REJUB

Revista Judicial Brasileira

especialização em direito digital
suplemento especial (2023)

ENFAM

Edição
Especial

https://doi.org/10.54795/RejuBEsp.DirDig.222

A PROVA DIGITAL NO PROCESSO JUDICIAL

DIGITAL EVIDENCE IN THE JUDICIAL PROCESS

CARMEN ELIZÂNGELA DIAS MOREIRA DE RESENDE
Juíza federal titular, membra da 4ª Turma Recursal dos Juizados Especiais Federais de Belo Horizonte – TRF 6ª Região e da Turma Nacional de Uniformização do Conselho da Justiça Federal – TNU. Graduada em Direito pela Pontifícia Universidade Católica – PUC-MG. Pós-graduada em Direito Público (PUC-MG), em Direito Processual Público pela Universidade Federal Fluminense – UFF e em Direito Sanitário pela Escola Superior do Ministério Público.
https://orcid.org/0009-0005-1279-6127

GUY ESTEVÃO BERKENBROCK
Graduado em Direito pela Faculdade de Direito de Joinville (2003). Pós-graduado (especialização) em Direito Processual Penal pela Universidade da Região de Joinville em parceria com a Escola Superior do Ministério Público do Estado de Santa Catarina (2004). Pós-graduado (especialização) em Direito e Gestão Judiciária pela Academia Judicial do Poder Judiciário do Estado de Santa Catarina (2011). Juiz de direito vinculado ao Tribunal de Justiça do Estado de Santa Catarina desde 2010.
https://orcid.org/0009-0006-9284-0964

LUIZ OCTÁVIO O. SABOIA RIBEIRO
Juiz de direito da 3ª Vara Cível de Cuiabá – TJMT. Juiz-membro do Tribunal Regional Eleitoral de Mato Grosso – TRE/MT. Graduado pela Universidade de Cuiabá – Unic. Pós-graduado em Direito Civil e Processo Civil e em Direito Penal e Processo Penal pela Universidade Estácio de

Sá. MBA em Gestão Judiciária pela Fundação Getulio Vargas – FGV. Pós-graduando em Direito Digital, cyber segurança e *data protection* pela PUC/PR.
https://orcid.org/0009-0000-2183-9479

MAGÁLI DELLAPE GOMES
Juíza de direito titular da 3ª Vara de Família e de Órfãos e Sucessões de Taguatinga – TJDFT. Graduada em Direito pela Universidade Potiguar. Pós-graduada em Direito Público pela Faculdade UniFuncesi – Processus/DF. Professora de Direito Civil.
https://orcid.org/0009-0006-3986-8984

RESUMO

O presente artigo aborda a prova digital no sistema judicial brasileiro, ante a acelerada evolução tecnológica da sociedade contemporânea. A pesquisa parte da premissa de que essa digitalização tem impactado de forma significativa e irreversível a maneira como as informações são geradas, armazenadas e compartilhadas, o que afeta diretamente a natureza das evidências apresentadas em processos judiciais, tornando imperativo um reexame dos paradigmas tradicionais de prova. O estudo destaca a importância crescente de dispositivos eletrônicos e plataformas *on-line* como fontes de prova, especialmente em casos penais. A análise de conteúdo de *smartphones*, computadores e outros dispositivos eletrônicos tornou-se uma rotina nas investigações criminais, dada a quantidade de dados e informações relevantes neles contidos. Este cenário apresenta desafios significativos em relação à admissibilidade, confiabilidade e integridade das provas digitais, questões estas que são exploradas em profundidade no artigo. Discute-se também a importância da formação e capacitação de juízes e demais profissionais do direito para lidar com tais desafios e a necessidade de

modernização e atualização do sistema digital, não somente quanto à infraestrutura tecnológica, mas também quanto à legislação e aos procedimentos. A pesquisa conclui que a prova digital representa não apenas uma evolução, mas uma verdadeira revolução no campo probatório, razão pela qual o sistema judicial, portanto, deve passar por um processo de modernização para incorporar essas novas formas de evidência de maneira eficaz e justa, garantindo assim a integridade e a eficácia do processo judicial no século XXI.

Palavras-chave: evolução tecnológica; provas; provas digitais; evidências; cadeia de custódia.

ABSTRACT

This article deals with digital evidence in the Brazilian judicial system, given the accelerated technological evolution of contemporary society. The research starts from the premise that digitalization has had a significant and irreversible impact on the way information is generated, stored and shared, which directly affects the nature of the evidence presented in legal proceedings, making it imperative to re-examine traditional paradigms of evidence. The study highlights the growing importance of electronic devices and online platforms as sources of evidence, especially in criminal cases. Analyzing the content of smartphones, computers and other electronic devices has become routine in criminal investigations, given the amount of relevant data and information they contain. This scenario presents significant challenges in relation to the admissibility, reliability and integrity of digital evidence, issues which are explored in depth in the article. It also discusses the importance of training judges and other legal professionals to deal with these challenges and the need to modernize and update the digital system, not only in terms of technological infrastructure, but

also in terms of legislation and procedures. The research concludes that digital evidence represents not just an evolution, but a veritable revolution in the field of evidence, which is why the judicial system must undergo a process of modernization.

Keywords: technological evolution; evidences; digital evidences; evidence; chain of custody.

SUMÁRIO

1 INTRODUÇÃO

Vivenciamos um período em que a sociedade se revela cada vez mais conectada, possibilitando, assim, constantes e frequentes mudanças, principalmente no tocante ao uso de novas tecnologias. As distâncias físicas estão sendo revisadas porque não fazem mais sentido, e as transformações do século XX, como internet e correio eletrônico, mensagens curtas e redes sociais, revelam-se cada vez mais presentes no cotidiano de todos. Graças à adaptabilidade e ao uso cada vez maior das tecnologias da informação e da comunicação, esses contatos tornaram-se parte integrante do dia a dia e estão influenciando todos os seus aspectos. A comunicação privada é uma das áreas mais revolucionadas da tecnologia. As comunicações eletrônicas são o

método preferido de comunicação porque oferecem velocidade, baixo custo e fácil acesso, o que é representado por instrumentos como o correio eletrônico, SMS e mensagens instantâneas, a exemplo do WhatsApp e Messenger.

Noutro giro, é certo que os países investem, cada vez mais, em plataformas digitais como forma de acesso a serviços públicos com menos burocracia. Esse movimento acontece em razão da incrível evolução tecnológica ocorrida nas últimas décadas, principalmente a partir do início da internet,[1] com a criação dos protocolos padrões TCP/ICP nos anos 70.[2] A popularização da internet se deu nos anos 80 com a abertura das redes para fins comerciais e o surgimento da conexão via *dial-up*.

A realidade atual gerou uma sociedade conectada, que produz uma quantidade enorme de dados diariamente,[3] capaz de modificar de modo evidente os mais variados aspectos da vida e as interações humanas, assim como a organização da sociedade, redesenhando desde a comunicação, com a substituição das cartas pelo correio eletrônico, dos telefonemas por mensagens instantâneas de texto, áudio ou vídeo, até os registros – públicos ou privados – que se pretendem perenes, e antes inscritos em papel, hoje são amplamente produzidos

[1] A evolução da internet é marcada pela explosão de grandes portais de serviços (Yahoo, Hotmail, Google, mensagens instantâneas, bate-papos etc.), assim como a facilitação na aquisição de computadores pessoais e a evolução da banda larga, com melhoria da conexão móvel, gerando, assim, a expansão para a utilização da rede em dispositivos que navegavam nas redes 3G, estando, atualmente, o Brasil em processo de migração do modelo 4G para o modelo 5G, que é realidade em alguns países como Japão, China e EUA.

[2] Os fundadores do protocolo TCP foram Net Vilton Cerf e Bob Kahn em 1973, o uso do termo internet se deu apenas em 1974 com a primeira publicação do TCP, ela sendo assinada na Universidade de Stanford por Vinton Cerf, Yogem Dalal e Carl Sunshine.

[3] O relatório Data Age 2025, do IDC, informa que a quantidade de dados criada, capturada, copiada e consumida em 2018 foi de 33 zettabytes, ou 33 trilhões de gigabytes. Esse número cresceu, em 2020, para 59 ZB e é esperado que atinja 175 ZB até 2025 — ou 175.000.000.000.000 gigabytes. Disponível em: https://www.datanami.com/2018/11/27/global-datasphere-to-hit-175-zettabytes-by-2025-idc-says/. Acesso em: 5 fev. 2023

pelos sistemas de informática; passando, ainda, por toda espécie de atividade que, prescindindo do contato presencial antes necessário ou criando possibilidades inéditas, vale-se da internet, por meio da qual se acessa e se transmite um volume imenso de informação, celebram-se negócios jurídicos e também se praticam atos ilícitos.

A prova digital agora é um tema de grande valor, uma vez que dispositivos eletrônicos ou a própria internet são as ferramentas mais populares para armazenar dados e informações. A coleta e a análise de evidências digitais de prova digital têm se tornado uma importante ferramenta na solução de discussões, demandas e crimes devido aos significativos avanços tecnológicos das últimas duas décadas.

Essa mudança comportamental da sociedade se reflete na atividade probatória dos processos judiciais de modo relevante, devendo ser destacado que os meios de prova – assim entendidos como "instrumentos ou atividades por intermédio dos quais os dados probatórios (elementos de prova) são introduzidos e fixados no processo" (Gomes Filho, 2005, p. 308) –permanecem essencialmente os mesmos, ao menos nos aspectos exteriores mais facilmente perceptíveis, enquanto as fontes de prova – "pessoas ou coisas das quais se possam extrair informações capazes de comprovar a veracidade de uma alegação" (Dinamarco, 2017, p. 97) –se alteram e reclamam a elaboração de novos critérios para o seu adequado exame.

No cotidiano forense atual, verifica-se o uso indiscriminado de provas digitais, mormente como reflexo do fato de que praticamente todo adulto hoje possui e utiliza um *smartphone*, aparelho que gera e armazena uma infinidade de informações, diversas delas com relevância probatória, como dados de base, conteúdo, localização etc.

Diante da ocorrência de tal fenômeno social e cultural, especialmente no processo penal, para além do exame de corpo de delito, em poucos anos, deixou-se de utilizar majoritariamente a prova oral para a formação da cognição judicial, para se fazer valer

também da prova digital como instrumento para a decisão. Hoje é raro um processo criminal em que não haja a análise de conteúdo do *smartphone* apreendido com o acusado.

Nesse sentido, veja-se recente artigo tratando do tema em debate:

> Se antes os órgãos investigativos ocupavam-se majoritariamente com provas testemunhais, documentais e periciais (focadas em objetos materiais), cada vez mais os vestígios digitais assumem destaque na persecução criminal. Isso por um motivo de todo evidente: as ferramentas tecnológicas e as plataformas de mídia social atualmente ocupam espaço fundamental na vida em sociedade, servindo como uma das principais formas de armazenamento de fotos, documentos, mensagens de texto e de voz, vídeos, *e-mails* e outros tipos de arquivos. Exatamente por isso, o conteúdo compartilhado nessas plataformas e guardado em nuvem, que pode ser entendido como supostamente criminoso, passa a ser considerado como possível espécie de prova processual — em específico, prova digital. Nessa perspectiva, quando o órgão investigativo entender que o acesso ao conteúdo digital armazenado em nuvem é importante para a elucidação dos fatos, ele deve solicitar formalmente ao juízo competente que determine a quebra de sigilo dos dados telemáticos armazenados em um determinado provedor de serviços de nuvem (como as empresas Google, Apple, Microsoft e outros) (Bicalho; Miranda, 2023).

Ou seja, a prova digital no processo brasileiro está onipresente, mas a legislação e os próprios operadores do direito e o sistema judicial não estão preparados para isso, salvo raras exceções.

A onipresença da prova digital envolve as mais diversas técnicas e provas, desde as mais simples até as mais complexas.

Nesse passo, é comum, por exemplo, a apresentação de *print screen*, com todas as suas fragilidades, às vezes complementado por uma ata notarial. Também é comum a apresentação de fotos de redes sociais ou de outras fontes abertas.

De outro lado, há casos notórios de utilização de tecnologia avançada. Veja-se o exemplo da divulgação pela mídia do uso de controversas[4] e avançadas técnicas de reconhecimento facial, por exemplo, na busca pela identificação dos responsáveis pela invasão do Congresso Norte-Americano em 2022[5] e aos prédios públicos de Brasília[6] em janeiro de 2023.

Também foi amplamente noticiado uma investigação internacional ainda mais sofisticada, por meio da qual a Federal Bureau of Investigation – FBI conseguiu infiltrar milhares de *smartphones* por eles próprios desenvolvidos e preparados especificamente para tal investigação, entre diversas organizações criminosas de todo o mundo, resultando na coleta de uma enormidade de provas dos mais diversos crimes, em vários países (United States, 2021).

Além disso, também foram amplamente noticiadas as investigações que resultaram na recuperação de bilhões de dólares

[4] *Cf.* CODED Bias. [*S. l.*]: Netflix, 2020. 1 video (1 h 25 min). Disponível em: https://www.netflix.com/br/title/81328723?s=a&trkid=13747225&t=cp&vlang=pt&clip=. Acesso em: 21 ago. 2023;
WESTERN GOVERNORS UNIVERSITY. **Facial recognition**: Why is it so controversial? [*S. l.*]: WGU, 16 Sept. 2019. Disponível em: https://www.wgu.edu/blog/facial-recognition-why-controversial1909.html#close. Acesso em: 21 ago. 2023;
FANG, Jiashun. **What Makes Facial Recognition Controversial**? Pittsburgh, PA: Arts Manegement and technology laboratory, 13 Feb. 2020. Disponível em: https://amt-lab.org/blog/2020/2/what-makes-facial-recognition-controversial. Acesso em: 21 ago. 2023.

[5] *Cf.* LOPES, André. Como o FBI usou reconhecimento facial para achar invasor do Capitólio. **Exame**, São Paulo, 21 abr. 2021. Disponível em: https://exame.com/tecnologia/como-o-fbi-usou-reconhecimento-facial-para-achar-invasor-do-capitolio/. Acesso em: 21 ago. 2023;
HARWELL, Drew; TIMBERG, Craig. How America's surveillance networks helped the FBI catch the Capitol mob. **The Washington Post**, Washington, 2 Apr. 2021. Disponível em: https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/. Acesso em: 21 ago. 2023.

[6] *Cf.* PRAZERES, Leandro. Os 3 focos das investigações sobre ação de bolsonaristas em Brasília. **BBC News Brasil**, Brasília, DF, 9 jan. 2023. Disponível em: https://www.bbc.com/portuguese/brasil-64206177. Acesso em: 21 ago. 2023;
ABBUD, Bruno. Como os terroristas que invadiram Planalto, STF e Congresso serão identificados pela PF. **Extra**, [*s. l.*], 9 jan. 2023. Disponível em: https://extra.globo.com/noticias/politica/como-os-terroristas-que-invadiram-planalto-stf-congresso-serao-identificados-pela-pf-25640924.html. Acesso em: 21 ago. 2023.

em Bitcoins furtados da *exchange* de criptomoedas Bitfinex e do *ransonware* (sequestro de dados por meio de criptografia) praticado contra a empresa Colonial Pipeline.[7]

Todavia, essa não é a realidade do cotidiano forense. Tais técnicas avançadas ficam adstritas a operações policiais pontuais.

Em suma, seja de forma avançada, seja de forma mais simples, a esmagadora maioria dos processos, hoje em dia, possui alguma espécie de prova digital.

Por essa e por diversas outras razões é que a doutrina vem apontando a necessidade cada vez mais urgente de preparação e capacitação dos atores envolvidos no processo para atuarem nessa nova realidade, o que ainda não ocorre. Ou seja, a exclusão digital bateu às portas dos tribunais.

Voltando à prova propriamente dita, ela constitui a razão que leva o órgão decisório a decidir sobre a ocorrência de fatos relevantes, associando o conteúdo às regras da ciência, experiência e lógica.

Percebe-se, portanto, que no atual cenário a produção da prova no processo ainda observa o rito próprio da juntada ou depósito em juízo dos documentos, da tomada de depoimentos e dos exames e vistorias periciais para esclarecimentos de ordem técnica; mas a fonte pela qual se acessa esses meios é que se revela o traço verdadeiramente distintivo do que se chama de prova digital, ostentando, assim, peculiaridades merecedoras de tratamento diferenciado.

Destaca-se, entretanto, ser notório que "a confiabilidade da prova documental – e a importância singular que os ordenamentos processuais lhe emprestam – assenta-se, exatamente, na estabilidade

[7] *Cf.* CHOW, Andrew R. Inside the Chess Match That Led the Feds to $3.6 Billion in Stolen Bitcoin. **Time**, New York, 10 Feb. 2022. Disponível em: https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/. Acesso em: 21 ago. 2023;
HEILWEIL, Rebecca. The rise of the crypto cop. **Vox**, [*s. l.*], 11 May 2022. Disponível em: https://www.vox.com/recode/2022/5/11/23065956/detectives-crypto-cops-irs-fbi-cyber-bitcoin. Acesso em: 21 ago. 2023.

do suporte em que a informação é registrada" (Marinoni; Arenhart, 2011, p. 563-564). O documento produzido eletronicamente pode ser alterado de forma suscetível à regravação, notadamente no fluxo de dados em rede de computadores, pois a informação armazenada "assume caráter temporário, é fungível e de grande volatilidade" (Ramos, 2014, p. 38).

De outro lado, cada vez que reproduzimos um documento, conseguimos uma cópia idêntica ao original, desde que utilizemos o mesmo meio ou um equivalente que seja apropriado para a transferência. No entanto, preservar o documento original com suas características distintivas pode superar a duração de um dispositivo de armazenamento, contribuindo para a durabilidade dos documentos ao longo do tempo.

2 PROVAS

2.1 Conceito

O termo prova vem do latim *proba*, representando um conceito de múltiplos significados nas linguagens corrente e jurídica.[8] Nesta última, prova geralmente se refere a três entendimentos: 1) atividade, que é o desejo de se provar algo; 2) resultado, ou seja, algo que foi provado; e 3) meio, no sentido da forma com que a prova vai ser realizada. A partir desses três sentidos, fala-se em atividade probatória, em resultado advindo da atividade e da forma pela qual ela foi elaborada. A atividade probatória é irradiada por comandos principiológicos e

[8] Moacyr Amaral faz uma ressalva sobre relevância da prova: "Já houve quem dissesse que a história da prova reflete toda a história da civilização e não menor autoridade que afirmasse não ser isso contestável. Das épocas mais remotas à era contemporânea, a prova vem acompanhando, no espaço, o avanço e os recuos dos povos, a evolução da civilização" (Santos, 1966-1968, p. 23).

legais, por força do neoconstitucionalismo[9] e do neoprocessualismo.[10] Desse modo, corroborando a prova como direito fundamental[11].

Em uma concepção de atividade probatória, o Direito Processual entende a prova como todo e qualquer elemento material dirigido ao juiz da causa para esclarecer o que foi alegado por escrito pelas partes, especialmente circunstâncias fáticas.[12] Nas palavras de Bueno (2010, p. 261), seria a prova "tudo que puder influenciar, de alguma maneira, na formação da convicção do magistrado para decidir de uma forma

[9] O Neoconstitucionalismo é entendido como a constitucionalização do Direito, à luz dessa realidade pondera Silva (2008, p. 18): "[...] a irradiação dos efeitos das normas (ou valores) constitucionais aos outros ramos do direito. O principal aspecto dessa irradiação [...] revela-se na vinculação das relações entre particulares e direitos fundamentais, também chamada de efeitos horizontais dos direitos fundamentais". Nesse sentido, Didier Júnior (2009, p. 25) afirma: "Vive-se, atualmente, uma nova fase da renovação do Direito Constitucional. Há diversas manifestações disso: a) parte-se da premissa de que a Constituição tem força normativa, e, por consequência, também têm força normativa os princípios e os enunciados relacionados aos direitos fundamentais; b) pela expansão da jurisdição constitucional (controle de constitucionalidade difuso e concentrado, como é o caso do Brasil); c) desenvolvimento de uma nova hermenêutica constitucional (com a valorização dos princípios da proporcionalidade e razoabilidade). A essa fase deu-se o nome de Neoconstitucionalismo ou pós-positivismo.

[10] Didier Júnior (2009, p. 26-27) sustenta que o Neoconstitucionalismo é: "[...] o estudo e aplicação do Direito Processual de acordo com essa nova proposta do pensamento jurídico". Ressalta que alguns doutrinadores chamam de formalismo-valorativo, em razão da importância que os valores constitucionais tutelados na esfera dos direitos fundamentais representam no aspecto de edificação e utilização do formalismo processual. Convém pôr em relevo que para o escritor essas premissas são similares a do Neoprocessualismo, que tem a função didática de remeter a noção do Neoconstitucionalismo, e, metodológica, porque representa a redefinição das categorias processuais, por isso o termo "neo", por caracterizar: "[...] o processualismo do final do século XIX, e meados do século XX".

[11] Os direitos fundamentais para visão de Araújo e Nunes Júnior (2008, p. 110), "constituem uma categoria jurídica, constitucionalmente erigida e vocacionada à proteção da dignidade humana em todas as dimensões". Destarte, é possível entender a prova como corolária não apenas do princípio do contraditório e da ampla defesa, mas também do princípio da dignidade da pessoa humana. À evidência, assim não o é que o direito a prova por ser um direito fundamental, é direcionado a proteção da dignidade da pessoa humana, por que faz uso dos seus mecanismos para dar azo as suas pretensões.

[12] CPC, 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" (Brasil, 2002).

ou de outra, acolhendo, no todo ou em parte, ou rejeitando o pedido do autor". Para Marinoni e Mitidiero (2011, p. 334), poderíamos definir 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". Desse modo, o conceito de prova abarca a produção dos meios e atos realizados no processo com a intenção de convencer o juiz sobre a verdade ou inverdade de uma alegação mediante os fatos relevantes para a solução do caso em questão.

Compreende-se, assim, a multiplicidade e a possível controvérsia nos entendimentos do conceito de prova na doutrina. Contudo, para a definição de um conceito atual, é fundamental que perspectivas superadas sejam excluídas a fim de que o entendimento seja compatível com as percepções contemporâneas do Direito nas quais se reconhece a impossibilidade de se enxergar a prova como um meio para a formação de uma certeza inquestionável dos acontecimentos ou para alcançar a verdade absoluta dos fatos, visto que se entende que a apresentação de provas processuais não é capaz de reconstituir uma situação em sua completa realidade, de modo a eliminar quaisquer dúvidas acerca da convicção formulada. A prova em seu sentido jurídico consiste na demonstração da verdade formal dos fatos discutidos, mediante procedimentos determinados, ou seja, através de meios legítimos.

O aspecto mais relevante na teoria geral da prova gira em torno do objeto de prova, o que seja, aquilo que deve ser provado no processo; responderia à pergunta: Sobre o que a prova deve recair? Tem-se, nesse sentir, que o objeto de prova são os fatos controvertidos relevantes.[13] Nesse aspecto, de acordo com a disciplina do art. 332 do CPC articulado com o art. 131 (o sistema de persuasão

[13] Fatos incontroversos/notórios, confessados não precisariam ser consequentemente provados; fatos irrelevantes/impertinentes também não dependem de prova.

racional como modelo de valoração da prova), não há hierarquia de provas, podendo ser utilizados meios de prova típicos e mesmo atípicos, desde que moralmente legítimos. Inexistindo hierarquia propriamente dita, o que se pode admitir, no máximo, é certa "preferência pela prova típica", na forma como determinada pelo legislador, diante da maior facilidade, para o julgador, na sua admissão, produção e valoração.

Contudo, é certo que historicamente, os documentos físicos possuíam a condição de se revelarem propícios a conferir estabilidade às alegações, evidenciando-se, inclusive, como prova pré-constituída apta a perpetuar, sem inclinações de ordem subjetiva, a memória dos atos e fatos jurídicos. Isso lhes rendeu tratamento especial na legislação brasileira e na estrangeira, que a eles têm conferido pleno crédito (Marinoni; Arenhart, 2011, p. 548-549), inclusive como único meio idôneo para a prova de determinados fatos, como mencionava o art. 401 do Código de Processo Civil instituído pela Lei n. 5.869, de 11 de janeiro de 1973 (CPC/73).[14]

Calha consignar que a teoria clássica realiza diferenciação entre fontes e meios de prova, em que os primeiros são os elementos (mecanismos) externos do processo aptos a provar; e os últimos são os elementos (mecanismos) internos do processo aptos a provar, ou seja, as formas pelas quais se podem produzir provas em juízo de acordo com a legislação processual do país (confissão, depoimento pessoal, interrogatório, testemunhas, documentos, perícia e inspeção judicial). Na prática, tem-se que nem toda fonte de prova pode se converter em meio lícito e apto de prova, diante justamente das restrições impostas pela legislação processual vigente, ex.: uma informação só poderá ser obtida de uma fonte se isso se enquadrar entre os meios de prova admitidos pelo sistema (Gonçalves, 2011, p. 372).

[14] CPC, art. 401. "A prova exclusivamente testemunhal só se admite nos contratos cujo valor não exceda o décuplo do maior salário-mínimo vigente no país, ao tempo em que foram celebrados " (Brasil, 1941).

Com a diferenciação entre fontes e meios de prova, resta evidenciado que nem toda fonte de prova pode ser convertida em meio de prova a ser utilizado na instrução do processo, visto que há restrições legais ao uso das provas, mesmo lícitas.

Note-se que, apesar da possibilidade de prova oral (depoimento das partes e prova testemunhal), a produção dela sempre foi realizada mediante estigma de desconfiança, na medida em que apesar da importância do depoimento pessoal, inclusive como elemento de confissão, o transcurso do tempo torna a memória humana passível de problemas, inclusive esquecimento, incremento de memórias inautênticas ou pior, comprometidas pela corrupção do depoente/testemunha e inviabilizadas por doenças degenerativas, óbito ou não localização. Dessa forma, é certo que embora inexista tarifação legal e estanque da prova no Código de Processo Civil, existe maior primazia e consequente superioridade na confiança da eficácia probatória da prova documental.

Destarte, a par das exigências de forma solene para determinados atos e das disposições sobre o teor de instrumentos particulares, o cuidado legislativo com a prova documental exige que o magistrado efetue a análise sob, no mínimo, dois prismas essenciais: i) força probante do documento, aspecto que se encontra relacionado com a origem e a respectiva credibilidade, inclusive sob o aspecto da cadeia de custódia realizada para a manutenção e preservação desse documento; e 2) necessidade de análise/filtragem sob o ângulo da fidedignidade das informações, quando existe transmudação do meio físico para o meio digital, ou quando não se está diante do documento original.

O presente artigo pretende discorrer acerca da produção da prova digital, levando em consideração a realidade vivenciada pela magistratura nacional na seara do processo civil, processo penal e nas demandas previdenciárias.

2.2 Prova digital

Ao nos referimos à prova digital, é normal o uso da expressão "documentação eletrônica" para referir-se aos dados e arquivos digitais. Todavia, as provas digitais possuem características diferenciadas, que conduzem ao seu enquadramento em uma classificação própria, muito embora as semelhanças entre a prova digital e o documento permitam a utilização do meio de prova documental como procedimento probatório em juízo.

Entende-se, de modo genérico, que prova digital é toda aquela que não é analógica. O termo "digital" abarca diversas realidades tecnológicas e os sistemas não eletrônicos de comunicação, incluindo a internet. Por isso, parte da doutrina assenta que o termo mais adequado para tratar desse tipo de prova seria "prova eletrônico-digital", que abrangeria a prova digital enquanto um dos elementos da prova eletrônica. Uma definição mais simples e objetiva é apresentada pelo Scientific Working Group on Digital Evidence, que entende essa prova como uma informação arquivada e/ou transmitida de forma binária cujo valor é probatório (Eastom, 2016).

Eoghan Casey (2011, p. 12) define *digital evidence* como "qualquer dado armazenado ou transmitido usando um computador que confirma ou rejeita uma teoria a respeito de como ocorreu um fato ofensivo ou que identifica elementos essenciais da ofensa como intenção ou a álibi".

Entretanto, o entendimento mais claro é o que define a prova digital como dados ou informações transmitidos ou armazenados na forma binária e que podem valer como prova. Tal conceito foi formulado na norma ISO/IEC 270372.

Em regra, toda evidência digital válida é governada por três pilares fundamentais: relevância: a evidência digital é considerada relevante quando se destina a provar ou refutar um elemento de

um caso específico que está sendo investigado; confiabilidade: este termo define a característica de "garantir que a evidência digital seja o que pretende ser"; e suficiência: o conceito de suficiência significa que a evidência digital seja suficiente para permitir que elementos questionados sejam adequadamente examinados ou investigados.

A preservação da prova é indispensável, e as características específicas da prova digital a dificultam, justamente por ser passível de alteração ou destruição, sendo um claro obstáculo para a manutenção de sua integridade e para o seu não repúdio.

Destaca-se que há cada vez mais espécies de prova digital consideradas como provas admissíveis, sendo a prova digital transmitida pela tecnologia Blockchain. Atualmente, existem três tribunais de internet na China, criados em Hangzhou, Pequim e Guangzhou (Conheça [...], 2021)[15]. Em 2015, o Supremo Tribunal Popular da China definiu, pela primeira vez, o conceito de prova digital no art. 116º da interpretação sobre implementação da Lei Processual Civil, por exemplo, os dados eletrônicos incluem: correio eletrônico, intercâmbio eletrônico de dados, blogue, microblogue, SMS, assinaturas eletrônicas, domínios e outras informações formadas ou preservadas em meio eletrônico.

Com base em tais considerações é de se destacar que se consideram como dados informáticos os programas de sistemas informáticos, documentos eletrônicos e dados pessoais, de localização ou de tráfego, podendo, assim, serem divididos da seguinte forma: dados de localização, caracterizados por indicarem a localização geográfica do equipamento terminal dos utilizadores de serviços de comunicação eletrônica que sejam disponíveis publicamente, além disso, esses

[15] O primeiro Tribunal de Internet do país foi criado em Hangzhou, centro de comércio eletrônico, em agosto de 2017. O segundo em setembro de 2018, enquanto autoridades reforçam as medidas para proteger transações comerciais, informações pessoais e propriedade intelectual *on-line*. O terceiro foi aberto em Guangzhou, no sul da China, em setembro de 2018.

dados também apontam o destinatário de uma comunicação; dados de tráfego, que são informações técnicas ou informáticas referentes a comunicações dadas por meio de tecnologias de informação e comunicação, que contêm dados quanto à origem, à hora, à duração, aos trajetos e aos serviços subjacentes da comunicação; dados de base, os pessoais relacionados à conexão à rede de comunicações, compõem esta categoria a identidade do assinante, bem como o número e a morada deste; e dados de conteúdo, cujas informações dizem respeito ao conteúdo de uma mensagem ou comunicação.

2.3 A Prova Documental Eletrônica – Lei n. 11.419, de 19 de dezembro de 2006

A Lei n. 11.419/2006 foi promulgada com o intuito de aprimorar a entrega da tutela jurisdicional, sob ênfase de uma cultura de celeridade e de transparência para o Poder Judiciário, ao dispor sobre a informatização do processo judicial (Brasil, 2006).

A legislação em questão possui como fim precípuo promover a emancipação do homem em uma sociedade digital, especifica, como meio eletrônico, qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais (I, art. 2º); como transmissão eletrônica, toda a forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores (II, art. 2º); como assinatura eletrônica, identificação inequívoca do signatário, seja a baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica, seja a obtida mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos (III, art. 2º).

Destaca-se, ainda, que o art. 11 da referida lei, estabelece que "os documentos produzidos eletronicamente e juntados aos processos

eletrônicos com garantia de origem e de seu signatário, na forma estabelecida nesta lei, serão considerados originais para todos os efeitos legais" (Brasil, 2006). Nesse seguimento, as provas digitais juntadas aos processos eletrônicos serão consideradas originais para todos os efeitos legais, se for possível a verificação de sua fonte.

Com fulcro no § 3º do art. 11 da lei mencionada, "os originais dos documentos digitalizados [...] deverão ser preservados pelo seu detentor até o trânsito em julgado da sentença ou, quando admitida, até o final do prazo para interposição de ação rescisória" (Brasil, 2006), para que seja possível a constatação de sua legitimidade, caso haja impugnação da parte oposta. Tal regra é deveras parecida ao que existia no art. 225 do Código Civil e no Código de Processo Civil. Logo, a novidade é conceder à parte contrária o ônus da prova quanto à arguição de falsidade da prova trazida aos autos, verificando sua autenticidade.

Conquanto não se olvide a essencial segurança jurídica e a polêmica reinante acerca da segurança da informação, mister se faz a necessidade em se derrubar o mito a respeito da concepção de que o documento cartáceo além de material oferece maior grau de segurança e durabilidade comparativamente ao eletrônico. Trata-se de flagrante equívoco na medida em que a informação armazenada em papel consubstancia original único, cujo extravio ou avaria redunda na perda do documento e de seu valor probatório, e a fragilidade material que lhe é inerente no tocante às respectivas preservação e segurança. Salienta-se diversamente que a forma eletrônica permite durabilidade superior, bem assim recuperação do documento, sua reprodução sucessiva, sem que estas impliquem a perda da característica de originalidade, nada obstante sejam, por força do uso, cognominadas de cópias.

A Lei n. 11.419, de 19 de dezembro de 2006, reconhece, ainda, a assinatura digital como garantia de autenticidade das informações

(art. 1º, § 2º, inciso, III[16] e art. 2º, § 2º[17]), ao que discorreremos sobre essa adiante, e passou a admitir a conservação dos autos em meio exclusivamente eletrônico, desde que garantida a integridade dos dados.[18]

No tocante à manipulação da informação armazenada eletronicamente, é de se consignar que a possibilidade de adulteração de documento não se traduz em fato novo ao meio jurídico, sendo utilizados, há longa data e para fim de prova, a atividade probatória e os serviços periciais. Reitera-se que a mudança se limita à forma da prova documental, se sob roupagem cartácea ou eletrônica, apenas isso, prevalecendo incessante busca, também no campo do processo, de segurança, sigilo, inviolabilidade da vida privada e do espaço íntimo de cada homem, como valores essenciais ao devido processo legal.

2.4 Obtenção das provas digitais

No que diz respeito à aquisição ou produção de prova, a palavra "prova" indica que o tribunal deve reconhecer o responsável por essa produção, de modo que esse processo siga a lei no que concerne à sua produção. No que se refere às peculiaridades, aos requisitos e aos princípios de validade da prova digital, compreende-se que

16 "§ 2º Para o disposto nesta Lei, considera-se: [...] III – assinatura eletrônica as seguintes formas de identificação inequívoca do signatário: a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica; b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos" (Brasil, 2006).

17 "§ 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações" (Brasil, 2006).

18 "§ 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares" (Brasil, 2006).

precisa respeitar os paradigmas legais para sua admissibilidade; ser apresentada em uma linguagem mais simples, entendendo que os operadores judiciários nem sempre compreenderão a linguagem técnica; ter durabilidade, demandando cuidado no recolhimento e conservação; e ter um padrão uniforme na sua produção, o que significa que as regras para tal devem ser as mesmas em todas as suas formas de apresentação e em todos os níveis de investigação forense digital (cível ou criminal).

Quanto aos documentos eletrônicos, a prática dos atos processuais por meio eletrônico não é novidade no Brasil, havendo a lei que instituiu o processo eletrônico resultado de outras leis e projetos de lei, em face dos avanços tecnológicos, com o intuito de um novo enfoque, mais ágeis, de acesso à jurisdição. Não restam dúvidas de que o documento eletrônico, por força da sua natureza terá que ter a sua autenticidade verificada, cabendo ao juiz fazer essa avaliação. Nesse âmbito, o art. 426: "O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor" (Brasil, 2006).

2.4.1 Cadeia de custódia

A obtenção da prova nos remete ao necessário cuidado com as fontes de prova obtidas fora do processo, inclusive pela dificuldade para a parte contrária contraditar tais elementos. Desse modo, "o tema de provas exige a intervenção de regras de 'acreditação', pois nem tudo que ingressa no processo pode ter valor probatório; há que ser 'acreditado', legitimado, valorado desde sua coleta até a sua produção em juízo para ter valor probatório" (Lopes Júnior, 2017, p. 412).

Surge assim, o instituto da cadeia de custódia com o objetivo de garantir a todos o devido processo legal, bem como os recursos a ele inerentes, como a ampla defesa, o contraditório e principalmente o direito à prova lícita, conforme estabelece a Constituição Federal e legislação infraconstitucional (art. 5º, LIV, LV e LVI da CF/88, arts. 7º e 369 do CPC e arts. 564, III, "d" e 157 do CPP).[19] A cadeia de custódia abarca todo o caminho que deve ser percorrido pela prova até sua exata análise e escorreita inserção no processo, sendo que qualquer interferência durante o trâmite processual pode resultar na sua imprestabilidade. Desse modo, não se pode limitar a garantia constitucional da prova, isso porque ela deve abranger também "a possibilidade de se indicar fontes de prova, de se exigir que elas venham ao processo, da mesma forma como foram obtidas, de utilizar os mecanismos de prova, pela metodologia legalmente definida, e de exigir a valoração dos elementos trazidos" (Edinger, 2016, p. 244).

Nesse sentido, a cadeia de custódia pode ser definida como "uma sucessão de eventos concatenados, em que cada um proporciona a viabilidade ao desenvolvimento do seguinte, de forma a proteger a integridade de um vestígio do local de crime ao seu reconhecimento

[19] Art. 5º, inciso LVI: "São inadmissíveis, no processo, as provas obtidas por meios ilícitos" (Brasil, 1988).

como prova material até o trânsito em julgado do mérito processual" (Dias Filho, 2012, p. 404).

Sobre o tema, Pacelli e Fischer (2020, p. 494) ensinam o seguinte:

> A doutrina e a jurisprudência há muito tratavam do que se denomina cadeia de custódia, que nada mais é do que a preservação e registro do caminho da prova, desde sua coleta até a apreciação pelo Poder Judiciário. A finalidade precípua é garantir a lisura e validade das provas que serão valoradas pelo julgador, maximizando-se o devido processo legal, sob duplo vetor: (a) tanto sob a ótica da necessária apuração dos fatos na sua maior inteireza (sendo decorrência das denominadas obrigações processuais penais positivas); (b) como também para permitir o exercício da ampla defesa e do contraditório a partir de provas e indícios que sejam considerados como válidos à luz do ordenamento jurídico."

2.4.2 Confiabilidade da prova digital

A evolução tecnológica está sempre a propiciar o uso de novos suportes, sem, contudo, desnaturar a essência nem a finalidade do registro de um fato, que caracterizam a prova em função de seu conteúdo (Marcacini, 1999, p. 75-76) e, portanto, inspiram igual prudência no reconhecimento da sua eficácia. Não é dizer que o suporte do documento seja indiferente. Os seus atributos ensejam debate a respeito da fidedignidade da prova digital e resistência à sua admissão.

A aversão ao novo não é algo inédito e permeia o cenário judicial e acadêmico desde a disseminação de novas tecnologias, principalmente aquelas denominadas exponenciais. Nesse sentido, a utilização das "novas tecnologias" sempre foi objeto de discussão na produção da prova judicial, pois aspetos como a confiabilidade e a integridade sempre permearam as preocupações acerca da matéria. Destaca-se que a utilização de fotografia, como "nova tecnologia", foi objeto de acaloradas discussões, passando, inclusive o legislador

a exigir a apresentação do "negativo". O aludido debate alterou a forma na atualidade, pois os "negativos" não são mais comuns e embora a familiaridade com a tecnologia permita evoluirmos em alguns aspectos, provoca novos temores, exigindo, assim, a constante evolução legislativa acerca do tema, principalmente quando se debate a produção da prova digital e a respectiva confiabilidade para fins judiciais.

Foi inserido no arcabouço jurídico brasileiro a Medida Provisória n. 2.200-2 de 2001, de efeitos perenizados pela Emenda à Constituição n. 32 de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, outorgando expresso reconhecimento aos documentos eletrônicos produzidos naqueles moldes;[20] aliada à Lei do Processo Judicial Eletrônico (Lei n. 11.419/2006) e do Código de Processo Civil editado em 2015, que passou a tratar da prova digital, embora com ambiguidades e imprecisões.

Tem-se, ainda, a Lei n. 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet no Brasil, ao cuidar de aspectos do tráfego de dados na internet, que acabou por tratar questões pertinentes à informática em geral e ao direito à prova (Brasil, 2014).

Na verdade, a dificuldade em relação à prova digital se inverteu: a onipresença da tecnologia, fora do restrito âmbito processual, e a crescente familiaridade dos profissionais do Direito com as fontes de prova que frequentemente interessam ao processo,[21] somados à legislação lacunosa, têm resultado na prevalência da confiança individual e subjetiva em cada específica fonte de prova, muitas vezes superficial e alheia às suas características técnicas, em detrimento de análise objetiva dos riscos que a atividade probatória envolve.

[20] "Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória" (Brasil, 2001b).

[21] Basta pensar nos históricos de conversas travadas por meio de aplicativos de celular, reproduzidos por imagem da tela do dispositivo.

A referida realidade faz com que muitas vezes se negligencie, como efeito desse crescente conforto com a prova digital, que documentos eletrônicos em sentido estrito e outras informações armazenadas em meio eletrônico são também suscetíveis de falsidade, não apenas ideológica, mas também material. As imagens da tela de um computador pessoal ou de um aparelho de telefonia móvel podem ser compostas sem qualquer especial exigência de habilidade em editores de imagens, ou mesmo em sítios eletrônicos que facilitam a criação inteiramente nova de uma reprodução visualmente indistinta de uma conversa autêntica. Há numerosas aplicações de internet para este fim, facilmente encontradas por intermédio de qualquer sistema de busca, que aqui não se listam para evitar a promoção de *software* não verificado, potencialmente malicioso.

A legislação previu o referido risco ao estabelecer que qualquer reprodução mecânica ou eletrônica tem o valor do original, se não for impugnada (art. 225 do Código Civil[22]), e que as fotografias digitais, assim como a forma impressa das mensagens eletrônicas, fazem prova do que reproduzem até a impugnação, cabendo, neste caso, a "autenticação eletrônica" ou a realização de perícia (art. 422, §§ 1º e 3º, do Código de Processo Civil).

No mesmo sentido, restou admitido o valor probatório dos documentos "produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário" (art. 11, *caput*, da Lei n. 11.419/2006), assim como os extratos digitais de bancos de dados, desde que atestada a conformidade com o original pelo emitente, sob as penas da lei (art. 425, inciso V, do CPC). O regramento legal é longe de ser exaustivo, e deve ser compatibilizado, na jurisdição

[22] "Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão" (Brasil, 2002).

criminal, com a necessidade de exame pericial do corpo de delito, independentemente de impugnação (art. 158 do Código de Processo Penal[23]), mas permite entrever que, para a atribuição de força probante a documentos eletrônicos e outras informações extraídas de meios digitais, "é fundamental avaliar o grau de segurança e de certeza que se pode ter, sobretudo quanto à sua autenticidade, que permite identificar a sua autoria, e à sua integridade, que permite garantir a inalterabilidade do seu conteúdo" (Didier Júnior; Braga; Oliveira, 2016, p. 221-222).

Os critérios que asseguram a autenticidade e a integridade dos registros de procedimentos legais eletrônicos são claramente evidenciados nas disposições do Direito Processual Instrumental, conforme estabelecido no art. 195 do Código de Processo Civil. Além disso, é viável aplicar esses mesmos critérios a qualquer registro eletrônico com potencial para ser utilizado como evidência em questões judiciais. Vale ressaltar que um dos requisitos cruciais é a avaliação minuciosa do ambiente de armazenamento dos dados, bem como a maneira como foram gerados. Isso também envolve considerar a finalidade e o método empregado na criação desses registros, incluindo a garantia de uma cadeia de custódia adequada e a capacidade de realizar investigações periciais para validação posterior.

Não obstante, algumas diretrizes podem, diante do cenário atual, ser traçadas visando a utilidade imediata e fundamentar o exame de evoluções futuras, para tanto distinguindo-se entre os instrumentos como documentos em sentido estrito que comportam a assinatura, documentos em sentido amplo, que podem, com maior ou menor concurso das pessoas a que digam respeito, ser captados ou mantidos

[23] "Art. 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado" (Brasil, 1941).

por terceiros idôneos, ou ainda gerados automaticamente por sistemas de informática.

2.4.3 Documentos em sentido estrito e semelhantes

Documentos em sentido estrito são aqueles que veiculam declarações, originados em uma pessoa, com uma finalidade própria, que assim se ligam ao respectivo autor (ex.: os contratos, a correspondência eletrônica, peças processuais etc.)

A autoria é o registro do conteúdo por aquele que se apresenta como responsável na produção. Nesse aspecto, há necessidade de que essa produção ocorra através de elementos de estabilidade comprovada, inclusive com a utilização de *softwares* específicos. Ademais, a inserção de assinatura eletrônica com criptografia assimétrica no padrão ICP-Brasil permite atribuir aos documentos digitais atributos tecnológicos que se revelam aptos a indicar elementos, como segurança, autenticidade e integridade.

A assinatura digital, tal como hoje reconhecida pela lei, é produto de sofisticada técnica elaborada a partir da criptografia assimétrica, que recebe tal denominação por não se basear em um segredo comum, como nas raízes históricas da prática. Em resumo, essa forma de criptografia atua a partir de um conjunto de chaves, compostas de uma sequência de caracteres gerados por computador, a partir de elementos aleatórios e fórmulas matemáticas avançadas que viabilizam a sua correlação. Com elas, permite-se que, a partir da chave pública,[24] qualquer pessoa ou dispositivo possa codificar conteúdo que apenas poderá ser decifrado pela chave privada,[25] bem como identificar a chave pública associada ao conteúdo codificado com a chave privada,

[24] Assim denominada porque passível de ampla divulgação, sem prejuízo à segurança do mecanismo.

[25] A posse é reservada ao emissor do par.

tudo sem ter acesso a ela; dessa forma, sem poder acessar conteúdo destinado ao seu detentor de forma protegida nem simular a autoria do código cifrado, que se relaciona exclusivamente à chave pública correspondente.

A aplicação de criptografia assimétrica torna impossível a decodificação, pois qualquer alteração, ainda que mínima na informação, revela-se tarefa tormentosa, inviabilizando a leitura do texto, que se torna inelegível, tornando o documento imprestável para os fins a que se destina.

A inserção de elementos de segurança com a utilização de *hashes*, *digests* ou *checksums* possibilita a vinculação do autor ao documento, através da geração de dados (expressões alfanuméricas), que se tornam conhecidos com a utilização do mesmo código algorítmico, o que permite, por exemplo, a certeza da integridade do conteúdo e a garantia de isenção de qualquer modificação, ainda, que ínfima.

Uma ferramenta importante é a utilização de proteção de assinaturas e senhas em duas etapas, para confirmar a identidade do usuário como titular da linha ou do endereço eletrônico.

Dentro do setor público em geral, especialmente no Poder Judiciário, é agora viável adotar a assinatura "por meio do registro do usuário no Poder Judiciário" (conforme o art. 1º, § 2º, inciso III, alínea *b*), dispensando o uso de um Certificado Digital A3, como estipulado na Lei n. 11.419, de 2006.

Por outro lado, existem métodos que não proporcionam nenhuma segurança, como a reprodução digitalizada de assinaturas manuscritas, erroneamente classificada por alguns como "assinatura eletrônica". Na verdade, trata-se de uma imagem digital que pode ser inserida em qualquer documento por qualquer pessoa, permitindo inclusive manipulações.

Mesmo no caso de utilização de sistema de *login* e senha (Certificado Digital A1) não se garante a integridade dos dados, visto

que não se utiliza a criptografia. Nesses casos, competirá ao juiz ponderar sobre a valoração dessas provas.

Também deve ser considerada a possibilidade de uso inadequado da assinatura digital, mesmo quando produzida por um Certificado Digital A3, como ocorre nos casos de ocultação da assinatura, substituída por uma verificação em um *site* da internet supostamente confiável, ou quando um terceiro utiliza um certificado físico.

Por fim, é importante destacar que existe a possibilidade de converter documentos digitais em documentos físicos, sem cumprir os requisitos mínimos de segurança, ao serem anexados a processos físicos (conforme o art. 439 do Código de Processo Civil). Isso pode permitir a edição e adulteração desses documentos.

Saliento ser elementar que "o valor probante do documento eletrônico deve ser sempre aferido no ambiente em que ele foi gerado" (Rinaldi, 2016, p. 638). Assim, sendo adotadas as cautelas necessárias, o documento digital oferece segurança superior ao seu semelhante físico, não merecendo, portanto, a resistência que inicialmente se lhe opôs.

2.4.4 Informações armazenadas eletronicamente

Atualmente existe uma gama de informações armazenadas eletronicamente, inclusive com potencial probatório, por exemplo, o extrato digital dos bancos de dados, que possui regulação no art. 11, § 1º, da Lei n. 11.419/2006, cuja força probante é estabelecida no art. 425, inciso V, do Código de Processo Civil[26].

Os bancos de dados, enquanto compilação de dados, obras e outros materiais organizados de uma maneira sistemática e ordenada,

[26] "Art. 425. Fazem a mesma prova que os originais: [...] 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" (Brasil, 2015).

devem proteger os direitos do autor e os dados pessoais, conforme a Diretiva n. 96/9/CE, do Parlamento Europeu e do Conselho da União Europeia.

Nesse aspecto deve ser consignado que a utilização dos dados mantidos por concessionárias de serviços públicos – ou de caráter público –, instituições financeiras e provedores de conexão à internet e de aplicação na internet deve ser devidamente justificada.

A manutenção de bancos de dados se revela uma tarefa de elevada complexidade com a exigência de política de *compliance* e a realização de múltiplas funções, para que seja revelada e garantida a utilização das informações enquanto prova judicial. Calha consignar que o pressuposto de legitimidade dos atos administrativos pode ser desconstituído diante de prova em contrário, e não desobriga o Poder Público, em caso de impugnação fundada, a apresentar o suporte documental e de boas práticas para manutenção dos bancos de dados pelos quais as informações são produzidas.

Deve, ainda, ser alertado que quando a informação é produzida em meio exclusivamente eletrônico, existe a possibilidade de vinculação dessa ao autor, a exemplo do que ocorre nas operações decorrentes de escrituração eletrônica das transações financeiras, ou quando geradas automaticamente por sistemas eletrônicos, com a finalidade de registro da utilização ou em função dela (ex.: ligações telefônicas, troca de mensagens, acesso a aplicações na internet etc.), inexistindo, nessas hipóteses, outro meio de prova possível, exigindo, ainda, a possível extração da informação dos bancos de dados digitais. Nessas situações, caso ocorra dúvida fundada a respeito da fidelidade da informação contida no banco de dados, haverá necessidade de apresentação de toda documentação técnica, política de *compliance* e informação do responsável pela base de dados quanto ao seu funcionamento. Saliento que a referida premissa se aplica, por exemplo, aos históricos de utilização de sistemas informáticos (*logs*).

O Marco Civil da Internet no Brasil não tratou a questão da confiabilidade dos dados constantes nos bancos de dados, possibilitando, atualmente, crítica doutrinária quanto à garantia do conteúdo dos documentos eletrônico.

Nada impede, porém, que na produção da prova se extirpe a dúvida com a adoção das providências estabelecidas pelo art. 425, inciso V, do Código de Processo Civil, ou através da produção de prova pericial.

O direito comparado prestigia em diversos casos a prova testemunhal, no que se refere à criação, à aquisição, à manutenção, à preservação e à extração da informação armazenada em meio digital, sem prejuízo, por exemplo, da análise de metadados e da adequada utilização do procedimento para extração dos dados.

A responsabilidade na extração dos dados digitais é tema de relevante importância, recebendo, inclusive, tratamento minucioso na alteração legislativa ocorrida em 2008 na Itália, com a alteração da Convenção sobre o Cibercrime, firmada em Budapeste (Council of Europe, 2001), a fim de que o Codice di Procedura Penale (Itália, 1988) passasse a exigir a conformidade dos dados extraídos aos respectivos originais e a sua inalterabilidade.

Em suma, a extração de informações de bancos de dados é um processo complexo que implica o acesso ao sistema informatizado, bem como aos controles de permissões, e o adequado manejo de ferramentas de auditoria, de preferência previamente instaladas, para que se possa chegar a um determinado conteúdo. Após, deve ser exigido a adoção de adequada e cuidados cadeia de custódia, inclusive com avaliação do suporte adequado e a garantia do responsável pela extração quanto à conformidade dos dados com os dados originais.

A prática forense, no entanto, tem revelado que práticas inadequadas são utilizadas no Poder Judiciário pátrio, inclusive com a juntada de documento com reprodução de baixa qualidade no corpo

dos arrazoados, como imagens de telas de computador etc., mas sem nenhum esclarecimento sobre a cadeia de custódia (criação e guarda dos dados), ou, ainda, sobre o método/metodologia de acesso aos dados ou a responsabilidade pela referida atividade.

A referida prática revela que a eficácia probatória dos bancos de dados digitais se compromete na seara judicial, na medida em que não se possibilita garantir a confiabilidade da informação na origem, tampouco que o que foi reproduzido nos autos corresponde ao que consta na origem (autenticidade), sem possibilidade de alteração desde a extração (integridade).

É necessário a compreensão de que a adequada produção da prova digital necessita de observância à legislação e às regulamentações existentes, bem como emissão de atestado do responsável pela extração dos dados, ou, ainda, por cautela, de extração dos dados acompanhada por notário e descrita em ata notarial.

2.4.5 Obtenção coercitiva das informações

É relevante mencionar outro aspecto em relação às informações armazenadas em meio eletrônico, que podem ser obtidas compulsoriamente, especialmente em processos criminais. Isso ocorre por meio da apreensão de dispositivos durante investigações criminais ou da obtenção de conjuntos de dados através de provedores de serviços *on-line*.

Em se tratando de processo penal, torna-se ainda mais importante a confiabilidade da prova obtida, que deve se mostrar autêntica e íntegra para servir como supedâneo a uma condenação.

Muitas vezes, são apresentadas apenas fotografias de dispositivos eletrônicos nos registros processuais, a fim de retratar conteúdo ilícito, como pornografia infantil, ou para reproduzir outras imagens relevantes para o crime em questão. Além disso, históricos

de comunicação entre criminosos sobre os delitos em investigação também são frequentemente apresentados.

No entanto, a reprodução fotográfica, mesmo no processo civil, é válida apenas até ser contestada. Isso ocorre porque a fotografia não garante a conformidade com o original (autenticidade) e, por razões maiores, não é considerada uma prova suficiente em processos criminais, a menos que seja submetida a um exame pericial conforme estabelecido pelo art. 158 do Código de Processo Penal.

Além disso, enfrentamos desafios advindos da crescente complexidade da microinformática moderna. Atualmente, é possível apagar remotamente o conteúdo de dispositivos eletrônicos, sem a necessidade de conhecimentos técnicos avançados, desde que esses dispositivos estejam conectados à internet. É possível, ainda, ativar criptografia que os torna praticamente inacessíveis para as autoridades públicas, mesmo quando estão equipadas com técnicas de análise avançadas e grande capacidade computacional. Esses cenários complexos demonstram que a preservação das informações digitais, sua autenticidade e integridade, requer uma abordagem mais cuidadosa e técnica do que muitas vezes é observada na prática forense. A compreensão da tecnologia, bem como a aplicação de metodologias apropriadas para coleta, análise e apresentação das provas digitais, é fundamental para garantir que a evidência seja confiável e aceitável em um contexto legal.

Essas situações são mencionadas apenas como exemplos, uma vez que as possibilidades e os desafios relacionados à atividade pericial são numerosos e requerem um estudo técnico mais aprofundado no campo da informática. Porém, mesmo nesses exemplos, é possível inferir que a produção de prova digital não se alinha com os métodos tradicionais de busca usados em outros tipos de crimes. Portanto, negligenciar a abordagem técnica pode comprometer a autenticidade e a integridade das informações que são relevantes como prova.

A questão central reside em que não há uma única técnica universal para o exame pericial de uma variedade de dispositivos com suas próprias características. Apesar disso, independentemente das técnicas empregadas, é papel tanto do julgador quanto das partes garantir a autenticidade e a integridade das informações submetidas à análise pericial, controlando os métodos utilizados com esse fim.

A natureza mutável dos meios de armazenamento digitais, se não for adequadamente protegida por meios suficientes, pode expor o conteúdo com relevância probatória a adições, remoções e alterações, o que pode levar à conclusão de que o material apreendido não está relacionado ao proprietário do dispositivo ou à conta em um serviço *on-line* específico (falta de autenticidade), ou que o material original foi intencionalmente alterado, seja substancialmente a ponto de distorcer o contexto, ou de forma pontual, com a inclusão de informações falsas em um conjunto aparentemente autêntico, comprometendo assim sua força como prova por falta de integridade.

Independentemente da solução técnica usada em cada caso, tal precaução só terá valor se a posse do material for restrita a indivíduos confiáveis e imparciais em relação ao resultado da investigação. Isso deve ser documentado de forma precisa, complementado por testemunhas, quando necessário, e registrado o uso de lacres, transporte e armazenamento.

Em última análise, a prova digital não deve ser subestimada ou simplificada, e é crucial que tanto as partes envolvidas quanto os julgadores considerem a natureza complexa dos meios eletrônicos e adotem abordagens rigorosas para garantir que a integridade e a autenticidade das informações sejam mantidas. Isso é especialmente vital em procedimentos legais, onde a validade da prova digital pode ter um impacto significativo nos resultados do caso.

Um exame pericial bem conduzido pode fornecer subsídios para a formação da convicção do julgador, incluindo detalhes sobre a utilização do dispositivo e sua localização geográfica.

Entretanto, a prova pericial não exclui o papel do julgador no entendimento dos métodos de investigação e na validação da prova. Tanto as partes quanto o juiz devem assegurar diretamente, com ou sem auxílio pericial, a validade da prova digital, garantindo que os atributos de autenticidade e integridade sejam mantidos desde a coleta até a avaliação.

3 CONCLUSÃO

Pela exposição contida nos tópicos precedentes, pretendeu-se demonstrar que a tecnologia abriu caminho, antes mesmo da disciplina legislativa, para a atividade probatória em meio eletrônico, considerando que a prova é um dos grandes pontos de contato entre o processo e a realidade exterior, cuja evolução necessariamente acompanha.

Essa antecipação foi possível porque, a despeito das peculiaridades do suporte digital, as informações armazenadas em meio eletrônico guardam com os documentos, em sentido amplo, identidade de conteúdos e finalidades. O suporte digital, por si só, permite a alteração irrestrita e indetectável das informações nele armazenadas, mas, paradoxalmente, oferece, na presença de determinadas cautelas, garantias de autenticidade e integridade superiores às que o suporte físico jamais foi capaz de propiciar.

Essa contradição enseja a oscilação da doutrina e da prática forense entre extremos, desde a absoluta desconfiança e prevenção em relação ao meio, até a confiança excessiva, desatenta aos atributos de cada específica fonte de prova. A proposição que se extrai dessas

premissas é de que a produção de prova digital depende, quando indisponíveis os direitos em litígio, inclusive no processo criminal, ou quando impugnada a reprodução, de escorreita demonstração de autenticidade e integridade, a ser assegurada por meios técnicos adequados, sob pena de o elemento de prova obtido de fonte digital não carregar eficácia probatória.

Tais meios não se restringem à previsão legal de assinatura digital de documentos eletrônicos, com o uso de certificado emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, mas alcançam também quaisquer outros mecanismos que, pelo uso adequado da tecnologia, possam garantir, ainda que parcialmente, os mesmos atributos; excluídos, porém, os esforços que nada garantem quanto à autenticidade e à integridade e se relacionam ao desconhecimento da prova digital, como a reprodução digitalizada de assinaturas manuscritas em documentos eletrônicos.

No específico caso dos extratos digitais de bancos de dados, além da atenção à formação do seu conteúdo na origem, a garantia de autenticidade e integridade depende de procedimento documentado de extração, que pode ser atestado pelo emitente, sob pena de responsabilidade civil e criminal, ou fiscalizado por delegado do serviço notarial, em ata própria; não se admitindo, contudo, imagens digitais coligidas sem nenhuma explicação, cuidado ou segurança, como tem sido recorrente na prática forense.

Por fim, em relação à fonte de prova que não escape à necessidade da técnica pericial para a sua produção, de que se destacam os materiais apreendidos no curso de investigação, é inafastável o controle jurisdicional da atividade do perito, de modo a garantir a autenticidade e a integridade, pela supervisão da técnica empregada e pela observação da cadeia de custódia, a fim de que o manejo do material com fins probatórios seja reservado a pessoas idôneas e desinteressadas no resultado da prova.

REFERÊNCIAS

ARAUJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. **Curso de direito constitucional**. 12. ed. São Paulo: Editora Saraiva, 2008.

BICALHO, Camila Fernandes; MIRANDA, Felipe Augusto Ribeiro de. O caso Anderson Torres e a admissão da prova digital no processo penal. **Consultor Jurídico**, São Paulo, 10 fev. 2023. Disponível em: https://www.conjur.com.br/2023-fev-10/bicalho-miranda-admissao-prova-digital-processo-penal. Acesso em: 10 fev. 2023.

BRASIL. **Decreto-Lei n. 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro: Presidência da República, 1941. Disponível em: http://bit.ly/30xq6z6. Acesso em: 27 set. 2019.

BRASIL. **Emenda Constitucional n. 32, de 11 de setembro de 2001**. Altera dispositivos dos arts. 48, 57, 61, 62, 64, 66, 84, 88 e 246 da Constituição Federal, e dá outras providências. Brasília, DF: Presidência da República, 2001a. Disponível em: http://bit.ly/2ud8LPS. Acesso em: 27 set. 2019.

BRASIL. **Lei n. 5.869, de 11 de janeiro de 1973**. Institui o Código de Processo Civil. Brasília, DF: Presidência da República, 1973. Disponível em: http://bit.ly/2RpgtP7. Acesso em: 27 set. 2019.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://bit.ly/2R70Vkd. Acesso em: 27 set. 2019.

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://bit.ly/389l1jk. Acesso em: 27 set. 2019.

BRASIL. **Lei n. 11.419, de 19 de dezembro de 2006**. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF: Presidência da República, 2006. Disponível em: http://bit.ly/38lABIN. Acesso em: 27 set. 2019.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://bit.ly/2Nz5KAA. Acesso em: 27 set. 2019.

BRASIL. **Lei n. 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: http://bit.ly/3738LR7. Acesso em: 27 set. 2019.

BRASIL. **Medida provisória n. 2.200-2, de 24 de agosto de 2001**. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF: Presidência da República, 2001b. Disponível em: http://bit.ly/2RuS5eG. Acesso em: 27 set. 2019.

BUENO, Cassio Scarpinella. **Curso sistematizado de direito processual civil**. 3. ed. São Paulo: Saraiva, 2010, v. 2, t. 1.

CABRAL, Antonio do Passo. A eficácia probatória das mensagens eletrônicas. **Revista de Processo**, São Paulo, v. 31, n. 135, p. 97-131, 2006.

CASEY, Eoghan. **Digital evidence and computer crime**: forensic science, computers and the internet: forensic science, computers and the internet. 3rd ed. New York: Elsevier, 2011.

CONHEÇA os Tribunais de Internet da China. **JuLaw**, [*s. l.*], 2021. Disponível em: https://julaw.ao/conheca-os-tribunais-de-internet-da-china/. Acesso em: 7 set. 2023.

CONSELHO DA UNIÃO EUROPEIA. Parlamento Europeu. **Directiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à protecção jurídica das bases de dados**. Estrasburgo: CUE, 1996. Disponível em: http://bit.ly/2uUBJ7C. Acesso em: 27 set. 2019.

COUNCIL OF EUROPE. **Convention on cybercrime**: ETS No. 185. Estrasburgo: Council of Europe, 2001. Disponível em: http://bit.ly/38iC7eF. Acesso em: 27 set. 2019.

DIAS FILHO, Claudemir Rodrigues. Cadeia de custódia: do local de crime ao trânsito em julgado; do vestígio à evidência. *In*: MOURA, Maria Thereza Rocha de Assis; NUCCI, Guilherme de Souza (org.). **Doutrinas essenciais** – processo penal. São Paulo: RT, 2012. v. 3. p. 404.

DIDIER JUNIOR, Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. **Curso de direito processual civil**. 11. ed. Salvador: Juspodivm, 2016, v. 2.

DIDIER JUNIOR, Fredie. **Curso de processo civil**: teoria geral do processo e processo de conhecimento. Salvador: Editora JusPodivm, 2009. v. 1.

DINAMARCO, Cândido Rangel. **Instituições de direito processual civil**. 9. ed. rev. e atual. São Paulo: Malheiros, 2017, v. 3.

EASTTOM, Chuck. **Digital Forensics, investigation and response**. Burlington, MA: Jones & Bartlett Learning, 2016.

EDINGER, Carlos. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 24, n. 120, p. 237-257, maio/jun. 2016.

FRIEDEN, Jonathan D.; MURRAY, Leigh M. The admissibility of electronic evidence under the Federal Rules of Evidence. **Richmond Journal of Law and Technology**, Richmond, v. 17, n. 2, p. 1-40, 2011.

GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). *In*: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (coord.). **Estudos em homenagem à professora Ada Pellegrini Grinover**. São Paulo: DPJ, 2005. p. 303-318.

GONÇALVES, Marcus Vinicius Rios. **Direito processual civil esquematizado**. São Paulo: Saraiva, 2011.

GOODE, Steven. The admissibility of electronic evidence. **The Review of Litigation**, Austin, v. 29, n. 1, p. 1-64, 2009.

ITÁLIA. **Decreto del Presidente dela Repubblica 22 settembre 1988, n. 447**. Approvazione del codice di procedura penale. Roma:

Normattiva, 1988. Disponível em: http://bit.ly/30xJz32. Acesso em: 27 set. 2019.

LOPES JÚNIOR, Aury. **Direito processual penal**. 14. ed. São Paulo: Saraiva, 2017.

MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. **Revista de Direito Imobiliário**, São Paulo, v. 22, n. 47, p. 70-101, 1999.

MARCACINI, Augusto Tavares Rosa. Provas digitais: limites constitucionais e o Marco Civil da Internet. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). **Direito & internet III**: Marco civil da internet, Lei n. 12.965/2014. São Paulo: Quartier Latin, 2015. v. 2. p. 455-473.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Prova**. 2. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2011.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Código de processo civil comentado**. 3. ed. rev. atual e ampl. São Paulo: Revista dos Tribunais, 2011.

NEVES, Daniel Amorim Assumpção. Da produção da prova documental (arts. 434 a 438). *In*: CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). **Comentários ao novo código de processo civil**. 2. ed. rev. atual e ampl. Rio de Janeiro: Forense, 2016. p. 633-636.

PACELLI, Eugênio; FISCHER, Douglas. **Comentários ao código de processo penal e sua jurisprudência**. São Paulo: Atlas, 2020.

RAMOS, Armando Dias. **A prova digital em processo penal**: o correio eletrônico. Lisboa: Chiado, 2014.

RASHBAUM, Kenneth N.; KNOUFF, Matthew F.; MURRAY, Dominique. Admissibility of non-U.S. electronic evidence. **Richmond Journal of Law and Technology**, Richmond, v. 18, n. 3, p. 1-76, 2012.

RINALDI, Luciano. Dos documentos eletrônicos (arts. 439 a 441). *In*: CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). **Comentários ao novo código de processo civil**. 2. ed. rev. atual e ampl. Rio de Janeiro: Forense, 2016. p. 329-334.

SANTOS, Manoel J. Pereira dos. Considerações iniciais sobre a proteção jurídica das bases de dados. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). **Direito & internet**: aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005. v. 1. p. 123-124.

SANTOS, Moacyr Amaral. **Prova Judiciária no cível e comercial**. 3. ed. São Paulo: Max Limonad, 1966-1968, v. 1.

SILVA, Virgílio Afonso da. **A constitucionalização do direito**: os direitos fundamentais nas relações entre particulares. 1. ed. 2. tir. São Paulo: Malheiros, 2008.

UNITED STATES. Attorney's Office. **FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown**. Southern District of California: USAO, 8 June 2021. Disponível em: https://www.justice.gov/usao-sdca/pr/fbi-s-

encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive. Acesso em: 21 ago. 2023.