. ed. São Paulo (SP): Saraiva, 2010.

CASTELLS, Manuel. **A sociedade em rede – a era da informação: economia, sociedade e cultura**. Tradução: Roneide Venâncio Majer, com a colaboração de Klauss Brandini Gerhardt. Atualização para a 6. ed.: Jussara Simões. 6. ed. ver. e ampl. São Paulo: Paz e Terra, 1999, p. 39-40.

FRANCOSKI, Denise; TASSO, Fernando. Capítulo 20. Segurança da Informação e Proteção de Dados Pessoais. In: FRANCOSKI, Denise; TASSO, Fernando. **A Lei Geral de Proteção de Dados Pessoais: LGPD: Aspectos Práticos e Teóricos Relevantes no Setor Público e Privado**. São Paulo (SP): Editora Revista dos Tribunais. 2021. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/capitulo-20-seguranca-da-informacao-e-protecao-de-dados-pessoais-parte-i-a-lei-geral-de-protecao-de-dados-pessoais-no-setor-publico/1279975775?utm_source=google&utm_medium=cpc&utm_campaign=doutrina_dsa&utm_term=&utm_content=capitulos&campaign=true&gad_source=1&gclid=Cj0KCQjwsc24BhDPArisAFXqAB1NrC6WonsducWUV44eld-hZWQiYqAgDMFfIMZGEJR8SWNm1vh5UVcaAg3PEALw_wcB#ftn.DTR.2021.7724-n2. Acesso em: 19 out.2024.

INTERNET SOCIETY. **Criptografia**. Disponível Em: <https://www.internetsociety.org/wp-content/uploads/2016/06/ISOC-PolicyBrief-Encryption-Portuguese.pdf>. Acesso em: 23 out.2024.

JANINI, Tiago Cappi. O documento eletrônico como meio de prova no Direito Tributário. In: **Direito Tributário Eletrônico**. Coord. Maria Rita Ferrogut. Colab. Renata Elaine Silva. São Paulo: Saraiva, 2010.

KIST, Dário José. **Prova Digital no Processo Penal**. 2. ed., Leme (SP): Mizuno, 2024.

LOPES JUNIOR, Aury; ROSA, Alexandre Morais da. A importância da cadeia de custódia para preservar a prova penal. **Consultor Jurídico (Conjur)**, publicado em 16 de janeiro de 2015 às 7h00. Disponível em: <https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal/>. Acesso em: 19 out.2024.

LUCIEN, Lucien Rocha. **Acreditação e admissibilidade de evidências digitais de crimes cibernéticos praticados em computação de nuvem: desafios na esfera judicial do Brasil**. Dissertação (Mestrado em Direito). Universidade de Brasília – UNB. Brasília. 2023.

MARANHÃO, Juliano Souza De Albuquerque; FLORÊNCIO, Juliana Abrusio; ALMADA Marco. Inteligência Artificial Aplicada ao Direito e o Direito da Inteligência Artificial. **Suprema - Revista de Estudos Constitucionais**, v. 1, n. 1, 2021, p. 154-180. Disponível em: <https://suprema.stf.jus.br/index.php/suprema/article/view/20>. Acesso em: 23 out.2024.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Código de processo civil comentado**. São Paulo (SP): Revista dos Tribunais, 3. ed., 2011.

MENDES, Josilene Maria Aparecida De Paula; MARQUES, João Victor Mota. **Modernização Tecnológica Do Processo Judicial No Brasil**. 2021. Disponível em: Acesso em: 23 out.2024.

OLIVEIRA, Fernanda Rosa de Vasconcelos. A Força Probante dos Documentos Digitalizados: Eficiência Versus Segurança Jurídica. **Revista Caderno Virtual**, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/4166>. Acesso em: 21 out.2024.

PASTORE, Guilherme de Siqueira. Considerações sobre a autenticidade e a integridade da prova digital. **Cadernos Jurídicos**, São Paulo (SP), ano 21, n. 53, p. 63-79, jan./mar. 2020.

RESENDE, Carmen Elisângela Dias Moreira de.; BERKENBROCK, Guy Estevão; RIBEIRO, Luiz Octávio O. Saboia; GOMES, Magáli Dellape. **Revista Judicial Brasileira (ReJuB)**, Ed. esp. Direito Digital, Brasília (DF), p. 145-186, jul./dez. 2023.

RODRIGUES, Bruno Alves. **A inteligência artificial no poder judiciário e a convergência com a consciência humana para a efetividade da justiça**. São Paulo: Thomson Reuters Brasil, 2021.

ROSA, Alexandre Moraes da. Limite Penal: o "*print screen*" é insuficiente à materialidade nos crimes digitais. **Consultor Jurídico (Conjur)**, publicado em 17 de junho de 2022, 15h44. Disponível em: <https://www.conjur.com.br/2022-jun-17/limite-penal-print-screen-materialidade-crimes-digitais/>. Acesso em: 19 out.2024.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas, 2014.

THAMAY, Rennan; TAMER, Maurício. **Provas no Direito Digital**. São Paulo (SP): Editora Revista dos Tribunais. 2022. Disponível em: <https://www.jusbrasil.com.br/doutrina/provas-no-direito-digital-ed-2022/1672935656>. Acesso em: 16 out.2024.

THAMAY, Rennan; TAMER, Mauricio. **Provas no direito digital: conceito da prova digital, procedimentos e provas digitais em espécie**. São Paulo/SP: Thomson Reuters Brasil, 2020.

UNIÃO EUROPEIA (EU). Parlamento Europeu. **Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n. 45/2001 e a Decisão n. 1247/2002/CE. Disponível em: [https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725#:~:text=Regulamento%20\(UE\)%202018%2F1725,o%20Regulamento%20\(CE\)%20n](https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725#:~:text=Regulamento%20(UE)%202018%2F1725,o%20Regulamento%20(CE)%20n). Acesso em: 19 out.2024.