O PANORAMA DA CADEIA DE CUSTÓDIA E SUA IMPLICAÇÃO NA VALORAÇÃO DA PROVA DIGITAL NO PROCESSO CIVIL

THE PANORAMA OF CHAIN OF CUSTODY AND ITS IMPLICATIONS FOR THE VALUATION OF DIGITAL EVIDENCE IN CIVIL PROCEEDINGS

Adriana Vieira da Costa [1]

RESUMO

A transição das interações sociais para o ambiente virtual, aliada à crescente adaptação dos profissionais do Direito às novas tecnologias, tem provocado uma rápida mudança no paradigma tradicional da prova documental, que perdurou por séculos. Essa transformação envolve a troca dos documentos em papel pelos eletrônicos ou digitais para o registro de informações juridicamente relevantes. A adoção desta nova forma de prova, conhecida como prova digital, tem gerado um fervoroso debate entre doutrinadores e juristas, especialmente devido à notável instabilidade dos dados armazenados de maneira eletrônica ou digital. A certeza de que a prova digital reproduz fielmente o fato que se deseja evidenciar está vinculada à demonstração de seus requisitos intrínsecos de autenticidade e integridade, além da consideração de seu requisito extrínseco, conhecido como cadeia de custódia. Tal instituto está intricada e composta, especialmente quando analisada dentro do âmbito do "acesso e desenvolvimento da justiça". Essa cadeia de custódia é crucial para garantir a integridade e a autenticidade das provas digitais; no entanto, sua relevância ultrapassa a mera admissibilidade, afetando a avaliação das evidências e, por conseguinte, o acesso e o progresso da justiça. O objetivo do presente artigo é analisar qual a consequência jurídico-processual da inobservância da cadeia de custódia da prova digital no processo civil. Por meio de pesquisa bibliográfica e documental procurou-se responder se a prova digital obtida sem observância da cadeia de custódia deverá ser inadmitida ou considerada nula no processo civil. Diferentemente do processo penal, no qual a cadeia de custódia é considerada um requisito legal de admissibilidade da prova digital, cuja inobservância acarreta a sua exclusão do processo criminal, no processo civil esse requisito extrínseco não impede a análise da sua autenticidade e integridade de acordo com as regras de distribuição dinâmica do ônus probatório. Conclui-se que não há, no processo civil, o mesmo rigor técnico-científico do processo penal, podendo o juiz, diante da prova digital produzida pelas partes, ainda que sem o respeito aos aspectos técnicos da cadeia de custódia, valorá-la considerando

[1] Doutora em Direito no Centro Universitário de Brasília (UNICEUB). mestrado em Direito Processual e Cidadania pela Universidade Paranaense (UNIPAR). Pós-Graduada em Direito Constitucional (FARO) e Pós-Graduada em Direito Processual Civil (FARO). Pós-Graduada em Metodologia no Ensino Superior (ULBRA). Pesquisadora do Jus Gentium - Grupo de Estudos e Pesquisas em Direito Internacional. Pesquisadora Grupo de Estudo em Processos Socioambientais Na Amazônia-GEPSA com o projeto ATUAÇÃO DOS STAKEHOLDERS EM PROCESSOS JUDICIAIS POR CRIMES AMBIENTAIS EM RONDÔNIA: Análise das decisões pautadas no desmatamento ilegal. Professora do magistério superior da Universidade Federal de Rondônia. atuando principalmente nos seguintes temas: Direito Processual Civil e ambiental, desenvolvimento sustentável e solução de conflitos. E-mail: adriana.vieira@unir.br

outros elementos constantes nos autos e, a partir deles, atribuir a confiabilidade e credibilidade que ela merece.

PALAVRAS-CHAVE: Direito Processual Civil; prova digital; cadeia de custódia; requisito de valoração da prova.

ABSTRACT
The transition of social interactions to the virtual environment, coupled with the growing adaptation of legal professionals to new technologies, has led to a rapid change in the traditional paradigm of documentary evidence, which has lasted for centuries. This transformation involves the exchange of paper documents for electronic or digital ones to record legally relevant information. The adoption of this new form of evidence, known as digital evidence, has generated fervent debate among scholars and jurists, especially due to the remarkable instability of data stored electronically or digitally. The certainty that digital evidence faithfully reproduces the fact it is intended to prove is linked to the demonstration of its intrinsic requirements of authenticity and integrity, as well as the consideration of its extrinsic requirement, known as chain of custody. This institute is intricate and composite, especially when analyzed within the framework of “access to and development of justice”. This chain of custody is crucial to guaranteeing the integrity and authenticity of digital evidence; however, its relevance goes beyond mere admissibility, affecting the evaluation of evidence and, consequently, access to and progress of justice. The aim of this article is to analyze the legal and procedural consequences of non-compliance with the chain of custody of digital evidence in civil proceedings. Through bibliographical and documentary research, we sought to answer whether digital evidence obtained without observing the chain of custody should be inadmissible or considered null and void in civil proceedings. Unlike criminal proceedings, in which the chain of custody is considered a legal requirement for the admissibility of digital evidence, the non-observance of which results in its exclusion from criminal proceedings, in civil proceedings this extrinsic requirement does not prevent the analysis of its authenticity and integrity in accordance with the rules of dynamic distribution of the burden of proof. It can be concluded that in civil proceedings there is not the same technical-scientific rigor as in criminal proceedings, and the judge, faced with digital evidence produced by the parties, even without respecting the technical aspects of the chain of custody, can value it by considering other elements in the case file and, based on them, attribute the reliability and credibility it deserves.

KEYWORDS: Civil Procedural Law; digital evidence; chain of custody; evidence assessment requirement

INTRODUÇÃO

Desde 2010, segundo Schwab (2016), vivemos a 4ª Revolução Industrial, caracterizada, principalmente, pela rápida evolução tecnológica, pela massificação da internet e pelo crescente movimento social de hiperconexão das pessoas e virtualização da realidade nesse *ciberespaço* (LÉVY, 1999), criando o que se denominou de *cibercultura* (LÉVY, 1999), expressão cunhada para descrever como a transferência das iterações pessoais, do intercâmbio de conhecimentos e da disseminação de informações para o meio digital acarretou profundas transformações econômicas, políticas, jurídicas e, principalmente, sociais. Desse fenômeno social surgiu a chamada Sociedade Digital.

É neste *ciberespaço* (LÉVY, 1999) não sujeito a limites geográficos e temporais onde os fatos jurídicos vêm ocorrendo com maior frequência, não raras vezes de forma fluída e fugaz como no mundo líquido preconizado por Bauman (2001), tornando-os não apenas altamente permeáveis à sociedade, mas, ao mesmo tempo, extremamente efêmeros e voláteis, podendo mudar ou se perder num piscar de olhos ou no tráfego de um *byte*.

Apesar dos alertas de Deleuze (1992, p. 219-226) e Bauman (2014) sobre os perigos advindos da Sociedade Digital, as pessoas vêm aceitando, inconscientemente, todo tipo de controle e vigilância ao renunciarem à sua privacidade e intimidade em detrimento da comodidade oferecida pela tecnologia, aplicações e serviços conectados de alguma maneira à internet.

Se a tecnologia afeta de maneira significativa a vida das pessoas, suas relações interpessoais e estamos indissociavelmente sujeitos a ela, o Direito, como criação imanente à sociedade, jamais sairia incólume dos recorrentes processos de metamorfose social. Ao contrário, é necessário que ele se adapte a cada nova realidade criada a partir da ruptura do paradigma anterior e o Estado, como detentor do monopólio das atividades legislativas e jurisdicionais, proveja os meios adequados para a solução dos novos conflitos que advierem dessas transformações sociais.

A velocidade cada vez maior com que essas mudanças ocorrem, contudo, torna praticamente impossível o cumprimento da missão estatal.

Segundo Pinheiro (2021, p. 73), na sociedade convergente os conceitos de espaço e tempo ganharam outra dimensão e a atividade legislativa não consegue acompanhar o ritmo da evolução tecnológica, tendendo assim a disciplina jurídica à autorregulamentação pelos próprios participantes para que o Direito siga a sua vocação de refletir as grandes mudanças culturais e comportamentais da sociedade.

A estratificação da legislação acaba por conferir ao Judiciário a função de romper com antigos paradigmas interpretativos baseados em arquétipos ultrapassados e desalinhados ao novo modelo social para conferir aos novos litígios latentes à sociedade uma solução mais consentânea com a atual realidade e, assim, promover a efetiva pacificação social.

No direito processual contemporâneo, sobretudo a partir do advento da Medida Provisória nº 2.200/2001, que instituiu a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil e passou a reconhecer a autenticidade, integridade e validade dos documentos eletrônicos produzidos utilizando o processo de certificação nela especificado, e da Lei nº 11.419/2006, que instituiu o Processo Judicial Eletrônico e autorizou a prática de atos processuais, a comunicação, o tráfego e o armazenamento de documentos e arquivos em formato digital, vem se observando, ao longo das últimas duas décadas, um gradual e irreversível movimento de substituição dos documentos em papel pelos eletrônicos ou digitais para registro de fatos juridicamente relevantes.

Desde então, a crescente familiarização dos profissionais do Direito com a tecnologia onipresente na sociedade atual e a migração, cada vez maior, das relações sociojurídicas para o ambiente virtual acarretaram um aumento significativo na utilização de informações produzidas, armazenadas ou obtidas eletrônica e digitalmente como meio de prova de fatos que, frequentemente, interessam aos processos.

Esse fenômeno foi responsável por um rápido movimento de ruptura do paradigma probatório anterior, com a substituição do documento em papel, como prova pré-constituída apta a perpetuar, sem propensões subjetivas, a memória dos fatos jurídicos (PINHEIRO, 2021, p. 261), pelos eletrônicos e digitais, muito embora sem a devida atenção às características técnicas e riscos envolvidos, a ponto de Pinheiro (2021, p. 262) propor o tratamento dessa nova espécie de prova em três níveis: cultural, com a quebra do paradigma social, dos usos e

costumes até hoje aceitos como dogmas; técnico, definindo-se o melhor procedimento para tratá-los; e jurídico, para garantir a sua validade como meio de prova.

Se “as provas são os meios processuais ou materiais considerados idôneos pelo ordenamento jurídico para demonstrar a verdade, ou não, da existência e verificação de um fato jurídico” (NERY JUNIOR, 1997, p. 611) e são, “ao mesmo tempo, meio, resultado e atividade” (ALVIM, 2017, p. 830), quanto mais completas, precisas e fidedignas forem, maior será a confiabilidade conferida pelo ordenamento jurídico.

Todo e qualquer novo meio de prova, portanto, pela sua própria natureza e finalidade, deve ser adequadamente disciplinado à nova realidade sociojurídica a fim de assegurar a realização de um processo justo, por se tratar de “um dos mais respeitados postulados inerentes à garantia política do devido processo legal” e “um dos fundamentais pilares do sistema processual contemporâneo” (DINAMARCO, 2017, p. 51).

A partir desse novo modelo probatório que ora se apresenta, diversos doutrinadores vêm buscando conceituar o que se convencionou chamar de prova digital, definir sua natureza jurídica e seus requisitos de admissibilidade e validade no processo.

Como assegurar que a prova digital apresentada no processo corresponda exatamente ao fato que por meio dela se pretende provar se os dados e metadados aquele sobre a qual foi construída podem ser facilmente alterados, adulterados, suprimidos, inseridos e/ou corrompidos, ainda que a espoliação seja involuntária? Sem um sistema técnico-científico-informacional que garanta a sua idoneidade, como considerá-la válida e eficaz a influenciar no convencimento do juiz?

Recentemente, a Quinta Turma do Superior Tribunal de Justiça, no julgamento do Agravo Regimental no *Habeas Corpus* nº 828.054-RN, decidiu ser inadmissível no processo penal a prova digital obtida com quebra da cadeia de custódia.

Essa decisão ocasionou diversas discussões na comunidade jurídica acerca da aplicação da referida *ratio decidendi* no processo civil e como deve ser analisada a cadeia de custódia nas ações de natureza não-penal, evidenciando a importância do tema do presente artigo.

O objetivo do presente artigo é analisar qual a consequência jurídico-processual da inobservância da cadeia de custódia da prova digital no processo civil. A quebra da cadeia de custódia da prova digital no processo civil acarreta a sua inadmissibilidade ou a sua nulidade?

Buscar-se-á, ao final, propor uma interpretação e aplicação do ordenamento jurídico vigente à cadeia de custódia da prova digital em harmonia com os princípios que regem o processo civil serão capazes de implicarem diretamente no desenvolvimento da justiça.

1 CONCEITO E NATUREZA JURÍDICA DA PROVA DIGITAL

Prova é um vocábulo polissêmico empregado, comumente, para indicar algo que possa servir ao convencimento de outrem.

No Direito, a palavra prova é plurissignificante e pode se referir ao fato que se pretende reconstituir, à atividade probatória em si, ao meio de prova utilizado, ao procedimento de produção e impugnação, ao resultado do procedimento probatório ou ao seu efeito na convicção do julgador.

Toda prova origina-se de uma fonte externa, preexistente ou contemporânea ao processo, de onde podem ser obtidas informações relevantes a comprovar a veracidade das alegações deduzidas pelas partes (p. ex. documento, pessoa, laudo técnico etc.).

As fontes de prova são classificadas em reais, nas quais o registro dos fatos e informações ocorre em suportes físicos (p. ex. prova documental e pericial), e pessoais, nas quais o registro dos fatos e informações se dá na memória das pessoas (p. ex. depoimento pessoal e prova testemunhal).

O Código de Processo Civil vigente estabeleceu, em linhas gerais, a produção, comunicação, armazenamento, validação e registro dos atos processuais eletrônicos e digitais (art. 193, CPC), definiu os requisitos de autenticidade, integridade, temporalidade, não repúdio, conservação e confidencialidade do registro do ato eletrônico (arts. 195 e 411, II, CPC), autorizou a gravação digital das audiências (art. 367, § 5º, CPC), o fornecimento de documentos por meio eletrônico (art. 438, § 2º, CPC) e a prática eletrônica de atos executivos (arts. 837, 854, 879, CPC), equiparou as reproduções digitalizadas de documentos em suporte físico e os extratos digitais de bancos

de dados públicos e privados aos seus originais (art. 425, V e VI, CPC) e disciplinou, superficialmente, a conversão, admissão e valor probante dos documentos eletrônicos (art. 439 a 441, CPC).

No arcabouço normativo vigente, a compreensão da prova digital passa, necessariamente, pela revisitação ao tradicional conceito de documento e pela dissociação do que ele representa juridicamente do seu substrato físico tangível, de maneira que a generalização conceitual possa abranger todos os registros das relações sociais e dos fatos ocorridos em ambiente eletrônico ou digital.

Wambier et al. (2005, p. 461) define documento como “todo objeto capaz de cristalizar um fato transeunte, tornando-o, sob certo aspecto, permanente”, pouco importando o suporte material que é utilizado, pois “para caracterizar documento basta a existência de uma coisa (inanimada) que traga em si caracteres suficientes para atestar o que ocorreu”.

O art. 4º, II, da Lei de Acesso à Informação (Lei nº 12.527/2011) define documento como a “unidade de registro de informações, qualquer que seja o suporte ou formato” e o art. 425, V, do CPC, ao tratar “os extratos digitais de bancos de dados públicos e privados”, os considera espécie de documento, ambos abrangendo a definição conceitual acima proposta pelo autor.

O Supremo Tribunal Federal, no julgamento do Recurso Ordinário em *Habeas Corpus* nº 95.689-SP, de relatoria do Ministro Eros Grau, já reconhecera que o termo “documento” não se restringia apenas “a qualquer escrito ou papel”, conforme se extrai da ementa abaixo transcrita:

> RECURSO ORDINÁRIO EM HABEAS CORPUS. PENAL. ABUSO DE PODER. REVOGAÇÃO DO ART. 350 DO CÓDIGO PENAL PELA LEI N. 4.895/65. INOCORRÊNCIA. CONFLITO APARENTE DE NORMAS. SOLUÇÃO. PRETENSÃO DE QUE O TERMO "DOCUMENTO" SE REFIRA A "QUALQUER ESCRITO OU PAPEL". IMPROCEDÊNCIA: CONCEITO ABRANGENTE. 1. a Lei n. 4.989/65 não revogou o artigo 350 do Código Penal. Há, na verdade, aparente conflito de normas, solucionado pela generalidade presente no artigo 350, parágrafo único, inciso IV do Código Penal, a abranger a conduta do paciente; conduta que não se enquadra em nenhum dos incisos dos artigos 3º e 4º da Lei n. 4.898/65. 2. O termo "documento" não se restringe "a qualquer escrito ou papel". O legislador do novo Código Civil, atento aos avanços atuais, conferiu-lhe maior amplitude, ao dispor, no art. 225 que "[a]s 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". Ordem denegada.

Neste sentido, podemos distinguir e definir três tipos de documentos: a) físico – documento produzido em algum suporte físico (p. ex. pedra, papel, tecido etc.) que permite o registro e acesso às informações através da interpretação dos signos nele gravados (p. ex. palavras, textos, desenhos, mapas, idioma etc.); b) eletrônico – documento produzido, acessado e interpretado por meio de um dispositivo eletrônico, cujos registros são codificados de forma analógica ou em dígitos binários e c) digital – documento produzido por meio de um dispositivo eletrônico e codificado exclusivamente em dígitos binários, cujos registros são acessados e interpretados apenas através de um programa ou sistema computacional.

Atualmente, portanto, a prova digital tem natureza jurídica de documento, no qual as informações sobre fatos juridicamente relevantes foram registradas em suportes físicos eletrônicos e codificados em formato analógico ou dígitos binários.

O PL nº 4.939/2020, que tramita no Congresso Nacional e "dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências", propõe a tipificação autônoma desse meio de prova, definindo-a como "toda informação armazenada ou transmitida em meio eletrônico que tenha valor probatório".

A proposta legislativa vai ao encontro do que pensam Thamay e Tamer (2020, p. 33) ao conceituarem prova digital como "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 a sua demonstração", que tem dupla finalidade: a) demonstrar um fato ocorrido no meio digital propriamente dito, denominado prova nato-digital no PL nº 4.939/2020 (p. ex. envio de um *e-mail* ou de uma mensagem por aplicativo de mensageria, postagem em rede social, disponibilização ou compartilhamento de vídeos na internet etc.) e b) demonstrar a existência ou não de um fato ocorrido fora do meio digital por intermédio de suportes digitais, denominado prova digitalizada no PL nº 4.939/2020 (p. ex. digitalização de documento físico, conversão de gravação e fotos analógicas em digitais etc.).

Na mesma linha é a definição proposta no *Electronic crime scene investigation: a guide for first responders, second edition*, publicado em 2008 pelo *U.S. Department of Justice, Office of Justice Programs, National Institute of Justice*, que considera prova digital todas as "informações e dados de valor para uma investigação que são armazenados, recebidos ou transmitidos por um dispositivo eletrônico" (tradução livre).

Segundo o PL nº 4.939/2020 e com embasamento na NBR/ISO 27037:2013 publicada pela Associação Brasileira de Normas Técnicas (ABNT), são consideradas fontes de prova eletrônicas e digitais quaisquer dispositivos eletrônicos, sistemas informáticos e redes de dados que coletem, processem, armazenem ou transmitam dados e/ou informações geradas originalmente em formato digital ou, se registradas em suporte analógico ou físico, sejam digitalizadas.

Compreende, portanto, todos os registros analógicos e/ou digitais existentes em suportes eletrônicos tangíveis (p. ex. computadores pessoais, discos rígidos, *smartphones*, *smartwatches*, *tablets*, câmeras etc.) e em suportes eletrônicos intangíveis ao usuário, a exemplo dos dados armazenados em serviços de computação em nuvem (p. ex. *iCloud*, *Google Drive*, *Dropbox*, *Onedrive* etc.), *sites*, páginas na *web* e aplicações de internet (redes sociais, aplicativos, plataformas etc.), a partir dos quais podem ser obtidas as provas.

Nesse segundo contexto teórico, a prova digital enquadrar-se-ia, atualmente, na categoria de meios moralmente legítimos, pois não possui regramento próprio, mas, com eventual aprovação do PL nº 4.939/2020, ganharia tipificação e autonomia em relação aos demais meios de prova.

Independentemente da corrente teórica que se adote, a prova digital abarca toda e qualquer informação produzida, armazenada ou transmitida em meio eletrônico ou digital, ainda que o fato tenha ocorrido no mundo real.

O que distingue, então, as várias fontes de prova reais é o suporte físico onde os fatos são registrados. Num passado não muito distante, o papel era o protagonista. Atualmente, ele cedeu lugar aos dispositivos eletrônicos e digitais.

2 AUTENTICIDADE E INTEGRIDADE DA PROVA DIGITAL

A prova digital, em razão da volatilidade intrínseca do próprio meio ambiente em que é produzida, deve conter certos requisitos que permitam ao julgador aferir a sua idoneidade. Esses requisitos foram definidos pela doutrina como autenticidade e integridade.

Thamay e Tamer (2020, p. 39) lecionam que a autenticidade e a integridade são pressupostos da prova digital.

Yamada (2022, p. 135) afirma que:

> Pede-se vênia para discordar dos referidos autores acerca da natureza jurídica desses atributos, pois se um fato ocorrido no mundo real ou no ambiente digital preenche as características necessárias à incidência de uma norma jurídica e se torna, assim, um fato jurídico, ingressando no plano da existência, a perquirição acerca da validade ou invalidade da utilização dos registros eletrônicos e digitais para fins probatórios no processo diz respeito aos requisitos que a prova digital deve satisfazer para alcançar os efeitos pretendidos.

Autenticidade, segundo a Lei de Acesso à Informação, é a "qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema" (art. 4º, VII, Lei nº 12.527/2011).

Segundo Yamada (2022, p. 136), "podemos decompor a autenticidade dos documentos eletrônicos e digitais em dois elementos, um objetivo, relativo à sua origem, e outro subjetivo, relacionado à identificação do(s) sujeito(s) envolvido(s)".

Casey afirma que (2011, p. 60):

> Para demonstrar que a prova digital é autêntica, geralmente é necessário convencer o tribunal de que ela foi obtida de um computador e/ou localização específicos, que foi extraída uma cópia completa e exata da prova digital e que ela permaneceu inalterada desde que foi coletada. Em alguns casos, também pode ser necessário demonstrar que informações específicas são precisas, como datas associadas a um arquivo específico que é importante para o caso. A confiabilidade da prova digital claramente desempenha um papel crítico no processo de autenticação, conforme discutido em mais detalhes posteriormente neste capítulo. (tradução livre)

Prado (2019, p. 95) defende que a autenticidade corresponde à "lei da mesmidade", o "princípio pelo qual se determina que 'o mesmo' que se encontrou na cena [do crime] é o 'mesmo' que se está utilizando para tomar a decisão judicial".

Thamay e Tamer (2020, p. 40) tratam da autenticidade apenas em seu aspecto subjetivo, conceituando-a como a "qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital" e "que assegura que o autor aparente do fato é, com efeito, seu autor real".

A identificação da autoria de um fato ocorrido no ambiente digital é essencial para a comprovação dos sujeitos envolvidos na relação jurídico-subjetiva que por meio dele se pretende provar, pois serão as partes envolvidas, segundo a lei civil, os titulares do direito ou os destinatários das obrigações.

Não se pode olvidar, contudo, que a identificação precisa da fonte da prova digital é, de igual modo, essencial à garantia da sua autenticidade.

A prova digital será autêntica, portanto, se não houver dúvidas quanto à sua origem e aos sujeitos envolvidos no fato que por meio dela se pretende provar.

Integridade, segundo a Lei de Acesso à Informação, é a "qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino" (art. 4º, VIII, Lei nº 12.527/2011).

Thamay e Tamer (2020, p. 45) afirmam que uma prova digital é íntegra quando "isenta de qualquer modificação em seu estado ou adulteração desde o momento da realização do fato até apresentação do resultado da prova".

Segundo Yamada (2022, p. 147), são "elementos intrínsecos à integridade da prova digital a completude, imutabilidade, temporalidade e credibilidade".

Ainda conforme o autor (YAMADA, 2022, p. 147):

> A prova digital, para ser considerada íntegra, deve ser completa, integral, sem supressões, de maneira a espelhar a integralidade do fato jurídico que por meio dela se pretenda provar, afinal, deve ela, em tradução livre, "contar toda a história e não apenas uma perspectiva particular" (IETF, 2002, p. 4).

A integralidade ou completude da prova digital exige conhecimento acerca do ecossistema eletrônico ou digital onde a prova foi produzida, permitindo que a coleta e análise esteja a ele contextualizada de maneira a confirmar ou afastar a ocorrência de fraudes. Nas palavras de Prado (2019, p. 75):

> O conhecimento das fontes de prova pela defesa é fundamental, porque a experiência histórica que precede a expansão da estrutura trifásica de procedimento penal, adequada ao modelo acusatório, contabiliza a supressão de elementos informativos como estratégia das agências de repressão que fundam as suas investigações em práticas ilícitas.
> Não custa sublinhar que apenas inadvertidamente eventual autor de ilicitudes probatórias permitiria a chegada ao processo de traços das referidas ilicitudes.
> Por isso, o exame da legalidade da investigação criminal concentrado com exclusividade no material apresentado pelo acusador em juízo é, de regra, inócuo ou no mínimo insuficiente.

Adverte Prado (2019, p. 85) que a coleta de material insuficiente ou a criação de obstáculos ao acesso da defesa às fontes de prova implica grave violação à equidade processual, pois “defender-se o acusado fazendo uso exclusivo do material probatório selecionado pelo acusador é o sonho que todo inquisidor nutre relativamente à posição de seu adversário processual”.

A imutabilidade da prova digital corresponde à demonstração de que os registros extraídos do equipamento eletrônico, sistema informático ou rede de dados não sofreram nenhuma modificação desde o momento da coleta até sua apresentação em juízo. É, segundo a Agência da União Europeia para a Cibersegurança (ENISA, 2019, p.12), “a aptidão para demonstrar que nenhuma modificação, exclusão, acréscimo ou outras alterações ocorreram ou poderiam ter ocorrido” (tradução livre).

A temporalidade da prova digital é a demonstração, utilizando uma fonte idônea, confiável e rastreável, do dia e horário em que o fato ocorreu ou foi registrado digitalmente.

A credibilidade da prova digital, segundo Yamada (2022, p. 149):

> Sem que se perca o rigor técnico-científico, as informações obtidas a partir da extração de registros digitais deve ser compreensível e crível às partes e julgadores, isto é, em tradução livre, ‘facilmente inteligível e crível para um tribunal’ (IETF, 2002, p. 4) e ‘convincente quanto aos fatos que ela representa’ (ENISA, 2019, p. 13), de modo que ‘o juiz no processo judicial deve ser capaz de confiar nela como verdade’ (ENISA, 2019, p. 13).

A prova digital será considerada íntegra, portanto, se completa, indene de adulterações, contiver marcação temporal confiável e for inteligível às partes e ao julgador.

3 CADEIA DE CUSTÓDIA DA PROVA DIGITAL

O registro do caminho percorrido pela prova digital desde a sua obtenção até a sua apresentação no processo é de suma importância para assegurar a sua autenticidade e integridade. Esse processo técnico-científico foi denominado cadeia de custódia.

A cadeia de custódia pode ser definida como “o processo de preservação da integridade da prova digital” (ENISA, 2014, p. 7) (em tradução livre). Sua importância para o processo é tamanha que a União Europeia e o Conselho da Europa (2020, p. 14) estabelecem que “a pessoa encarregada de coletar as provas é responsável por manter a integridade do material recuperado e garantir a sua cadeia de custódia” (em tradução livre).

Thamay e Tamer (2020, p. 47) a definem como o processo de preservação da autenticidade e integridade da prova digital durante todas as etapas da sua produção, que vão “desde sua identificação, coleta, extração de resultados, até a apresentação no processo ou procedimento de destino”.

Casey ensina que (2011, p. 60):

> Cadeia de custódia e documentação da integridade são importantes para demonstrar a autenticidade da prova digital. A cadeia de custódia adequada demonstra que a prova digital foi adquirida a partir de um sistema e/ou local específico e que foi continuamente controlada desde que foi coletada. Assim, a documentação adequada da cadeia de custódia permite ao tribunal vincular a prova digital ao crime. Documentação incompleta pode resultar em confusão sobre onde a prova digital foi obtida e pode levantar dúvidas sobre a confiabilidade da prova digital. (tradução livre)

Segundo Yamada (2022, p. 150), ao contrário da autenticidade e da integridade, que são componentes intrínsecos da prova digital, a cadeia de custódia se apresenta como um atributo extrínseco, tendo como objetivo garantir a preservação dos demais requisitos.

Souza et al. (2023, p. 57) afirma que:

> Na legislação brasileira há pouco referência direta aos requisitos de uma prova obtida a partir da realidade, sobretudo em relação a provas digitais. Entretanto, podemos considerar os princípios da cadeia de custódia listados no artigo 158-A do CPP, que propõem etapas essenciais para a manutenção da autenticidade de prova, desde a sua origem até seu descarte.

Saad Netto et. al (2023, p. 271) define:

> Em sentido amplo, a locução *cadeia de custódia* corresponde ao conjunto das sucessivas etapas e procedimentos capazes de esclarecer como ocorreu a aquisição, a guarda e, por fim, a devolução ou o descarte do objeto submetido aos cuidados dos entes responsáveis por esse processo. Desse modo, uma vez estabelecida a *cadeia de custódia* de um determinado bem, seja físico ou digital, é possível verificar, por meio de um processo de rastreabilidade, tanto a lisura de suas sucessivas etapas quanto a própria origem ou a procedência desse bem.

A Associação Brasileira de Normas Técnicas, ao editar a norma técnica NBR ISO/IEC 27037:2013 para tratar do processo de identificação, coleta, aquisição e preservação de inúmeras provas digitais existentes, buscou contribuir para sua admissibilidade, confiabilidade e força probatória, instituindo uma padronização e o emprego de uma série de métodos práticos aceitos mundialmente para, através do registro da cadeia de custódia, demonstrar “a cronologia de movimento e do manuseio da potencial evidência digital” (ABNT, 2013, p. 11).

O manuseio inadequado das informações digitais, dada a sua volatilidade, pode expor os dados a adulterações, ainda que involuntárias, e colocar em xeque seu valor probante. Sobre o tema, adverte Jones (2023, p. 41):

> A tecnologia trouxe consigo novas formas de produção, armazenamento e transmissão de dados, o que torna necessário repensar os procedimentos tradicionais de cadeia de custódia. Enquanto as evidências físicas era relativamente tangíveis e fáceis de rastrear, as evidências digitais são voláteis e podem ser facilmente modificadas ou destruídas sem deixar rastros visíveis. Isso exige a adoção de práticas e ferramentas especializadas para garantir a autenticidade, a integridade e a confiabilidade dessas evidências.

A cadeia de custódia, à luz da legislação e da norma técnica acima mencionada, deve ser auditável, transparente, confiável e pública.

Segundo Yamada (2022, p. 151):

> A auditabilidade e transparência da cadeia de custódia significam dizer, em tradução livre, que a “apreensão, acesso, armazenamento ou transferência da prova digital ser totalmente documentada, preservada e disponibilizada para revisão por um terceiro independente que deve não apenas ser capaz de repetir essas ações, mas também obter o mesmo resultado” (EUROPEAN UNION AND COUNCIL OF EUROPE – CYBERCRIME@IPA, 2020, p. 14).

> Para a demonstração da cadeia de custódia é necessário, portanto, que todas as ações executadas durante o processo de identificação, coleta, aquisição e preservação da prova digital sejam documentadas e estejam disponíveis para avaliação das partes e, se for o caso, de um terceiro independente (perito), que, ao reproduzir os mesmos passos utilizando os mesmos procedimentos, métodos e instrumentos, obterá o mesmo resultado.
> Esses procedimentos, métodos e instrumentos utilizados durante o processo de produção da prova digital e registro da cadeia de custódia devem se mostrar tecnicamente justificáveis e confiáveis, o que significa dizer, em tradução livre, que "não deve haver nada sobre a maneira como as provas foram coletadas e posteriormente tratadas que possam lançar dúvidas sobre sua autenticidade ou veracidade" (EUROPEAN UNION AND COUNCIL OF EUROPE – CYBERCRIME@IPA, 2020, p. 13).
> Por fim, em regra, todos os processos (art. 93, IX, da CRFB), assim como os atos processuais, são públicos (art. 189, CPC), devendo a produção da prova digital ostentar essa mesma qualidade, salvo se os dados a que ela se refere forem, pela sua natureza privada ou íntima, sigilosos.
> A documentação e demonstração de toda a cadeia de custódia da prova digital é fundamental para não colocar em risco a autenticidade e integridade dos registros armazenados eletrônica e digitalmente.

A cadeia de custódia, portanto, é um procedimento técnico que visa a assegurar que as informações obtidas de uma fonte de prova eletrônica ou digital apresentadas como prova no processo correspondam exatamente àquelas coletadas pela autoridade policial ou pela própria parte.

3.1 Cadeia de custódia da prova digital no processo penal

No processo penal, a cadeia de custódia foi instituída pela Lei nº 13.964/2019, que incluiu o art. 158-A ao Código de Processo Penal e a definiu como "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

Segundo estabelece o art. 158-B do CPP, a cadeia de custódia compreende as seguintes etapas: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte.

Segundo Saad Netto et al. (2023, p. 254):

> Longe de representar uma burocratização processual da documentação histórica dos vestígios, o disciplinamento da cadeia de custódia pela referida lei representa um grande avanço para a efetividade de todo sistema de justiça criminal, posto que o instituto emerge como eficiente ferramenta para que os diversos destinatários da prova pericial possam verificar não somente a origem dos vestígios, por meio da sua rastreabilidade, mas, sobretudo, sua autenticidade e integridade, de forma a afastar o risco de eventuais erros judiciais.
> Todavia, em que pese o aperfeiçoamento e a modernização promovidos pela Lei n. 13.964/2019 na legislação processual pena brasileira, perdeu o legislador a oportunidade de disciplinar dois pontos relevantes para uma implementação mais completa do instituto da cadeia de custódia. Trata-se do não disciplinamento da custódia dos vestígios digitais e das consequências jurídicas da quebra ou não da observância do instituto, problema que repercute diretamente na análise judicial quanto à admissibilidade ou à valoração da prova pericial.

A positivação da cadeia de custódia no ordenamento jurídico trouxe consigo a obrigatoriedade de os órgãos de persecução penal sistematizarem os procedimentos e etapas previstos nos arts. 158-A e 158-B do CPP.

É, nas palavras de Saad Netto et al. (2023, p. 275):

> Em síntese, a cadeia de custódia pode ser compreendida como o conjunto de sucessivos procedimentos técnico, científicos e administrativos, instituídos pelos órgãos ou institutos de perícia criminal oficiais, com o objetivo de manter a preservação e a documentação cronológica dos vestígios relacionados a uma infração penal, desde seu reconhecimento até o seu descarte, com o intuito de permitir a identidade, a rastreabilidade, a integridade e a autenticidade dos vestígios.

A cadeia de custódia no processo penal, conforme ensinamentos de Prado (2019, p. 97), é regida pelos princípios da mesmidade e da desconfiança, os quais visam a "garantir o juízo mediante a redução dos riscos de erro judiciário, consistindo no fundamento lógico e epistemológico da 'cadeia de custódia das provas'.".

Segundo o Aury Lopes Junior (*apud* SAAD NETTO et al., 2023, p. 276-278), a mesmidade representa "a garantia de que a prova valorada é exatamente e integralmente aquela que foi colhida, correspondendo, portanto, 'a mesma'" e a desconfiança "consiste na exigência de que a prova (documentos, DNA, áudios etc.) deva ser 'acreditada', submetida a um procedimento que demonstre que tais objetos correspondem ao que a parte alega ser.".

A cadeia de custódia da prova tem expressa previsão legal e, no processo penal, constitui-se múnus público decorrente do devido processo legal criminal.

Saad Netto et al. (2023, p. 275) defende:

> Logo, conclui-se que, à luz da doutrina da criminalística e em observância ao princípio do devido processo legal, e seus corolários da ampla defesa e contraditório, e assim como o princípio da verdade real ou atingível e ao próprio direito à prova pericial, a cadeia de custódia deve alcançar todo e qualquer vestígio reconhecido e coletado ao longo da *persecutio criminis*, que tenha relação com a infração penal, objeto da investigação preliminar e/ou da jurisdição penal, sujeitando-se, portanto, ao controle estatal quanto a sua integridade, idoneidade e mesmidade, sob pena de prejudicar a efetividade da justiça penal.

Jones (2023, p. 42) nos alerta de um ponto significativo a ser considerado é a privacidade e a proteção dos dados. A tecnologia tornou viável a coleta em larga escala de informações pessoais, o que pode impactar a privacidade das pessoas envolvidas em um processo. É essencial assegurar que a coleta e o uso de evidências digitais mantenham o respeito aos direitos individuais e estejam alinhados às leis e normas de proteção de dados que estão em vigor.

A Quinta Turma do Superior Tribunal de Justiça, no julgamento do Agravo Regimental no *Habeas Corpus* nº 828.054 – RN, de relatoria do Ministro Joel Ilan Paciornik, reconheceu a inadmissibilidade da prova digital obtida com quebra da cadeia de custódia em acórdão assim ementado:

> PROCESSUAL PENAL. AGRAVO REGIMENTAL NO HABEAS CORPUS. TRÁFICO DE DROGAS. APREENSÃO DE CELULAR. EXTRAÇÃO DE DADOS. CAPTURA DE TELAS. QUEBRA DA CADEIA DE CUSTÓDIA. INADMISSIBILIDADE DA PROVA DIGITAL. AGRAVO REGIMENTAL PROVIDO.
> 1. O instituto da cadeia de custódia visa a garantir que o tratamento dos elementos probatórios, desde sua arrecadação até a análise pela autoridade judicial, seja idôneo e livre de qualquer interferência que possa macular a confiabilidade da prova.
> 2. Diante da volatilidade dos dados telemáticos e da maior suscetibilidade a alterações, imprescindível se faz a adoção de mecanismos que assegurem a preservação integral dos vestígios probatórios, de forma que seja possível a constatação de eventuais alterações, intencionais ou não, dos elementos inicialmente coletados, demonstrando-se a higidez do caminho percorrido pelo material.
> 3. A auditabilidade, a repetibilidade, a reprodutibilidade e a justificabilidade são quatro aspectos essenciais das evidências digitais,

> os quais buscam ser garantidos pela utilização de metodologias e procedimentos certificados, como, e.g., os recomendados pela ABNT.
> 4. A observação do princípio da mesmidade visa a assegurar a confiabilidade da prova, a fim de que seja possível se verificar a correspondência entre aquilo que foi colhido e o que resultou de todo o processo de extração da prova de seu substrato digital. Uma forma de se garantir a mesmidade dos elementos digitais é a utilização da técnica de algoritmo hash, a qual deve vir acompanhada da utilização de um software confiável, auditável e amplamente certificado, que possibilite o acesso, a interpretação e a extração dos dados do arquivo digital.
> 5. De relevo trazer à baila o entendimento majoritário desta Quinta Turma no sentido de que "é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia" (AgRg no RHC n. 143.169/RJ, relator Ministro Messod Azulay Neto, relator para acórdão Ministro Ribeiro Dantas, Quinta Turma, DJe de 2/3/2023).
> 6. Neste caso, não houve a adoção de procedimentos que assegurassem a idoneidade e a integridade dos elementos obtidos pela extração dos dados do celular apreendido. Logo, evidentes o prejuízo causado pela quebra da cadeia de custódia e a imprestabilidade da prova digital.
> 7. Agravo regimental provido a fim de conceder a ordem de ofício para que sejam declaradas inadmissíveis as provas decorrentes da extração de dados do celular do corréu, bem como as delas decorrentes, devendo o Juízo singular avaliar a existência de demais elementos
> probatórios que sustentem a manutenção da condenação.

A cadeia de custódia no processo penal é, portanto, requisito de admissibilidade da prova digital produzida pelo órgão acusador, cuja inobservância acarreta a ilicitude da prova e sua consequente exclusão do processo à luz do devido processo legal (art. 5º, LIV, CRFB c/c art. 158-A, CPP).

3.2 Cadeia de custódia da prova digital no processo civil

Diferentemente do processo penal, não há na legislação processual civil dispositivo normativo que trate da cadeia de custódia da prova digital.

O Código de Processo Civil de 2015, como visto, consagrou o princípio da liberdade probatória (art. 369, CPC), admitindo o uso de qualquer meio de prova no processo, e, diante da inexistência de regras específicas, a prova digital deve ser tratada, no atual contexto processual, como uma prova documental.

Assim, no processo civil, será considerada autêntica a prova digital se "a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei" (art. 411, II, CPC) ou se "não houver impugnação

da parte contra quem foi produzido o documento" (art. 411, III, CPC), e será ela íntegra se não for suscitada a sua falsidade (art. 408 c/c art. 427, ambos do CPC).

Estará infirmada a fé da prova digital se impugnada a sua autenticidade (art. 428, I, CPC), incumbindo à parte que produziu o documento o ônus de comprová-la (art. 429, II, CPC), e/ou for declarada judicialmente a sua falsidade (art. 427, CPC), cabendo à parte que a arguiu o ônus de prová-la (art. 429, I, CPC).

O processo civil é regido pela distribuição dinâmica do ônus da prova, cabendo ao autor provar o fato constitutivo do seu direito (art. 373, I, CPC) e ao réu a existência de fato impeditivo, modificativo ou extintivo do direito daquele (art. 373, II, CPC).

Vê-se, portanto, que no processo civil é ônus das partes demonstrarem a autenticidade e a integridade da prova digital apresentada de acordo com as alegações por elas deduzidas durante a instrução probatória.

A ausência de manifestação no momento processual oportuno ou a falta de comprovação das alegações deduzidas acarretam presunção de veracidade da prova digital produzida. Neste contexto, a inobservância da cadeia de custódia da prova digital carreada aos autos no processo civil não produz as mesmas consequências do processo penal.

No sistema processual civil vigente, as provas não possuem hierarquia ou valor predeterminado, sendo apreciadas, sopesadas e valoradas pelo juiz de forma conjunta e conforme o contexto apresentado (art. 371, CPC).

Não é razoável exigir-se no processo civil o mesmo rigor técnico-científico do processo penal. Neste, o órgão acusador é o Estado, que tem não apenas o ônus de provar a culpa do acusado, mas o dever de prover os meios necessários para que lhe seja assegurado o devido processo legal, afastando o risco de acusações infundadas ou lastreadas em provas duvidosas, daí porque "exige-se, conforme o art. 158-A a 158-F, CPP, a estrita obediência ao disciplinamento envolvendo toda a coleta de vestígios deixados em locais ou em vítimas de crime" (SAAD NETTO et al., 2023, p. 230).

Já no processo civil, as partes estão sujeitas à distribuição dinâmica do ônus da prova, inclusive da digital trazida ao processo por qualquer uma delas. Não há exigência legal para que se observe o mesmo procedimento previsto nos

arts. 158-A a 158-F do CPP para a cadeia de custódia, não sendo cabível a sua aplicação analógica por incompatibilidade com o princípio esculpido no art. 369 do CPC.

Enquanto no processo penal o Estado-acusador assume uma condição de parte hipersuficiente detentora dos meios para a produção adequada das provas contra o acusado, no processo civil a regra é de isonomia entre os litigantes (art. 7º, CPC), inclusive aqueles considerados hipossuficientes (art. 98, CPC), os quais não têm, usualmente, condições técnicas e/ou financeiras de promover a produção da prova digital com observância da cadeia de custódia prevista no processo penal, tampouco de arcar com eventuais honorários periciais (arts. 95 e 465, § 3º, CPC).

Para o processo civil, a prova digital, salvo se esta for obtida por meio ilícito (art. 5º, LVI, CRFB), não será inadmitida como meio de prova, mas apenas declarada nula pela inobservância da cadeia de custódia como requisito extrínseco, pois a confiabilidade e força probante nela depositada passa pela avaliação do “grau de 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 et al., 2016, p. 221-222).

CONCLUSÃO

Ao longo das últimas duas décadas, a crescente familiarização dos profissionais do Direito com a tecnologia e o uso cada vez maior de registros digitais de fatos relevantes para o processo foram os responsáveis pela ruptura do paradigma probatório documental há séculos existente, com a substituição dos documentos em papel pelos eletrônicos ou digitais para registro de fatos juridicamente relevantes, dando origem à denominada prova digital.

Embora não caminhe na mesma velocidade do desenvolvimento tecnológico, o direito processual contemporâneo tem buscado acompanhar as mudanças trazidas por esse fenômeno, reconhecendo a validade dos documentos eletrônicos produzidos na forma da lei, instituindo o Processo Judicial Eletrônico e autorizando a prática dos atos processuais em formato digital.

Diante, porém, da lacuna legislativa ainda existente, diversos doutrinadores vêm buscando conceituá-la, definir sua natureza jurídica e estabelecer seus requisitos de admissibilidade e validade no processo visando a assegurar que a prova digital apresentada corresponda exatamente ao fato que por meio dela se pretende provar.

A partir da interpretação e aplicação das normas processuais atualmente vigentes, podemos inferir que a prova digital tem natureza jurídica de documento, no qual as informações sobre fatos juridicamente relevantes foram registradas em fontes eletrônicas ou digitais.

Dessa maneira, toda e qualquer informação obtida dessas fontes reais, ainda que o fato que por meio dela se pretenda provar tenha ocorrido no mundo analógico, pode ser admitida como prova documental no processo.

Em razão da volatilidade intrínseca própria do meio ambiente onde é produzida, a doutrina definiu certos requisitos que permitam ao julgador aferir a idoneidade da prova digital. São eles a autenticidade e a integridade.

São consideradas autênticas, portanto, as provas digitais cuja proveniência não se duvida e cuja autoria do fato que por meio delas se pretende provar possa ser confirmada, ainda que indiretamente, pela fonte eletrônica ou digital onde estão armazenados e de onde foram extraídos os registros. Para que as informações obtidas, por sua vez, sejam consideradas íntegras, devem elas estar completas (sem fracionamentos ou omissões), não sofrerem nenhuma modificação do seu estado original (acréscimos, supressões ou adulterações), possuírem marcação temporal idônea (identificação do momento em que o fato ocorreu ou foi ao menos registrado digitalmente) e serem totalmente inteligíveis (em linguagem natural de fácil compreensão) e críveis (confiáveis) às partes e ao julgador.

Além desses requisitos intrínsecos, a doutrina defende um terceiro requisito, extrínseco a ela, denominado cadeia de custódia, cuja finalidade é justamente garantir a preservação da autenticidade e integridade da prova digital desde a sua coleta até a sua apresentação em juízo.

A importância da cadeia de custódia foi expressamente reconhecida pelo legislador infraconstitucional que, por meio da Lei nº 13.964/2019, a positivou nos arts. 158-A e 158-B do Código de Processo Penal. Sua relevância para o processo penal é tamanha que a Quinta Turma do Superior Tribunal de Justiça,

no julgamento do Agravo Regimental no *Habeas Corpus* nº 828.054 – RN, de relatoria do Ministro Joel Ilan Paciornik, reconheceu a inadmissibilidade da prova digital obtida com quebra da cadeia de custódia.

A partir dessa decisão paradigmática, os operadores do Direito passaram a debater se a consequência jurídico-processual da inobservância da cadeia de custódia da prova digital no processo penal é a mesma para os processos de natureza não-penal, como o processo civil, trabalhista, eleitoral e administrativo, por exemplo, evidenciando a necessidade de aprofundamento dos estudos sobre o tema objeto do presente artigo.

Seria, pois, a quebra da cadeia de custódia da prova digital causa de inadmissibilidade ou nulidade da prova no processo civil?

O direito à prova assume feições distintas no processo penal e no processo civil. Enquanto este é regido pelos princípios da isonomia entre os litigantes (art. 7º, CPC) e da liberdade probatória (art. 5º, LV, CRFB c/c art. 369, CPC), naquele vigoram os princípios do devido processo legal penal (art. 5º, LIV, CRFB), da inocência (art. 5º, LVII, CRFB) e do *in dubio pro reo* (art. 386, VII, CPP) em favor do acusado.

Em qualquer espécie de processo são inadmissíveis as provas obtidas por meios ilícitos (art. 5º, LVI, CRFB), assim consideradas aquelas em que houve acesso ou utilização ilegal da fonte de prova, acarretando, nessas hipóteses, a sua inadmissibilidade e consequente descarte ou exclusão do processo criminal ou civil. Está-se diante de uma prova ilícita propriamente dita.

Noutros casos, porém, apenas o instrumento endoprocessual utilizado é inadequado para a reprodução dos fatos no processo, ocasionando a sua nulidade e consequente desconsideração para fins de formação do convencimento do julgador. É a chamada prova ilegítima.

O respeito à cadeia de custódia e suas etapas (art. 158-B, CPP), no processo penal, é um dever do órgão acusador decorrente do devido processo legal, sendo considerada ilícita toda e qualquer prova obtida com violação às normas constitucionais e legais (art. 157, CPP). É, portanto, requisito de admissibilidade da prova digital, cuja inobservância acarreta a ilicitude da prova e sua consequente exclusão do processo.

Diferentemente do processo penal, não há na legislação processual civil norma que exija, expressamente, a observância da cadeia de custódia como requisitos de admissibilidade da prova digital.

No sistema processual civil vigente, as provas não possuem hierarquia ou valor predeterminado, sendo apreciadas, sopesadas e valoradas pelo juiz de forma conjunta e conforme o contexto apresentado (art. 371, CPC), aplicando-se à prova digital, pela sua natureza, as mesmas regras da prova documental quanto ao momento da sua produção (art. 434, CPC) e manifestação da parte contrária (art. 436, CPC), ônus da prova (arts. 373 e 429, CPC) e força probante (arts. 405 a 428, CPC).

O processo civil é regido pela distribuição dinâmica do ônus da prova, cabendo ao autor provar o fato constitutivo do seu direito (art. 373, I, CPC) e ao réu a existência de fato impeditivo, modificativo ou extintivo do direito daquele (art. 373, II, CPC). Assim, será considerada autêntica a prova digital se a autoria estiver identificada por qualquer outro meio legal de certificação, inclusive eletrônico, nos termos da lei" (art. 411, II, CPC) ou se "não houver impugnação da parte contra quem foi produzido o documento" (art. 411, III, CPC), e será ela íntegra se não for suscitada a sua falsidade (art. 408 c/c art. 427, ambos do CPC).

Por outro lado, estará infirmada a fé da prova digital se impugnada a sua autenticidade (art. 428, I, CPC), incumbindo à parte que produziu o documento o ônus de comprová-la (art. 429, II, CPC), e/ou for declarada judicialmente a sua falsidade (art. 427, CPC), cabendo à parte que a arguiu o ônus de prová-la (art. 429, I, CPC).

No processo civil, é ônus das partes demonstrarem a autenticidade e a integridade da prova digital apresentada de acordo com as alegações por elas deduzidas durante a instrução probatória. A ausência de manifestação no momento processual oportuno ou a falta de comprovação das suas alegações acarretam presunção de veracidade da prova digital produzida.

Neste contexto, conclui-se que a inobservância da cadeia de custódia da prova digital carreada aos autos no processo civil não produz as mesmas consequências do processo penal, pois, enquanto naquele as partes estão sujeitas à distribuição dinâmica do ônus da prova, inclusive da digital trazida ao

processo por qualquer uma delas, neste há exigência legal para que se observe o procedimento previsto nos arts. 158-A a 158-F do CPP.

Não se mostra razoável, portanto, a aplicação analógica do disposto nos arts. 158-A a 158-F do CPP ao processo civil por incompatibilidade com o princípio da liberdade probatória consagrado no art. 369 do CPC.

Há que se fazer, assim, o *distinguishing* quando se tratar da análise da admissibilidade da prova digital no processo civil, eis que a *ratio decidendi* do julgamento proferido pela Quinta Turma do Superior Tribunal de Justiça no Agravo Regimental no *Habeas Corpus* nº 828.054 – RN não se aplica aos processos não-penais.

Embora a inobservância da cadeia de custódia no processo penal ocasione a inadmissibilidade da prova digital, no processo civil a consequência será apenas a declaração da sua eventual nulidade pelo juiz se não convencido, por outros meios de prova, que ela é autêntica e íntegra.

A inobservância da cadeia de custódia no processo civil, como instrumento endoprocessual utilizado de maneira inadequada, torna a prova digital, portanto, ilegítima, e não ilícita.

É importante, diante da cada vez maior sujeição da sociedade à tecnologia e às provas dos fatos juridicamente relevantes pelo meio digital, que o PL nº 4.939/2020 em tramitação no Congresso Nacional trate da prova digital de forma ampla e abrangente, disciplinando-a de maneira adequada a cada espécie de procedimento dadas as particularidades próprias dos processos de natureza penal e não-penal.

De modo que um tratamento legislativo completo e minucioso sobre a prova digital não só torna a administração da justiça mais eficaz, mas também aumenta a confiança da sociedade no sistema jurídico, assegurando que as evidências sejam manuseadas de forma justa e transparente.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO/IEC 27037:2013, 2013.

ALVIM, Arruda. **Manual de direito processual civil**: teoria do processo e processo de conhecimento, 17. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2017.

BARRETO, Alexandre G.; WENDT, Emerson. **Inteligência e investigação criminal em fontes abertas**. 3. ed. Rio de Janeiro: Editora Brasport, 2020.

BAUMAN, Zygmunt. **Vigilância líquida**: Diálogos com David Lyon. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Habeas Corpus nº 828054-RN (2023/0189615-0). Agravante: Wesley Gomes do Nascimento. Agravados: Ministério Público Federal e Ministério Público do Estado do Rio Grande do Norte. Impetrado: Tribunal de Justiça do Estado do Rio Grande do Norte. Relator: Ministro Joel Ilan Paciornik. Brasília, 23 de abril de 2024. Publicado no DJe de 29/04/2024. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301896150&dt_publicacao=29/04/2024 . Acesso em 4 jun. 2024

BRASIL. Supremo Tribunal Federal. Recurso Ordinário no Habeas Corpus nº 95689-SP. Recorrente: João Carlos da Rocha Mattos. Recorrido: Ministério Público Federal. Relator: Ministro Eros Grau. Brasília, 2 de setembro de 2008. Publicado no DJe de 17/10/2008. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22RHC%2095689%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 16 mai. 2021.

BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 168052-SP. Paciente: Rodrigo Ricardo Laurindo. Impetrante: Arai de Mendonca Brazao. Coator: Superior Tribunal de Justiça. Relator: Ministro Gilmar Mendes. Brasília, 20 de outubro de 2020. Publicado no DJe de 02/12/2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22HC%20168052%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 16 mai. 2021.

BRASIL. Supremo Tribunal Federal. Agravo em Recurso Extraordinário nº 1042075-RJ com Repercussão geral (Tema 977). Recorrente: Ministério Público do Estado do Rio de Janeiro. Recorrido: Guilherme Carvalho Farias. Relator: Ministro Dias Toffoli. Brasília, 23 de novembro de 2017. Publicado no DJe de 12/12/2017. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ARE%201042075%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 8 jul. 2024.

CASEY, Eoghan. Digital evidence and computer crime: forensic science, computers and the internet. 3rd ed. Elsevier: 2011. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=lUnMz_WDJ8AC&oi=fnd&pg=PP1&dq=Digital+evidence+and+computer+crime:+forensic+science,+computers+and+the+internet.+3rd+edition&ots=aLq1CjzMVc&sig=NFQSvIG1HjTL7R2DzKSytnItrxk#v=onepage&q=Digital%20

evidence%20and%20computer%20crime%3A%20forensic%20science%2C%20computers%20and%20the%20internet.%203rd%20edition&f=false . Acesso em: 16 mai. 2021.

DELEUZE, Gilles. **Post-scriptum sobre as Sociedades de Controle**. Trad. Peter Pál Pelbart. Conversações: 1972-1990. Rio de Janeiro: Ed. 34, 1992.

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

DINAMARCO, Cândido Rangel. **Instituições de direito processual civil**. 7ª ed. V. 3. São Paulo: Malheiros, 2017.

ESTADOS UNIDOS DA AMÉRICA. *Federal Rules of Evidence*. Disponível em: https://www.law.cornell.edu/rules/fre. Acesso em: 21 maio 2021.

ESTADOS UNIDOS DA AMÉRICA. U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, NATIONAL INSTITUTE OF JUSTICE. ***Electronic Crime Scene Investigation: A Guide for First Responders - Second Edition***, 2008. Disponível em: https://www.ojp.gov/pdffiles1/nij/219941.pdf. Acesso em: 21 mai. 2021.

INTERNET ENGINEERING TASK FORCE (IETF). ***RFC 3227: Guidelines for evidence collection and archiving***, 2002. Disponível em: https://www.rfc-editor.org/rfc/rfc3227.html. Acesso em: 21 mai. 2021.

JONES, Franklin. **Rastreando a verdade: a cadeia de custódia da prova.** Maringá: 2023.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

MARQUES, José Frederico. **Elementos de direito processual penal**. v. II. Campinas: Bookseller, 1997.

NERY JUNIOR, Nelson. **Princípios do processo na Constituição Federal**. 10. ed. São Paulo: Revista dos Tribunais, 2010.

NERY JUNIOR, Nelson *et al.* **Código de Processo Civil comentado**. 3. ed. São Paulo: RT, 1997.

PRADO. Geraldo. **A cadeia de custódia de prova no processo penal.** 1ª ed., São Paulo: Marcial Pons, 2019.

PRADO, Geraldo. Texto correspondente à palestra intitulada “A interface entre o Direito Digital e o Processo Penal”, no Ciclo Permanente de Palestras com o tema “Consequências do Uso da Inteligência Artificial no Processo Penal”, oferecido pelo Núcleo de Estudo Luso-Brasileiro da Faculdade de Direito da Universidade de Lisboa (NELB), ao lado da professora Janaina Matida e do professor Alexandre Morais da Rosa, em 20 de janeiro de 2021, às 13 horas (horário de Brasília), transmitida pelo aplicativo Zoom. Disponível em:

https://www.conjur.com.br/dl/artigo-geraldo-prado.pdf. Acesso em: 19 mai. 2021.

PINHEIRO, Patricia Peck. **Direito Digital**. 7. ed. rev., atual. e ampl., São Paulo, SP: Saraiva, 2021.

RANGEL, Paulo. **Direito processual penal.** 29. Ed. Barueri: Atlas, 2021.

SAAD NETTO, Cláudio et al. **O direito à prova pericial no processo penal.** São Paulo: Thomson Reuters Brasil, 2023.

SCHWAB, Klaus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

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

THAMAY, Rennan; TAMER, Mauricio. **Provas no Direito Digital**: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Editora Thomson Reuters, Revista dos Tribunais, 2020.

UNIÃO EUROPEIA. EUROPEAN UNION AND COUNCIL OF EUROPE – CYBERCRIME@IPA. ***Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors and Judges, versão 2.1***, 2020. Disponível em: https://rm.coe.int/0900001680a22757. Acesso em: 22 mai. 2021.

UNIÃO EUROPEIA. EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). ***Electronic Evidence - a basic guide for First Responders***, 2015. Disponível em: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders. Acesso em: 21 mai. 2021.

UNIÃO EUROPEIA. EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ***Cooperation across CSIRTS, LE and the Judiciary - Handbook, Document for trainers***, 2019. Disponível em: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/cooperation-across-csirts-and-law-enforcement/support-the-fight-against-cybercrime-training-material-csirt-le-jud-cooperation-handbook.pdf. Acesso em: 22 mai. 2021

YAMADA, Vitor Leandro. **Requisitos legais da prova digital: autenticidade, integridade e cadeia de custódia.** *in* Provas digitais no processo do trabalho: realidade e futuro. MISKULIN, Ana Paula Silva Campos; BERTACHINI, Danielle; AZEVEDO NETO, Platon Teixeira de Azevedo (coord.). 1. ed. Campinas: Ed. Lacier, 2022.

WAMBIER, Luiz Rodrigues; ALMEIDA, Flavio Renato Correia de; TALAMINI, Eduardo. **Curso avançado de processo civil**. V.1. São Paulo: Revista dos Tribunais, 2005.