PONTÍFICIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Faculdade Mineira de Direito

Luiz Roberto Paciarelli

DA PROVA DIGITAL NO PROCESSO JUDICIAL

Belo Horizonte
2024

Luiz Roberto Paciarelli

DA PROVA DIGITAL NO PROCESSO JUDICIAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade Mineira de Direito da Pontifícia Universidade Católica de Minas Gerais.

Orientador: Prof. Dr. Vicente de Paula Maciel Júnior.

Área de concentração: Democracia, Constituição e Internacionalização.

Belo Horizonte

2024

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Paciarelli, Luiz Roberto
P117d Da prova digital no processo judicial / Luiz Roberto Paciarelli. Belo Horizonte, 2024.
209 f. : il.

Orientador: Vicente de Paula Maciel Júnior

Dissertação (Mestrado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito

1. Prova digital. 2. Prova documental. 3. Prova (direito) - Inovação tecnológica. 4. Produção de prova. 5. Prova (direito) - Legislação - Brasil. 6. Tecnologia e direito - Brasil. 7. Direito digital. I. Maciel Júnior, Vicente de Paula. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito. III. Título.

CDU: 347.94

Ficha catalográfica elaborada por Fabiana Marques de Souza e Silva - CRB 6/2086

Luiz Roberto Paciarelli

DA PROVA DIGITAL NO PROCESSO JUDICIAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade Mineira de Direito da Pontifícia Universidade Católica de Minas Gerais.

Área de concentração: Democracia, Constituição e Internacionalização.

Prof. Dr. Vicente de Paula Maciel Júnior (Orientador)

Prof. Dr. José Alfredo de Oliveira Baracho Júnior - PUC Minas (Banca Examinadora)

Prof. Dr. Natália Chernicharo Guimarães - UFJF (Banca Examinadora)

Belo Horizonte, 13 de dezembro de 2024.

AGRADECIMENTOS

Ao Prof. Dr. Vicente de Paula Maciel Júnior, nosso orientador, por sua acolhida generosa e irrestrita em um momento de muita dificuldade, por ser uma inspiração para todos os alunos que cruzam seus caminhos de professor e de ser humano.

Aos meus pais, Roberto e Fátima e minha irmã, Fernanda**,** por sempre estarem presentes, nos bons e maus momentos.

À Procuradoria-Geral de Belo Horizonte, pela confiança em nós depositada.

Ao universo, por ser tão generoso e sempre nos apresentar desafios na medida da nossa capacidade.

RESUMO

O objeto de estudo desta dissertação é a prova digital no processo judicial. Por isto, seu objetivo foi examinar o fenômeno das provas digitais com base nos fundamentos da Teoria Geral das Provas, da análise das provas na Constituição Federal/1988, e da investigação acerca da compatibilidade entre esse novo instituto e o modelo processual constitucional, essencial ao estudo do processo contemporâneo. Ademais, buscou-se, ainda que de forma sucinta, reconstruir e discutir os fenômenos sociais que impulsionaram o atual giro linguístico, que transferiu o conjunto de relações sociais do mundo físico para o digital, no qual as interações jurídicas ganham crescente relevância, à medida que o ambiente digital se expande no cotidiano. Para atingir tais objetivos, a metodologia utilizou as pesquisas bibliográfica, documental e qualitativa exploratória. As tratar das provas digitais, a pesquisa enfocou a multiplicidade de desafios enfrentados pelo jurista contemporâneo, como o conflito entre princípios constitucionais, a distribuição do ônus da prova, a transição de um sistema probatório típico para um atípico, entre outras questões que vêm sendo intensamente debatidas, sobretudo no âmbito do Judiciário e do Legislativo.

Palavras-chave: provas digitais; giro linguístico; teoria geral das provas; direito digital;

ABSTRACT

This study focused on digital evidence in judicial processes. Because of that, its objective was to examine the phenomenon of digital evidence based on the foundations of the General Theory of Evidence, the analysis of evidence in the Federal Constitution of 1988, and the investigation of the compatibility between this new institute and the constitutional procedural model, which is essential to the study of contemporary processes. Furthermore, the work aimed, albeit briefly, to reconstruct and discuss the social phenomena that propelled the current linguistic shift, which transferred the set of social relations from the physical world to the digital, space where legal interactions have gained increasing relevance as the digital environment expands in daily life. To achieve such purposes, the methodology included the bibliographic, documentary, and exploratory qualitative research. When addressing digital evidence, our research focused on the multiplicity of challenges faced by contemporary legal scholars, such as the conflict between constitutional principles, the distribution of the burden of proof, the transition from a typical evidentiary system to an atypical one, among other issues that have being intensely debated, particularly within the Judiciary and the Legislature.

Keywords: digital evidence; linguistic turn; general theory of evidence and proof; digital law.

LISTA DE QUADRO

LISTA DE ABREVIATURAS E SIGLAS

ABINEE	Associação Brasileira de Indústria Elétrica e Eletrônica
ABNT	Associação Brasileira de Normas Técnicas
ACEL	Associação Nacional das Operadoras Celulares
AC-RAIZ	Autoridade Certificadora Raiz
ADC	Ação Declaratória de Constitucionalidade
ADI	Ação Direta de Inconstitucionalidade
ADO	Ação Direta de Inconstitucionalidade por Omissão
ADPF	Arguição de Descumprimento de Preceito Fundamental
AGPS	Assisted Global Positioning System
AGRG	Agravo Regimental
AMAT	Associação Mineira dos Advogados Trabalhistas
ANATEL	Agência Nacional de Telecomunicações
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
Art.	Artigo
AS	Autonomous System
CCAI	Comissão Mista de Controle das Atividades de Inteligência
CCOM	Comissão de Comunicação
CERN	Conseil Européen pour la Recherche Nucléaire
CGI	Comitê Gestor da Internet
CLT	Consolidação das Leis do Trabalho
CNJ	Conselho Nacional de Justiça
CPC	Código de Processo Civil
CPP	Código de Processo Penal
CRFB/1988	Constituição da República Federativa do Brasil de 1988
CSNET	Computer Science Network

DARPA	Defense Advanced Research Projects Agency
Des.	Desembargador(a)
DoD	Departamento de Defesa
EC	Emenda Constitucional
ENIAC	Electronic Numerical Integrator and Computer
ENISA	European Union Agency for Cybersecurity
ERB	Estação Rádio Base
EXIF	Exchangeable Image File Format
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HC	Habeas Corpus
HTML	HyperText Markup Language
IBCCRIM	Instituto Brasileiro de Ciências Criminais
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ID	Identifier
IEC	International Electrotechnical Commission
IEFT	Internet Engineering Task Force
IM	Instant Messaging
IMAP	Internet Messaging Access Protocol
INFOJUD	Sistema de Informações ao Judiciário
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITI	Instituto Nacional de Tecnologia da Informação
JPEG	Joint Photographic Experts Group
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet

MILNET	Military Network
MJSP	Ministério da Justiça e Segurança Pública
MLAT	Mutual Legal Assistance Treaty
MMS	Multimedia Messaging Service
MP	Medida Provisória
MPRJ	Ministério Público do Estado do Rio de Janeiro
MS	Mandado de Segurança
NBR	Norma Brasileira
NCP	Network Control Protocol
NSF	National Science Foundation
NSFNET	National Science Foundation Network
ONU	Organização das Nações Unidas
OSINT	Open Source Intelligence
PDF	Portable Document Format
PGP	Pretty Good Privacy
PGR	Procuradoria-Geral da República
PIN	Personal Identification Number
PL	Projeto de Lei
POP	Post Office Protocol
PPS	Partido Popular Socialista
RE	Recurso Extraordinário
RENAJUD	Sistema de Restrições Judiciais sobre Veículos Automotores
REsp	Recurso Especial
RFC	Request for Comments
RMS	Recurso em Mandado de Segurança
ROT	Recurso Ordinário Trabalhista
SISBAJUD	Sistema de Busca de Ativos do Poder Judiciário

SLAID	Surveillance Legislation Amendment (Identify and Disrupt)
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
STM	Superior Tribunal Militar
TCP/IP	Transmission Control Protocol/Internet Protocol
TCU	Tribunal de Contas da União
TJMG	Tribunal de Justiça de Minas Gerais
TLS	Transport Layer Security
TRT	Tribunal Regional do Trabalho
TST	Tribunal Superior do Trabalho
UCLA	Universidade da Califórnia Angelina
URL	Uniform Resource Locator
WWW	World Wide Web

SUMÁRIO

1 INTRODUÇÃO

Vivemos na Era da Informação e o avanço da tecnologia ocasionou um verdadeiro giro linguístico, deslocando as relações humanas de um ambiente físico para um digital.

Atualmente, transações negociais são realizadas virtualmente, conversas de cunho pessoal travadas, contatos profissionais entre colegas de trabalhos e entre empregadores e empregados são conduzidos por meio de plataformas digitais como o *WhatsApp* e *e-mail*, agilizando negociações e decisões. Entretanto crimes são perpetrados, diariamente, neste ambiente virtual.

Essas negociações, relações e crimes causam impacto e, inevitavelmente, chegam à atividade jurisdicional do Poder, especialmente no que diz respeito à produção e utilização de provas digitais. Nesse contexto, importantes desafios surgem para a proteção dos direitos fundamentais e para a efetividade do processo judicial, em um novo paradigma social em que a tecnologia se faz cada vez mais presente.

Destarte, faz-se premente a investigação sobre o uso da prova digital no processo judicial sob a perspectiva do processo constitucional, no qual se busca garantir um processo justo e respeitoso aos direitos fundamentais constitucionais das partes envolvidas.

Como se verá, muitas questões, aparentemente simples, envolvem soluções difíceis e conflitos de princípios. Exemplificamos: o autor de determinada demanda traz aos autos uma cópia da tela do *Facebook*, para dar suporte à alegação de que foi difamado. Se o réu impugna a prova (cópia de tela), argumentando tratar-se de uma montagem, como o autor provará que, de fato, houve a postagem, tendo em vista a facilidade de edição de quaisquer mídias em meios digitais?

Ainda, se o empregado de uma empresa alega estar doente, mas é visto por outro empregado em uma praia, diante desse forte indício de má conduta, em eventual demanda de reintegração, o juízo poderia requerer a apresentação dos dados de geolocalização do empregado, ou este procedimento seria invasão à sua privacidade?

E, ainda, na seara penal, questionamos: o espelhamento de WhatsApp de suspeito de perpetrar um crime seria permitido em caso de requerimento judicial?

Novas tecnologias de espionagem devem ser utilizadas pela Segurança Pública ou isso levaria a uma fragilização do Estado Democrático de Direito?

A fim de investigar questões como essas, estruturamos este trabalho em 6 capítulos.

No capítulo 1, Introdução, contextualizamos nosso tema, justificamos sua escolha, principalmente pela premência de se investigar o uso da prova digital no processo judicial, e definimos o objetivo geral de examinar o fenômeno das provas digitais a partir de fundamentos da Teoria Geral das Provas, da análise das provas na Constituição da República Federativa do Brasil de 1988 (CRFB/1988), e da investigação sobre a compatibilidade entre esse novo instituto e o modelo processual constitucional, este essencial ao estudo do processo contemporâneo. Apresentamos, ainda, neste capítulo, a estrutura desta dissertação.

No capítulo 2 abordamos a Teoria Geral da Prova, com o objetivo de definir, com clareza, noções fundamentais, tais como conceito, destinatários, objeto, valoração, finalidade e ônus da prova, além de fazermos uma breve incursão no estudo epistemológico sobre a verdade, com foco no Direito e, em especial, na matéria probatória. Essa abordagem visa a estabelecer as premissas necessárias para o desenvolvimento do nosso tema, a saber, as provas digitais.

No capítulo 3 estabelecemos a diretriz fundamental que deve orientar qualquer solução em matéria probatória: a adoção das lentes do modelo de processo constitucional, com a definição de princípios constitucionais que dão suporte à atividade probatória, é dizer: a prova na Constituição Federal/ 1988.

Dedicamos o capítulo 4 a explicar como chegamos à atual configuração social, relacionando conceitos de disruptura tecnológica, o giro linguístico e o surgimento de um novo direito probatório decorrente desse contexto.

Ao longo do capítulo 5, temas palpitantes concernentes às provas digitais foram objeto de análise, durante a qual buscamos compreender a compatibilidade dos novos elementos de prova com questões de fundo constitucional, como adiantamos anteriormente, com a apresentação de conceitos tecnológicos e diversos temas atualmente debatidos. Vários dos julgados aqui colacionados são bem recentes, alguns sequer decididos ainda.

Finalmente, no capítulo 6, tecemos considerações e apresentamos nossas conclusões sobre nossa pesquisa.

É um novo mundo que vislumbramos e em que entramos.

2 TEORIA GERAL DA PROVA

Para dar início a este estudo, é necessário estabelecer alguns fundamentos da Teoria Geral da Prova, por meio de esclarecimentos conceituais preliminares sobre o instituto das provas judiciais, tudo isso sem a pretensão de esgotar o tema. Esses fundamentos são essenciais para que possamos atingir o objetivo geral deste trabalho: a investigação das provas digitais.

Antes de iniciarmos o estudo das provas, e com esteio na doutrina de Leal (2021, p. 269-274), é importante distinguir alguns termos atinentes à matéria.

Leal (2021, p. 270) concatena os conceitos fundamentais de prova a partir do exemplo da perícia, como o “meio de prova para o exame de elementos de prova com a elaboração final do laudo, que é o instrumento de prova”.

Assim, há de se falar em a) meio, b) elementos e c) instrumento de prova.

O (a) meio se refere à forma/procedimento como se obtém determinada prova, já os (b) elementos, à informação extraída por meio do recurso utilizado. O resultado desse procedimento, por meio do qual se obtém determinadas informações, são materializadas através do (c) instrumento da prova. É o suporte físico.

Com isso esclarecido, adentra-se o estudo da teoria geral das provas.

2.1 Conceito de prova

O termo "prova" tem origem no latim *probatio*, que significa prova, ensaio, verificação, inspeção, exame, argumento, razão, aprovação ou confirmação. Ele deriva do verbo *probare* (*probo, as, are*), que significa provar, ensaiar, verificar, examinar, reconhecer por experiência, aprovar, estar satisfeito com algo, persuadir alguém de algo ou demonstrar (Santos, 1952, p. 11).

Vários são os conceitos que a doutrina empresta ao instituto da prova. Marques (1958, p. 360), em raciocínio claro, define a prova como instrumento que permite às partes influenciar a convicção do juiz sobre os fatos que alegaram, além de ser o meio utilizado pelo magistrado para investigar os fatos em que as partes envolvidas no conflito baseiam suas alegações.

Por seu turno, Santos (1990, p. 329) destaca a distinção entre os sentidos da prova, descrevendo-a no sentido objetivo, como meios para fornecer ao juiz o

conhecimento da verdade dos fatos apresentados em juízo. No sentido subjetivo, a prova refere-se à convicção formada no espírito do juiz sobre a verdade desses fatos. Assim, a prova judicial deve ser entendida como um conjunto que reúne esses dois aspectos, objetivo e subjetivo, os quais se complementam e não podem ser considerados separadamente, sendo avaliados tanto como fato quanto como indução lógica.

Theodoro Júnior (2023, p. 797), por sua vez, tem visão praticamente idêntica, lecionando que o sentido objetivo da prova diz do instrumento hábil a demonstrar a ocorrência de determinado fato, como um documento ou uma testemunha, enquanto o sentido subjetivo é a convicção formada psiquicamente quanto ao fato diante do instrumento probatório apresentado.

Por seu lado, Thamay e Tamer (2022, RB-1.2) postulam que a prova é o instrumento jurídico destinado a confirmar a ocorrência de um fato, e, se afirmativo, a definir ficam suas características e circunstâncias. Ela responde não apenas à questão de o fato ter acontecido ou não, mas também de como se deu e quais foram os sujeitos envolvidos, tanto ativos quanto passivos. A pessoa encarregada de interpretar juridicamente o fato precisa não apenas saber se ele ocorreu, mas também conhecer todos os seus detalhes. Em síntese, a prova é o meio pelo qual se forma a convicção sobre um fato específico, é tratada como instrumento, pois não é fim em si mesma, “mas mecanismo vocacionado à demonstração ou não do fato sobre o qual se pretende dar a leitura jurídica devida”.

Já Couture (2008, p. 100) resume seu argumento, afirmando que, no direito civil, a prova é um método jurídico para verificar as alegações das partes, sendo produzida por iniciativa do magistrado apenas em casos excepcionais e de incomensurável importância prática.

Nunes, Bahia e Pedron (2021, p. 681) chamam a atenção para o fato de que o direito constitucional à prova está atrelado ao contraditório e à ampla defesa, pela própria literalidade do art. 5º, LV da CRFB/1988 , que preconiza que “aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes” (Brasil, [2024a]) Assim é que a perfeição das garantias processuais se dá por meio das alegações das partes, ganhando corpo por meio das provas produzidas no processo. Concluem que uma Teoria da Prova que esteja de acordo com o Código de Processo

Civil (CPC) de 2015 (Brasil [2024d]), necessariamente, deve levar em conta a inclusão das provas nos autos, como forma de concretização da ampla defesa e do contraditório, com consequente provimento jurisdicional fundamentado.

Por fim, evocando o escólio de Dias (2022, p. 683), ele conceitua as provas como meios procedimentais (meios de prova), através dos quais os fatos litigiosos são apresentados aos sujeitos processuais e ficam registrados nos autos (instrumentos de prova). Elas buscam reconstruir, nos autos, eventos (elementos de prova) que ocorreram no passado.

De tudo quanto foi exposto, observamos que o conceito de prova é algo intuitivo, sendo mais importante relacioná-lo ao sistema de proteção dos direitos individuais e coletivos do processo constitucional decorrente do Estado Democrático de Direito do que propriamente buscar definir se se trata de instrumento, de fruto de uma cognição ou se possui sentido a ou b.

Sampietro (2022) destaca que o CPC/2015 evidencia claramente que um dos principais reflexos do modelo constitucional de processo reside na ampliação do direito probatório. Ao prezar pela atipicidade dos meios de prova, o art. 369 do Código não só reforça as garantias constitucionais do devido processo legal, do contraditório e da ampla defesa (CRFB/1988, art. 5º, LIV e LV), como também assegura que as partes litigantes tenham o direito de utilizar todos os meios legais e moralmente aceitáveis, para comprovar a veracidade das alegações apresentadas em juízo.

Corroborando esse ponto, após esboçar seu próprio conceito de prova, Lucon (2016) ensina que a premissa fundamental para a análise da legislação infraconstitucional sobre provas é que elas representam uma manifestação da garantia constitucional de acesso à justiça. Essa premissa abrange o direito à apresentação de provas, à produção das provas autorizadas com respeito ao contraditório e o direito à adequada valoração das provas produzidas. Não é por acaso que a CRFB/1988 assegura aos litigantes, em todos os processos, o respeito ao contraditório e à ampla defesa, com todos os meios e recursos a ela inerentes. O ordenamento jurídico brasileiro, considerando inconstitucional qualquer tentativa de excluir do Poder Judiciário a apreciação de lesão ou de ameaça a direito, deve igualmente possibilitar que as partes influenciem, de maneira eficaz, a formação do convencimento judicial (Lucon, 2016, p. 571).

2.2 Destinatários da prova

Hartmann (2023, p. 244) conceitua prova como o meio que permite persuadir alguém de algo, no direito usualmente o magistrado, aquele que, por meio da cognição, reconstruirá os fatos pretéritos, a fim de dar às partes uma solução adequada para a situação posta à sua apreciação. Ressalva, entretanto, que os demais participantes do processo também são destinatários da prova, uma vez que a interpretação equivocada do juiz sobre as provas pode redundar em decisão injusta.

Nunes, Bahia e Pedron (2021, p. 687-688) compartilham dessa mesma visão, lembrando que o Enunciado n. 50 do Fórum Permanente de Processualistas Civis enuncia que todos que podem fazer uso da prova são seus destinatários, os juízes, as partes ou os interessados.

Leal (2018) caminha nesse mesmo sentido, ao destacar ser impossível divorciar a produção probatória do devido processo legal/constitucional. Nesse sentido, leciona:

> O meio lícito de obtenção da prova nas democracias é desenvolvido em paradigmas do devido processo legal que impõe a participação lógico-procedimental probatícia das partes na preparação do provimento (sentença) e não como sujeitos passivos (privados de liberdade procedimental) de um provimento em tempo insuficiente e em espaço vazio do procedimento que se define pela radicalização do "princípio da oralidade" para realização de direitos (Leal, 2018, p. 273).

Assim, os pronunciamentos estatais são legitimados apenas quando tanto os autores quanto os destinatários se reconhecem como coautores e participantes de sua construção, encontrando-se aí o conceito de legitimidade dos atos de poder democráticos. Essa dimensão dialogal e discursiva, fundamental para o Estado Democrático de Direito, baseia-se na liberdade de escolha e ação, assim como na igualdade de oportunidades para todos os participantes. É nessa direção que a produção probatória não deve ser orientada apenas para o juiz, mas para todos os atores processuais, a fim de que possam exercer o contraditório substancial e, consequentemente, os pronunciamentos estatais gozem de legitimidade (Paolinelli, 2014, p. 67).

Almeida (2013, p. 53-54) vai mais além, ensinando que, não obstante a prova tenha por finalidade convencer o juiz da veracidade dos fatos controversos e

relevantes para o julgamento da questão posta à apreciação, o magistrado não é o único destinatário da prova. Assevera o autor que a prova tem entre seus destinatários a própria sociedade. Isso, porque, no controle da atividade estatal, em que está inclusa a jurisdicional, a sociedade tem o direito de conhecer os motivos, as provas, inclusive, porque em seu nome foi proferida tal decisão, partindo da premissa de que no Estado Democrático de Direito, o poder é exercido pelo povo e em função do povo.

Hoje, a doutrina que encontra no juiz o único destinatário da prova está obsoleta. Mesmo Theodoro Júnior reviu seu posicionamento ao longo dos anos, mormente em função do Novo CPC. Nas versões mais antigas de seu *Curso de direito processual* (como a 52. ed., de 2011, v. 1), advogava que o juiz era o único destinatário das provas. Nas edições mais recentes, entretanto, aderiu ao processo constitucional na espécie, quando leciona que, em decorrência da garantia constitucional do contraditório e da ampla defesa, não cabe ao juiz determinar ou restringir autoritariamente as provas que podem ser utilizadas pelas partes, uma vez que o atual CPC assegura às partes "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" (art. 369) (Brasil, [2024d]), restando obliterado o entendimento estabelecido à luz da legislação antiga de que, sendo o juiz o destinatário da prova, teria o poder discricionário de indeferir outros meios instrutórios, por desnecessários diante da circunstância de já se achar convencido. No processo justo, o convencimento judicial não pode se formar antes que a instrução da causa esteja exaurida para os litigantes, a quem se assegura, como norma fundamental, a cooperação e influência na decisão de mérito justa e efetiva (Theodoro Júnior, 2023, p. 798).

2.3 Objeto da prova

É controverso o que seja exatamente o objeto da prova. Parte da doutrina entende que são os fatos e outra parcela que são as alegações de fato.

Para a segunda corrente doutrinária, “o fato ocorreu ou não, existe ou não, enquanto a veracidade atinge exclusivamente as alegações de fato”, podendo ser verdadeiras ou falsas. A preocupação, neste aspecto, é com se provar o quanto foi

alegado. Já para a primeira corrente, o objeto são os fatos, uma vez que nem sempre o objeto da prova é constituído de alegações (Neves, 2015, p. 487).

A primeira doutrina encontra em Theodoro Júnior (2023, p. 800) um renomado expoente que leciona existirem alguns que defendem que a prova não se refere aos fatos em si, mas às alegações das partes. No entanto, essas alegações, na verdade, são afirmações sobre fatos que fundamentam as pretensões apresentadas em juízo. Assim, provar uma alegação significa demonstrar a veracidade desses fatos, de modo que, segundo a lei processual, os meios de prova legais e moralmente legítimos são utilizados no processo “para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz” (CPC/2015, art. 369) (Brasil, [2024d]). Dessa forma, são os fatos litigiosos que constituem o objeto da prova.

Fux (2023, p. 421), compartilha dessa visão, quando afirma que “o objeto da prova são os ‘fatos’, posto que ‘o direito’, em princípio, não se prova, mas, antes, se ‘conhece.’”

Santos (1990, p. 333) é outro renomado jurista que adere a essa visão.

Didier, Braga e Oliveira (2019, p. 65-66), por sua vez, são partidários da segunda corrente, entendendo que a atividade probatória consiste na demonstração de veracidade de uma alegação. Quanto ao fato, não há muita controvérsia, aconteceu ou não aconteceu, sendo, assim, insuscetível de adjetivações como “bom”, “correto” ou “condizente com a verdade”. As alegações, sim, são relevantes, à medida que podem ser verazes ou mentirosas, qualidades das quais se depreende a pertinência de prová-las, de tal maneira que o objeto da prova é a alegação do fato, que possui três características: controvérsia, relevância e determinação.

Essa posição é também defendida por Câmara (2006, p. 406-407), por razões praticamente idênticas.

Também perfila essa corrente Almeida (2013, p. 49), para quem a definição do objeto da prova está intrinsecamente atrelada ao próprio conceito de prova. Para aqueles que atribuem à prova um sentido de demonstração, provar significa mostrar, ou não, a ocorrência de um determinado fato. Já quem atribui à prova um sentido de verificação, considera que o objeto da prova é a alegação sobre os fatos, ou seja, a hipótese ou versão da realidade estabelecida pelas partes.

A norma jurídica associa fatos específicos a determinadas consequências jurídicas. São esses fatos que originam direitos, impedem seu surgimento, os

modificam ou os extinguem. Portanto, esses são os fatos que precisam ser objeto de prova. Quando, em juízo, se afirmar a ocorrência dos fatos descritos na norma e se solicitar a aplicação da consequência jurídica estabelecida por ela, é necessário demonstrar a ocorrência dos fatos alegados. Além disso, a conclusão de que uma alegação é verdadeira pressupõe a prévia demonstração do fato alegado. Em outras palavras, confrontar a alegação com a realidade para verificar sua veracidade só é possível com a demonstração, prévia ou não da ocorrência do fato alegado. O fato precisa ser provado para que a alegação de sua ocorrência seja aceita como verdadeira. (Almeida, 2013, p. 49).

2.4 Valoração da prova

Pode ser definida como o juízo de aceitabilidade dos resultados produzidos a partir da utilização da prova. Consiste na verificação dos enunciados fáticos levados aos autos por meio dos instrumentos de prova, bem como em um reconhecimento de valor dessas provas na formação de convencimento do julgador sobre os fatos controversos (Abellán, 2022, p. 250).

Trata-se de um tema deveras sensível. Em determinadas demandas, a prova documental será soberana, em dados litígios somente a prova pericial será aceitável. Ainda há demandas sobre questões de fato que encontram na prova oral o grande sustentáculo da decisão judicial (Fux, 2023, p. 431).

Historicamente, houve três formas de valoração da prova:

a) prova legal;
b) livre convencimento; e
c) persuasão racional ou livre convencimento motivado (Almeida, 2013, p. 102).

No primeiro sistema - o de prova legal (tarifário) -, os juízes eram espectadores passivos, pois,

a) havia uma predeterminação normativa da eficácia das provas ou
b) para a prova de determinados fatos exigia-se a demonstração de sua ocorrência por formas já estabelecidas (Nunes; Bahia; Pedron, 2021, p. 684).

Esse sistema não pode ser considerado método de avaliação da prova, pois impõe ao juiz a obediência a valores predefinidos, conforme as provas apresentadas. Por exemplo, no direito medieval, mesmo que o juiz acreditasse na veracidade do depoimento de uma testemunha específica, ele não poderia basear sua decisão apenas nesse elemento, devido à regra *testis unus testis nullus* (uma só testemunha não basta). Além disso, o depoimento de um cidadão nobre prevalecia sobre o de um servo. Esse sistema também era chamado de prova tarifada, porque todas as provas tinham um valor predeterminado (Fux, 2023, p. 431).

Depois, houve o sistema de livre convencimento – o de prova livre, diametralmente oposto ao critério da prova legal.

Nesse sistema, prevalece a convicção íntima do juiz, que possui total liberdade para investigar a verdade e avaliar as provas. Não há regras que restrinjam essa investigação, seja quanto aos meios de prova, seja quanto ao método de avaliação. Esse sistema vai ao extremo de permitir que o juiz se convença, com base em elementos fora dos autos e em oposição às provas apresentadas pelas partes. Embora tenha sido defendido entre os povos germânicos, esse sistema peca por seus excessos, que chegam a conflitar com o princípio fundamental do contraditório, indispensável em qualquer direito processual moderno (Theodoro Júnior, 2023, p. 805).

Na apreciação livre da prova, o julgador não está adstrito sequer a considerar verdadeiros os fatos sobre cujas preposições as partes concordam, podendo chegar a conclusões diversas daquelas deduzidas pelas partes (Miranda, 1974, p.213-214).

O terceiro sistema é apontado por grande parte da doutrina como o de persuasão racional do juízo ou livre convencimento motivado. (Neves, 2015, p. 503), o qual teria sido consagrado pelo art. 371 do CPC, que aponta que “o juiz apreciará a prova constante dos autos, independentemente do sujeito que a tiver promovido, e indicará na decisão as razões da formação de seu convencimento” (Brasil, [2024d]).

Alguma cautela deve ser adotada quanto à adoção dessa terminologia, entretanto.

Theodoro Júnior (2023) explica que alguns pontos devem ser observados para que se mantenha a sintonia do processo civil com a CRFB/1988, partindo deste raciocínio:

> (a) o convencimento não é livre e, portanto, não pode ser arbitrário, pois fica condicionado às alegações das partes e às provas dos autos;
> (b) a observância de certos critérios legais sobre provas e sua validade não pode ser desprezada pelo juiz (arts. 375 e 406) nem as regras sobre presunções legais;
> (c) o juiz fica adstrito às regras de experiência quando faltam normas legais sobre as provas, isto é, os dados científicos e culturais do alcance do magistrado são úteis e não podem ser desprezados na decisão da lide;
> (d) as sentenças devem ser sempre fundamentadas e tratar sobre todos os pontos levantados pelas partes, o que impede julgamentos arbitrários ou divorciados da prova dos autos (Theodoro Júnior, 2023, p. 808).

Nunes, Bahia e Pedron (2021) não são partidários da ideia de um livre convencimento motivado. Apontam que, com a superação do sistema de prova livre, surge uma perspectiva constitucional da prova, na qual a formação do provimento é comparticipada. O CPC inova ao retirar a expressão “livre convencimento do juiz”, restando proscrita a noção de que o destinatário precípuo da prova é o juiz, especialmente a de que o magistrado possa apreciar as provas com liberdade absoluta, sendo bastante a indicação de motivos para a oferta de seu pronunciamento. Apontam, ainda, que o único mecanismo fiscal (accountability) do CPC/1973 seria a licitude da prova, sistema esse que permitia toda sorte de alvedrios e enviesamentos decisórios, sendo isto inaceitável em um processo que se diz constitucional. (Nunes; Bahia; Pedron, 2021, p. 685).

Didier Júnior, Braga e Oliveira (2021, p. 124) compartilham dessa visão, anunciando que a extirpação do advérbio “livremente” do Novo CPC não foi fruto do acaso. Trata-se de um silêncio eloquente, de modo que a apreciação do juiz não é livre, como se o julgador pudesse apreciar as provas como bem entendesse. Nesse diapasão, seria incorreta a designação de “livre convencimento motivado” para o atual sistema de valoração da prova, como princípio fundamental do processo civil brasileiro.

Ommati (2021, 3.5) chega mesmo a apontar a inadequação do termo “motivação”, em um contexto de Estado Democrático de Direito, indicando que o correto seria “fundamentação”, quando leciona que ela deve explicar as razões pelas quais o Judiciário aceita ou rejeita determinada interpretação e compreensão do Direito estabelecidas pelo cidadão. A fundamentação não serve para expor a opinião pessoal de um juiz, desembargador ou ministro sobre o direito; isso constitui

motivação, algo irrelevante para o direito democrático. O objetivo da fundamentação é fixar a decisão juridicamente correta, independentemente das posições pessoais dos magistrados. Com a constitucionalização do direito fundamental à fundamentação, não há mais que se falar em livre convicção motivada, ou em decidir conforme a própria consciência, como muitos juízes e doutrinadores ainda insistem em fazer.

2.5 Finalidade da prova: uma orientação comparticipada

Didier Júnior, Braga e Oliveira (2019, p. 62) ensinam que há três teorias que procuram explicar a finalidade da prova: a) a que sustenta que seu objetivo é alcançar a verdade, b) a que parte da compreensão de que a finalidade da prova é fixar formalmente os fatos levados ao processo, e c) a que entende que o objetivo de carrear provas aos autos é formar o convencimento do julgador, levando-o a alcançar um grau suficiente de certeza sobre o que está sendo discutido.

Chegar-se à verdade plena, se é que ela existe, é tarefa impossível, utopia.

Diante da impossibilidade de se conseguir a verdade absoluta e do impotente instrumentalismo da segunda teoria, chega-se residualmente à terceira noção, de as provas dotarem o julgador de determinado grau de certeza sobre a matéria objeto de discussão.

Marinoni e Arenhart (2022, p. 63) chegam a afirmar que “é possível dizer que a prova não tem por objeto a reconstrução dos fatos que servirão de supedâneo para a incidência da regra jurídica abstrata que deverá [...] reger o caso concreto”.

De fato, Miranda (1974, p. 225-226) leciona que a finalidade processual da prova é persuadir o juiz, que, além de suas qualidades humanas, como inteligência, reflexão e raciocínio, deve seguir regras de convicção impostas pelo Estado que o designou como seu representante.

Santos (1952, p. 15) sustenta visão similar, afirmando que “a prova visa, como fim último, a incutir no espírito do julgador a convicção da existência do fato perturbador do direito a ser restaurado”.

A finalidade da prova jamais pode ser divorciada de uma noção constitucional de processo, devendo sua produção e apreciação sempre serem permeadas pelo

plexo de garantias fundamentais[1], mormente o devido processo constitucional, o contraditório, a ampla defesa e a fundamentação das decisões judiciais, tendo por base as provas dadas no processo.

Assim, de fato pode se afirmar que a função das provas em juízo é a de formar o convencimento do magistrado, que não pode se desonerar do dever de julgar, mas, sempre com respeito às garantias fundamentais. Afinal, em um processo comparticipado, as provas vocacionam-se não só ao magistrado, mas a todos os envolvidos no processo, o que faz sugerir uma visão mais moderna do instituto das provas, em linha com a Carta Magna/1988 e com os princípios e as garantias dela decorrentes.

Por fim, pode-se sintetizar que a finalidade da prova é conduzir o entendimento do magistrado sobre as questões postas à sua apreciação, assegurando às partes o pleno exercício da participação no processo, de forma a contribuírem para a resolução mais justa e adequada do litígio.

2.6 Ônus da prova

Se fazermos uma simples consulta em qualquer prestador de serviço de busca da internet, como o Google, entenderemos que o vocábulo ônus tem como sinonímia a palavra obrigação, mais especificamente outros termos, como encargo, gravame, dever, compromisso, responsabilidade, incumbência, pensão (Neves, 2024).

Ocorre que, em matéria probatória, o termo ônus deve ser lido de maneira diametralmente oposta, como uma faculdade. Na verdade, pode se caracterizar o ônus probatório enquanto tal, apenas porque a parte que não fizer uso dessa faculdade incorrerá na consequência jurídica de que a sua não utilização será levada em conta para fundamentar a decisão do juiz no caso concreto.

[1] A terminologia envolvendo "princípios fundamentais" e "garantias fundamentais" frequentemente se sobrepõe, especialmente no âmbito dos direitos processuais. Enquanto os princípios fundamentais expressam valores estruturantes que orientam o ordenamento jurídico, as garantias fundamentais configuram instrumentos que asseguram a concretização desses valores. No entanto, essa diferenciação é especialmente imprecisa em relação aos institutos processuais, como o devido processo constitucional, que, simultaneamente, reflete um princípio orientador e opera como uma garantia de proteção aos direitos das partes. Por essa razão, adotamos ora o termo “garantias”, ora “princípios”, indistintamente.

É isso que Theodoro Júnior (2023, p. 816) quer dizer, quando afirma que, no direito processual, ônus refere-se à conveniência de um indivíduo agir de determinada maneira, para evitar consequências desfavoráveis decorrentes de sua omissão. Em outras palavras, esse conceito sugere que o ônus não é uma obrigação, mas uma atitude positiva de um sujeito para evitar prejuízos processuais.

A ideia de que o ônus da prova implica direito da parte adversa é equivocado. Antes, é um imperativo do próprio interesse de cada litigante, tratando-se de uma situação de risco, em que aquele que não demonstra o quanto alegado pode perder a causa. Demonstrando-se a veracidade dos fatos que a lei designa é que essa carga é afastada (Couture, 2008, p. 116).

Assim, as partes têm a faculdade de provar os fatos das alegações que fundamentam sua pretensão. A prova não deve ser produzida porque há uma obrigação ou um dever legal para tanto, mas, porque se não o fizer, corre o risco de não ter sua pretensão acolhida. Dito de outra maneira, trata-se mais de uma necessidade que de uma obrigação (Almeida, 2013, p. 56).

A doutrina divide o ônus da prova em dois sentidos: subjetivo e objetivo. O aspecto subjetivo seria dirigido às partes, como uma espécie de incentivo do sistema, para que as partes tragam prova da alegação dos fatos constituintes do seu direito. É a maneira mais incisiva com que o sistema estimula o enriquecimento do material probatório. Expliquemos.

Uma vez que o ônus da prova é alocado sobre a parte que, segundo uma regra da experiência utilizada pelo legislador, estaria de posse da prova, onerando-a, o legislador estaria incentivando as partes a levarem provas para o processo, forrando-o com os elementos necessários para a formação da convicção judicial.

Partindo da premissa de que o processo, via de regra, lida com versões contraditórias dos fatos, o legislador incumbe a cada parte a tarefa de aportar aos autos as provas que a beneficiariam. Assim, essa faceta do ônus da prova seria uma espécie de sanção à inércia, uma necessidade criada pelo desejo de sagrar-se exitoso na demanda, fazendo com que o litigante se esforce para trazer todos os meios de prova de que disponha aos autos e, por conseguinte, contribuir para o deslinde dos fatos (Ramos, 2022, p. 68-69).

Já o aspecto objetivo do ônus da prova se associa à figura do juiz, não estando relacionado à atividade das partes de maneira imediata. Isso, porque, uma vez que o

aspecto objetivo do ônus da prova entra em jogo, a atividade probatória das partes já se encerrou. Esse aspecto objetivo do ônus da prova parte da premissa de que o juiz não pode considerar, em sua decisão, a alegação por uma das partes de fato que não restou provado nos autos. Serve, portanto, como regra de julgamento, quando, após toda a produção probatória pelas partes e após a determinação de ofício pelo juiz, o fato alegado ainda não restar esclarecido (Ramos, 2022, p. 66-67).

Esse aspecto objetivo sofre críticas da melhor doutrina. É que, quando o constituinte elege o ideal democrático como autorizador da ampla participação do cidadão no provimento jurisdicional, estimulando a cooperação, é inconcebível que não se adote o modelo cooperativo de processo. Destarte, as normas de distribuição do ônus da prova devem ser consideradas como regras de procedimento, sendo imprescindível comunicar às partes que determinado fato não está devidamente aclarado, de modo que o sujeito onerado possa tentar se desincumbir de seu encargo probatório, evitando uma decisão surpresa pautada na distribuição do ônus da prova. “No modelo cooperativo de processo, não é viável assumir que o ônus da prova seja um dever de provar ou que apenas importante ao tempo da elaboração do provimento jurisdicional”, sob risco de implicar decisões não fundamentadas adequadamente, e baseadas tão somente na inércia de uma das partes (Nunes; Bahia; Pedron, 2021, p. 694-695).

2.6.1 Distribuição do ônus da prova

Uma relevante inovação trazida pelo CPC/2015 é a mudança na regra de distribuição do ônus da prova. Se antes essa era estática, tendo por regra que caberia ao autor o ônus da prova sobre o seu direito, agora é dinâmica, sendo possível que o magistrado, diante das peculiaridades do caso, avalie quem tem melhores condições de se desincumbir do ônus probatório, seja de ofício ou a requerimento das partes (Nunes; Bahia; Pedron, 2021, p. 699).

Não obstante a regra consubstanciada no art. 373, *caput*, do CPC/2015, de que cabe ao autor o ônus da prova, no que respeita ao fato constitutivo de seu direito e ao réu quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor, aparecem possibilidades de distribuição do ônus da prova em determinadas hipóteses legais previstas no §1º do art. 373, quando for impossível ou de excessiva dificuldade

o cumprimento do encargo por uma das partes ou quando houver maior facilidade da obtenção da prova pela parte contrária.

Além disso, o Código de Defesa do Consumidor (CDC), em seu art. 38 (Brasil, [2022a]), estabelece que o ônus da prova da veracidade e a correção da informação ou da comunicação publicitária cabe a quem as patrocina.

Esse tópico será objeto de estudo mais detalhado no capítulo no qual abordamos as provas digitais.

2.7 Prova e verdade

Ao abordarmos os problemas enfrentados pela prática jurídica no que respeita às provas, é imperativo tratar de um tema filosófico de relevância para o instituto das provas: a verdade.

Não pretendemos esgotar o instituto, mas esboçar uma relação entre a busca da verdade e a utilização de provas no processo. Afinal, o que se pretende em um processo com o emprego de provas é justamente demonstrar o acontecimento de um determinado fato que acarrete uma potencial consequência jurídica.

Como dito anteriormente, a verdade última e real é inalcançável, todavia, é indispensável ter um norte, a fim de que a demonstração da ocorrência de um fato leve a um provimento jurisdicional, razão pela qual o estudo do instituto da verdade, ainda que sucintas, merece algumas considerações.

2.7.1 Michele Taruffo: anotações sobre verdade

Em sua obra *Uma simples verdade: o juiz e a construção dos fatos*, Taruffo (2016) dedica um capítulo inteiro à questão da verdade, iniciando-o a partir de um apanhado histórico, recordando que o conceito de verdade foi dado por superado na “embriaguez pós-moderna”, sendo proposta sua extirpação da filosofia por autores como Richard Rorty, para quem a verdade nada mais seria que um consenso sobre algo entre amigos. Assim, no pós-modernismo, uma abordagem cínica à verdade acabou por imperar, resultando na crença da existência de verdades múltiplas, de tal maneira que, se pessoas suficientes tomassem algo por verdadeiro, esse algo seria verdadeiro.

O paradoxo ínsito a essa abordagem é que se cada um tem a sua verdade pessoal, ninguém comete erros, ou seja, a verdade é relativa. Sob a ótica dessa lógica, houve um tempo em que era verdade que os negros eram seres inferiores aos brancos, assim como também era verdade universal medieval que a Terra era plana e o Sol girava em torno dela.

Com o tempo, os efeitos dessa embriaguez começaram a esvanecer, embora não fosse possível retornar ao status quo ante, com o que a passagem do pós-modernismo, para o que Taruffo (2016) chama de pós-pós-modernismo, implicou notáveis mudanças de perspectiva, no que respeita ao problema da verdade.

Ninguém fala de verdades ou certezas absolutas nesse pós-pós-modernismo, o que seria “privilégio do fanático”, mas delineiam-se formas de realismo crítico que convergem sobre importantes pontos, como o de que há sentido em julgar que o mundo externo existe. Não se trata de algo em que possamos ou não acreditar, mas um pressuposto indispensável para a própria possibilidade de pensarmos a realidade, a partir de opiniões ou teorias.

O segundo ponto de convergência diz de uma ideia de que todo enunciado relativo a acontecimentos no mundo real é verdadeiro ou falso, em função desses acontecimentos no mundo real, o que denomina uma concepção correspondista da verdade, segundo a qual a realidade externa existe objetivamente, e constitui a medida que determina a veracidade ou falsidade dos enunciados sobre ela.

Taruffo (2016) acentua que, ainda que alguém não se filie a essa tese realista, é possível escapar da “espiral solipsista típica do ceticismo pré e pós-moderno”.

Trata-se da concepção epistêmica da verdade surgida com Dewey, segundo a qual, a verdade de um enunciado corresponde à existência de razões válidas para julgar-se verdadeiro um enunciado.

Com tudo isso, Taruffo (2016) aponta restar claro que a verdade é objetiva, digna de ser cultivada por si mesma.

Reconhece, entretanto, que a ideia de verdade é culturalmente relativa, uma vez que pode haver culturas a) em que o conceito de verdade não exista ou não importe ou b) que utilizam métodos diferentes para buscar a verdade, o que a contextualizaria naquela cultura.

Apesar de essa dupla relatividade da ideia de verdade reabrir o problema, Taruffo (2016) aponta que não parece justificável um relativismo extremo e niilista

sobre o conceito de verdade, sendo a verdade de um enunciado correspondente aos acontecimentos que aquele enunciado descreve. Se assim não fosse, chegaríamos à conclusão de que existem infinitos conceitos de verdade, todos substancialmente equivalentes. Isso equivaleria a dizer que a verdade não se relaciona ao seu contexto real, mas à metodologia de cada um.

Resta daí Taruffo (2016, p. 96-104) entender a verdade como a correspondência entre um enunciado sobre determinado fato e a ocorrência desse fato no mundo objetivo, que é real.

2.7.2 Da verdade como correspondência

Aristóteles (1969, p. 107) talvez tenha sido um dos primeiros a apresentar uma concepção de verdade como correspondência, ao formular que “dizer daquilo que é que não é, ou daquilo que não é que é, é falso, enquanto dizer daquilo que é que é, ou daquilo que não é que não é, é verdadeiro”.

Vale dizer que Aristóteles (1969) apresenta um conceito centrado na Lógica para tratar da verdade: se A, então A, se B então B. Mas, A não pode ser B e B não pode ser A, porquanto conceitos excludentes.

Essa noção é particularmente importante à medida que, como já comentamos, surgiu nas últimas décadas o que foi denominado veriphobia, definido como “um profundo ceticismo ou um completo repúdio da verdade como um critério viável para o estudo dos fenômenos epistêmicos” (Goldman, 1999, p. 7).

A refutação dessa aversão à verdade é particularmente adotada pela Escola de Girona, cujo maior expoente é Taruffo (2016).

Como já visto, Taruffo (2016, p. 95), discorrendo sobre o tema, lembra que, no período pós-moderno, o conceito de verdade foi segregado, sendo considerado instrumento superado e não confiável, no qual “acabou por ser dominante uma abordagem cínica à verdade, assim como à objetividade e ao conhecimento”.

Ramos (2022, p. 22-23), aluno de Taruffo em Girona, também aborda essa questão, sendo enfático no sentido de que devemos defender a existência da verdade, a qual independe de sujeitos, sendo, por isto, objetiva, “e que algo é verdadeiro quando corresponde ao ‘mundo lá fora’, à realidade; isto é, mediante a adoção de uma visão correspondista da verdade”. Com isso, Ramos quis dizer que algo é verdadeiro,

na medida em que corresponda à realidade.

A abordagem correspondista assume que a verdade nada mais é que a correspondência entre o enunciado sobre o acontecimento de um fato e o acontecimento desse fato.

Ramos (2022, p. 25) afirma que algo análogo acontece no Direito, pois a verdade de um enunciado diz somente do que acontece no mundo real, não do que foi decidido pelo julgador, apresentando o simples exemplo de que a proposição “Pedro matou Maria” será verdadeira se, no mundo real, Pedro tiver matado Maria, em uma verdadeira correspondência entre afirmação e mundo real.

Ainda que ninguém acredite que Pedro tenha matado Maria, isso não altera a realidade. Não é o sujeito, a partir de suas percepções, que cria a realidade. Ela existe a partir do momento em que a realidade se relaciona diretamente ao enunciado que descreve essa realidade.

Essa visão correspondista é adotada por filósofos como Wittgenstein e Russel. Haack (2002), ao relacionar tais autores a essa visão de correspondência da verdade à realidade, assevera:

> O mundo consiste em coisas simples, ou átomos lógicos, em diversos complexos ou arranjos, que são os fatos. E, em uma linguagem perfeitamente clara, o arranjo das palavras em uma proposição atômica verdadeira refletiria o arranjo das coisas simples no mundo. A ‘correspondência’ consiste neste isomorfismo estrutural (Haack, 2002, p. 133-134).

Lynch (2001, p. 9) retoma a lógica aristotélica, afirmando que a visão realista mais venerável é certamente a teoria da correspondência da verdade, a visão de que uma proposição é verdadeira apenas quando corresponde à realidade. Afirma-se, frequentemente, que este é o objetivo, reiteramos, da afirmação de Aristóteles de que “dizer aquilo que é, não é, ou aquilo que não é, é, é uma falsidade; dizer que aquilo que é, é, e aquilo que não é, não é, é verdadeiro".

Esses aspectos são cruciais para uma compreensão da noção da verdade como correspondência, especialmente no Direito, assumindo a premissa de que o objeto da prova é a alegação sobre um fato, não o fato em si, sob uma visão plenamente correspondista.

2.7.3 A verdade no processo judicial

A prova judicial implica, de certa maneira, uma verificação - ou confrontação - das alegações das partes, com os elementos por elas fornecidos em juízo com o condão de firmar ou invalidar essas afirmações. Trata-se de um método reconstrutivo, dado que se destina justamente a reconstruir fatos. Partindo desse pressuposto, a prova judicial seria propriamente um método de investigação dos fatos, de modo que alguns autores tratam o objeto da prova como verdade, ou, pelo menos, certa classe de verdade (Dellepiane, 1958, p. 39-40).

Amendoeira Júnior (2012, p. 507) corrobora esse entendimento, quando afirma que o que se busca com a prova é a verdade quanto ao fato sobre o qual versa o processo (fato controvertido), destacando, entretanto, as limitações que o juiz enfrenta em sua atuação de conduzir o processo, dados os limites impostos por lei.

Para Ferrer-Beltrán (2023b, p. 52-53), a prova, como atividade, tem a função de comprovar a ocorrência dos fatos aos quais o Direito atribui consequências jurídicas, ou, em outras palavras, determina a veracidade das proposições que descrevem esses fatos. O êxito do sistema probatório é alcançado, quando as proposições sobre os fatos declarados provados, são verdadeiras. Para o autor espanhol, é evidente que a busca pela verdade é o objetivo principal da atividade probatória no processo judicial, embora não seja o único objetivo.

Por outro lado, Santos (1952), em sua obra *Prova judiciária no cível e comercial*, não concebia a busca pela verdade absoluta, lecionando que a verdade consiste na conformidade da noção ideológica com a realidade. Ele defendia o conceito de uma verdade relativa, em oposição à verdade absoluta, sempre buscada, mas nunca plenamente alcançada. Dado que a verdade só pode ser perseguida e percebida por meio dos sentidos e da inteligência, fica evidente, considerando a precariedade dos primeiros e a insuficiência da segunda, a necessidade de uma visão relativa da conformidade entre a noção ideológica e a realidade. Por isso, a verdade é algo que varia no tempo e no espaço. Assim, exemplifica: na verdade de ontem - a pena é uma vingança - cede à verdade de hoje - a pena é um método de ressocialização (Santos, 1952, p. 12).

Nas palavras de Nunes, Bahia e Pedron (2021), deve-se

> atentar [...] que os fatos passados jamais serão plena ou objetivamente retratados nos autos: a uma porque há, necessariamente, limitação de tempo e dinheiro para se avançar indefinidamente na busca dos fatos; a duas porque toda reconstrução é sempre uma interpretação; por fim, porque se espera que cada parte traga aquilo que demonstre suas próprias razões, ou seja, há uma parcialidade normal no recorte que autor e réu farão dos eventos" (Nunes; Bahia; Pedron, 2021, p. 683).

Marinoni e Arenhart (2022, p. 63) afirmam que, embora "toda a teoria processual esteja [...] calcada na ideia e no ideal de verdade [...], não se pode negar que a ideia de se atingir, por meio do processo, a verdade real sobre determinado acontecimento não passa de mera utopia".

Carnelutti (2009, p. 22) foi um grande crítico do conceito de verdade que se pretenda absoluta, constatando toda a parcialidade daquilo que se entende como verdade, com o entendimento de que "cada homem [...] é uma parte. Precisamente por isto, nenhum homem chega a alcançar a verdade. Aquela que cada um de nós crê ser a verdade não é senão um aspecto dela". Também assenta a noção de que a coisa julgada não é a verdade, mas um substituto da verdade, aquilo que é convencionado como verdade.

Para o jurista italiano, a verdade está no todo e não na parte, tornando oca qualquer pretensão de definição de verdade. O todo é demais para qualquer ser humano. Afinal, cada qual experimenta a realidade de acordo com a percepção de seus sentidos, de modo que não se pode falar em algo absoluto, completo e acabado, quando se parte de um ponto de vista limitado e singular.

Marinoni e Arenhart (2022, p. 37) enfatizam o entendimento de que não é possível falar em uma verdade absoluta, quando afirmam que a reconstrução de um fato ocorrido no passado sempre é influenciada pelas perspectivas pessoais de cada pessoa que presenciou o fato, ou mesmo o julgador, que tem seu próprio arcabouço de experiências e por ele é influenciado.

Quando do confrontamento de fatos, o julgador não estaria em condições de proferir uma sentença que reflete a verdade, mas tão somente sopesar, de forma falha, as evidências trazidas aos autos, revelando a fragilidade de tal processo.

Isso não quer dizer que seja inútil a busca pela reconstrução dos fatos, mas, apenas que se deve ter em conta a falibilidade de qualquer método que busque a

verdade absoluta, o que realça ainda mais a importância dos limites impostos pelo processo constitucional, como o contraditório, a isonomia, o devido processo constitucional e o acesso à Justiça.

2.7.4 Verdade formal e verdade substancial: da irrelevância de sua distinção

Uma distinção histórica clássica para o processo é a de verdade formal, teoricamente suficiente para o âmbito cível, e verdade substancial, necessária para o processo penal.

A verdade formal seria aquela constante do processo e juridicamente apta a sustentar a decisão judicial, enquanto a substancial demandaria uma absoluta correspondência entre o conceito apresentado e a essência da realidade.

A premissa é a de que o processo penal, por lidar com a liberdade do sujeito, exigiria um grau absoluto de certeza de um fato, enquanto as matérias afetas à esfera civil não demandariam tamanha imposição.

Ocorre que essa distinção perde relevância, especialmente diante de um Estado Democrático de Direito, em que interesses humanos são colocados em posição de destaque, seja na esfera penal, seja na cível, como questões relativas a família, dignidade, capacidade jurídica e direitos metaindividuais (Marinoni; Arenhart, 2022, p. 34-35).

Taruffo (2016), fundamentado em outras premissas, afirma tratar-se de uma falácia a distinção entre verdade formal – ou processual - e real. É que a distinção, supostamente, estaria no fato de que no processo existem normas que condicionam a apuração de fatos e regras que limitam a busca da verdade. A falácia é que não se pode dizer que existem diferentes formas de verdade, uma dentro e outra fora do processo: a verdade dos enunciados sobre o acontecimento de fatos é determinada pela ocorrência dos fatos no mundo real, retomando uma visão correspondista. Isso pode acontecer tanto dentro quanto fora do processo. Ainda que determinadas normas condicionem a busca da verdade a certos parâmetros, isso não quer dizer que essas condicionantes determinem a descoberta de uma verdade diferente daquela encontrada fora do processo. O problema não diz respeito à verdade, mas aos limites que a disciplina processual consente que os fatos sejam apurados (Taruffo, 2016, p. 106-107).

Didier Júnior, Oliveira e Braga (2019, p. 61) trazem o mesmo escólio de Taruffo, aduzindo que a verdade com que a ciência - e também o processo - deve se preocupar é sempre relativa e contextual. A par de seu objetivo de pacificação social, o processo é método de investigação de problemas, mediante a participação em contraditório das partes e cooperação dos sujeitos envolvidos.

Diante desse panorama, desaparece qualquer utilidade de tal distinção para efeito de apreciação de provas, com o condão de se formar o convencimento do julgador.

2.8 Síntese do capítulo

Com o propósito de introduzir o leitor ao tema objeto de estudo da presente pesquisa, o trabalho começou pela exploração do instituto que, ao fim e de forma mais genérica, é objeto de exame: a prova judicial. Nessa trilha, abordamos tópicos elementares, de modo a caminharmos para o universo das provas digitais. Apresentamos visões, muitas vezes divergentes, sobre os conceitos de prova, seus destinatários, seu objeto, sua finalidade, valoração, o instituto do ônus da prova e sua distribuição, bem como fizemos uma brevíssima incursão pelo instituto da verdade, primeiro pela ótica da filosofia, adotando a obra de Taruffo (2016) como guia, para depois conceituarmos verdade como correspondência, que guarda grande sintonia com a atividade praticada nos tribunais, a fim de se formar o convencimento do julgador, e pôr fim às questões postas à apreciação.

Em seguida, tratamos das reflexões doutrinárias sobre a verdade no processo judicial e da irrelevância da clássica distinção entre verdade formal e verdade real para o Direito. Com tudo isso, notamos que a visão prevalente sempre era orientada pelo processo constitucional. Cada instituto abordado neste contexto se prestou a sustentar a premissa de que as provas constituem um direito constitucional inserido em um microssistema estruturado por um conjunto de garantias processuais inarredáveis, em um processo que se pretende dotado de legitimidade.

3 DA PROVA NA CONSTITUIÇÃO FEDERAL/1988

3.1 Do direito processual constitucional

A importância desta subseção decorre da necessidade de compreendermos alguns elementos básicos que compõem a estrutura de um processo em um Estado Democrático de Direito, instaurado após a superação dos paradigmas a) liberal, que tem início com a revolução industrial, e b) social, decorrente do esgotamento do primeiro modelo em meados do século XX, após as duas Grandes Guerras e a crise econômica mundial da década de 1930.

Assim, visamos a examinar a estreita relação entre Estado Democrático de Direito e o modelo vigente de processo lastreado na CRFB/1988 e indissociável das ideias de Estado Democrático e de Estado de Direito, de modo que podemos mesmo afirmar que o processo tem por escopo o próprio fortalecimento do Estado Democrático de Direito.

Tudo isso em vista da noção de que o direito à produção de provas constitui faculdade processual que emana dos direitos fundamentais do acesso à Justiça, do contraditório e da ampla defesa, dentre outros, integrando o plexo de prerrogativas jurídicas asseguradas pelo devido processo constitucional.

De acordo com Didier Júnior, Braga e Oliveira (2019), a evolução da ciência processual costumeiramente é dividida em três fases:

a) o praxismo, ou sincretismo, em que fica ausente a distinção entre processo e direito material;
b) o processualismo, momento em que as fronteiras entre o direito adjetivo e o direito material foram demarcadas; e
c) o instrumentalismo, com o qual se busca estabelecer uma relação circular de interdependência entre o direito material e o adjetivo:

> o direito processual concretiza e efetiva o direito material, que confere ao primeiro o seu sentido [...]. Na fase instrumentalista, o processo passa a ser objeto de estudo de outras ciências jurídicas, como a sociologia do processo – que se concentrou nos estudos sobre o acesso à justiça. Além disso, há grande preocupação com a efetividade do processo, tema que não existia até então, e a tutela de novos direitos, como os coletivos (Didier Júnior; Braga; Oliveira, 2019, p. 52).

Didier Júnior, Braga e Oliveira (2019, p. 52) lecionam, ainda, que, hoje, “parece mais adequado [...] considerar a fase atual como uma quarta fase da evolução do direito processual. Não obstante mantidas as conquistas do processualismo e do instrumentalismo, a ciência teve de avançar e avançou.

E é, justamente nesse ponto, que a ciência processual se encontra, no que é notadamente denominado processo constitucional por grande parte da doutrina.

Para Ferreira (2015), esse movimento de aproximação da Carta de 1988 com o processo garante, preserva e promove os direitos fundamentais expressos na supracitada Constituição, passando o processo a ser visto sob uma nova perspectiva. Com a promulgação da CRFB/1988, ocorreu uma valorização de direitos e garantias fundamentais, dando origem a uma nova fase do pensamento constitucional, conhecida como Neoconstitucionalismo.

Paralelamente, com a evolução do direito processual, ocorreu a constitucionalização desse ramo, inaugurando uma nova fase denominada Neoprocessualismo. Essas transformações foram concretizadas no novo CPC/2015 (Ferreira, 2015).

Ou seja, estamos diante da indissociabilidade entre:

a) uma CRFB/1988 que arquiteta e concebe o Estado como Democrático e de Direito, com os objetivos primários de resguardar as pessoas do abuso desse Estado e de concretizar direitos fundamentais; e
b) de um modelo de processo que concorre para a consecução desses fins, sendo vocacionado para a perfeição desses objetivos, por meio de garantias enunciadas em seu texto.

Assim, é possível vislumbrarmos que o paradigma processual vigente é orientado para a concretização dos princípios fundamentais, razão de ser do Estado Democrático de Direito, que é de Direito por sua aptidão, para limitar o poder do Estado, a fim de garantir a ordem pública e proteger a Democracia, e. Democrático, porque elaborado pelo povo e para o povo.

Então, a ideia subjacente à de um processo constitucionalizado é a de que este processo passa a ser visto como um instrumento garantidor da concretização do exercício de direitos fundamentais, não simplesmente o de uma estrada em que o

primeiro passo é a propositura de uma demanda e o último o provimento estatal.

Isso visaria mais à satisfação de interesses privados que à concretização do que o art. 1º do CPC/2015 vai chamar de valores e normas fundamentais estabelecidos na CRFB/1988.

Esse movimento ganhou força no Brasil de forma tardia, enquanto já era o paradigma predominante nas sociedades ocidentais avançadas ao redor do mundo, desde meados do século XX.

Baracho Júnior (2023, p. 15) ensina que a jurisdição constitucional abstrata ganhou grande impulso na Europa após a Segunda Guerra Mundial, com o estabelecimento de diversos tribunais constitucionais. Posteriormente, esse movimento também se expandiu para a América Latina, especialmente após a redemocratização que marcou a região ibérica nas décadas de 1980 e 1990.

Em artigo publicado na Revista Eletrônica do Curso de Direito da PUC Minas Serro sobre o tema, a Professora Paolinelli (2016) também enfrenta essa questão, do ponto de vista do Direito brasileiro, ao asseverar que a

> concepção de processo constitucional como garantia de concretização e exercício de direitos fundamentais só foi possível a partir do momento em que a Constituição Brasileira de 1988 elegeu o Estado Democrático de Direito como matriz principiológica apta a orientar e reger toda e qualquer concepção normativa (Paolinelli, 2016, p. 33).

É a partir da vigência do Estado Democrático de Direito, com a promulgação da Carta de 1988, que o direito processual passa a extrair sua validade diretamente da CRFB/1988, com o asseguramento de todas as prerrogativas fundamentais inerentes ao processo.

Então, a chave para a compreensão do fenômeno da constitucionalização do processo civil é o advento do Estado Democrático de Direito. Mesmo assim, o texto legal só veio a consagrar esse entendimento, explicitamente, em 2015, com a edição do Novo Código.

E é a partir dessa leitura que entendemos superada a visão instrumentalista do processo e a norma superior volta-se para a fusão com a norma inferior, uma vez que, sob a ótica constitucional do processo, a relação entre normas infraconstitucionais e as constitucionais não é puramente hierárquica. O conteúdo de uma necessariamente deve corresponder ao de outra. Superior e inferior. Inferior e superior. As normas não

são unidirecionais. Amalgamam-se; são recíprocas (Didier Júnior, Oliveira; Braga, 2019, p. 55).

Perguntando-se o que é o processo constitucional, a professora (2016) aponta que a investigação parte do argumento de que o processo constitucional, por meio de uma abordagem sistemática e metodológica, é visão científica que examina as relações diretas e indiretas das normas processuais com a CRFB/1988, demonstrando como o processo constitucional reforça a tendência de constitucionalização do direito e institui garantias que asseguram o exercício dos direitos fundamentais.

Partindo das noções de Estado Democrático de Direito, conforme os princípios traçados pela CRFB/1988, evidenciamos que o processo e a jurisdição têm fundamento de validade nessa Carta. Um paralelo é traçado entre direitos e garantias fundamentais, destacando que as garantias constitucionais são essenciais para a efetivação dos direitos. Paolinelli (2016, p. 1) analisa as teorias que delineiam e sustentam o modelo constitucional de processo democrático, concluindo que o processo constitucional, sob uma perspectiva democrática, se constitui como uma metodologia normativa que garante o exercício e a concretização dos direitos fundamentais, proporcionando ao cidadão controle efetivo e participação na formação dos atos de poder estatal.

Fica evidente que se pretende tratar o processo como meio de efetivação dos direitos fundamentais e o cumprimento dos objetivos instituídos pelo constituinte, cuja atividade jurisdicional, muitas vezes, se incumbirá de prover.

É em face dessa noção de Processo Constitucional que o estudo da prova judicial deve se balizar.

Almeida (2013) trata a prova como direito humano e fundamental das partes no processo judicial. Isso vale tanto para aquele que apresenta a prova quanto para a parte que deverá sobre ela se manifestar.

Em obra dedicada à teoria dos elementos gerais da prova, o autor deixa claro que seu foco é a prova como instituto de perfeição do exercício dos direitos fundamentais por meio do processo, apontando que as Constituições, especialmente após a Segunda Guerra Mundial, promoveram uma verdadeira constitucionalização do processo judicial, definindo suas linhas mestras. Isso não apenas ressalta a importância do processo para a concretização dos direitos assegurados pela ordem

jurídica, mas também destaca a relevância das garantias processuais estabelecidas em favor das partes.

O Brasil não ficou alheio a esse movimento, como demonstra a Carta de 1988, na qual observamos que regras e princípios destinados à disciplina do processo compõem o denominado "direito constitucional processual". As partes, em um processo judicial, são titulares do direito de produzi-las, sendo o instituto caracterizado como legítimo direito humano, porque o reconhecimento dado por vários tratados e diversas convenções internacionais do direito de uso de provas para demonstrar a veracidade daquilo que se alega é, em si, o direito à prova, sendo expressamente reconhecida no Direito Internacional a existência do direito à prova como Direito Humano (Almeida, 2013, p. 146).

Isso assim é, porque os direitos fundamentais são intrínsecos à dignidade humana, pois se baseiam nela e servem como fundamento essencial de qualquer comunidade humana. Sem o reconhecimento desses direitos, o valor supremo da dignidade da pessoa perderia sua força, comprometendo a base de toda sociedade civilizada (Baracho, 2008, p. 108).

Esta é uma noção que deve estar bem delimitada, para se dar prosseguimento à pesquisa, uma vez que buscamos trilhar um caminho lógico que apontasse para a necessidade de se considerar a produção de provas em um novo contexto linguístico, como um instituto que habilitasse o Estado a promover a prestação jurisdicional, em consonância com a Norma Suprema de 1988, garantindo a verdade no processo, sem que se olvidassem de princípios e garantias fundamentais.

Parte-se, então, para o estudo dos princípios fundamentais que orientam a produção probatória em um contexto de Estado Democrático de Direito tutelado por um processo constitucionalizado.

3.2 Direito processual constitucional e princípios fundamentais atinentes à produção probatória

O direito à produção de provas decorre diretamente da Carta Federal, como corolário do Estado Democrático de Direito e é uma garantia processual fundamental, sem a qual não há a perfeição desse paradigma estatal, restando afastada qualquer possibilidade de um processo comparticipado e construído democraticamente, como

pretendeu o constituinte.

Assim é que surge uma miríade de princípios que sustentarão a produção de provas, como o contraditório, a ampla defesa, o devido processo constitucional e a vedação à prova ilícita.

Leal (2018, p. 272) disserta que o instituto jurídico da prova, em sua base teórica, possui como eixo fundamental a categoria de tempo-meio, que assegura a conquista teórica do processo coinstitucionalizado, o qual se configura pela conjunção e garantia dos institutos jurídicos da isonomia, ampla defesa, do contraditório e do devido processo legal. O art. 5º, inciso LVI, CRFB/1988 condiciona a realização procedimental da prova à utilização de meios lícitos.

A partir dessa premissa de que o direito à prova possui fundo constitucional, é que se pretende pincelar os fundamentos que o animam, sem, no entanto, esgotar o tema, por não ser objeto da presente pesquisa, mas trazer premissas fundamentais para seu desenvolvimento.

3.2.1 Do contraditório

Thamay e Tamer (2022, RB-1.1) definem o contraditório como um estado ideal em que as partes do processo devem sempre ter ciência de tudo que ocorre durante a ação, na petição inicial, defesa, nos despachos e nas decisões, bem como quaisquer outros atos processuais, de modo que possam efetivamente influir no convencimento do julgador ou da autoridade, especialmente, a partir da possibilidade de manifestação ou reação, em face do que tomam conhecimento. Assim, surge o binômio ciência e resistência, o primeiro indispensável e o segundo eventual. É dessa maneira que as partes sempre devem ser informadas de todos os atos do processo, a fim de que lhes seja oportunizada a possibilidade de manifestação. Porém, em função do princípio dispositivo, a opção de se manifestar, ou não, deve ser vista como ônus da parte, a qual deverá suportar as consequências de optar entre a manifestação e a inércia.

Prosseguem Thamay e Tamer (2022) com o raciocínio de que o princípio do contraditório assume um significado mais amplo e abrangente no contexto contemporâneo, em que o binômio puro e simples não atende o ideal democrático do constituinte. Asseveram que

> [...] o estado ideal das coisas, cuja determinação de constante busca e máxima eficácia advém do postulado constitucional do contraditório, tem por norte a possibilidade concreta e verificável de que a parte possa influir no entendimento e convencimento do julgador ou da autoridade sobre os fatos alegados. No fenômeno da constitucionalização do processo, que se dá notadamente pelo elenco de seus princípios no art. 5º da Constituição Federal, o contraditório se apresenta renovado, integrado pelo direito de influência e pelo dever de debate jurisdicional, ao que se agrega, por lógica e natureza das coisas, a instrução probatória (Thamay; Tamer, 2022, RB-1.1).

Tudo isso leva à conclusão de que o efetivo contraditório e a capacidade de influência no processo passam pela possibilidade de produção probatória em relação ao fato discutido. Os mesmos autores, em comparativa e inspiradora passagem, afirmam que “os princípios constitucionais da inafastabilidade e do contraditório, sem o mecanismo da prova, seriam como almas errantes em busca de seus corpos que pudessem lhes dar vida concreta”. (Thamay; Tamer, 2022, RB-1.1).

Nunes, Bahia e Pedron (2021, p. 399) adotam raciocínio parecido. Fazem uma crítica ao sistema processual brasileiro, comparando-o a um ambiente em que os interesses não cooperativos são prevalentes, pela própria dinâmica fática. Isso, porque os julgadores estão imersos em um sem-número de processos, buscando a otimização numérica de seus julgados, enquanto as partes praticam a litigância estratégica, com o único condão de obter êxito. Ou seja, trata-se de uma patologia que não reflete os comandos normativos impostos pelo processo constitucional. É um ecossistema em que cada um, premido por um ambiente de muita pressão, está apenas preocupado com o resultado final.

A comparticipação proposta pelos autores não quer dizer de uma colaboração entre as partes e o juiz, como defendido por correntes doutrinárias estrangeiras, mas, de uma cooperação embasada em um contraditório dinâmico que leva em conta as garantias de influência, debates e não surpresa, “na necessária participação de sujeitos interdependentes no ambiente processual durante todo o procedimento estruturado por princípios processuais constitucionais”. A cooperação não é mais mera colaboração, mas corolário do contraditório como garantia de influência no processo (Nunes; Bahia; Pedron, 2021, p. 400).

Didier Júnior, Braga e Oliveira (2019, p. 107), ao dissertarem sobre o princípio do contraditório, decompõem-no em duas garantias: a da participação e a da possibilidade de influência na decisão. A primeira, identificada com a dimensão formal

do princípio, é a garantia de ser comunicado, ouvido e a de falar efetivamente, participando do processo. É o conteúdo mínimo do princípio do contraditório, representando a visão tradicional sobre o tema, em que basta que o órgão jurisdicional dê ouvido à parte para que o princípio seja satisfeito. No entanto, essa acepção é insuficiente, surgindo, então, a dimensão substancial do processo, que garante a efetiva possibilidade de influência das partes na decisão do órgão jurisdicional, o chamado poder de influência. Assim, não basta que a parte seja ouvida no processo; é necessário que ela, efetivamente, possa influenciar o conteúdo da decisão.

Isso, porque o princípio democrático é perfeito, somente na medida em que os titulares do Poder, o povo, possam participar dos atos de manifestação do Poder, como é o caso de uma decisão judicial.

É precisamente na acepção substancial do princípio do contraditório, que se evidencia a estreita relação entre este princípio e a produção probatória, pois o contraditório assegura que ambas as partes possam participar ativamente do processo de formação de provas, promovendo a equidade e a transparência. Nesse sentido, cada parte possui o direito não apenas de apresentar suas próprias provas, mas também de contestar as provas apresentadas pela outra parte e de contribuir, significativamente, para o esclarecimento dos fatos. Essa dinâmica reforça a busca por uma jurisdição de qualidade no processo judicial, garantindo que a decisão final seja fundamentada em uma apreciação justa e completa das provas, respeitando os direitos e a influência das partes envolvidas.

3.2.2 Da ampla defesa

Outro princípio fundamental intimamente relacionado ao instituto das provas está previsto no art. 5º, LV, da CRFB/1988, junto com o contraditório, no qual se lê: “ LV (55) - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes” (Brasil, [2024a]).

Primeiramente, nota-se que é um instituto relacionado à garantia de defesa técnica pelas partes (direito fundamental de representação com o advogado), ou seja, que todo participante em processo possa contar com um profissional capacitado para promover a defesa de seus interesses (Nunes; Bahia; Pedron, 2021, p. 461-462).

Leal (2018, p. 264), tratando do tema, discorre que o direito à ampla defesa é corolário do princípio do devido processo legal (constitucional) caracterizado pela participação dos advogados nas partes ou junto aos interessados para a estruturação dos procedimentos jurisdicionais, [...] porque qualquer ato jurisdicional sem a vinculação do advogado é ato ilegítimo pela falta de suporte constitucional à sua validez, conforme estabelece claramente o art. 133 da Carta de1988.

Então, a primeira dimensão da ampla defesa diz do direito fundamental a representação por advogado.

Outra dimensão concerne ao direito de utilização de todo o arsenal argumentativo para a defesa dos interesses controvertidos em juízo.

Nunes, Bahia e Pedron (2021, p. 462) advertem que, ainda que intimamente relacionados, não se deve confundir o princípio da ampla defesa com o princípio do contraditório. É que este diz da possibilidade de oferecer resistência a um provimento judicial, enquanto aquele se relaciona ao direito “à exauriência argumentativa com todos os meios jurídicos a ela inerentes [...]”.

Lado outro, Didier Júnior, Braga e Oliveira (2019, p. 115) sustentam que ambos os princípios estão indissoluvelmente amalgamados, e que a ampla defesa nada mais seria que “o aspecto substancial do contraditório”, restando superada a tradicional distinção entre os princípios.

Barroso (2023, p. 279), também sem distingui-los, afirma serem especificações do princípio do devido processo legal, expressando o direito de ser ouvido, de produzir provas e de ter seus argumentos apreciados motivadamente, acrescentando que, no processo penal, esse conjunto de direitos é frequentemente denominado garantismo, termo que se refere ao direito de ser notificado da acusação, apresentar defesa, produzir provas, ser julgado por um juiz imparcial e, como regra geral, ter direito a, pelo menos, um recurso que permita a reavaliação das questões de fato e de direito..

Sem direito à ampla defesa, não se cogita direito à prova, uma vez que o julgador só pode fundamentar sua decisão, a fim de fixar direitos e obrigações das partes, em fatos cuja veracidade tenha sido comprovada, pois o fato que não é comprovado no processo, é juridicamente irrelevante. O direito à prova constitui, por isso mesmo, manifestação fundamental do direito de defesa (Almeida, 2013, p. 117).

O que resulta é que a doutrina diverge quanto à distinção entre contraditório e ampla defesa, mas não quanto a serem a essência do direito de produção de provas

em juízo.

3.2.3 Do devido processo constitucional

Este processo extrai sua validade do art. 5º, LIV da CRFB/1988, que o denomina “devido processo legal”, pois parte da noção de que o processo deve obedecer ao quanto disposto em lei.

Tal proposição não está incorreta, mas pensamos que a expressão apropriada seria “devido processo constitucional”. Isso, por uma questão de lógica.

Ora, se o processo deve obediência a uma lei e todas as leis devem estar em conformidade com a CRFB/1988, parece lógico que o processo estará, ao fim, adstrito às disposições constitucionais, que serão apenas reveladas no plano legal.

Ademais, adotando o entendimento de se estar diante de um devido processo legal, corre-se o risco de que princípios processuais fundamentais sejam solapados, por conta de uma redação legal que não leve esses princípios em conta, tornando o processo mais difícil do que já é, e permitindo discricionariedades.

Nunes, Bahia e Pedron (2021) caracterizam de forma precisa esse princípio, ao observarem que o que se busca com o devido processo constitucional é

> que todo exercício de poder público ou privado para a tomada de decisões deve seguir etapas formais obrigatórias asseguradoras de direitos previstas em lei e na Constituição, e, ter sido formado por um processo que atenda aos direitos fundamentais, garantindo o exercício dinâmico do contraditório e da ampla defesa com todos os meios que lhe são inerentes (Nunes; Bahia; Pedron, 2021, p. 389).

Deve-se pensar um devido processo constitucional, pois decisões ou pronunciamentos judiciais não são atos isolados do órgão jurisdicional. Eles são alcançados sob a rigorosa disciplina dos princípios constitucionais (devido processo constitucional) e através de uma estrutura normativa metodológica (devido processo legal). Isso assegura que tais decisões sejam construídas com base nos argumentos desenvolvidos em contraditório por aqueles que serão afetados por seus efeitos, em torno das questões de fato e de direito que estão em disputa no processo (Dias, 2022, p. 249).

Assim, percebemos a preocupação da moderna doutrina com um processo que esteja calcado no respeito aos princípios e às garantias fundamentais, perquirindo a

comparticipação dos atores processuais, a fim de que os fatos alegados possam ser devidamente debatidos e apreciados.

É imperativo destacar, ainda, que o julgador não pode deixar de apreciar demanda levada à sua apreciação, como se depreende do art. 140 do CPC/2015, como corolário do princípio do acesso à Justiça, insculpido no art. 5º, XXXV da CRFB/1988.

Assim, o devido processo constitucional balizará o convencimento do julgador, que deverá sempre se ater às suas competências constitucionais e exercer seu múnus em respeito às normas processuais constitucionais.

Exemplo disso está no art. 5º, LVI, da CRFB/1988 de que se depreende serem inadmissíveis as provas obtidas por meio ilícito.

Em um panorama de processo constitucional, essa garantia deve ser compreendida como princípio que pretende evitar o arbítrio das autoridades e tornar o Estado dotado de fortes instituições, obedientes à sua Constituição e leis.

Repise-se: a atividade judicante só poderá contribuir para perfazer o Estado Democrático de Direito, quando as instituições que lhe animam seguirem um processo que extraia sua validade diretamente da CRFB/1988.

3.2.4 Da fundamentação

Instituto que se relaciona diretamente à atividade probatória, pois, somente a partir da fundamentação que o jurisdicionado poderá exercer controle sobre a decisão proferida e, especialmente, extrair as informações a respeito de como o julgador decidiu, se valorou devidamente as provas postas à apreciação nos autos.

É dessa maneira que surge um processo comparticipado, em que todos os envolvidos são parte ativa na construção da decisão.

A fundamentação, no Direito Brasileiro, surge no art. 93, IX CRFB/1988, de que se depreende

> que todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação (Brasil, [2024a]).

Assim, não é difícil alcançar a conclusão de que o dever de fundamentação possui natureza de direito fundamental do jurisdicionado.

Como se pode deduzir da leitura do texto, é princípio que diz do dever do julgador, que materializa a figura do Estado, exercendo seu poder-dever de jurisdição, de expor as razões para decidir da maneira como decidiu.

A decisão não fundamentada é passível de nulidade, como se depreende do texto constitucional, revelando o caráter axiológico do instituto da fundamentação.

Didier Júnior, Braga e Oliveira (2019) apontam que sua importância é tamanha que,

> ainda [...] que não houvesse disposição constitucional expressa nesse sentido, o dever de motivar não deixaria de corresponder a um direito fundamental do jurisdicionado, eis que é consectário da garantia do devido processo legal e manifestação do Estado de Direito. A regra da motivação compõe o conteúdo mínimo do devido processo legal (Didier Júnior; Braga; Oliveira, 2019, p. 382-383).

Nas palavras de Taruffo (2016, p. 272), ao discorrer sobre as provas no processo, a “motivação dos fatos que inclui os enunciados relativos às circunstâncias que constituem os fatos principais da causa representa um aspecto essencial daquilo que se pode definir como ‘justificativa interna' da decisão analisada globalmente”.

Vale dizer que se trata do suporte fático-concreto trazido para o campo de aplicação da regra jurídica adotada como critério de decisão. Ao fim e ao cabo, é um enunciado que estabelece uma correlação entre as premissas de direito e a de fato, permitindo ao jurisdicionado estabelecer um controle sobre essa atividade de jurisdição a partir da análise das razões que levaram o julgador a decidir da maneira como o fez.

Didier Júnior, Oliveira e Braga (2019, p. 381) lecionam ser “comum o entendimento de que o convencimento judicial está fundado, sempre ou quase sempre, num juízo de verossimilhança. Esse entendimento se baseia na ideia de que a “verdade” é um ideal inatingível - e, por isso, não deve ser buscada como objetivo do processo.

Dias (2022, p. 255), evocando o escólio de Fazzalari, relaciona o instituto da jurisdição ao da fundamentação, ao lecionar que “se a jurisdição somente atua mediante o devido processo constitucional e se o processo é procedimento que se desenvolve em contraditório entre as partes, em condições de paridade, fundamentar

a decisão jurisdicional é justificar o órgão estatal julgador, no processo, as razões pelas quais a decisão foi proferida". (2022, p. 255).

Dias (2022), em incursão pela legislação comparada, aponta que o Estado brasileiro segue o modelo italiano, especialmente devido à enunciação do princípio da fundamentação no plano constitucional. Esse caráter de enunciação é reforçado pelo art. 11 do CPC, que estabelece que todos os julgamentos dos órgãos do Poder Judiciário serão públicos e todas as decisões fundamentadas, sob pena de nulidade. O paralelo com a Itália é evidente, pois a Constituição italiana, em seu art. 111, prescreve que "todos os provimentos jurisdicionais devem ser motivados". Em consonância, o CPC italiano, ao dispor sobre o conteúdo da sentença em seu art. 132, prevê "a concisa exposição do desenvolvimento do processo e dos motivos de fato e de direito da decisão".

Assim como no Brasil, o Estado italiano reforçou o princípio da fundamentação de forma clara e inequívoca. Na França, embora não haja disposição semelhante na Constituição, CPC, em seu art. 455, determina que "o julgamento deve ser motivado". Situação semelhante ocorre na Alemanha, onde, apesar da ausência de previsão constitucional, o § 313 do CPC estabelece a necessidade de que a sentença inclua os fatos e os fundamentos jurídicos, traduzindo o dever do órgão jurisdicional de motivá-la (Dias, 2022, p. 251-252).

Constata-se, portanto, que a fundamentação está intrinsecamente associada à produção probatória, uma vez que confere ao litigante – ou a quem tenha interesse – a capacidade de fiscalizar o ato decisório, o que ocorre a partir da compreensão da fundamentação da decisão do magistrado, que deve esclarecer porque as provas foram valoradas da maneira que foram.

Por fim, apenas se requer cautela quanto ao emprego da terminologia "motivação", que é fonte de forte crítica por parte da doutrina processual mais moderna, o que foi explorado anteriormente, em subseção sobre o objeto da prova, no capítulo sobre a Teoria Geral da Prova.

3.2.5 Do princípio do acesso à Justiça

A primeira noção que se deve ter clara é a de que Justiça, como pretensão de validade sobre a correção normativa, não deve ser confundida com a atividade

jurisdicional em si e nem ser alcançada apenas por meio do Judiciário em sua atuação sobre os litígios que ocorrem na sociedade, pois é necessário “observar o modelo constitucional de processo, como condição legitimadora do provimento estatal em substituição a uma vontade instrumentalizadora de uma racionalidade solipsista e redentora” (Nunes; Bahia; Pedron, 2021, p. 491-492).

Nunes, Bahia e Pedron (2021, p. 500) explicam que a contribuição do conceito de "acesso à Justiça", em termos discursivos abrange não apenas o direito de apresentar uma demanda ao Judiciário, mas, principalmente, a existência de um espaço processual no qual são garantidos às partes todos os princípios que compõem o devido processo constitucional, essencial para que o provimento seja legítimo, dotado de racionalidade comunicativa e que assegure a aplicação da "norma correta".

É justamente nesse espaço que a produção de provas surge como uma das facetas da materialização do princípio do acesso à Justiça.

Assim, é possível afirmar que também do princípio do acesso à Justiça decorre o direito à prova. Isso, porque esse princípio diz ao direito à tutela dos direitos, tornando certa a existência do direito à efetividade dos instrumentos para a sua consecução, caso da prova. Sem a demonstração da ocorrência do fato deduzido em juízo não será possível a prestação da tutela pretendida, ao passo que a ausência de concessão da tutela a direito assegurado pela ordem jurídica, inclusive por insuficiência na demonstração de sua existência, “impede a jurisdição e o processo de alcançarem o fim a que se destinam, afetando, com isso, a sua efetividade” (Almeida, 2013, p. 127).

3.2.6 Do princípio da vedação à prova ilícita

Este princípio é previsto, explicitamente na CRFB/1988, em seu art. 5º, LVI, que estabelece serem inadmissíveis no processo as provas obtidas por meio ilícito.

A lei processual enfatiza o comando constitucional, à medida que o art. 369 do CPC estabelece a liberdade probatória, condicionando-a, entretanto, a que os meios empregados para se provar a verdade dos fatos alegados sejam legais, bem como moralmente legítimos.

O Código de Processo Penal (CPP) caminha no mesmo sentido, quando, em seu art. 157, estabelece que as provas ilícitas, “assim entendidas as obtidas em

violação a normas constitucionais ou legais" (Brasil, [2024b]), são inadmissíveis no processo e devem ser desentranhadas dos autos.

Magalhães (2006, p. 179), tratando do tema sob a perspectiva do processo penal, explica que a questão da inadmissibilidade da prova ilícita no processo resulta do conflito existente entre a exigência de tutela da pessoa humana, mormente sua intimidade, e a exigência de tutela da comunidade, principalmente a segurança social. De um lado, há as garantias individuais da pessoa humana que devem ser observadas, durante a atuação investigatória dos órgãos persecutórios e pelo particular, principalmente as relativas à intimidade, vida privada e imagem das pessoas; de outro lado, há a exigência de punição dos criminosos.

Já Marinoni e Arenhart (2022, p. 292) corroboram a perspectiva de que a razão de ser da vedação decorrente do art. 5º, LVI da CRFB/1988 é a insuficiência de se sancionar a prova ilícita apenas no plano do direito material, sendo necessário negar eficácia a tais provas no processo. "O art. 5º, LVI, da CF não vedou a violação do direito material para a obtenção da prova – *pois isso já está proibido por outras normas*, mas proibiu que tais provas tenham eficácia no processo".

É de se observar que o ordenamento jurídico proíbe tanto as provas obtidas por meio ilícito, a exemplo de uma confissão obtida mediante tortura, quanto as provas ilícitas em si, como um documento adulterado.

O tratamento dado às provas ilícitas pelo processo penal é diferente daquele atribuído pelo processo civil, sendo preciso notar que, no primeiro, o réu é informado de seu direito de permanecer calado, termos do art. 5º, LXIII da CRFB/1988, enquanto, no segundo, as partes têm o dever de dizer a verdade. Essa distinção reflete a diferença dos bens jurídicos atinentes a cada matéria. Enquanto no processo penal, o direito a permanecer calado deriva do direito à liberdade, no processo civil não há um único bem correlato, sendo impossível determinar qual o bem de maior valor, o que está se discutindo no processo ou a ilicitude da prova, de modo que "a norma do art. 5º, LVI, da Constituição Federal pode ser conjugada com a opção do processo penal, mas, quando pensada em face do processo civil, apenas pode se ligar a uma falta de opção, ou melhor, de que essa opção seja feita no caso concreto" (Marinoni; Arenhart, 2022, p. 293).

Vale dizer que no processo civil, quando do choque de direitos fundamentais, a questão deve ser resolvida pelo princípio da proporcionalidade. Os autores Marinoni

e Arenhart (2022, p. 294) comentam, ainda, que os tribunais alemães e norte-americanos admitem as exceções à vedação da utilização de provas ilícitas, quando necessárias à satisfação de interesses considerados superiores no caso concreto, seja a natureza do que se decide pública ou privada. A proporcionalidade se mostra essencial para a justiça no caso concreto.

Nunes, Bahia e Pedron (2021) apontam que a jurisprudência acerca do tema no Supremo Tribunal Federal (STF), tem início com o julgamento do HC 69.912, em 1993, em que prolatada decisão que é considerada paradigma. É que, anteriormente, havia uma ideologia segundo a qual o magistrado poderia superar a ilicitude da prova, para se chegar à suposta verdade real. Por ventura do aludido julgamento, entretanto, o Ministro Moreira Alves realizou uma cisão epistemológica no instituto da prova, ao separar os conceitos de prova ilícita e prova ilegítima, ambas passando a ser encaradas como espécies do gênero prova antijurídica. A prova ilícita seria a prova criada com violação de norma penal, vale dizer: a CRFB/1988, ao preconizar a proibição de provas obtidas por meio ilícito, estaria proibindo apenas as provas obtidas a partir do cometimento de um crime, cuja consequência processual seria a declaração de nulidade da prova e aplicação da teoria dos frutos da árvore envenenada, para a qual todas as provas obtidas por meio da prova ilícita seriam nulas e deveriam ser extirpadas do processo. Já a prova ilegítima estaria relacionada à violação da norma processual, implicando outra consequência: a nulidade do instrumento da prova, mas a não aplicação da teoria dos frutos da árvore envenenada, “permitindo a derivação para outras provas obtidas a partir da primeira”.

Nos julgamentos seguintes, a discussão sobre a aplicabilidade da teoria do Ministro Moreira Alves ao processo civil foi levantada e, quando do julgamento do HC 389.808, foi assentado que, em caso de confronto entre princípios, deveria ser feito um juízo de valor para verificar qual deles tinha mais peso relativo no caso concreto. “Se ficasse registrado que, no balanceamento entre a prova ilícita e outro direito com mais peso, o tribunal poderia receber uma prova ilícita e julgar afastar sua nulidade” (Nunes; Bahia; Pedron, 2021, p. 701-702).

Os mesmos autores ponderam, entretanto, que apenas as provas e decisões derivadas diretamente da prova ilícita serão nulas. Assim, são nulas as provas obtidas de forma independente, porém, válidas as provas que, apesar de terem derivado de prova ilícita, puderem ser obtidas de outra maneira. Quanto à decisão, aquela

fundamentada em prova ilícita ou derivada será nula, bem como a decisão proferida em processo no qual a prova ilícita e as derivadas não tiverem sido retiradas dos autos, desde que contrárias à parte prejudicada (Nunes; Bahia; Pedron, 2021, p. 702-703).

Didier Júnior, Braga e Oliveira (2019, p. 116) reforçam que “a doutrina e os tribunais não aceitam as chamadas provas ilícitas por derivação”, citando posicionamento, nesse sentido, por parte do STF, por ventura do julgamento do HC 69.912-RS, em 16 de dezembro de 1993, de Relatoria do Ministro Sepúlveda Pertence, destacando algumas exceções, como a derivação mediata (inexistência de nexo de causalidade) (não é essa prova ilícita que determina a decisão, ela simplesmente está no processo) e a descoberta inevitável (prova que seria obtida de qualquer maneira), o que também é reconhecido pela jurisprudência norte-americana.

3.3 Síntese do capítulo

Após expormos sobre a Teoria Geral da Prova no capítulo 2, nosso foco se voltou para a análise da prova à luz da CRFB/1988, precedida por uma breve introdução ao modelo processual mais adequado ao contexto atual: o processo constitucional. O texto enfatizou que apenas um processo que harmonize a CRFB/1988 com as normas infraconstitucionais pode, efetivamente, assegurar os direitos fundamentais, ao estabelecer garantias processuais que permitam ao povo, titular do poder, o pleno exercício desse poder.

Na sequência, foram examinados os principais princípios constitucionais que orientam a atividade probatória, destacando-se que, sem eles, qualquer tentativa de legitimar o processo se revela inútil. Esses princípios, apresentados como indissociáveis dentro do microssistema do direito probatório, formam um complexo axiológico-normativo, cujo estudo se mostra essencial para alicerçar a pesquisa sobre as provas digitais.

4 DA DISRUPTURA TECNOLÓGICA

4.1 Novos paradigmas

É notória a transformação, em âmbito global, com o advento da denominada Era da Informação.

Tratando do atual paradigma social em que vivemos, o sociólogo e professor universitário espanhol Castells (2000) se refere às características que definem essa nova realidade, sendo cinco as principais:

a) a informação é sua principal matéria-prima, servindo efetivamente como tecnologia para agir sobre a informação, e não apenas informação para agir sobre a tecnologia, ao contrário do que se viu nas revoluções tecnológicas anteriores;
b) a penetrabilidade dos efeitos das novas tecnologias é evidente, pois a informação é integral a toda atividade humana, moldando todos os processos de nossa atividade individual e coletiva;
c) a lógica de redes parece se aplicar a qualquer sistema ou conjunto de relações, com a morfologia da rede estando bem adaptada à complexidade e aos modelos de interação crescentes.

Além disso, da difusão das redes surge um crescimento exponencial, dadas as conexões aumentadas;

d) a flexibilidade do sistema de redes, no qual processos são reversíveis e organizações podem ser fundamentalmente alteradas pela reorganização de seus componentes, distinguindo-se pela capacidade de reconfiguração em uma sociedade caracterizada por constante mudança e fluidez organizacional; e, finalmente,
e) a crescente convergência de tecnologias específicas para um sistema altamente integrado, no qual trajetórias tecnológicas antigas ficam literalmente impossíveis de se distinguirem em separado (Castells, 2000, p. 108-109).

Publicada originalmente em 1996, a obra de Castells (2000) é de suma importância para a compreensão da mudança paradigmática na forma como nos comunicamos, mediante um giro linguístico que desloca a comunicação de um ambiente físico para o virtual.

À toda evidência, resta clara a mudança social em curso. Não é preciso muito esforço para que nos lembremos de que a rede mundial de computadores - Internet - até há algumas décadas, era de pouquíssima utilização entre usuários comuns, sendo sua exploração primordialmente levada a cabo por órgãos militares norte-americanos.

Foi na década de 1990 que a internet passou a ser utilizada por usuários civis, especialmente nos Estados Unidos.

As atuais *Big Techs*, como *Microsoft, Amazon, Meta, Apple e Alphabet* (*Google*) a) foram fundadas após a difusão do que o autor chama de sistema de redes ou b) tiveram de ser completamente reinventadas, após o *boom* tecnológico que levou à disruptura dos então vigentes padrões sociais.

As empresas de tecnologia anteriores a essa época, ou mesmo as oriundas desse florescimento tecnológico que não souberam se adaptar, perderam espaço e foram rapidamente devoradas por suas concorrentes, antenadas com as diretrizes da Era da Informação.

Concomitantemente a isso, ocorre uma grande mudança social marcada pela migração das interações humanas do ambiente físico para o das plataformas digitais, como o *Facebook*, o *WhatsApp* e o *Instagram*. A comunicação passa a acontecer em um ecossistema aberto e pulverizado, em que estamos todos ligados em rede.

É diante desse contexto, com o deslocamento das relações sociais do ambiente físico para um virtual, que investigamos os impactos desse giro no direito probatório.

4.2 Breve histórico da recente revolução tecnológica que leva a uma nova forma de linguagem

Um importante marco, no que respeita ao giro linguístico decorrente da atual disruptura tecnológica, tem início em meados da década de 1940, com o advento do primeiro computador, denominado Electronic Numerical Integrator and Computer (ENIAC) desenvolvido a pedido do exército dos Estados Unidos para seu laboratório de pesquisa balística.

Da Encyclopaedia Britannica pudemos extrair que o ENIAC era algo menos que o sonho de um computador universal. Projetado especificamente para calcular valores para tabelas de alcance de artilharia, faltavam alguns recursos que o tornariam uma máquina mais útil em geral. Utilizava painéis de conexão para comunicar instruções à máquina; isso tinha a vantagem de que, uma vez programadas as instruções, a máquina funcionava em velocidade eletrônica. As instruções lidas em um leitor de cartão ou outro dispositivo mecânico lento não seriam capazes de acompanhar o ENIAC totalmente eletrônico. A desvantagem era que demorava dias para religar a máquina para cada novo problema. Esta era uma deficiência tão grande que só com uma grande dose de generosidade o ENIAC poderia ser chamado de programável (Swaine; Freiberger, 2024).

Isso claramente revela que em nada o ENIAC lembrava os atuais computadores. As telas eram periféricas nos primeiros microcomputadores e só ganharam popularidade no final dos anos 1970. A invenção do computador pessoal ocorreu não apenas de forma independente dos grandes fabricantes, mas em oposição a eles, o que transformou a informática em um meio para a criação, comunicação e simulação em grande escala (Lévy, 1993, p. 62).

Paralelamente à invenção do computador para uso pessoal, outro fenômeno que mudaria para sempre a forma como as pessoas interagem estava em seu nascedouro: trata-se da internet, que daria início à Era da Informação ou Era Digital.

Esse espantoso salto da rede mundial de computadores que observamos nos dias atuais é consequência de sua criação em meados da segunda metade do século XX, pela Agência de Projetos de Pesquisa Avançada (ARPA), do Departamento de Defesa dos Estados Unidos.

Após o lançamento do Sputnik 1, primeiro satélite artificial produzido pelo programa soviético, em 4 de outubro de 1957, os centros de tecnologia dos Estados Unidos, em meio à Guerra Fria, entraram em estado de alerta (Breve [...], 2023).

Como discorre Castells (2000, p. 82-83), uma das estratégias de resposta foi criar um sistema de comunicação invulnerável a ataques nucleares, a partir de uma rede independente de centros de controle, para que a informação procurasse suas próprias rotas ao longo da rede, podendo fazê-lo a partir de qualquer ponto. Era um sistema distribuído de dados, chamado ARPANET, que entrou em funcionamento 12 anos depois do lançamento do Sputnik, em 1º de setembro de 1969, tendo nós na

Universidade da Califórnia Angelina (UCLA), na Universidade da Califórnia de Santa Bárbara, no Stanford Research Institute e na Universidade de Utah.

Logo ela seria utilizada por pesquisadores e cientistas, tornando-se difícil distinguir as comunicações científicas e conversas pessoais da pesquisa militar.

Em 1º de janeiro de 1983, um importante marco fez presença nessa jornada, a transição do protocolo *host* da Advanced Research Projects Agency Network (ARPANET) de Network Control Protocol (NCP) para Transmission Control Protocol/Internet Protocol (TCP/IP), protocolo de praticamente todas as redes de computadores atuais. Esta foi uma transição no estilo *flag-day*, exigindo que todos os *hosts* fizessem a conversão simultaneamente, sob pena de que tivessem que se comunicar por meio de mecanismos bastante improvisados. Essa transição foi cuidadosamente planejada ao longo de vários anos, antes de realmente ocorrer o que se deu de forma surpreendentemente ordenada e tranquila. O TCP/IP fora adotado como padrão do Departamento de Defesa três anos antes, em 1980. Isso permitiu que a Defesa começasse a compartilhar a base tecnológica da internet Defense Advanced Research Projects Agency (DARPA), tendo levado à eventual divisão das comunidades militar e não militar. Em decorrência disso, em 1983 houve a cisão entre ARPANET, dedicada a fins científicos, e a Military Network (MILNET), vocacionada aos interesses militares (Leiner *et al.,* 1997, p. 9).

Em meio a tudo isso, no final dos anos 1970, a National Science Foundation (NSF), percebendo o enorme impacto da ARPANET na pesquisa universitária, permitiu que cientistas de todos os Estados Unidos compartilhassem dados e colaborassem em projetos de pesquisa. No entanto, para ingressar na ARPANET, uma universidade precisava ter um contrato de pesquisa com o Departamento de Defesa (DoD). Muitas não tinham esse contrato. A resposta inicial da NSF foi financiar a Computer Science Network (CSNET) em 1981. Ela conectava departamentos de ciência da computação e laboratórios de pesquisa industrial à ARPANET, via linhas discadas e alugadas.

Em meados dos anos 1980, a NSF foi além, e decidiu projetar um sucessor para a ARPANET que seria aberto a todos os grupos de pesquisa universitária, que viria a ser a National Science Foundation Network (NSFNET) (Tanebaum; Wetheral, 2010, p. 59).

Com o estrondoso sucesso da rede da NSF, a ARPANET se tornou obsoleta e foi desligada, em 28 de fevereiro de 1990. Assim, a NSF, a partir de sua plataforma NSFNET, assumiu o controle da Internet, fato que durou até 1995, quando, a partir de pressões comerciais e do crescimento de empresas privadas e redes cooperativas sem fins lucrativos, o governo encerrou essa última espinha dorsal, prenunciando a privatização da Internet, “quando inúmeras ramificações comerciais das redes regionais da NSF uniram forças para formar acordos colaborativos entre redes privadas” (Castells, 2000, p. 83).

Fato é que havia muito potencial para a transmissão de dados, mas pouca infraestrutura que permitisse um tráfego exponencial de informação. Em 1995, a tecnologia de transmissão de dados estava em seu estágio embrionário.

A solução para essa barreira passou por um novo salto tecnológico que permitiu a difusão da Internet na sociedade: a criação de um novo sistema, a teia mundial (www: *world wide web*), que teve origem na Europa, a partir de pesquisas conduzidas pelo cientista britânico Tim Berners-Lee, no âmbito do Conseil Européen pour la Recherche Nucléaire (CERN) (European Council for Nuclear Research, 2024).

Esse aplicativo foi capaz de fornecer o sustentáculo para a livre propagação da informação a partir de ferramentas como a linguagem de marcação de hipertexto (Hypertext Markup Language - HTML), que consiste em um texto digital interativo - *link* - no qual certas palavras, frases ou elementos gráficos levam a outras páginas da *web*, documentos ou recursos. Esses *links* possibilitam uma navegação não linear, permitindo que os usuários explorem informações de maneira mais flexível e personalizada. Outra ferramenta é a padronização de formato de endereços: URL (Castells, 2000, p. 88).

A World Wide Web (WWW) foi distribuída gratuitamente pela Internet e, em pouco tempo, foi fundado o navegador da *web Mosaic* criado para funcionar em computadores pessoais. (University of Illinois Urbana-Champaign, 2023)

Logo, novos navegadores foram arquitetados e a internet estava pronta para deslanchar.

É possível perceber, então, dois movimentos paralelos:

a) um em que o primeiro computador é lançado - o ENIAC - e posteriormente evoluído para uso pessoal; e

b) o advento da internet, como resposta a uma ação da União Soviética pelos centros de tecnologia do Departamento de Defesa dos Estados Unidos da América.

Com a fusão desses dois dispositivos - uma estrutura física (computador pessoal) e uma rede descentralizada de comunicação -, a internet floresce exponencialmente em ambiente privado e, com isso, provoca uma disruptura tecnológica de tal maneira que a noção de que uma nova linguagem estava construindo o mundo se tornou evidente, não apenas servindo como instrumento de transmissão de imagens mentais.

A seguir, no Quadro 1, apresentamos a cronologia de eventos no domínio da tecnologia da informação e da informática, ao longo do século XX, que catalisaram a transformação social que vivenciamos atualmente. Esta análise está fundamentada na bibliografia referida nos parágrafos anteriores.

Quadro 1 - Cronologia do desenvolvimento da tecnologia da informação e informática causadores da atual reconfiguração social

Ano/período	Evento	Descrição
1939 a 1945	Segunda Guerra Mundial	Concentração de esforços no desenvolvimento de tecnologias e início da guerra fria.
1943-1946	Desenvolvimento e lançamento do ENIAC	Desenvolvimento e lançamento do primeiro computador digital programável, eletrônico e de uso geral por John Mauchly e J. Presper Eckert
1957	Lançamento do Sputnik 1	Primeiro satélite artificial da Terra, lançado pela União Soviética, mergulhando os centros de tecnologia dos Estados Unidos em estado de alerta.
1969	Entrada em funcionamento do ARPANET	Como resposta ao avanço da tecnologia soviética, os EUA lançam um sistema distribuído de dados, feito para ser invulnerável a ataques nucleares, a partir de uma rede independente de centros de controle, para que a informação procurasse suas próprias rotas ao longo da rede.
Anos 1970	Invenção dos computadores pessoais	Desenvolvimento de computadores para uso pessoal, como o Kenbak-1 (1971), o Altair 8800 (1975) e o Apple 1 (1976).
1980	Adoção do protocolo TCP/IP como padrão do Departamento de Defesa dos EUA	Esse novo protocolo trouxe maior flexibilidade e escala, permitindo a interconexão de redes diversas e o crescimento da internet global, dando suporte a um número muito maior de dispositivos e redes, essencial para a expansão da internet.
1981	Criação da CSNET	A *National Science Foundation* (NSF) cria a CSNET (*Computer Science Network*), uma rede de computadores que permitiu que cientistas de diversas universidades nos Estados Unidos compartilhassem dados e colaborassem em projetos de pesquisa.
1983	Transição do protocolo *host* da ARPANET de NCP para TCP/IP para todos os hosts	*Flag day* em 1º de janeiro de 1983. Todos os dispositivos e redes conectados à ARPANET tiveram que migrar simultaneamente para o novo protocolo TCP/IP, substituindo o antigo NCP
1983	Cisão entre ARPANET e MILNET	A ARPANET continuou a servir à pesquisa acadêmica e científica, enquanto a MILNET foi estabelecida para uso militar e de defesa.

1985	Criação da NSFNET	Rede de computadores criada pela NSF, como avanço em relação à CSNET, se tornando a espinha dorsal da internet moderna, ao conectar e suportar outras redes regionais e acadêmicas, facilitando a colaboração e o compartilhamento de informações científicas.
1991	Lançamento da *world wide web* - www	Desenvolvido por Tim Berners-Lee no âmbito do CERN, esse aplicativo foi capaz de fornecer o sustentáculo para a livre propagação de informação a partir de ferramentas como a linguagem de marcação de hipertexto (HTML – *hypertex markup language*)
1993	Lançamento do *Mosaic*	Primeiro navegador a ser usado no Windows e a ganhar popularidade.
1995	Desativação da NSFNET	À medida que houve mobilização comercial, o governo optou por descontinuar a rede NSFNET e deixar a gerência da rede por conta de servidores privados de internet.
1995	Início do gerenciamento da rede por provedores de serviço de internet privados	Internet como a conhecemos hoje, servindo especialmente a propósitos comerciais.

Fonte: Elaborado pelo autor.

Se pensávamos em um futuro com carros voadores e teletransporte, podemos dizer que os seres humanos, talvez, tenham operado algo ainda mais grandioso: ter acesso a um universo inimaginável de dados em poucos anos.

Assim, verificamos que as relações humanas passam de um espaço físico para um virtual e que a linguagem é desenvolvida nesse espaço, ganhando novos contornos, e moldando a forma como o mundo é explorado.

A revolução da tecnologia da informação levou ao desenvolvimento da linguagem, a digital, tendo a internet como seu principal catalisador (Guimarães, 2023, p. 71).

Estamos cada vez mais imersos em conversas digitais com pessoas não fisicamente presentes. Muitas vezes, elas pertencem a lugares totalmente diferentes dos nossos. A tecnologia digital reduziu as distâncias globais e permitiu o acesso às mais diversas pessoas e suas culturas.

A integração da tecnologia em diversos aspectos da vida tem alterado significativamente as interações humanas e a estrutura da sociedade. Isso inclui mudanças na forma como nos comunicamos, como a substituição de cartas por *e-mails* e telefonemas por mensagens instantâneas de texto, áudio ou vídeo. Além disso, os registros, tanto públicos quanto privados, que antes eram feitos em papel com precauções específicas, agora são amplamente substituídos por sistemas informáticos. A internet desempenha um papel fundamental nesse processo, permitindo acesso e transmissão de vastas quantidades de informações, realização de transações legais mas, infelizmente, facilitando a prática de atividades ilícitas.

(Pastore, 2020, p. 65).

Se a linguagem é proativa e ferramenta poderosa para transformar o mundo, é nesse contexto que os juristas devem se dedicar a compreender a transição de um modelo tradicional de provas para um atípico. Além disso, devem investigar como alinhar o uso dessas novas provas ao modelo de processo constitucional, assegurando que direitos e garantias fundamentais não sejam comprometidos em face dessa nova realidade.

4.3 Da linguagem como ferramenta de construção do mundo.

É perceptível que essa disruptura tecnológica leva a uma remodelagem da nossa sociedade e, especialmente, a um giro linguístico.

Haraway e Kunzro (2009, p. 10) atentam para o fato de que não existe sujeito ou subjetividade fora da história e da linguagem, fora da cultura e das relações de poder.

Assim, não haveria de se falar em relações sociais fora de um dado contexto que envolve história, linguagem, cultura e relações de poder, e o Direito, como ciência social aplicada.

Além disso, a linguagem deve ser compreendida como algo vivo, e apenas consistente em meio a um determinado grupo de vocábulos para designar objetos, pessoas, lugares etc., definição que restringiria, indevida e simploriamente, o fenômeno linguístico. Antes, deve ser pensada como algo que influi diretamente na percepção de mundo do observador e do observado.

A hipótese dos linguistas Sapir, canadense, e seu aluno Benjamin Lee Whorf, americano, sustenta essa visão. Em *The status os liguistics as a science*, Sapir (1929, p. 209) argumenta que a linguagem é um guia para a “realidade social”. Ela condiciona poderosamente todo o nosso pensamento sobre problemas e processos sociais. Os seres humanos não vivem apenas no mundo objetivo, nem somente no mundo da atividade social, como normalmente entendido, mas estão muito à mercê da linguagem particular que se tornou o meio de expressão de sua sociedade. Assim, seria uma ilusão imaginar ser possível as pessoas se ajustarem à realidade, sem o uso da linguagem, e lamentável pensar que a linguagem é meramente um meio incidental de resolver problemas específicos de comunicação ou reflexão. A verdade

é que o “mundo real” é, em grande medida, inconscientemente construído com base nos hábitos linguísticos do grupo. Nenhuma língua é suficientemente similar a outra para ser considerada como representando a mesma realidade social. Os mundos em que diferentes sociedades vivem são distintos, não meramente o mesmo mundo com rótulos diferentes anexados.

Com isso, os linguistas querem dizer que a linguagem não deve ser compreendida como um mero instrumento de comunicação de imagens mentais, mas como ferramenta essencial que dá corpo à sociedade à medida que a molda. A máxima da teoria desses estudiosos é a relação entre linguagem, pensamento e percepção do mundo.

Saussure (2006), considerado o criador da Linguística, em sua obra trata da mutabilidade da língua, ao propor que

> o tempo, que assegura a continuidade da língua, tem um outro efeito, em aparência, contraditório com o primeiro: o de alterar mais ou menos rapidamente os signos linguísticos e, em certo sentido, pode-se falar, ao mesmo tempo, da imutabilidade e mutabilidade do signo (Saussure, 2006, p. 89).

Postula, ainda, o linguista suíço que a língua é uma tarefa constante de todas as pessoas. É usada e moldada por uma massa de indivíduos, sendo algo que todos utilizam rotineiramente. Nesse sentido, a língua é única e não pode ser comparada a outras instituições. As regras de um código legal, os rituais de uma religião, os sinais marítimos, entre outros, envolvem apenas um número limitado de pessoas e por um período restrito de tempo. Já a língua é algo de que todos participam a todo momento, o que faz com que ela esteja continuamente sob a influência de todos (Saussure, 2006, p. 88).

Vale dizer: ele sagazmente percebeu que a linguagem não era um instituto homogêneo ou imutável, mas que sua mudança leva tempo, por conta de uma natural “resistência da inércia coletiva a toda renovação linguística”.

Embora talvez seja precoce falar em revolução, a noção de um giro linguístico nos parece adequada. Isso, porque, concatenando as noções de a) mutabilidade da língua e de b) que essa mutabilidade decorre da participação de todos, em uma sociedade em rede, à qual todos estamos ligados, a velocidade com que as inovações tecnológicas ocorrem assume uma escala muito grande, favorecendo a velocidade

das inovações linguísticas.

Lévy (1993, p. 46) propõe uma reflexão sobre a temporalidade social e os modos de conhecimento que emergem das tecnologias intelectuais baseadas na informática.

Em suas palavras, “se a humanidade construiu outros tempos, mais rápidos, mais violentos que os das plantas e animais, é porque dispõe deste extraordinário instrumento de memória e de propagação das representações que é a linguagem”.

Vale dizer, que Lévy (1993) também compreende a linguagem como algo que modula nossa interação com o mundo, pensando-a proativamente. A partir das narrativas que surgem, cria-se uma espécie de “trava” que torna o tempo irreversível, apontando para um caminho inexorável de transformações, da arte rupestre, à mais moderna forma de comunicação tecnológica, passando pela criação da matemática, como forma de exprimir ideias sobre a compreensão da natureza.

O ser humano, por viver em sociedade, comunica-se, o tempo todo, com seus semelhantes. Na maior parte das vezes, isso ocorre mediante o uso de sistemas de signos, sendo o principal deles as línguas, como o português, o inglês, o italiano, o espanhol, o alemão, o japonês etc. (Terceiro Neto, 2019, p. 22).

De fato, a linguagem possui um papel fundamental na transformação social, construindo ambientes cada vez mais sofisticados.

Atualmente, como mencionado anteriormente, o espaço de comunicação migrou para o das plataformas virtuais, o dito ciberespaço, de modo que a linguagem utilizada passa a ser própria desse *locus*.

Devido à sua plasticidade e elasticidade, o ciberespaço permite combinar, articular e integrar formatos não textuais em textuais, imagens em sons e vice-versa - tudo em um fluxo contínuo de negociações intersemióticas. (FERRARI, 2014, p. 35).

É justamente a partir dessa perspectiva linguística que devemos pensar os novos fundamentos da sociedade e de sua organização.

4.4 Do giro linguístico a um novo direito probatório

Diante da magnitude de tais mudanças sociais, sejam em seu conteúdo ou na velocidade com que se dão, aquele velho adágio que ouvimos ao longo de nossas vidas acadêmicas nas faculdades de Direito ressoa: “o direito anda sempre atrás de

seu tempo", com algumas variações, como "a sociedade caminha mais rápido que o direito", mas sempre com a mesma ideia subjacente, que é a de apontar para o fato de que o Direito, especialmente por meio da atividade legiferante, teria mais vocação para regular situações à medida que vão ocorrendo, do que propriamente atuar proativamente como modelador da sociedade.

O que dizer, então, diante do giro linguístico em curso?

Asensi, em artigo de 2013, preceituou que existe uma disjunção estrutural entre as mudanças sociais e a capacidade do Estado, especialmente o Legislativo, de acompanhar essas transformações. Sob uma perspectiva sociológica, tal questão evoca o debate sobre se o direito é responsável por modelar a sociedade ou se, ao contrário, é a sociedade que influencia e transforma o direito. Embora o direito possa influenciar a sociedade, como demonstrado em pesquisas no direito penal, de família e comercial, atualmente constatamos, cada vez mais, a sociedade moldando o direito, dado que o processo legislativo não acompanha as rápidas mudanças sociais. As transformações sociais eram mais lentas no passado, mas hoje ocorrem rapidamente, criando grandes desafios para o direito. Exemplos incluem a popularização dos *smartphones* em poucos anos, a mudança no turismo internacional e a invasão do comércio eletrônico nas relações de consumo, além da possibilidade de realização de audiências judiciais por meio de computadores, celulares e *tablets*, de qualquer lugar do mundo.

Não há dúvidas de que a sociedade está passando por uma mudança estrutural global, especialmente no que respeita à forma como a comunicação acontece. Porém, uma questão persiste: deve o Direito curvar-se diante dos fatos sociais e buscar regulá-los, apenas quando já ubíquos em nossa sociedade ou, a partir da ideia do Direito como ciência social aplicada hábil a promover mudanças de forma proativa, definir os rumos que a sociedade deve tomar?

A partir dessas reflexões, emerge a necessária investigação sobre as provas digitais no âmbito judicial, uma realidade que se impõe pela própria dinâmica social. Essa análise, como já mencionado, é conduzida à luz do processo constitucional, que serve de referencial teórico para a investigação.

Nunes (2024) destaca que é

> [...] evidente que na sociedade digital vivemos uma era *onlife*, na qual as experiências reais e virtuais se fundem, e que impõe a percepção de uma virada tecnológica do direito de modo a encarar o impacto das tecnologias de informação e comunicação na adaptação e interpretação do sistema jurídico, de modo que o código deontológico do Direito imponha mecanismos cooperativos de governança e controle do ambiente digital (Nunes, 2024).

O Judiciário, cada vez mais, se vê diante da necessidade do exame de provas digitais, desde aquelas decorrentes de interações em redes sociais, como *WhatsApp, Facebook* e *Instagram*, uso de dados de geolo*calização e cópias de* e-mail, até outras bem mais sofisticadas que envolvem técnicas como *blockchain* e espelhamento de mensageiros instantâneos.

Ocorre que os dados se tornam cada vez mais facilmente editáveis, diante do conhecimento crescente acerca da manipulação de novas tecnologias. As *deepfakes* são exemplo bastante notório do potencial de adulteração de dados digitais.

Assim, surgiu a reflexão sobre a utilização de provas eletrônicas no processo judicial e sua compatibilização com um modelo constitucional de processo que visa a perfazer direitos fundamentais.

Se, por um lado, com a aceleração do tráfego de informações na sociedade, é tentadora a ideia de se conferir celeridade aos processos judiciais, não se deve descuidar das garantias fundamentais do processo, basilares da atividade jurisdicional que deflui do Estado Democrático de Direito.

Deve haver um equilíbrio, pois não se desconhece o problema da morosidade do Poder Judiciário, sendo o caso de se questionar se o próprio sistema de metas imposto pelo Conselho Nacional de Justiça (CNJ) não faz com que a lógica social da CRFB/1988 seja subvertida em favor de um ideário neoliberal de produtividade, o que redunda no sacrifício do desenho de Estado almejado pelo constituinte.

Vejamos, por exemplo, algumas metas nacionais estabelecidas para o Poder Judiciário em 2023:

> Meta 1- Julgar mais processos que os distribuídos (todos os segmentos)
>
> Julgar quantidade maior de processos de conhecimento do que os distribuídos no ano corrente, excluídos os suspensos e sobrestados

> no ano corrente.
>
> Meta 2- Julgar processos mais antigos (todos os segmentos)
>
> Identificar e julgar até 31/12/2023:
>
> • Superior Tribunal de Justiça: pelo menos, 99% dos processos distribuídos até 31/12/2019.
> • Tribunal Superior do Trabalho: 100% dos processos distribuídos até 31/12/2019, e pelo menos 90% dos processos distribuídos até 31/12/2020.
> • Justiça Estadual: pelo menos, 80% dos processos distribuídos até 31/12/2019 no 1º grau, 90% dos processos distribuídos até 31/12/2020 no 2º grau, e 90% dos processos distribuídos até 31/12/2020 nos Juizados Especiais e Turmas Recursais.
> • Justiça Federal: No 1º e 2º graus, 100% dos processos distribuídos até 31/12/2018 e 85% dos processos distribuídos em 2019; e nos Juizados Especiais Federais e nas Turmas Recursais, 100% dos processos distribuídos até 31/12/2020.
> • Justiça do Trabalho: pelo menos, 93% dos processos distribuídos até 31/12/2021, nos 1º e 2º graus.
> • Justiça Eleitoral: 70% dos processos distribuídos até 31/12/2021.
> • Justiça Militar da União: pelo menos 95% dos processos distribuídos até 31/12/2020 nas Auditorias e 99% dos processos distribuídos até 31/12/2021 no STM (Conselho Nacional de Justiça, 2023).

Dessa forma, cria-se um cenário em que o magistrado, pressionado por um sistema que prioriza a celeridade dos processos judiciais em detrimento do respeito aos direitos fundamentais e às normas processuais que asseguram esses direitos, pode incorrer em descuidos na análise das provas.

Esses descuidos, por sua vez, podem resultar em danos, maior morosidade processual, proliferação de recursos e, eventualmente, a arguição de nulidade do processo, especialmente com o crescente uso de provas eletrônicas.

Como visto anteriormente, é impossível negar que a atividade legiferante do Estado, nos atuais moldes, encontra sérias dificuldades para acompanhar as mudanças sociais, especialmente no que respeita à migração das interações interpessoais de um ambiente físico para um espaço virtual.

Destarte, não é difícil aferir que as provas digitais têm cada vez mais impacto em todos os organismos que exercem a Jurisdição, naturalmente, conduzindo o sistema de provas de um formato de tipicidade para um de atipicidade, e gerando uma série de questões a serem pensadas.

A pergunta fundamental que surge, então, é: como garantir respeito aos princípios basilares do processo constitucional quando do manejo da prova eletrônica

no processo judicial, diante da possibilidade de adulteração e manipulação de conteúdo digital?

Adotando esse norte, a hipótese é a de que a garantia do respeito ao processo constitucional passa pela rigorosa apuração da autenticidade e integridade da prova eletrônica no processo judicial, podendo ser alcançada por meio da adoção de medidas de segurança adequadas, tais como criptografia, certificação digital, *blockchain*, controle de acesso, e auditoria das operações realizadas.

Refletindo sobre a segurança e a confiabilidade dos documentos eletrônicos, Didier Júnior, Braga e Oliveira (2019, p. 254-255) destacam que, para atribuir valor probatório a esses documentos, é essencial avaliar o grau de segurança e de certeza em relação à sua autenticidade e integralidade. A autenticidade permite identificar a autoria, enquanto a integralidade garante a inalterabilidade do conteúdo. Apenas a certeza sobre esses aspectos pode assegurar a eficácia probatória dos documentos. Eles acrescentam que têm sido desenvolvidas técnicas para aumentar a segurança e a confiabilidade dos documentos eletrônicos, vinculando a autenticidade à integridade do conteúdo. Se o conteúdo for alterado, o elo entre o novo conteúdo e o autor original se desfaz.

Não é demais recordar o teor do Enunciado n. 297 da IV Jornada de Direito Civil do CNJ, que estabelece que o documento eletrônico tem valor probante, desde que seja apto a conservar a integridade de seu conteúdo e idôneo a apontar sua autoria, independentemente da tecnologia empregada.

Outra questão que surge é como conciliar a utilização de provas digitais e princípios como os do acesso à Justiça, à realização de provas e o contraditório com outros princípios fundamentais que, muitas vezes, entram em conflito com estes, como a privacidade, a intimidade e a liberdade de expressão?

É importante esclarecer que o uso de provas digitais no processo judicial é uma realidade, sendo ingenuidade qualquer tentativa de refreá-lo. De qualquer maneira, sua utilização no processo judicial não é incompatível com uma noção constitucionalizada de processo, devendo apenas se assegurar de que protocolos de segurança sejam obedecidos, quando da preservação da prova, bem como se sopese no caso concreto o valor fundamental a prevalecer, como tem sido feito pelos tribunais de todo o país, especialmente pelo STF, como mostraremos, ao longo do próximo capítulo.

É que a produção de prova constitui direito fundamental da pessoa que pretende deduzir pretensão em juízo, a fim de demonstrar o quanto alega, como corolário lógico do direito de acesso à Justiça, consubstanciado no art. 5º, XXXV da CRFB/1988.

Entretanto, as partes envolvidas no processo judicial devem se acautelar, ao máximo, para que o novo modelo de produção probatória seja orientado pelos princípios fundamentais que regem o Estado Democrático de Direito, sendo a prova vista como direito humano e direito fundamental em um horizonte mais amplo, mas jamais partindo de um ponto de sacrifício de garantias fundamentais como o devido processo constitucional, contraditório, ampla defesa, fundamentação, legalidade e boa-fé, o que justifica, plenamente, a adoção de medidas de segurança, que contribuem para a formação de um Estado Democrático de Direito mais forte.

Para tanto, devemos pensar em um binômio, que, por um lado, orientará a efetividade daquilo que se pretende provar e, por outro, garantirá a veracidade do objeto da prova, a partir de uma visão constitucional do processo.

Por fim, impende frisar que, não obstante as espantosas mudanças vivenciadas ao longo dos últimos anos, devemos sempre lembrar que vivemos em um Estado Democrático de Direito e que as garantias para a preservação de direitos fundamentais continuam vigentes.

Com tudo isso, repisemos, não pretendemos voltar no tempo e coibir o uso de provas digitais no processo judicial, mas apenas compatibilizar o instituto dessas provas, decorrente de um novo modelo de linguagem, fundado nas relações sociais via plataformas eletrônicas, com os princípios fundamentais que norteiam o Estado Democrático de Direito.

4.5 Síntese do capítulo

Para facilitar a compreensão do fenômeno das provas digitais, é fundamental entendermos as transformações por que passa a sociedade, matéria abordada neste capítulo. O surgimento de novas tecnologias vem provocando uma profunda reconfiguração nas relações sociais. Não é a primeira vez na história que novos recursos são introduzidos na sociedade provocando esse rearranjo.

Quando da instituição da agricultura, seguramente os seres humanos tiveram uma mudança radical em seu estilo de vida, ao deixarem de ser nômades para serem sedentários fixados em apenas um lugar. Não é diferente dessa vez. O que causa inquietude é a velocidade desse movimento, dado o alcance dessas novas tecnologias da Era Digital, especialmente com a) a formatação do computador para uso pessoal e b) a propagação da internet pelo mundo, desde seu momento embrionário, até sua abertura total. Com isso, a partir de meados da década de 1990, as relações sociais passam a migrar maciçamente do espaço físico para o virtual, ocasionando um giro linguístico, uma nova maneira de comunicação com o mundo.

Reiteramos que a linguagem deve ser compreendida como um fenômeno vivo, capaz de moldar a realidade, de forma que o que é comunicado no ambiente virtual contribui para a construção do mundo onde vivemos. Nesse contexto, as relações jurídicas também se desenvolvem a partir dessa nova forma de expressão, exigindo que o Direito se mantenha sempre em sintonia com a realidade atual, tornando-se um instrumento de transformação social, e não apenas um regulador de fatos passados. Com o avanço das interações no espaço digital, as provas emergem desse ambiente, marcando uma transição de um sistema tradicional de provas típicas para um naturalmente vocacionado para as provas atípicas. Esse momento de transição traz consigo diversas inquietações, sendo as mais prementes:

a) a necessidade de assegurar confiabilidade às provas digitais; e
b) o surgimento de conflitos entre princípios fundamentais. Isso posto, de maneira mais fluida, adentramos a questão das provas digitais.

5 DAS PROVAS DIGITAIS

Por sua própria natureza e finalidade, a prova segue as alterações pelas quais passam as relações jurídicas de direito material das quais os litígios se originam, bem como a realidade que as envolve. É natural, portanto, que o marcante avanço das tecnologias nos últimos anos implique a alteração da forma pela qual se estabelecem essas relações e inspire o recurso a novos meios de acautelar informações para o futuro, acarretando, então, significativa mudança no perfil dos elementos que servem a reconstituir, no processo, os fatos pretéritos que se mostrem pertinentes ao desate de uma controvérsia (Pastore, 2020, p. 64).

Como exemplo, é amplamente reconhecido que "a confiabilidade da prova documental – e a importância singular que os ordenamentos processuais" lhe atribuem – baseia-se, precisamente, na estabilidade do suporte em que a informação é registrada. No entanto, os documentos produzidos em meio eletrônico podem, em geral, ser alterados facilmente em suportes de armazenamento regraváveis. Particularmente no fluxo de dados, em uma rede de computadores como a internet, a informação armazenada em meio eletrônico assume um caráter temporário, é fungível e altamente volátil, o que parece contradizer a natureza e a própria utilidade da prova documental (Pastore, 2020, p. 64).

É diante dessas peculiaridades que as provas digitais merecem um estudo exaustivo e minucioso por parte dos juristas, de modo que o direito se mantenha em compasso e sintonia com os avanços sociais.

5.1 Internet: algumas noções tecnológicas elementares

5.1.1 Números IP

O endereço de protocolo de internet (endereço IP) é definido legalmente pelo Marco Civil da Internet (MCI) - Lei n. 12.965 de 23 de abril de 2014 -, que preconiza em seu art. 5º, III, tratar-se do "código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais" (Brasil, [2021b]).

Na verdade, o IP é um número que o provedor de internet atribui a um dispositivo toda vez que ele acessa a internet, identificando a máquina que estiver conectada a ela naquele momento – apenas naquele momento. Cada vez que um usuário se conecta, um IP é atribuído a ele, e quando ele se desconecta, esse mesmo IP é liberado e pode ser usado por outro usuário. Essa identificação do terminal que recebeu determinado IP não inclui o respectivo usuário, entretanto. Para se chegar à pessoa que está operando o *device*, algumas informações adicionais serão necessárias, como um *login* ou *nickname* (Capanema, 2024, p. 42).

Quando se tem apenas o IP, outras medidas probatórias devem ser adotadas, como o requerimento de uma busca e apreensão do computador (Provas [...], 2023).

Ao navegar na internet e digitar um nome de domínio, o usuário está na verdade procurando o endereço IP do servidor que hospeda aquele domínio, para estabelecer uma comunicação com ele. Diferentemente do sistema de telefonia convencional, no qual a comunicação ocorre entre duas ou mais pessoas através de um circuito exclusivo, na internet a comunicação não se dá por um circuito fixo. Em vez disso, as mensagens são trocadas entre os usuários na forma de pacotes que trafegam pela rede por rotas variadas (Teixeira, 2024, p. 18).

A importância principal do número do IP está relacionada à localização, uma vez que, a partir do cruzamento do número IP com outros dados, como a data da conexão (dia e hora), é possível vincular o IP a um usuário identificável, classificado pela LGPD, em seu art. 5º, I, como dado pessoal (informação relacionada a pessoa natural identificada ou identificável) (Capanema, 2024, p. 50).

Importante, ainda, mencionar que, atualmente, experimentamos a transição dos padrões de IP, passando do IPv4 (por exemplo, 200.181.13.43) para o IPv6 (por exemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334). O IPv6 oferece uma capacidade muito maior de distribuição de endereços IP, permitindo um número maior de conexões em todo o mundo. Devido ao esgotamento dos endereços disponíveis no IPv4, foi necessário criar uma alternativa técnica para viabilizar novas conexões durante essa fase de transição: o compartilhamento do mesmo IP por várias máquinas, chamadas de portas lógicas, de modo que cada usuário conectado a um IP compartilha uma porta lógica específica. Durante essa fase de transição, para identificar corretamente um usuário, não é suficiente apenas saber o IP, a data e a hora da conexão; é também necessário conhecer a porta lógica de origem, caso

contrário, se o IP for compartilhado, a identificação precisa do usuário se torna inviável. Portanto, tecnicamente, assim como os logs de conexão, a informação da porta lógica de origem deve ser armazenada e apresentada pelo provedor de aplicação (Thamay; Tamer, 2022, RB-2.6).

Analogamente, seria como se as portas lógicas fossem os ramais de um número principal, o IP. Quando se busca o IP, e não a porta lógica de origem, é impossível saber de onde veio a "ligação" (Provas [...], 2023).

Por fim, é importante abordar a figura do administrador de sistema autônomo, elemento que o MCI designa em seu art. 5º, IV, como

> a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP, geograficamente referentes ao País (Brasil, [2021b]).

Esse conceito se refere, principalmente, aos provedores de conexão (acesso), que têm a finalidade de conectar o usuário por meio do roteamento de blocos de endereços IP administrados por delegação do CGI.br, entidade à qual devem estar devidamente cadastrados. Portanto, os provedores de acesso são responsáveis por manter a conexão, assegurando condições de privacidade e a possibilidade de identificar seus clientes (Teixeira, 2015, p. 1-2).

Assim, um Sistema Autônomo (AS, na sigla em inglês) é uma entidade composta por um conjunto de redes IP e roteadores geridos por uma única organização ou Provedor de Serviços de Internet (Internet Service Provider - ISP). Esses sistemas têm a função de rotear o tráfego de dados entre diversas redes, assegurando a conectividade entre elas (O Que [...], 2024).

5.1.2 Provedores

O MCI classifica os provedores em duas categorias: a) os de conexão e b) os de aplicação.

Capanema (2024) leciona que, embora não haja definição legal desses termos, o Marco Civil trouxe conceitos relacionados, como os de conexão à internet, ou seja, "a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP" (art. 5º, V) e o de

aplicações de internet, definido no art. 5º, VII, como o “conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet” (Capanema, 2024, p. 53).

Assim, propõe as seguintes definições:

> Provedores de conexão: pessoas naturais ou jurídicas que prestam, de forma gratuita ou onerosa, o serviço de conexão à internet, mediante o fornecimento de um número IP, permitindo, assim, a troca de pacotes de dados na rede.
>
> Provedores de aplicação: pessoas naturais ou jurídicas que prestam, de forma gratuita ou onerosa, acesso a sites, serviços, aplicativos e outras funcionalidades oferecidas na internet. (Capanema, 2024, p. 53).

Um provedor de conexão é uma entidade jurídica que oferece serviços para permitir que seus consumidores acessem a internet. Sua caracterização se dá pelo simples fato de viabilizar a conexão dos dispositivos de seus clientes à rede. São os tradicionais provedores com os quais estamos familiarizados, como Net Virtua, Brasil Telecom, GVT e operadoras de telefonia celular como TIM, Claro e Vivo, que oferecem serviços de conexão 3G e 4G (Ceroy, 2020).

Os provedores de aplicação, por sua vez, são responsáveis por oferecerem ao usuário uma variedade de serviços, como armazenamento de dados, serviços de mensagens eletrônicas, disponibilização de conteúdos e acesso à informação. Assim, podemos afirmar que o provedor de aplicações fornece serviços e conteúdo, mas não o acesso à internet. Dentre os mais conhecidos estão *Facebook, Google* e *WhatsApp* (Barreto Junior; Leite, 2017, p. 395).

Essa distinção é importante não só do ponto de vista teórico, mas prático, uma vez que há dispositivos jurídicos que regulam especificamente cada um deles. Exemplo disso é o dever de guarda de registros, cujos prazos são diferentes, dependendo se se tratar de provedor de aplicação ou de conexão, como mostramos, a seguir.

Teixeira (2024) lembra a doutrina de Marcel Leonardi, na qual ele distingue entre vários tipos de provedores.

> Provedor de *backbone* é o que detém as estruturas de rede, capaz de possibilitar o tráfego de informações; provedor de acesso é o fornecedor de serviços que possibilita o acesso de seus usuários à

> internet; provedor de correio eletrônico é o que fornece serviço de envio, recebimento e armazenamento de mensagens eletrônicas; provedor de conteúdo é o que disponibiliza e armazena, em seus servidores, informações criadas por terceiros ou meios próprios (alguns chamam impropriamente de provedor de informação o responsável pela criação dessas informações, sendo melhor denominá-los apenas autores da informação); e, por fim, provedor de hospedagem é o que permite o armazenamento de sites, blogs, redes sociais etc., com seus textos, imagens, sons e informações em geral. (Teixeira, 2024, p. 19).

Para efeito legal, especialmente o MCI, a distinção entre os provedores de conexão e de aplicação se mostra suficiente.

5.1.3 Registros (logs)

Como explicado anteriormente, ao acessar a internet, um *device* se vale de um IP dinâmico que muda a cada novo acesso. Assim, para atender ao princípio da responsabilização dos agentes que utilizam a internet, conforme previsto no art. 3º, VI do MCI, os provedores devem exercer controle sobre a utilização desse IP, de modo a permitir a identificação de usuários que tenham praticado condutas ilícitas (Capanema, 2024, p. 58).

Em seu art. 5º, que trata de definições, MCI trata de registros de conexão e de acesso a aplicações, o primeiro sendo definido como “o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados”, enquanto o segundo é tido como o “conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP” (Brasil, [2021b]).

Vale dizer, o registro de conexão é aquele que deve ser armazenado pelo provedor de conexão, abrangendo:

a) as informações de data e hora do início e término da conexão;
b) a duração dessa conexão; e
c) o número IP utilizado pelo terminal.

Esses registros devem ser guardados em sigilo pelo provedor de conexão pelo prazo de 01 ano, nos termos do art. 13 do MCI (Brasil, [2021b]).

Já os registros de acesso a aplicações de internet dizem justamente dos provedores de aplicação. A lei determina que devem ser mantidas sob sigilo as informações referentes a data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Esses provedores de aplicação devem guardar os respectivos registros de acesso a aplicações pelo prazo de 06 meses, conforme dispõe o art. 15 do MCI.

5.1.4 Criptografia

Consiste em uma importante metodologia para resguardar a segurança, privacidade, liberdade de expressão e outros princípios fundamentais, conforme se depreende do voto do Ministro Edson Fachin por ocasião do julgamento da Arguição de Descumprimento de Preceito Fundamental (ADPF) n. 403 (Brasil), em que assenta que a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões que geralmente ocorrem através de comunicações *on-line*, como em e-mails, mensagens de texto e outras formas de interação, de modo que a criptografia, em particular, é um meio de assegurar a proteção de direitos essenciais para a vida pública em uma sociedade democrática, sendo mesmo contraditório que, em nome da segurança pública, se deixe de promover e buscar uma internet mais segura, direito de todos e obrigação do Estado. Medidas que, de acordo com a melhor evidência científica, trazem insegurança aos usuários só se justificam, se houver certeza comparável dos benefícios obtidos em outras áreas (Brasil, 2021c).

A técnica da criptografia consiste no uso de algoritmos criptográficos (cifras) para converter uma mensagem compreensível (*plaintext*) em mensagem cifrada (*ciphertext*), utilizando uma informação secreta conhecida como chave criptográfica.

Apenas aqueles que possuem essa chave podem decifrar a mensagem e torná-la legível novamente. A principal função desse sistema é garantir a confidencialidade do conteúdo da informação, protegendo-a contra acessos não autorizados (Liguori, 2022, p. 15).

Duas espécies de encriptação são mais utilizadas: as simétricas, que usam apenas uma chave para codificar e decodificar o conteúdo, e as assimétricas, que

usam uma chave pública para codificar e uma chave privada para decodificar.

Gil, Israel e Parsons (2018, p. 6) explicam que a criptografia simétrica é o termo usado quando a mesma chave é utilizada, tanto para criptografar quanto para descriptografar dados. Esse tipo de sistema funciona bem para manter a segurança de dados estanques, mas tem suas limitações quando em trânsito. Isso, porque as partes envolvidas na troca de dados teriam de combinar o código da chave antecipadamente, de modo que só elas o saibam. Entretanto, em um ambiente de transmissão de dados em rede, como a internet, as partes não poderão compartilhar uma chave secreta e a sua distribuição em rede pública seria demasiado perigosa.

Daí a criação da criptografia assimétrica, frequentemente chamada de criptografia de chave pública, que aborda esse problema usando um par de chaves gerado criptograficamente, que possuem uma relação matemática especial entre si. Em tais sistemas, uma das chaves é mantida em segredo (a privada) e a outra (a pública) é disponibilizada livremente: ela pode ser compartilhada abertamente por meio de uma rede não segura. Nesse modelo, mesmo que as partes nunca tenham se encontrado, a parte que envia a mensagem pode publicar sua chave pública *on-line* (por exemplo, em seu *site*, na sua conta do *Twitter,* ou em servidores dedicados à facilitação de trocas de chaves públicas) e a destinatária pode, então, usar a chave pública do mensageiro para criptografar mensagens que somente este poderá descriptografar, usando a chave privada única e secreta associada à chave pública que ela compartilhou. A criptografia de chave pública é essencial para proteger o tráfego na *web* e as comunicações *on-line*, sendo a base de tecnologias de criptografia como Transport Layer Security (TLS) / Secure Sockets Layer (SSL) e Pretty Good Privacy (PGP). (Gil; Israel; Parsons, 2018, p. 6-7).

Em suma: são duas chaves distintas, uma pública, de quem encripta a mensagem, e outra privada, que fará a desencriptação.

Vários protocolos são utilizados para a criptografia de dados. Souza, Munhoz e Carvalho (2023, p. 41-42) citam o Transport Layer Security (TLS), que combina esses dois tipos de criptografia. Este protocolo funciona, trocando chaves públicas entre os dois lados da comunicação. Cada lado gera uma senha única e a envia para o outro, que a decifra com sua chave privada. Após essa troca inicial (*handshake*), uma chave privada compartilhada é usada para criptografar o conteúdo da comunicação com um algoritmo simétrico, que é mais eficiente para grandes volumes de dados.

Tão importante é a criptografia para a segurança dos dados digitais, que Assange *et al*. (2013) fundadores da *WikiLeaks,* escreveram um documento intitulado "*Um chamado à luta criptográfica*", constante da obra *Cypherpunks.*

Assange *et al*. (2013, p. xx) argumentam que se nada for feito, "em poucos anos a civilização global se transformará em uma distopia da vigilância pós-moderna, da qual só os mais habilidosos conseguirão escapar". Para chegar a essa conclusão, apoiou-se na sua experiência de 6 anos com a WikiLeaks, que entrou em conflito com diversos dos mais poderosos Estados do mundo. Explica ele que, no novo mundo da internet, abstraído do velho mundo dos átomos concretos, havia um sonho de independência.

Contudo, os Estados e seus aliados rapidamente se anteciparam para controlar esse novo mundo, dominando suas bases físicas compostas por um substrato de cabos de fibras óticas, satélites e servidores. O Estado logo aprendeu a usar seu controle sobre esse espaço físico para assumir o controle do reino digital e impedir a tão almejada independência e, infiltrando-se nos cabos de fibra óptica, nas estações terrestres e nos satélites, iria mais longe, interceptando, em massa, o fluxo de informações do novo mundo - sua própria essência. Ao mesmo tempo, todos os relacionamentos humanos, econômicos e políticos seriam afetados. O Estado se agarraria às veias e artérias da nova sociedade, devorando vorazmente cada relacionamento expresso ou comunicado, cada página lida na internet, cada *e-mail* enviado e cada pensamento buscado no *Google*. Ele armazenaria esse conhecimento — bilhões de interceptações por dia — em enormes depósitos ultrassecretos, acumulando um poder inimaginável. Esse tesouro intelectual privado e coletivo da humanidade seria incessantemente minerado com algoritmos de busca de padrões cada vez mais sofisticados, enriquecendo o tesouro e ampliando o desequilíbrio de poder entre os interceptores e o mundo inteiro de interceptados. E, então, o Estado refletiria o que aprendeu de volta ao mundo físico, para iniciar guerras, programar drones, manipular comitês das Nações Unidas e acordos comerciais, além de realizar favores à sua vasta rede de indústrias, *insiders* e capangas conectados (Assange *et al*., 2013, p. 22).

Vicente de Paula Maciel Júnior (2019) faz constatação similar:

> A imagem frequentemente passada de que o desenvolvimento e a revolução informacional foram oriundos de jovens brilhantes que

> desenvolveram computadores e programas em garagens de suas casas é um devaneio pueril. Como desmitifica Castells, foi o Estado, principalmente através do interesse do Departamento de Defesa Americano, por interesses militares de desenvolvimento e hegemonia de poder bélico e tecnológico sobre a União Soviética e os empresários que deram início à revolução tecnológica no Vale do Silício.
>
> A identificação desses "senhores aliados" na produção de uma nova economia, a informacional, é de grande relevância para a compreensão de seu mecanismo de atuação, bem como na responsabilização pelos efeitos dessa política que canaliza o fluxo de informações, pessoas, capitais e gera impactos decorrentes de um mundo conectado e em rede (Maciel Júnior, 2019, p. 16).

A partir dessa percepção, Assange *et al*. (2013, p. xx) argumentam que a única esperança contra o domínio total das informações pelo Estado reside na criptografia. "O universo acredita na criptografia". A razão para isso é que é mais fácil criptografar informações que descriptografá-las. Sugerem, ainda, que o universo apresenta essa propriedade que permite que um indivíduo ou grupo de indivíduos codifique algo de maneira confiável e automática, "de maneira que nem todos os recursos e nem toda a vontade política da mais forte superpotência da Terra será capaz de decifrá-lo". Por fim, afirmam que "uma criptografia robusta é capaz de resistir a uma aplicação ilimitada de violência. Nenhuma força repressora poderá resolver uma equação matemática" (Assange *et al*., 2013, p. 23).

5.2 Provas digitais: conceitos, características e natureza jurídica

5.2.1 Conceitos

Silva (2022, p. 199-200) define prova judicial como "todo mecanismo colocado à disposição das partes para que consigam convencer o juiz a respeito da existência de fato afirmado na causa de pedir, nas razões defensivas e/ou em manifestações posteriores".

A partir da análise do art. 369 do CPC/2015, é possível inferir que as partes têm o direito de utilizar tanto provas típicas quanto atípicas, para provarem os fatos que fundamentam seu pedido ou defesa, a fim de influir na convicção do juízo, desde que as provas, obviamente, sejam lícitas.

Silva (2022) argumenta que a atual disruptura, ocasionada pelo advento de novas tecnologias, leva a mudanças radicais na sociedade e nas relações humanas, o que ocorre desde o final do século passado. Afirma que “estamos caminhando a passos largos do mundo físico para o mundo virtual”, explicando que, com o giro linguístico e a migração das relações sociais e jurídicas para o ambiente virtual, as provas dos atos e fatos jurídicos, dos contratos e do cumprimento ou descumprimento de suas cláusulas estão cada vez mais presentes no espaço-tempo digital. Com todos os dados armazenados em arquivos eletrônicos, mídias sociais e nuvens, muitas pessoas já não imprimem mais esses dados. Fotografias reveladas, contratos impressos e outros documentos físicos estão desaparecendo. As comunicações são predominantemente virtuais, utilizando tecnologias de informática e telecomunicações, e ninguém mais imprime ou degrava conversas e outros dados resultantes dessas interações (Silva, 2022, p. 200).

É a partir desse cenário que se faz mister construir uma teoria das provas digitais, e trazer segurança para o operador do direito, que navega em inexplorados mares.

Assim, tratando do conceito de prova digital, é imprescindível trazer o escólio de Thamay e Tamer (2022), para os quais esta pode ser conceituada 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 sua demonstração. A prova digital é o meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo (Thamay; Tamer, 2022, RB-1.3).

Vale dizer que há duas acepções para o termo provas digitais: a primeira diz da demonstração de um fato que ocorreu inteiramente em suporte digital. Exemplo clássico disso é o de postagem caluniosa ou difamadora em plataformas de rede social, como o *Facebook* ou o *Instagram*. O fato todo ocorreu em meio digital, mais especificamente por meio de um provedor de aplicação, cabendo ao interessado a demonstração de autenticidade e integridade daquela informação desabonadora publicada na rede social.

O segundo caso, de um fato que ocorreu no mundo real, mas pode ser provado por meios digitais, pode ser exemplificado por alguém que alega não ter condições

suficientes para pagar pensão alimentícia, mas esbanja capacidade econômica nas redes sociais. Isso fica ainda mais claro quando Thamay e Tamer (2022) destacam que

> a prova digital pode ser entendida como a demonstração de um fato ocorrido nos meios digitais, isto é, um fato que tenha como suporte a utilização de um meio digital. E [...] em que, embora o fato em si não tenha ocorrido em meio digital, a demonstração de sua ocorrência pode se dar por meios digitais (Thamay; Tamer, 2022, RB-1.3).

O que importa, na verdade, para a definição da prova como digital é que a ocorrência de determinado fato seja evidenciada por um meio digital, tenha esse fato ocorrido em suporte digital ou não.

Capanema (2024, p. 191-192), complementando o escólio de Thamay e Tamer, afirma que essas provas se apresentam na forma de documentos, em duas espécies:

a) digitais ou digitalizados, aqueles hospedados em arquivos, localmente - em discos rígidos ou mídias externas -, ou remotamente, em servidores ou sistemas de nuvem; e
b) resultado de interceptação telemática, ou seja, os denominados arquivos “grampeados”, circulando em uma comunicação e copiados por meio de interceptação telemática. A relevância jurídica dessa distinção advém da base normativa diferente, que define requisitos formais próprios para a preservação de uns ou de outros.

Ademais, embora ambos os tipos resultem em provas documentais, as exigências para a sua obtenção variam: no primeiro caso, o procedimento é mais simples, enquanto no segundo, os dados só podem ser obtidos mediante determinação judicial e em investigações criminais (Provas [...], 2023).

5.2.2 Características

Embora haja alguma variedade de entendimentos quanto aos elementos ínsitos à prova digital, definimos alguns que nos pareceram essenciais às provas digitais.

Denise Vaz (2012) aponta para a imaterialidade, volatilidade, suscetibilidade à clonagem e a necessidade de dispositivo para transmissão, sendo, nesta esteira,

secundada por Furlaneto Neto e Santos (2020). Assim, apresentamos e discorremos, a seguir, essas características:

a) imaterialidade: ausência de representação física facilita a transmissão e contribui para o grande armazenamento de conteúdos nos sistemas informáticos. As provas digitais podem ser transmitidas sem a necessidade de movimentação física;
b) volatilidade: fato de sofrer constantes mudanças. Apresenta-se frágil, facilmente se submetendo a alterações ou ao desaparecimento com a modificação da sequência numérica que a compõe;
c) suscetibilidade à clonagem e facilidade de dispersão: característica que, devido à sua imaterialidade, torna a prova digital extremamente suscetível ao processo de clonagem. Pode ser facilmente copiada e transmitida a outros dispositivos eletrônicos, oferecendo risco à preservação da originalidade do arquivo utilizado como prova;
d) necessidade de dispositivo para transmissão: dependência de um dispositivo físico para a sua exposição, extração ou transmissão, em que pese sua imaterialidade, e independentemente do meio físico onde se encontre armazenada. Constituindo-se por combinações numéricas restritas ao ambiente digital, necessita de dispositivos físicos para o processamento e exteriorização. Portanto, o dispositivo para transmissão é a única forma de acesso ao teor da prova (Furlaneto Neto; Santos, 2020, p. 6).

Por seu turno, Júlio Baía[2] fala em volatilidade, replicabilidade, reprodutibilidade, repetibilidade e necessidade de dispositivo para transmissão, o que também nos soa correto.

Conforme Júlio Baía, a replicabilidade se refere à capacidade de reprodução ou duplicação de dados digitais de maneira consistente e exata, sendo essencial para a garantia da integridade e confiabilidade das provas digitais, algo similar à repetibilidade, que diz da possibilidade de se realizar um mesmo procedimento sob idênticas condições, e obter resultados igualmente idênticos. Já a reprodutibilidade

[2] Webinário realizado por Júlio Baía em 24 de abril de 2023 intitulado *Provas digitais no processo do trabalho* com apoio da Associação Mineirada da Advocacia Trabalhista.

refere-se à capacidade de diferentes pessoas, utilizando métodos semelhantes, mas em diferentes ambientes e contextos, obterem resultados consistentes e equivalentes ao analisar os mesmos dados.

5.2.3 Natureza jurídica

Dada a importância crescente das provas digitais nos processos e, especialmente as novidades que elas trazem, alguns autores acreditam que o mais adequado seria tratá-las como um novo meio de prova, isto é, não as encaixando propriamente como uma prova documental (Silva, 2022, p. 205).

Alertemos, entretanto, para o fato de que, legalmente, provas digitais podem ser incluídas na categoria de prova documental em sentido amplo (art. 422 e parágrafos do CPC); ou serem consideradas documentos eletrônicos (arts. 439 a 441 do CPC).

Carnelutti (1982, p. 158) entende que a forma predominante de documentação, de representação de um fato por meio de um objeto, tem sido - e ainda é - sua expressão por um meio que lhe dê suporte permanente, ou seja, a fixação desse fato em um objeto externo, de uma ideia que uma pessoa recebeu do próprio fato: este é o mecanismo da representação gráfica, visual, musical, etc.

Marques (1959, p. 395) compartilha dessa visão, quando leciona que documento é uma prova histórica real, pois representa eventos e fatos passados em um objeto físico, atuando como um instrumento de convicção.

Vale dizer, documento é um objeto capaz de materializar um fato, seja por meio da escrita, de sinais, gráficos, símbolos etc. Assim, filmes, fotos, transcrições e desenhos são considerados documentos (Thamay; Tamer, 2022, RB 2.1).

Deve-se cuidar apenas que nem todo documento constitui prova documental, bastando lembrar que todo ato processual é documentado. Nesse diapasão, o depoimento de uma testemunha é documentado, mas nem por isso perde sua natureza de prova testemunhal. O mesmo vale para a prova pericial. Por ser emitido um laudo, que será juntado aos autos de forma documental, sua natureza não muda de prova pericial para documental (Marinoni; Arenhart, 2022, p. 667).

Diante dessas considerações, acreditamos que, dadas as especificidades e nuances da matéria, a prova digital deve ser considerada uma prova documental

eletrônica. Assim é possível conciliar a inteligência (a) de que as informações que servirão para demonstrar a ocorrência de um fato (no meio real ou físico) necessitam de um suporte para a sua apresentação com (b) a certeza de que esse suporte é inerentemente mais volátil que um físico, como o papel.

Embora possamos alegar que um documento físico também seja suscetível a falsificações, o que seria um argumento hábil a atrair a natureza de simples documento às provas digitais, parece-nos claro que estas são muito mais frágeis, merecendo destaque em relação ao estudo dos demais documentos em geral, conferindo-lhes especificidades próprias.

Em suma, consideramos que a prova digital tem natureza jurídica de prova documental eletrônica, sendo prova atípica, ao menos até que sobrevenha legislação processual robusta que a indique como prova autônoma, e descreva procedimentos a fim de dotá-la de autenticidade e integridade.

5.3 A origem da informação

A informação pode se originar de fontes abertas ou fechadas.

As abertas são aquelas acessíveis ao público sem restrição ou necessidade de credenciamento, como jornais, revistas, periódicos acadêmicos, livros e, em maior escala, dados disponíveis na internet. A coleta de dados úteis dessas fontes para a verificação de fatos é conhecida como inteligência em fontes abertas (*Open Source Intelligence* - OSINT). O uso de fontes abertas tem ganhado importância crescente no mundo jurídico, sendo aceito nos tribunais como meio válido de prova. O advento das redes sociais, em particular, fez com que as pessoas passassem a compartilhar suas preferências, *hobbies* e personalidades na internet, tornando-as acessíveis a amigos, familiares e ao público em geral (Cavalcanti, 2018, p. 7).

Yamada (2021, p. 45) define a OSINT como “um modelo de inteligência que localiza, seleciona e obtém, através de dados disponíveis e acessíveis a qualquer pessoa, informações de fontes públicas para, em conjunto com outras fontes, produzir conhecimentos”, destacando que as provas obtidas na fonte aberta são produzidas de forma voluntária pela parte, sem que seja necessária autorização judicial para o seu emprego.

A fonte aberta se caracteriza por estar livremente disponível, sem proteção, não havendo necessidade de uso de senha ou intervenção judicial para acessar seu conteúdo. Sua utilização pode decorrer de atividade humana ou automatizada, “em que programas e *scripts* rastreiam *sites* e páginas da internet para a coleta de dados” (Capanema, 2024, p. 288).

Exemplos de seu uso são a comprovação de relação de amizade ou interesse entre autor e testemunha em processo judicial, por meio de publicação no *Facebook*, fotografias em redes sociais no ambiente de trabalho, após o fim da jornada regular para demonstrar sobrejornada, e *tweets* que comprovem crimes como a injúria racial.

Algumas das principais ferramentas de disponibilização de dados em formato aberto são o *Google, Twitter, Facebook* e *Instagram*. Porém, há um sem-número de ferramentas, de imagens, fotos, vídeos, geolocalização e mapas, procura de pessoas, dados sobre domínios, redes sociais e aplicativos de mensagens, meios de transporte, dados dos Poderes Executivo, Judiciário, Legislativo, bancos, moedas e criptomoedas etc. Literalmente, tudo que está na internet e permita a qualquer pessoa conseguir localizar uma informação que seja de seu interesse.

Existem, ainda, as informações acessíveis a partir de fontes fechadas, cuja obtenção de dados depende de algum tipo de autorização.

Bertachini (2021) classifica a obtenção de autorização como:

a) judicial, aquela que demanda ordem do juízo, como a quebra do sigilo, telefônico, bancário ou fiscal, bem como a interceptação telefônica; e
b) de restrição de acesso, “em regra, por login e senha, quando, para ter acesso a determinada fonte, deve haver autorização a ser dada pelo órgão ou empresa a qual esteja subordinado”. (Bertachini, 2021, p. 9).

Azevedo, Munhoz e Carvalho (2023, p. 56) definirão as informações acessíveis a partir de fontes fechadas como “informações privadas de usuários ou empresas, mantidas dentro de um banco de dados de plataformas, de acesso restrito ou protegido, que podem ser requeridas mediante convencimento do magistrado sobre sua relevância no caso.”

Nessa mesma linha, Barreto, Wendt e Caselli (2017, p. 34) afirmam que o acesso às fontes fechadas carece de autorização especial, uma vez que são de

caráter restrito a entidades públicas ou privadas. É dizer que a obtenção desses dados e conhecimentos depende de algum tipo de autorização, existindo obstáculos à sua obtenção.

Diante disso, pode se afirmar que as informações de fonte aberta são públicas e estão disponíveis para quem quiser acessar, sendo produzidas muitas vezes pelo próprio indivíduo, prescindindo de sua privacidade. As informações de fonte fechada, por sua vez, demandam autorização especial, não sendo, pois públicas.

5.4 A prova digital como meio de prova atípico

Comoglio (1999) leciona que a projeção direta do formalismo, nos seus perfis inerentes de garantia e legalidade processual, deveria ser, como é sabido, a tipicidade das provas e dos meios de prova, segundo um catálogo normativamente predefinido. De fato, a elencação heterogênea das fontes e dos procedimentos probatórios reforça a impressão – um tanto superficial – de uma pretendida taxatividade das previsões legais destinadas a esgotar, *a priori*, o número e as formas dos instrumentos de busca judicial da verdade.

A impressão permaneceria – sustentamos – mesmo quando, na regulação de casos particulares, a admissibilidade expressa de qualquer meio de prova ocasionalmente sugerisse uma tipicidade não absoluta, mas relativa, e, portanto, derrogável (pelo menos, por força da lei). A ideia dominante do *numerus clausus*, ao postular a virtual completude das fontes e dos métodos de conhecimento do *factum probandum*, não deixa, contudo, de reconhecer, na generalidade de certos conceitos ou nas potenciais capacidades expansivas, a possibilidade de adequar automaticamente a tipologia probatória à evolução da gnoseologia moderna e ao progresso científico (Comoglio, 1999, p. 21-22).

Conforme previsto no art. 5º, inciso XXXV, da CRFB/1988, a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito, consagrando o princípio do acesso à Justiça. Esse dispositivo constitucional não impõe qualquer limitação ao acesso à Justiça; pelo contrário, sua redação abstrata visa a permitir uma ampla busca pela tutela jurisdicional. Sob essa perspectiva, podemos afirmar a atipicidade do direito de ação. Em razão dessa irrestrição ao acesso à Justiça, é essencial que essa garantia também se aplique à amplitude probatória, sob pena de limitar a própria

garantia constitucional da ação e da defesa. Portanto, a chamada atipicidade dos meios probatórios, que integra o direito fundamental à prova, decorre da atipicidade do direito de ação (Engelmann, 2023).

Assim, seria mesmo dispensável que o legislador infraconstitucional explicitasse a matéria, mas ele fez questão de fazê-lo por meio da edição do art. 369 do CPC.

Como prenunciado, provas atípicas são aquelas que não constam de maneira taxativa nos códigos normativos.

Do Título V - Da Prova - do Livro III - Dos Fatos Jurídicos - do Código Civil de 2002 (CC/2002) (Brasil, [2024c]), são arrolados os seguintes tipos de prova de fato jurídico: confissão, documento, testemunha, presunção e perícia.

Já o art. 369 e seguintes do Código de Processo Civil de CPC/2015 estabelecem procedimentos para a coleta de provas baseadas em confissão, documento, testemunha e perícia.

Esse mesmo dispositivo, sensível à dificuldade de se provar um fato jurídico apenas por meio daqueles arrolados em lei, confere a possibilidade de as partes utilizarem provas que não essas, preconizando que as “partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.” (Brasil, [2024d]).

Desde que os meios utilizados sejam moralmente legítimos e não se trate de prova constitucionalmente ilícita, os sujeitos processuais podem empregar qualquer meio de prova sem distinção entre os típicos e os atípicos. Além disso, o regime de preclusões e eventualidade não favorece a proposição e produção de provas em etapas, condicionadas à utilidade do meio para estabelecer a verdade dos fatos e influenciar eficazmente a convicção.

O texto legal não sugere uma preferência por um regime de precedência condicionada (primeiro as provas típicas e, subsidiariamente, as atípicas). Pelo contrário, o art. 369 do CPC assegura o direito ao uso indistinto de qualquer meio de prova, desde que observadas as restrições legais e constitucionais. Portanto, a utilização de provas atípicas na formação do convencimento exige um ônus argumentativo adequado, de modo a comparar o meio utilizado, ainda que não previsto em lei, com a garantia da parte. (Müller, 2017, II-1.3).

Barzotto (2022) entende que, cada vez mais, as provas atípicas produzidas em ambiente digital, serão prevalentes:

> Pode-se dizer que as provas no processo terão grandes transformações porquanto serão cada vez mais produzidas atipicamente, por conta da entrada do processo no movimento de digitalização da sociedade. Ou, dito de outro modo, com a sociedade digital as pessoas deixam rastros ou pegadas na rede mundial de computadores, as quais podem ser seguidas pela autopublicidade dada pelas postagens na internet ou em aplicativos de comunicação em massa, ou mesmo ainda pela simples geolocalização de celulares, por exemplo (Barzotto, 2022, p. 95).

A migração de um modelo de provas típicas para um que incorpora cada vez mais provas atípicas, como as digitais, reflete o impacto direto da transformação digital nas práticas jurídicas. Por isso, as interações humanas mediadas por tecnologia demandam novas formas de captura, armazenamento e verificação de provas, ampliando o rol de elementos probatórios que devem ser aceitos pelos tribunais.

5.5 Legislação pertinente

Não obstante a relevância do tema, em face das mudanças sociais visíveis a olhos nus, fato é que se trata de uma realidade muito recente, de uma verdadeira disruptura por todos os ângulos que observemos. Assim, a legislação ainda é nova e carece de mais diretrizes, com a jurisprudência se ocupando de interpretar o instituto das provas digitais, segundo a CRFB/1988 e as normas já existentes, especialmente no que respeita a provas e princípios gerais do direito processual e material.

Marinoni e Arenhart (2022, p. 684) advertem sobre a atual insuficiência de legislação, ao apontarem para a “carência efetiva de dispositivos para tratar da força probante do documento eletrônico, especificamente em razão da dificuldade em se ter por autêntica a informação transmitida por via digital”.

Assim, cabe tratar das principais normas que, de alguma maneira, são relevantes para a temática das provas digitais.

5.5.1 Marco Civil da Internet - Lei n. 12.965, de 23 de abril de 2014

O MCI, Lei n. 12.965, de 23 de abril de 2014 (Brasil, [2021b]), estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil e é considerado uma espécie de "Constituição da internet", no país.

Ao regular o uso da internet no Brasil, o MCI buscou harmonizar princípios como a garantia da liberdade de expressão e de comunicação, a proteção da privacidade e dos dados pessoais e a responsabilização dos agentes, conforme suas atividades.

Longhi (2024) aponta para o fato de que o MCI é o centro de um microssistema de proteção ao consumidor usuário de serviços da internet, devendo, necessariamente, ser lido conjuntamente com o CDC, o CC/2002 e a CRFB/1988, além da Lei Geral de Proteção de Dados (LGPD), que o complementou e trouxe alterações em seu texto.

O MCI é marcado pelo seu conteúdo principiológico, reconhecendo como fundamentais, em seus arts. 2º e 3º, os princípios da utilização da internet, como:

a) o respeito e garantia à liberdade de expressão;
b) os direitos humanos;
c) o desenvolvimento da personalidade;
d) o exercício da cidadania em meios digitais;
e) a pluralidade;
f) a diversidade;
g) a abertura;
h) a colaboração;
i) a livre iniciativa;
j) a livre concorrência;
k) a defesa do consumidor;
l) a finalidade social da rede;
m) a proteção da privacidade;
n) a preservação e garantia da neutralidade de rede;
o) a preservação da estabilidade;
p) a segurança e funcionalidade da rede;

q) a responsabilização dos agentes de acordo com suas atividades;
r) a preservação da natureza participativa da rede; e
s) a liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos na Lei.

O texto legal se fundamenta em três princípios axiológicos que orientam a utilização da internet no Brasil: neutralidade, privacidade e liberdade de expressão. (Teixeira, 2024, p. 45).

A neutralidade da internet significa que o acesso dos usuários deve ser livre e igualitário, independentemente da finalidade. Isso inclui realizar pesquisas, fazer compras, se comunicar por *e-mail*, usar redes sociais, jogar, visualizar e postar conteúdos como textos, fotos e vídeos. O tratamento deve ser neutro, sem diferenciação com base no uso que o internauta faz da rede. Assim, o usuário pode utilizar a conexão para qualquer propósito (*e-mails, blogs*, etc.) sem pagar valores diferentes e sem fiscalização do provedor. O MCI reforça o princípio da neutralidade, exigindo que os responsáveis pela transmissão, comutação ou roteamento tratem todos os pacotes de dados de forma igual, sem distinção por conteúdo, origem, destino, serviço, terminal ou aplicação. (art. 9º, *caput*). (Teixeira, 2024, p. 45).

Esse princípio é atribuído a Tim Wu, para quem “neutralidade de rede é um princípio muito simples, que sugere que você tem o direito de acessar a informação que quiser, é sobre a liberdade das pessoas de se comunicarem”. E ainda, “diz respeito à liberdade de expressão no nosso tempo, pois protege o direito de pessoas criarem websites, blogs, páginas wikis, o que for, e poder alcançar outros usuários” (Wu apud Forgioni; Miuri, 2015, p. 1277).

Ele é enunciado no art. 3º, IV e no art. 9º do Marco Civil (Brasil, [2021b]). A proteção à privacidade também mereceu especial atenção do legislador.

Os escândalos de espionagem internacional, no segundo semestre de 2013, ajudaram a amadurecer a discussão sobre a importância da privacidade no Brasil e a fortalecer as regras sobre proteção à privacidade e aos dados pessoais. Essa proteção foi elevada ao *status* de princípio fundamental da regulamentação da internet no país (art. 3º do MCI) (Blum, 2022, p. 159).

Nesse contexto, a privacidade não é apenas um princípio enunciativo, mas uma garantia fundamental do texto legal em conformidade com a CRFB/1988. Assim, é

direito do usuário a inviolabilidade e o sigilo do fluxo de suas comunicações (art. 7º, I), destacando-se que a privacidade e a liberdade são condições essenciais para o pleno exercício do direito de acesso à Internet (art. 8º, *caput*).

O MCI também busca evitar práticas de vigilância, comuns nos modelos de negócios de muitos provedores e instituições públicas, regulando o registro e a disponibilização de dados referentes à conexão e ao acesso a aplicações da Internet. Para isso, o art. 5º do MCI utiliza conceitos que estruturam o funcionamento da rede, como o da internet, terminal, administrador de sistema autônomo, endereço IP, conexão à internet, registro de conexão, aplicações de internet e registro de acesso a aplicações de internet (Longhi, 2024).

A privacidade ainda é resguardada por dispositivos específicos, como o art. 10, que estabelece que

> a guarda e disponibilização dos registros de conexão e de acesso a aplicações de internet, [...] bem como de dados pessoais e do conteúdo de comunicações privadas devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (Brasil, [2021b]).

O art. 11 mantém sintonia com essa preocupação, quando estabelece que, em todas as operações de coleta, armazenamento, guarda e tratamento de registros, dados pessoais ou comunicações realizadas por provedores de conexão e aplicações de internet, nos quais pelo menos uma dessas ações ocorra em território nacional, devemos, obrigatoriamente, cumprir a legislação brasileira e garantir os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e registros.

Além disso, desponta como pedra de toque do MCI a liberdade de expressão, como se dessume do art. 2º, caput, art. 3º, I e art. 8º, todos com nítida carga principiológica.

5.5.1.1 Do dever de guarda de informações pelo provedor de internet

O MCI, em seu art. 4º, traz os conceitos de registro de conexão e registro de acesso a aplicações na Internet.

O primeiro é classificado como “o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados”, e o segundo como “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP” (Brasil, [2021b]).

Atualmente, cabe ao administrador de sistema autônomo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 01 (um) ano, nos termos do art. 13 do MCI.

Já em relação aos provedores de aplicação, o prazo é menor ainda, de 06 meses, de acordo com o art. 15 do MCI, e diz respeito apenas a pessoas jurídicas que exerçam atividade de forma organizada profissionalmente (Brasil, [2021b]).

5.5.1.2 Do fornecimento de informações pelo provedor de internet

O fornecimento de informações pelos provedores de internet está intimamente ligado ao cumprimento do requisito de autenticidade da prova digital. É o que comprova que o autor aparente do fato digital é o autor real.

Não é suficiente acessar um perfil e alegar que ele é real. Via de regra, os provedores de internet não fazem verificação documental da legitimidade da criação de determinado perfil. Assim é que existe uma estrutura disposta no MCI - Lei n. 12.965, de 23 de abril de 2024 - de formação probatória prévia, orbitando especialmente ao redor do art. 22, vocacionada ao fornecimento de informações (Prova [...], 2024), que dispõe que

> a parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet (Brasil, [2021b]).

Cabe, neste ponto, o pequeno reparo de que o legislador expressamente tratou de processo cível ou penal, não contemplando na redação o processo trabalhista. Entendemos que não se trata de um silêncio eloquente, mas de um lapso, pois não há, sob o prisma constitucional, razão alguma para tal distinção.

O art. 22, parágrafo único, estabelece, ainda, os requisitos para acesso aos registros dos provedores de internet, quais sejam,

a) ordem judicial;
b) fundados indícios de ocorrência de ilícito;
c) justificativa da utilidade; e
d) período ao qual os registros se referem (Brasil, [2021b]).

É evidente que a identificação do autor de um ilícito praticado na internet é um processo complexo, envolvendo tanto provedores de conexão quanto de aplicação. Ademais, o MCI não delineou o caminho a ser seguido da identificação do ilícito até a descoberta da verdadeira identidade do autor.

A partir dessa perspectiva, Thamay e Tamer (2022, RB-2.5) sistematizaram o procedimento para a identificação da autoria ou a certificação da autenticidade de um fato digital na internet, que consiste em um processo de cinco fases:

a) identificação e preservação do fato na internet;
b) identificação do provedor de aplicação utilizado;
c) obtenção das informações junto ao provedor de aplicação;
d) identificação do provedor de conexão utilizado; e
e) obtenção das informações junto ao provedor de conexão. Todavia, nem sempre todas essas fases serão necessárias. Por exemplo, o provedor de conexão pode ser diretamente identificado em casos de recebimento de *e-mail*, no qual é possível identificar o IP de conexão no cabeçalho técnico da mensagem eletrônica.

Então, diante de um possível ilícito, a parte ofendida deve partir da ponta final: o provedor de aplicação. Assim, a parte interessada, primeiramente, preserva a prova, depois aciona judicialmente o provedor de aplicação, requerendo-lhe justificadamente os registros de acesso a aplicações, como o número IP, a porta lógica, data e hora. Desse modo, o provedor devolverá um relatório com os dados que tiver e buscar-se-á descobrir o responsável pelo ilícito.

O passo seguinte dependerá da resposta do provedor. Se o autor puder ser identificado a partir de algum dado pessoal que torne certa a autenticidade, a prova da autoria está formada, dispensando as demais diligências.

Entretanto, se forem obtidas apenas informações como IP, porta lógica, data e hora, o interessado deverá acessar um *site* como o maxmind.com e inserir o IP para identificar o provedor de conexão. Em seguida, deve acionar judicialmente esse provedor, solicitando a disponibilização dos dados cadastrais do usuário que utilizou aquele IP na data e hora especificadas (Provas [...], 2023).

Por fim, no que tange ao acesso às comunicações privadas, é imprescindível destacar que o art. 10, § 2º, do MCI permite o acesso ao conteúdo de comunicações armazenadas, como os *e-mails*, mediante ordem judicial. Ademais, o art. 10, § 3º autoriza a obtenção de dados cadastrais, tais como qualificação pessoal, filiação e endereço. Nesse caso, as autoridades administrativas podem requerer tais informações diretamente, enquanto particulares necessitam de autorização judicial para obtê-las.

5.5.2 Lei Geral de Proteção de Dados - Lei n. 13.709, de 14 de agosto de 2018

As novas tecnologias possibilitam que sejam apresentadas provas nos processos contendo uma grande quantidade de dados e metadados, como mensagens de texto, áudios, vídeos trocados em ambientes privados, e fotografias com informações que podem indicar localização, endereços e até mesmo IPs. Muitos desses dados são considerados sensíveis, pois podem revelar informações pessoais, como orientação sexual, etnia, religião e filiação partidária. Diante dessa realidade, a LGPD foi criada para estabelecer regras sobre o tratamento adequado desses dados pessoais.

Em contraponto à LGPD, existem princípios constitucionais como o da publicidade processual e o direito à produção de provas. Assim, é necessário equilibrar esses princípios para garantir o exercício do direito à elucidação dos fatos por meio de provas digitais, sem desrespeitar a proteção de dados pessoais (Barzotto, 2022, p. 193).

5.2.2.1 Breve histórico do instituto da privacidade: Estados Unidos da América e Europa.

A preocupação com a privacidade esteve, por muito tempo, restrita a uma pequena parcela da população. Ao longo da história, em diferentes sociedades e contextos, essa noção foi percebida de formas variadas, ajustando-se conforme os círculos sociais. Daí afirmar-se que a privacidade é flexível, moldável consoante o tempo e o lugar, sendo valorizada por uma cultura e, em alguns casos, até considerada dispensável por outra. Desde que o ser humano começou a demarcar limites, estabelecendo um espaço de convivência separado dos demais, surgiu a ideia que mais tarde evoluiria para o conceito de privacidade. Assim, podemos afirmar que suas raízes estão na noção de espaço físico (Peixoto; Ehrhardt Júnior, 2018, p. 35-36).

A partir do século XIX, com o desenvolvimento da fotografia e a facilidade de reproduzir imagens, aliadas ao poder de disseminação da informação pela mídia impressa, iniciaram-se os problemas de privacidade que enfrentamos hoje. Assim, no final do referido século, no ano de 1890, foi publicado nos Estados Unidos o *The Right to Privacy*, de Louis Brandeis e Samuel Warren, artigo em que defendiam o direito à privacidade como um direito da personalidade (Peixoto; Ehrhardt Júnior, 2018, p. 35-36).

Os autores estadunidenses, ao analisarem o caso Yovatt v. Winyard, 1 J. & W. 394 (1820), no qual se discutia o direito de propriedade, relataram que o réu, enquanto empregado do autor, obteve acesso clandestino ao seu livro de receitas e fez cópias, levando à concessão de uma injunção com fundamento na violação de confiança e do dever fiduciário. No entanto, eles destacaram a dificuldade de estabelecer uma distinção jurídica clara entre esse caso e uma situação em que um terceiro estranho ao autor obtém acesso indevido ao livro.

Propuseram, então, em livre tradução nossa, que tais direitos, seja qual for sua natureza exata, não são decorrentes de contrato ou de confiança especial, mas, sim, direitos *erga omnes*; e o princípio que tem sido aplicado para proteger esses direitos não é, na realidade, o da propriedade privada, a menos que essa palavra seja usada em um sentido ampliado e incomum. O princípio que protege escritos pessoais e qualquer outra produção do intelecto ou das emoções é o direito à privacidade, e a lei

não tem um novo princípio a formular, quando estende essa proteção à aparência pessoal, às palavras, relações pessoais, domésticas, aos atos ou outras relações quaisquer (Brandeis; E Warren, 1890).

No contexto europeu, a primeira legislação a tratar da proteção de dados foi a a LGPD (*Hessisches Datenschutzgesetz*) do Estado de Hesse, Alemanha Ocidental, promulgada em 7 de outubro de 1970. Em 1973, a Suécia se tornou o primeiro país europeu a implementar uma lei nacional sobre proteção de dados. Essa legislação introduziu conceitos fundamentais, como o registro central de informações de processamento de dados pessoais e o procedimento de licenciamento, que abriu o registro público ao escrutínio dos cidadãos e consumidores, servindo também como uma ferramenta de cumprimento legal para as agências de proteção de dados. Esses conceitos formaram a base das primeiras legislações europeias de proteção de dados (Peixoto; Ehrhardt júnior, 2018, p. 41).

Em 1977, foi publicada a lei federal alemã de proteção de dados (*Bundesdatenschutzgesetz*). No ano seguinte, a França editou sua lei sobre proteção de dados e liberdades (*Loi Informatique et Libertés*) e, em 1981, foi elaborado “o primeiro [...] tratado internacional referente à proteção de dados pessoais, a Convenção 108, instituída em 1981, em Estrasburgo, na França, ainda consagrado como um dos mais relevantes instrumentos envolvendo o tema globalmente” (Fachinetti; Camargo, 2021).

Em 1983, surgiu na Alemanha o conceito de autodeterminação informativa, que tem suas raízes históricas em uma decisão da Corte Constitucional alemã sobre a Lei do Censo Alemão (*Volkszählungsgesetz*), de 1982. Essa lei, de forma ampla, mas por vezes genérica, exigia que os cidadãos alemães fornecessem uma série de dados pessoais para permitir o mapeamento espacial e geográfico da população.

Entre as disposições mais vagas estavam as em que se previa a possibilidade de cruzamento dessas informações com outras bases públicas para a finalidade indefinida de "execução de atividades administrativas", evocando a concepção do "Estado Espião" imaginado por George Orwell, em seu livro *1984*, publicado em 1949, em cujo enredo o escritor britânico apresentava uma distopia (sociedade ideal) e explorava temas como manipulação da verdade, repressão à liberdade vigilância, controle totalitário, uma forma de crítica social na qual ele alertava sobre os males e perigos de certas tendências ou escolhas humanas.

Após diversas contestações, a Corte Constitucional declarou a inconstitucionalidade parcial da lei, estabelecendo que o compartilhamento dos dados pessoais deveria ocorrer, exclusivamente, para a finalidade estatística específica do censo. No início de sua decisão, a Corte reconheceu o direito do indivíduo de controlar seus próprios dados pessoais, introduzindo a expressão autodeterminação informacional ou autodeterminação informativa. Assim, essa ideia emergiu da dimensão subjetiva da proteção de dados como um direito fundamental (Tamer, 2022, p. 24).

A diferença temporal entre o “velho mundo” e o “novo mundo” é notável. Nos Estados Unidos, a discussão sobre privacidade ganhou relevância ainda no século XIX, enquanto na Europa, a preocupação concreta com o tema só emergiu no pós-guerra, especialmente após a invenção do computador. Inicialmente, a privacidade nos Estados Unidos estava relacionada ao direito de não ser incomodado, uma extensão do direito à vida, protegendo a integridade física e, posteriormente, os aspectos morais. O conceito de *right to privacy* envolvia a ideia de ser deixado em paz, sem interferências.

Já o movimento pela privacidade, que surgiu na Europa na segunda metade do século XX, se desvinculou do sentido físico do *right to privacy* americano, porquanto a preocupação central dos europeus passou a ser o novo paradigma tecnológico que ampliou o processamento de dados pessoais através do uso de computadores, focando-se, então, no controle sobre esses dados e na proteção das informações pessoais. As raízes da privacidade nos Estados Unidos estão em um direito do indivíduo, de caráter negativo, enquanto que as europeias estão na sociedade, apresentando características de direito positivo, no qual se exige do Estado que tome medidas para garantir a proteção de dados pessoais (Peixoto; Ehrhardt Júnior, 2018, p. 41-42).

5.2.2.2 A proteção de dados no Brasil

A partir da discussão europeia sobre a necessidade de proteção jurídica dos dados e da privacidade das pessoas que teve início na década de 1970, resultou a criação da Diretiva n. 95/46/CE, a qual posteriormente foi substituída pelo Regulamento n. 2016/679 (GDPR - General Data Protection Regulation, ou

“Regulamento Geral de Proteção de Dados”), publicada em 2016. Essa norma europeia exerceu uma forte influência na aprovação de legislações de proteção de dados em vários países, inclusive o Brasil. Em consequência, em 14 de agosto de 2018, foi incorporada ao ordenamento jurídico brasileiro a Lei n. 13.709/2018 (Brasil, [2022d]), conhecida como LGPD (Teixeira, 2024, p. 55).

O desenvolvimento de regulações específicas para a proteção de dados também ganhou, ao longo dos anos, respaldo teórico, com destaque para preceitos advindos da CRFB/1988, dentre eles os da privacidade. O descontrole e a incerteza sobre quem tem direito de acessar os dados pessoais afetam o poder de escolha que delimita e define a esfera pessoal de cada indivíduo. A necessidade de proteção jurídica para aqueles que confiam seus dados pessoais a entidades públicas ou privadas se tornou evidente à medida que esses dados adquiriram valor econômico e passaram a ser utilizados para fins comerciais (Silva, 2021, p. 92).

O conceito de dado de computador vem no art. 1º da Convenção de Budapeste, como “qualquer representação de fatos, informações ou conceitos numa forma adequada para o processamento num sistema de computador que inclua um programa capaz de fazer o sistema realizar uma tarefa” (Brasil, 2023a).

O art. 1º da LGPD estabelece que a Lei “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado” (Brasil, [2022d]) e tem por escopo a proteção dos “direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”, ou seja, trata de um tipo especial de dados, os pessoais.

A LGPD foi sancionada com a premissa de que todo dado pessoal possui relevância e valor. Por essa razão, o conceito de dado pessoal foi ampliado, assim como na GDPR, de forma que os dados pessoais são considerados informações relativas a uma pessoa singular identificada ou identificável, conforme estipulado pelo art. 5º, I da LGPD. Dessa forma, mesmo que certos dados pareçam irrelevantes em um determinado momento, ou não façam referência direta a uma pessoa específica, quando são transferidos, cruzados ou organizados, podem resultar em informações específicas sobre uma pessoa. Esses dados podem, inclusive, conter informações de caráter sensível (Silva, 2021, p. 97).

Doneda (2024), remetendo à Convenção n. 108, de 1981, também conhecida como Convenção de Estrasburgo, recorda que o Conselho Europeu, por ocasião de sua elaboração, criou uma definição para informação pessoal condizente com essa ordem conceitual. Nos termos da Convenção, informação pessoal é “qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação”, de modo que é possível inferir o que caracteriza determinada informação como pessoal, ou seja, o fato de estar vinculada a uma pessoa, com potencial de revelar algum aspecto seu, o que é bem similar ao conceito de dado estabelecido pelo art. 5º, I da LGPD, seguindo tendência já existente por ocasião da elaboração da Lei de Acesso à Informação - Lei n. 12.527, de 18 de novembro de 2011 (Brasil, [2022c]) -, que, em seu art. 4º, IV, define informação pessoal como aquela relacionada à pessoa natural identificada ou identificável (Doneda, 2024).

Doneda (2024) destaca a relação intrínseca entre a privacidade e a informação pessoal, sugerindo que a privacidade aumenta na medida em que a disseminação de informações pessoais diminui, e vice-versa. Essa correlação serve de base para demonstrar como a proteção das informações pessoais foi incorporada ao ordenamento jurídico, emergindo como uma extensão da tutela do direito à privacidade. Em outras palavras, a defesa da privacidade naturalmente incluiu a proteção das informações pessoais como necessidade jurídica (Doneda, 2024).

A leitura do art. 2º da LGPD deixa claro que é possível extrair os fundamentos da disciplina da proteção de dados pessoais, que são o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Assim, LGPD abrange todas as relações jurídicas estabelecidas tanto digitalmente quanto fisicamente, sendo aplicável a qualquer pessoa física ou jurídica que realize o tratamento de dados pessoais. Isso inclui entidades de direito público (como a União, Estados, Municípios e suas autarquias) e entidades de direito privado (como empresas, associações, fundações, partidos políticos, igrejas, entre outros), conforme disposto nos arts. 1º e 3º da lei. Em resumo, a LGPD se aplica a todas as operações de tratamento de dados, independentemente do meio utilizado, seja físico

ou digital (Teixeira, 2024, p. 56).

É importante, ainda, distinguir as expressões dado pessoal e dado sensível. Enquanto o primeiro, de acordo com o art. 5º, I, se relaciona simplesmente à informação acerca de pessoa natural identificada ou identificável, o segundo é definido no art. 5º, II da LGDP como “o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”, merecendo tutela legal ainda maior, como se dessume do art. 11, que impõe uma série de restrições ao tratamento desses dados.

Os princípios a serem observados quando do tratamento de dados pessoais são elencados no art. 6º da Lei:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil, [2022d]).

Esse último dispositivo merece destaque, pois diz da necessidade de organização dos operadores para que possam, eventualmente, apresentar documentos em determinado procedimento administrativo ou mesmo para um processo judicial (Provas [...], 2023).

A lei ainda dispõe pormenorizadamente sobre o tratamento de dados, passando pelos seus requisitos, do tratamento de dados de crianças e adolescentes, do término do tratamento de dados, direitos do titular, responsabilidade e outros.

5.5.3 ICP-Brasil - Medida Provisória n. 2.200-2, de 24 de agosto de 2001

A Medida Provisória em tela (Brasil, [2020]) instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão (Brasil, 2024b) com forte esteio na hierarquia e centralização de operações.

Essa cadeia hierárquica tem o Instituto Nacional de Tecnologia da Informação (ITI) como a Autoridade Certificadora Raiz (AC-RAIZ) da ICP-Brasil, conforme o art. 13, a quem, enquanto primeira autoridade da cadeia de certificação, e nos termos do art. 5º da MP 2.200-2/2001, compete executar Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil,

> emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP (Brasil, [2020]).

Vale dizer que essa autarquia é a responsável pelo credenciamento de outras autoridades certificadores para que emitam certificados digitais. Atualmente, ela possui 23 autoridades certificadoras de primeiro nível a ela associadas, como a Certisign, Inmetro, Serasa, entre outras empresas conhecidas. Essas 23 autoridades certificadoras de primeiro nível possuem 122 autoridades certificadoras de segundo nível a elas vinculadas. Por exemplo, a OAB é uma autoridade certificadora de segundo nível, associada à Certisign. Na ponta da cadeia, estão as 2.436 autoridades de registro (Brasil, 2024b).

O certificado digital da autoridade certificadora de segundo nível é emitido pela autoridade certificadora de primeiro nível, que, por sua vez, tem seu certificado digital emitido pelo ITI, que fornece seu próprio certificado digital, porque ele é autoassinado (Dicionário [...], 2023).

À autoridade de registro compete identificar e cadastrar usuários, encaminhar solicitações de certificados à autoridade certificadora a que está vinculada e manter registros de suas operações de acordo com o padrão oficial brasileiro (ICP-Brasil), conforme art. 7º da MP n. 2.200-2/2001 (Brasil, [2020]).

Assim, quando o usuário preenche os requisitos para a obtenção do certificado digital, a autoridade de registro aciona a autoridade certificadora, que emite o certificado digital do usuário, que nada mais é que a declaração da identidade virtual do titular, de modo que o usuário recebe um par de chaves único formado por uma chave privada e uma pública, nos termos do art. 6º da Medida Provisória.

Há várias classes de certificado digital e com distintas finalidades. Os certificados digitais de classe A (A1, A2, A3 e A4) são de assinatura digital. Os certificados de classe S (S1, S2, S3 e S4) são de sigilo, que têm por condão conferir a confidencialidade de certificados utilizados para criptografia. Já os certificados T3 e T4 são de carimbo de tempo, e muito importantes para a preservação da prova digital (Dicionário [...], 2023).

Assim, é possível notar que a estrutura da ICP-Brasil é composta por uma forte hierarquia de órgãos que realizam a identificação virtual de pessoas físicas e jurídicas. Isso possibilita que documentos com assinatura digital possuam a mesma validação que os impressos em papel. Todos os procedimentos de identificação, certificação e validação de documentos digitais estão integrados ao sistema federal. O Instituto Nacional de Tecnologia da Informação, principal autoridade da ICP-Brasil, está subordinado à Casa Civil da Presidência da República, nos termos do art. 3º da Medida Provisória n. 2.200-2/2001 (Brasil, [2020]).

Trata-se, pois, de infraestrutura criada para garantir a validade de assinaturas eletrônicas e transações na internet, por meio da utilização de certificados digitais e de uma hierarquia que remonta à Presidência da República, caracterizada por uma forte capilarização.

5.5.4 Outros dispositivos normativos

Capanema (2024) faz um apanhado das normas jurídicas e técnicas aplicáveis às provas digitais, de modo que é salutar apontá-las.

Não obstante não haja regramento próprio sobre as provas digitais, vários dispositivos legais têm repercussão sobre a temática, além daqueles já expostos anteriormente. São eles:

a) Lei n. 9.296/96 estabelece o procedimento das interceptações telefônicas e telemáticas (Brasil, [2019a]);
b) Lei n. 9.472/97 - Lei da ANATEL -, em seu art. 72, trata da divulgação das informações do usuário de telefonia (Brasil, [2021a]);
c) CC/2002 cuida das reproduções eletrônicas (art. 225) (Brasil, [2024c]);
d) Lei do Processo Eletrônico - Lei 11.419/2006 - define os parâmetros legais para o emprego de meios eletrônicos no processo judicial, dispondo sobre a realização de atividades processuais eletrônicas e definindo as regras para a validade jurídica das informações eletrônicas, tratando de documentos eletrônicos e arguição de falsidade em seu art. 11, caput e §2º (Brasil, [2022b]);
e) Lei 9.613/98, alterada pela Lei n. 12.683/2012 dispõe sobre o acesso do Ministério Público e da autoridade policial

> aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito, conforme o art. 17-B (Brasil, [2023]);

f) CPC trata de documentos eletrônicos (art. 439 a 441) (Brasil, [2024d]);
g) Decreto n. 8.771/2016 regulamenta o MCI (Brasil, 2016a);
h) CPP, em tipos penais específicos, admite a requisição de dados cadastrais (eletrônicos ou não) de suspeitos (art. 13-A) (Brasil, [2024b]); e, mediante ordem judicial, de informações de empresas prestadoras de serviço de telecomunicação e/ou telemática (art. 13-B) que permitam a localização da vítima ou dos suspeitos do delito em curso (Capanema, 2024, p. 193-194, 2024).

Atualmente, está em curso o Projeto de Lei (PL) n. 4.939/2020, de autoria de Leal (2020), do PSD/RJ, apresentado em 15 de outubro de 2020.

O PL “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” (Leal, 2020).

Diante do atual contexto, de escassas e esparsas normas sobre a matéria, consideramos premente uma lei específica para a matéria que trace orientações específicas para a sua utilização nos tribunais, dirimindo interpretações diferentes sobre o tema.

Atualmente, o PL está aguardando parecer do relator na Comissão de Comunicação (CCOM) da Câmara dos Deputados.

O texto em questão é um normativo composto por 38 artigos, cuja justificativa está alinhada com os pontos discutidos ao longo desta análise. Destacamos, a seguir, um excerto desse texto, com o intuito de ilustrar a afirmação de que o PL mantém coerência com o que foi exposto neste texto:

> Neste cenário, as legislações vigentes, a exemplo do Marco Civil da Internet (Lei n. 12.965/14), da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18) e do Projeto do Senado de Combate a Notícias Falsas (Projeto de Lei n. 2.630/20), objetivaram conceituar e regular este novo ambiente de fatos jurídicos, mas não trouxeram em seu bojo a definição suficiente de conceitos e protocolos probatórios. A evidência digital tem natureza e comportamento distinto das conhecidas evidências físicas, confortavelmente assentadas em classificações documentais, testemunhais e periciais. Sua natureza eletrônica, consubstanciada hodiernamente em um padrão binário, mas já caminhando para novas codificações quânticas, revela a premente necessidade de complementar as normas vigentes que trouxeram a regulação do uso de dados pessoais, relações sociais por meio da Internet, transparência da informação, processamento eletrônico e armazenamento massivo de documentos em formato nato-digital. As velhas práticas probatórias solidificadas no ambiente físico, uma vez transportadas para os meios eletrônicos, ganham alcance ampliado, o que necessita ser harmonizado, também, com os impactos da cibernética nos direitos fundamentais (Leal, 2020).

5.6 Pressupostos de validade e utilidade das provas digitais

A confiabilidade das provas sempre foi uma preocupação central do legislador, de modo que a aptidão da prova documental a rememorar fatos sempre foi destacada, como se depreende do art. 401 do CPC instituído pela Lei n. 5.869, de 11 de janeiro

de 1973 (CPC/1973) (Brasil, [2015]), em que ficou estipulado que a prova exclusivamente testemunhal apenas seria aceita nos contratos que não excedessem o décuplo do salário mínimo.

Nessa mesma toada, Pastore (2020) sugere uma certa fragilidade das provas pessoais, sobre as quais

> pesa um estigma de desconfiança, pela pouca efetividade do depoimento pessoal para a obtenção de informações relevantes e, em especial, pelo frequente comprometimento da prova testemunhal pelo esquecimento, pelas falsas memórias, pela parcialidade ou corrupção do depoente, ou mesmo pela morte ou impossibilidade de localização da testemunha (Pastore, 2020, p. 65).

Não obstante qualquer tipo de hierarquia entre as provas seja incompatível com o processo constitucional, na prática, e mesmo consoante análise de alguns dispositivos legais, percebemos a prevalência da prova documental sobre a testemunhal.

Essa introdução tem importância, ao resgatar a noção de confiabilidade da prova, fundamental no atual contexto em que as provas digitais, cada vez mais, ganham relevância.

Apesar de a prova documental ser inerentemente mais segura pelas suas próprias características, ela também está sujeita a influir negativamente na avaliação dos fatos, como acontece na sua falsificação ou adulteração.

Assim é que o legislador, a par das exigências de forma solene para determinados atos e das disposições sobre o teor de instrumentos particulares, demonstra alguns cuidados na disciplina da prova documental, “exemplificativamente, na disciplina dos pormenores do conteúdo e do momento da lavratura das escrituras públicas, quanto ao que deve ser declarado, como as declarações devem ser conferidas pelos subscritores, quem deve assinar o instrumento público e de que modo os presentes devem se identificar para a prática do ato (art. 215, §§ 1º, 2º e 5º, do Código Civil)” (Pastore, 2020, p. 65).

Diante desse panorama, em que vislumbrada ficou a importância atribuída à confiabilidade da prova, é possível deduzirmos pelo menos duas premissas relevantes para o tratamento da prova digital: a) a força probatória do conteúdo de um documento está vinculada à sua origem e, consequentemente, à credibilidade do que foi registrado nele; e b) a precisão das informações, quando não há acesso direto ao

original, está sujeita à confiança da pessoa responsável por transformá-las em formato documental para inclusão nos registros do processo (Pastore, 2020, p. 66).

Como podemos inferir, a confiabilidade está intimamente relacionada à noção de segurança, havendo várias tecnologias que visam a dotar as relações virtuais de maior certeza. Didier Júnior, Braga e Oliveira (2019), colhendo exemplos de Antônio Terêncio Marques, citam:

a) a assinatura digital;
b) as firmas biométricas;
c) as senhas pessoais, como o “Número de Identificação Pessoal” (Personal Identification Number , o PIN) e o password; e
d) a esteganografia que transforma uma informação em código. Além dessas técnicas, os autores destacam a criptografia, em que “a declaração é cifrada e transformada em um código ininteligível àquele que não conhece o padrão para a decifração” (Didier Júnior; Braga; Oliveira, 2019, p. 255).

Em suma, a confiabilidade diz da aptidão para proporcionar algum grau de certeza da ocorrência de determinado fato no mundo material - ou virtual - a partir da prova produzida, necessidade que se torna mais palpitante quando se está a tratar de provas digitais, que podem ser facilmente editáveis, lançando dúvida sobre a sua origem.

Marinoni e Arenhart (2022, p. 679) apontam para o fato de que os documentos eletrônicos representam um grande desafio, indicando que a confiabilidade da prova documental - e a importância única que os ordenamentos processuais lhe atribuem - baseia-se na estabilidade do suporte em que a informação é registrada. Um documento em papel possui alto valor probatório, porque é difícil alterar seu conteúdo sem deixar evidências de falsificação. Em contraste, um documento escrito na areia da praia teria pouco valor, pois o suporte (a areia) é altamente vulnerável, e pode ser facilmente apagado sem deixar rastros. Esse é o problema central dos documentos eletrônicos: o suporte no qual a informação é registrada é virtual, o que permite que alguém com conhecimentos básicos de informática possa adulterar a informação sem deixar vestígios. Dessa forma, é extremamente complicado conceder aos documentos eletrônicos o mesmo valor probatório que se atribui aos documentos tradicionais.

Embora sejam argumentos válidos, não se pode ignorar que as relações sociais são travadas, cada vez mais, por meio de plataformas eletrônicas, de modo que as provas digitais devam ser objeto de estudo, a fim de que o direito possa andar a par da realidade, regulando-a, e não a ela se curvando.

Fundadas na noção de confiabilidade das provas em geral, surgem os pressupostos de validade e utilidade das provas digitais:

a) autenticidade;
b) integridade; e
c) preservação da cadeia de custódia.

A deficiência de qualquer desses fatores, quando da coleta e utilização da prova que pretende demonstrar a ocorrência de um fato, redundará, inevitavelmente, na fragilidade da confiança depositada nessa prova.

Didier Júnior, Braga e Oliveira (2019, p. 254) salientam que a preocupação com esses elementos é perene e fulcral no direito probatório digital, especialmente em vista da evolução tecnológica, que indica que, cada vez mais, os documentos eletrônicos serão usados, especialmente no trânsito jurídico de bens e serviços. É dessa forma que, a fim de que se possa atribuir valor probante aos documentos digitais, é fundamental aquilatar o grau de certeza de autenticidade e integridade. Sem essa garantia, não é possível conferir eficácia probatória a esses documentos.

A quebra da isonomia processual e o desrespeito ao devido processo constitucional podem ocorrer quando as partes não têm garantia de que as provas apresentadas são confiáveis e não foram adulteradas. Isso compromete o direito ao contraditório, à ampla defesa e à influência legítima das partes no processo judicial.

Portanto, a implementação de medidas de segurança, a preservação adequada das evidências digitais e o cumprimento estrito das normas processuais são essenciais para assegurar um processo judicial justo, e em conformidade com os princípios democráticos e constitucionais.

Dias (2015) destaca o papel do devido processo constitucional para assegurar a produção probatória em consonância com o direito ao contraditório, quando leciona que aquele - devido processo constitucional - deve conduzir um procedimento que possa garantir o direito da parte à prova, como extensão da garantia de defesa plena,

dentro de uma estrutura técnico-normativa contraditória, para permitir o conhecimento dos fatos ou declarações narrados pelas partes em seus raciocínios, e a valoração das provas apresentadas por elas para demonstrar suas narrativas, com o objetivo de obterem um pronunciamento favorável às suas reivindicações (Dias, 2015, p. 155).

Assim, não podemos vislumbrar um sistema de provas digitais no qual não sejam garantidas a autenticidade, a integridade da prova e a preservação da cadeia de custódia, sob pena de fragilização da isonomia processual, desrespeito ao devido processo constitucional e às próprias instituições garantidoras do Estado Democrático de Direito.

5.6.1 Autenticidade

Prevista no art. 4°, inciso VIII da Lei de Acesso à Informação 12.527/11, a autenticidade se define como a qualidade da informação produzida, expedida, recebida ou modificada por determinado indivíduo, por equipamento ou sistema. Isso, ainda encontra previsão no art. 195 do CPC.

Thamay e Tamer (2022) conceituam o termo, lecionando que

> por autenticidade deve ser entendida a qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital. Ou seja, é a qualidade que assegura que o autor aparente do fato é, com efeito, seu autor real. É a qualidade que elimina toda e qualquer hipótese válida e estruturada de suspeição sobre quem fez ou participou da constituição do fato no meio digital (Thamay; Tamer 2022, RB-1.4).

Didier Júnior, Braga e Oliveira (2019, p. 254) afirmam que determinado documento é autêntico “quando a autoria aparente corresponde à autoria real”.

No âmbito internacional, Yamada (2022, p. 136) lembra que o tema é abordado em diversos normativos, como a Request for Comments (RFC) 3227 (IEFT, 2002, p. 4) e o Guia Eletrônicos de Provas - um guia básico para policiais, promotores e juízes (União Europeia e Conselho da Europa (Electronic Evidence Guide - a basic guide for police officers, prosecutors and judges (European Union and Council of Europe - CyberCrime@IPA, 2020, p. 9), o qual estabelece que “a prova eletrônica não é diferente da prova física, como um documento registrado em um pedaço de papel”, sendo “necessário garantir que a prova seja autêntica”.

Yamada (2022) propõe duas indagações para se aferir a autenticidade da prova digital, uma de natureza objetiva, relativa à sua origem, e outra de natureza subjetiva, referente à identificação do sujeito envolvido com as questões, a seguir:

a) de onde provém o documento digital? e
b) quem é o autor ou quem são os sujeitos envolvidos no fato registrado no documento digital?

A primeira pergunta demanda a identificação da origem do documento eletrônico, o suporte em que foi produzido, armazenado ou transmitido, antes de ser identificado, coletado e preservado.

Já a segunda pergunta é respondida com a identificação da autoria do fato digital. É a certeza quanto ao autor (Yamada, 2022, p. 136-141).

O conceito de Thamay e Tamer (2022) anteriormente explanado – a qualidade da prova digital que permite a certeza com relação ao autor do fato digital – possui caráter nitidamente subjetivo.

Assim, é forçoso concluir que o requisito da autenticidade da prova digital resta cumprido, quando se identifica a origem e a autoria do fato digital; o suporte em que foi produzido, armazenado, ou transmitido, e o autor.

Por fim, cabe destacar que em grande parte dos processos, a parte demonstra apenas a integridade do conteúdo, e não sua autenticidade. Se o autor alega que foi ofendido pelo réu em uma rede social, juntando um *print* e levando uma ata notarial aos autos, a autenticidade, ainda assim, não resta provada. É o asseguramento de que aquela conexão partiu do terminal usado por ele no momento da ofensa que constitui a prova de que a conta é efetivamente do réu-agressor, o que causa risco de a prova ser impugnada, e, subsequentemente, ocorrer sua perda.

5.6.2 Integridade

Outro pressuposto de validade e utilidade da prova digital é a integridade, definida pela Lei de Acesso à Informação, em seu art. 4º, VIII, como a “qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino” (Brasil, [2022c]).

O decreto federal n. 10.278, de 18 de março de 2020, estabelece em seu art. 3º, IV, que integridade é o “estado dos documentos que não foram corrompidos ou alterados de forma não autorizada” (Brasil, 2020a).

Também encontra expressa previsão na legislação processual (art. 195 do CPC) e na estipulação de diretrizes para o tratamento dos registros eletrônicos e digitais, visando a assegurar a integridade da prova digital pela Norma Brasileira (NBR) / International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) n. 27037/2013 (Associação Brasileira de Normas Técnicas, 2013).

A integridade da prova é definida por Thamay e Tamer (2022, RB-1.4) “como a qualidade da prova digital que permite a certeza com relação à sua completude e não adulteração”, concluindo que a prova digital íntegra é aquela que não sofreu qualquer modificação em seu estado, desde a realização do fato até a apresentação do resultado prova. “Prova digital íntegra, portanto, é aquela não modificada ou adulterada, apta, portanto, a demonstrar a reprodução do fato em sua completude e integridade”.

Em evento denominado *As provas digitais no processo do trabalho*, realizado em 24 de abril de 2023 e promovido pela Associação Mineira dos Advogados Trabalhistas (AMAT), Júlio Baía[3] sustenta que a integridade é composta por 4 pilares:

a) completude;
b) imutabilidade;
c) temporalidade; e
d) credulidade.

A primeira determina que a prova obtida de qualquer fonte digital deve ser íntegra, sem omissões, refletindo plenamente o fato jurídico que se deseja demonstrar. Por exemplo, conversas de *WhatsApp* com mensagens apagadas não possuem integridade.

Imutabilidade consiste na demonstração, no processo, de que a prova se apresenta sem adulterações e no mesmo estado em que se encontrava quando

[3] Webinário realizado por Júlio Baía em 24 de abril de 2023 com apoio da Associação Mineira dos Advogados Trabalhistas.

coletada, refletindo os mesmos dados e informações relativos ao fato jurídico, desde aquele momento. Exemplo disso é a chave ICP-Brasil, que garante a imutabilidade do documento por meio de um par de chaves de criptografia assimétrica.

Já a temporalidade se refere ao carimbo de tempo da prova digital, sendo essencial, quando da coleta da prova digital, a demonstração de sua marcação temporal, contendo data e hora da ocorrência do fato, com a utilização de uma fonte do tempo confiável e rastreável. Isso é importante, porque a data e a hora de criação e/ou modificação de um arquivo dependem das informações fornecidas pelo computador ou dispositivo eletrônico que o gerou (tempo do sistema), podendo ser facilmente alteradas mesmo após o arquivo ser salvo, sem exigir grandes conhecimentos técnicos.

Por fim, conforme Júlio Baía, a credibilidade diz respeito à característica de que a prova digital deve ser compreensível às partes e aos julgadores, ou seja, facilmente inteligível e crível para um tribunal.

Yamada (2022, p. 145) aborda a normatização internacional, especialmente as orientações emitidas pela Agência da União Europeia para a Cibersegurança (ENISA) (European Union Agency for Cybersecurity) e pelo Departamento de Justiça dos Estados Unidos.

No caso europeu, a European Union Agency for Network and Information Security (2015, p. 6) publicou o manual *Prova eletrônica: um guia básico para primeiros* (*sistemas) respondentes*.” (*Electronic evidence - a basic guide for first responders*), que dispõe sobre a integridade da informação como seu primeiro e mais importante princípio. Do manual, se pode depreender que, de todos os princípios, este é provavelmente o mais importante e, em assim sendo, é vital que esse requisito seja tratado com a mais elevada primazia, devendo ser o fator principal na decisão sobre o que fazer (e o que não fazer).

A preocupação com a facilidade de edição de dados digitais fica diante da noção de que dados digitais são voláteis e a facilidade com que os meios digitais podem ser invadidos e modificados implica que a documentação de uma cadeia de custódia é crucial para estabelecer a autenticidade das provas. Além disso, todos os processos de exame devem ser documentados para que, se necessário, possam ser replicados (European Union Agency for Network and Information Security, 2015, p. 6).

Nos Estados Unidos, o Departamento de Justiça trata da integridade no seu manual *Investigação da Cena de crime eletrônico: um guia para primeiros respondentes, segunda edição* (*Electronic crime scene investigation: a guide for first responders, second edition)*, quando sugere aos socorristas cautela no manuseio dos dispositivos eletrônicos, a fim de que a integridade das informações ali contidas seja preservada (US Department of Justice, Office of JUSTICE Programs, National Institute of Justice, 2008, p. 28).

Yamada (2022, p. 145) propõe uma indagação a fim de perquirir sobre a integridade da prova digital: “a prova digital é aquilo que ela diz ser? ” Para responder a esta pergunta, devemos analisar sistemicamente o ecossistema digital em foi que produzida a prova, uma vez que o valor probante do conteúdo necessariamente deve ser aferido em relação ao ambiente em que se originou.

Assim, deduzimos que a integridade é elemento fundamental para a garantia da confiança e imparcialidade do sistema judicial. No contexto das provas digitais, a facilidade de manipulação torna crucial a implementação de protocolos rigorosos para garantir a preservação da integridade dessas evidências.

Tamanha é a importância da integridade de um documento eletrônico, que a Lei n. 11.419/2006 (Brasil, [2022b]), que trata da informatização do processo judicial, condiciona, em seu art. 12, a conservação dos autos do processo em suporte eletrônico à sua proteção por meio de sistemas segurança de acesso que garantam a preservação e integridade dos dados.

A premência disso se comprova com o fato de que o Superior Tribunal de Justiça (STJ) já se depara com questões palpitantes sobre a integridade das provas digitais. A decisão monocrática no recurso em Habeas Corpus (HC) n. 186.138/SP, publicada em 03 de abril de 2024 e de relatoria da Ministra Daniela Teixeira, deu provimento ao recurso por vício na coleta de dados, sob o argumento de que

> a autoridade responsável pela colheita de dados e informações digitais deve zelar pela sua integridade, especialmente face à volatilidade dos dados que são armazenados digitalmente, a fim de fazer com que seja possível se verificar se algum deles foi alterado, suprimido ou adicionado, após a sua coleta inicial (Brasil, 2024f).

Alguns métodos para a preservação da integridade da prova digital, com maior ou menor confiabilidade, são:

a) a ata notarial, que tem a integridade da prova certificada por um tabelião, no momento de sua elaboração, embora padeça de alguma ineficiência, à medida que seu custo é elevado, não garante não ter havido espoliação anterior e não assegura a autenticidade em seu aspecto subjetivo; e
b) serviços que fazem o isolamento, espelhamento e a preservação de fatos ocorridos no meio digital, como os oferecidos por empresas como *Verifact* e *OriginalMy*, por meio da utilização da ICP-Brasil, ou por registro na rede *blockchain*, respectivamente as tecnologias empregadas pela primeira e segunda empresas supracitadas.

5.6.3 Cadeia de custódia

Yamada (2022, p. 150) observa que, ao contrário da autenticidade e da integridade, elementos intrínsecos à prova digital, a cadeia de custódia é um atributo extrínseco, cuja finalidade é garantir a preservação desses outros requisitos.

A cadeia de custódia diz de uma preocupação com a idoneidade de todo o iter da prova digital, de sua coleta, seu manuseio e sua preservação.

Assim, por meio da preservação da cadeia de custódia, é possível imunizar a autenticidade e a integridade em todas as etapas da produção da prova digital, da sua identificação e coleta à extração de resultados e à apresentação no processo ou procedimento final. Isso permite construir um registro histórico completo da evidência, abrangendo toda a trajetória da prova. A ideia é que, se alguém repetir os mesmos passos realizados na produção da prova, o resultado será exatamente o mesmo. (Thamay; e Tamer, 2022, RB-1.4).

A Lei n. 13.964, de 24 de dezembro de 2019 (Pacote Anticrime) (Brasil, 2019a) traz o conceito de cadeia de custódia, ao incluir o art. 158-A ao CPP, definindo-a 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” (Brasil, [2024b]).

A cadeia de custódia é uma parte fundamental do processo de investigação, porque garante que as provas possam ser aceitas no sistema judicial. A cadeia de custódia documentará os termos relacionados a quando, onde, por que, quem e como, no uso de provas, em qualquer fase do processo investigativo. As questões da cadeia

de custódia tornam-se muito importantes, pois a autenticidade da prova deve ser mantida, de acordo com a condição em que foi descoberta pela primeira vez, sendo preservada até a sua apresentação nos autos. O escopo da cadeia de custódia inclui todos os indivíduos envolvidos no processo de aquisição, coleta, análise de evidências, registros de tempo, bem como informações contextuais que incluem rotulagem de casos e a unidade e laboratório que processa evidências (Prayudi; Azhari, 2015, p. 1).

Importante destacar, entretanto, que a segurança da cadeia de custódia não se aplica apenas na seara penal, mas em todas as esferas do direito, pois, repisemos, trata-se de um atributo de garantia da autenticidade e integridade do conteúdo que se pretende preservar.

Pastore (2020) observa que, independentemente da solução técnica adotada em cada caso, essa precaução só tem valor se a posse do material for restrita a pessoas idôneas e desinteressadas pelo resultado da investigação, comprovada por um registro documental fiel e, se necessário, complementada por testemunhas. Deve-se também anotar o uso de lacres, transporte e acondicionamento. Essa prática é conhecida no direito estrangeiro como cadeia de custódia (*chain of custody*), um requisito fundamental para a admissibilidade da prova digital, conforme identificado na paradigmática decisão do caso Lorraine v. Markel American Insurance Co (Pastore, 2020, p. 76-77).

Sua importância, sob a ótica do processo constitucional, é destacada no julgamento do Recurso em HC n. 77.836/PA, cujo voto do Ministro Relator Ribeiro Dantas publicado em 12 de fevereiro de 2019 revela que

> a cadeia de custódia tem como objetivo garantir a todos os acusados o devido processo legal e os recursos a ele inerentes, como a ampla defesa, o contraditório e, principalmente, o direito à prova lícita. O instituto abrange todo o caminho que deve ser percorrido pela prova até sua análise pelo magistrado, sendo certo que qualquer interferência durante o trâmite processual pode resultar na sua imprestabilidade (Brasil, 2024f).

No julgamento do Agravo Regimental (AGRG) no recurso ordinário em HC n. 143.169/RJ (Brasil, 2023b), de relatoria do Ministro Messod Azulay, da Quinta Turma do STJ, julgado em 07 de fevereiro de 2023, foi destacada a inadmissibilidade de provas digitais sem registro documental dos procedimentos adotados pela polícia para

preservação da integridade, autenticidade e confiabilidade dos elementos informáticos.

O recurso foi provido nos termos do voto do Ministro Ribeiro Dantas, destacando que “a principal finalidade da cadeia de custódia é garantir que os vestígios deixados no mundo material por uma infração penal correspondem exatamente àqueles arrecadados pela polícia, examinados e apresentados em juízo (Brasil, 2023b).

Assim, a autoridade policial que apreende um computador ou outro dispositivo de armazenamento digital deve copiar integralmente (*bit to bit*) o conteúdo, criando uma imagem dos dados que espelha fielmente o conteúdo original. Cabe ao Estado comprovar a integridade e confiabilidade das fontes de prova que apresenta, não sendo possível presumir a veracidade das alegações estatais, quando os procedimentos da cadeia de custódia são descumpridos. No processo penal, o Judiciário deve controlar a legalidade das ações do Estado-acusação com base no direito, e não na confiança que o Estado-acusação deposita em si mesmo.

Uma vez que, no caso, a polícia não tenha documentado os atos de arrecadação, armazenamento e análise dos computadores apreendidos, nem garantido a integridade dos dados sob sua custódia, revelou-se a impossibilidade de assegurar que os dados periciados sejam íntegros e idênticos aos originais.

Por fim, o Ministro Relator asseverou que, “devido à quebra da cadeia de custódia, são inadmissíveis as provas extraídas dos computadores do acusado e as provas delas derivadas, conforme a aplicação analógica do art. 157, § 1º, do CPP” (Brasil, 2023b).

Como podemos observar, a quebra da cadeia de custódia compromete toda a confiabilidade da prova digital.

5.7 A preservação e produção da prova digital

Se o art. 369 do CPC permite o emprego de todos os meios legais como prova dos fatos em que, fundados o pedido ou a defesa, a questão que surge concerne à confiabilidade das provas digitais, como discutido anteriormente.

Segundo Souza, Munhoz e Carvalho (2023, p. 51), o ambiente digital é muito mais volátil, podendo ocorrer situações em que um material pode ser adulterado ou

mesmo fabricado, sem que sejam deixados vestígios suficientes para a verificação de sua autoria e integridade. É a partir dessa constatação que surge “uma demanda por maior cuidado no processo de sua extração e documentação, para que seja confiável e, sobretudo, corresponda com a realidade dos fatos”.

Prosseguem com a constatação de que a forma como os dados que servirão como prova são coletados, preservados e analisados é de importância fulcral, pois diz da confiabilidade da evidência. Muitos métodos utilizados para o registro de fatos no meio digital podem não oferecer o grau de confiança necessário a respeito de sua origem e integridade. Assim, seriam geradas provas frágeis, incapazes de se sustentarem em face de questionamentos mais consistentes (Souza; Munhoz; Carvalho, 2023, p. 51).

A questão principal é o grau de confiabilidade das provas digitais. Os autores ilustram essa importância, ao distinguirem as provas entre as obtidas a partir de procedimentos burocráticos e aquelas oriundas da “realidade concreta”. Obviamente, as primeiras gozarão de um grau maior de confiança, por terem sido geradas em um ambiente controlado, com procedimentos específicos vocacionados para o asseguramento de confiança. Já aquelas produzidas a partir de uma realidade externa demandam maior cuidado, pois dependem, essencialmente, da adequação dos procedimentos utilizados para a documentação do fato que se pretende provar (Souza; Munhoz; Carvalho, 2023, p. 52).

Com tudo isso, ainda não se pode dizer de uma garantia absoluta de veracidade. O exercício de compreensão da realidade faz parte da evolução do conhecimento humano, de modo que a realidade muda e as tecnologias vêm em sua salvaguarda.

O que temos são meios mais ou menos confiáveis de coletarmos e preservarmos as provas digitais, que mantêm o contraditório ou o tornam inviável.

Nesse cenário, Souza, Munhoz e Carvalho argumentam que apenas a autenticidade e a integridade não são requisitos suficientes para garantir um patamar de credibilidade à prova digital obtida de fonte externa, mas, ainda, a completude sobre a integridade do fato, a temporalidade, marcando sua referência temporal, a auditabilidade, em que haja inteligibilidade e publicidade da prova e a cadeia de custódia (Souza; Munhoz; Carvalho, 2023, p. 53).

Dessa maneira, ao carrear uma prova digital aos autos, é necessário seguir um protocolo que confira confiabilidade à evidência, que, necessariamente, envolverá isolamento, coleta e preservação da evidência.

Com essa noção em mente, se torna possível vislumbrarmos a importância de uma preservação (registro) bem-feita da prova digital que se pretende produzir.

De acordo com Capanema (2024), esse procedimento pode ser realizado de duas maneiras: a) pela cópia ou b) pela interceptação. O primeiro consiste na reprodução de um conteúdo armazenado - estanque-, a exemplo de arquivos, páginas de internet, *posts* de redes sociais, vídeos em plataformas específicas, *e-mails*, discos rígidos, áudios, e conversas gravadas em aplicativos de comunicação. Enfim, é a coleta daquilo que já aconteceu.

Para tanto, é fundamental a garantia da cadeia de custódia, sendo possível demonstrar que aquele conteúdo copiado e apresentado no processo tem uma origem certa: em determinado *site* ou computador, em certo dia ou horário. Alguns exemplos citados pelo autor para a preservação da cópia são a *Verifact,* o *Gmail* e a ferramenta *archive. today* (Capanema, 2024, p. 209-210).

Capanema (2024) explica que a grande importância da preservação ocorre pela possibilidade de o conteúdo ser indisponibilizado ou apagado por quem o produziu, como postagens no *Instagram* e comentários no *Twitter.* Sob o prisma jurídico, “a preservação se mostra importante para comprovar o requisito de ‘fundados indícios da ocorrência do ilícito’, necessário para autorizar o requerimento de acesso aos registros de conexão e de aplicação”, nos termos do art. 22, parágrafo único, I, do Marco Civil, que preconiza que a parte interessada em formar conjunto probatório em processo judicial pode requerer ao juízo que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet, desde que haja fundados indícios da ocorrência do ilícito (Capanema, 2024, p 212-213).

Outra forma de preservação é a interceptação, que pode ser de natureza privada e pública.

A primeira se refere à captação do conteúdo de comunicação de caráter privado entre pessoas certas e determinadas. Diz respeito à privacidade e intimidade dos indivíduos, devendo obediência aos requisitos do art. 5º, XII da CRFB/1988 e à Lei n. 9.296/96 (Brasil, [2019a]).

Já a de natureza pública diz da comunicação pública normalmente direcionada a um número indeterminado de pessoas, em que aquele que comunica renuncia à sua intimidade. Exemplos são *streamings* de vídeo e *lives*, muito em voga por conta da pandemia. Pela sua própria natureza, dispensa o atendimento dos requisitos das normas anteriormente elencadas (Capanema, 2024, p. 213-214).

A cópia é estanque, a interceptação em trânsito.

Então, a preservação, para Capanema (2024, p. 215) é a própria confecção da prova, sua "elaboração", o registro do fato que ocorreu, enquanto a produção ocorre após a coleta; é a sua apresentação em processo judicial, administrativo ou procedimento arbitral, normalmente como arquivo em formato Portable Document Format (PDF) ou, ainda, em arquivo de mídia.

Souza, Munhoz e Carvalho (2023, p. 57) utilizam terminologia diferente para identificar o processo de registro da prova, tomando como referência a norma ABNT NBR ISO/IEC 27037:2013, que congloba uma série de recomendações que visam à padronização do tratamento de provas digitais, que irão contribuir para a sua admissibilidade, força probatória e confiabilidade, quando da apresentação dos fatos. Ou seja, constituem um conjunto de métodos internacionalmente aceitos, cujos passos são padronizados de sua coleta à apresentação em juízo.

Observam uma semelhança entre o iter que deve ser percorrido segundo a norma ABNT e aquele proposto para a cadeia de custódia no art. 158-B do CPP, acrescido pela Lei n. 13.964, de 2019, especialmente no que respeita ao isolamento, coleta e preservação da evidência (Souza; Munhoz; Carvalho, 2023, p. 58).

O isolamento é definido pelo CPP como o ato de evitar que se altere o estado das coisas, devendo-se isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e ao local de crime. É o conjunto de medidas que busca preservar o fato de adulteração ou contaminação, do início e durante a coleta e preservação da prova. Assim, quanto maior o cuidado nesta etapa, menor a possibilidade de impugnação da prova (Souza; Munhoz; Carvalho, 2023, p. 59-60).

Na sequência, temos a coleta, definida pelo CPP como o ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza. Em outras palavras, trata-se do registro sistemático das informações concernentes ao caso, "respeitando seu estado original, bem como anotando detalhes sobre sua origem e sobre o método empregado durante a extração" (Souza; Munhoz;

Carvalho, 2023, p. 60).

Por fim, a preservação consiste na realização de procedimento de proteção dos dados coletados, ainda em um contexto de isolamento, com o condão de proteger a integridade dos dados (Souza; Munhoz; Carvalho, 2023, p. 60).

Souza, Munhoz e Carvalho (2023, p. 67) ainda diferenciam integridade dos arquivos de integridade da prova. Para os autores, garantir a integridade digital dos arquivos cria uma evidência de que o conteúdo não foi manipulado desde o momento em que foi preservado, sem emitir opiniões sobre o que está sendo preservado. A integridade da prova, ou seja, a confiança de que reflete fielmente os fatos, está diretamente associada à realização de um conjunto de procedimentos que incluem o isolamento, a coleta e a preservação da evidência. Essas etapas proporcionam segurança quanto à origem do conteúdo e à sua não manipulação anterior, à sua preservação. Embora o primeiro seja de natureza técnica, o segundo é de origem jurídica, o que, frequentemente, causa confusão entre eles.

Independentemente de como se olhe para a preservação e a apresentação de provas, deve ser pacífico que esse processo deve ter por norte a preservação da autenticidade e da integridade, de modo a conferir confiabilidade ao conteúdo que está sendo levado a juízo.

5.8 Tecnologias para a preservação da prova digital

Sem a ambição de abordar exaustivamente o tema, é importante destacar as principais tecnologias disponíveis para a preservação da prova digital, conferindo-lhe a confiabilidade necessária para a garantia de autenticidade e integridade do documento digital que será produzido.

5.8.1 Código hash

Souza, Munhoz e Carvalho (2023, p. 62) explicam que o código *hash* é o produto de um algoritmo matemático “que produz uma sequência de caracteres pequena (normalmente de 32 a 256 caracteres), com base no conteúdo de um determinado arquivo”. Qualquer pequena alteração desse conteúdo acarreta uma drástica mudança em toda a sequência de caracteres.

Pastore (2021) também aborda o tema:

> Mais comum, porém, é aplicar a assinatura aos chamados *hashes*, *digests* ou *checksums*, que são produtos de algoritmos capazes de reduzir grandes quantidades de dados a uma sequência menor, usualmente de tamanho determinado, alcançada de modo unidirecional. Ou seja, submetido um conjunto de dados a um determinado algoritmo, que resume fragmentos de conteúdo distintos a uma representação igual, de modo a reduzi-los, resulta uma sequência de caracteres própria para identificar o documento, que não é única, pela própria natureza, mas suficientemente distintiva para evitar confusão ou adulteração em um mesmo contexto. Com isso, vincula-se ao autor do documento o *hash* e, se o documento a conferir produzir o mesmo código, quando submetido ao mesmo algoritmo, ter-se-á a certeza da integridade do conteúdo, isento de qualquer mínima modificação (Pastore, 2021, p. 70).

Brenol (2024) informa que a segurança das operações *hash* está calcada em três características:

a) Saída de tamanho fixo: o valor de entrada pode e normalmente é variável, mas as saídas têm o mesmo tamanho de código, ou seja, a mesma quantidade de letras, caracteres e números;
b) Eficiência no tráfego: a operação eficiente significa que a função, apesar de completa, não pode ser pesada, ou seja, não poderá comprometer a velocidade de processamento e tráfego dos dados;
c) Determinação: o valor do bloco de dados inseridos na entrada da função *hash* (*input*) será equivalente ao valor da saída (*output*), ou seja, não há perda na codificação ou decodificação (Brenol, 2024).

Ludgero, Medeiros e Ribeiro (2022, p. 221) utilizam o exemplo da empresa *Verifact*, que usa práticas forenses para espelhamento de fatos digitais, executando a verificação da integridade do arquivo por meio de cálculos *hash* e de outras medidas. “Para a garantia e a integridade do conteúdo e dos arquivos de metadados, a plataforma utiliza-se do método de código *hash*, confiável.”

Trata-se de uma representação matemática usada para identificar se o conteúdo digital não foi alterado.

A propósito, há uma explicação de como o mecanismo é utilizado:

> Imediatamente após a geração dos arquivos resultantes da captura técnica, é gerado um laudo PDF que consta todos os códigos HASH dos arquivos. Os códigos HASH são "impressões digitais" dos arquivos e, caso seja alterado um único dado sequer, o código será divergente do constante no laudo. Depois, o laudo PDF é protegido com uma assinatura digital da Verifact e o Carimbo de Tempo ICP/BR. Caso o laudo seja alterado, as assinaturas perdem sua validade, denunciando a alteração. Se as assinaturas do laudo estiverem integras, os códigos HASH, por sua vez, poderão ser usados para validar os arquivos externos. Se o novo código HASH gerado do arquivo externo não coincidir com o constante no relatório, o mesmo não se encontra mais integro. Este método é usado de maneira consistente por peritos em todo o mundo como forma de preservar a integridade de evidências (Verifact, 2024).

Ou seja, assim que o fato digital é capturado, gera-se um laudo de que constam todos os códigos *hash* dos arquivos. Em seguida, o laudo é protegido com uma assinatura digital e o Carimbo de Tempo ICP/BR, assuntos em comento na subseção a seguir, que garantem sua imutabilidade. Assim, eles são protegidos de adulteração, uma vez que qualquer manipulação posterior resultará em um código *hash* completamente diferente daquele constante do laudo.

Por ventura do julgamento do AGRG em HC n. 143.169/RJ, de Relatoria do Ministro Jesuíno Rissato, a Quinta Turma do STJ deu parcial provimento ao recurso, por conta da inobservância dos procedimentos técnicos necessários a garantir a integridade das fontes de prova arrecadadas pela polícia, sendo incabível “simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia” (Brasil, 2023b). Apesar de o voto não ter fixado o iter que deveria ter sido percorrido pela autoridade policial, houve grande ênfase quanto ao uso da técnica de algoritmo *hash:*

> Aplicando-se uma técnica de algoritmo hash, é possível obter uma assinatura única para cada arquivo - uma espécie de impressão digital ou DNA, por assim dizer, do arquivo. Esse código hash gerado da imagem teria um valor diferente caso um único bit de informação fosse alterado em alguma etapa da investigação, quando a fonte de prova já estivesse sob a custódia da polícia. Mesmo alterações pontuais e mínimas no arquivo resultariam numa hash totalmente diferente, pelo que se denomina em tecnologia da informação de efeito avalanche (Brasil, 2023b).

5.8.2 Certificação digital

De acordo com Souza, Munhoz e Carvalho (2023),

> a certificação digital é uma tecnologia criptográfica que permite a assinatura de documentos de modo confiável, com o uso de chaves privadas e públicas. A técnica envolve a entrega de uma chave privada associada a um certificado criptográfico para uma determinada pessoa ou entidade jurídica, que pode assinar documentos a partir dela (Souza; Munhoz; Carvalho, 2023, p. 63).

A integridade e autoria da assinatura são passíveis de validação a partir das chaves públicas do certificado criptográfico correspondente. É dizer: tem-se uma pessoa, física ou jurídica que possui uma espécie de identidade digital a qual é suscetível de verificação por um meio público, em assinaturas de documentos, acessos a sistemas e outros (Souza; Munhoz; Carvalho, 2023, p. 63).

No Brasil, o certificado individual, que corresponde à identificação virtual, necessariamente, deve ser emitido por agentes pertencentes à ICP-Brasil, instituída por meio da Medida Provisória 2.200-2, de 24 de agosto de 2001, de cujo art. 1º se depreende ter por condão “garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras” (Brasil, [2020]).

As chaves são emitidas por agentes autorizados, a quem, nos termos do art. 6º da referida Medida Provisória, compete “emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes, e manter registro de suas operações”.

Quando da emissão de uma chave por esses agentes autorizados, o certificado criptográfico possui o que é chamado de “hereditariedade validável”, ou seja, é possível aferir se a chave foi emitida por um agente outorgado pela autoridade central ICP/Brasil (Souza; Munhoz; Carvalho, 2023, p. 64).

Conforme o Ministério da Gestão e da Inovação em Serviços Públicos “a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão” (Brasil, 2024b). É justamente essa identidade digital garantida por um órgão governamental que traz segurança ao sistema.

A assinatura de um documento digital também deve contar com o que se denomina carimbo de tempo ou *timestamp*, a fim de dotar de integridade a prova que se pretende produzir.

No Portal do Serviços e Informações do Brasil é possível extrair que o carimbo do tempo “é um selo que atesta a data e a hora exatas em que um documento foi criado e/ou recebeu a assinatura digital, criando evidências de sua existência temporal e, ao mesmo tempo, garantindo a validade de sua assinatura digital” (Brasil, 2024c).

Souza, Munhoz e Carvalho (2023) sumarizam a importância da certificação digital para a higidez da prova digital:

> O uso da assinatura certificada de um determinado emissor, associada ao carimbo de tempo, gera imutabilidade digital criando meios de se verificar qualquer alteração em determinado conteúdo digital e cumprindo a função de preservação da informação no longo prazo (Souza; Munhoz; Carvalho, 2023, p. 64).

Atualmente, é uma tecnologia usada por empresas como a *Verifact* (2022, 2023, 2024), talvez a mais conhecida fornecedora do serviço de preservação de evidências digitais.

De acordo com Ludgero, Medeiros e Ribeiro (2022), a *Verifact* emprega um *mix* de tecnologias, usando práticas forenses para espelhamento de fatos digitais, como o uso de ambientes controlados e limpos, sem ruídos, pontos de acesso à internet seguros, coleta de metadados técnicos sobre fontes e conteúdos e verificação da integridade do arquivo por meio de cálculos *hash* e de outras medidas. Para cada sessão, um novo ambiente é criado no servidor da empresa para registro isolado de outros ambientes ou registros anteriores. Após o processamento das informações, o ambiente é destruído e os dados da sessão são apagados como medida de segurança (Ludgero; Medeiros; Ribeiro, 2022, p. 221).

Durante a sessão de captura, o usuário, por meio da interface fornecida, poderá registrar sua evidência digital. Após a conclusão, o relatório é lacrado com assinatura digital do certificado digital *Verifact* emitido pela autoridade de certificação brasileira da ICP-Brasil (Ludgero; Medeiros; Ribeiro, 2022, p. 221).

No Portal da Verifact (2022) é possível também compreender a importância da utilização de certificação digital no processo, que resulta em uma prova autêntica e integral:

> O resultado é a emissão de um relatório técnico certificado com as telas registradas, dados e metadados técnicos auditáveis para uma eventual perícia técnica, além de um vídeo de registro da navegação, com áudio, além de arquivos baixados durante a sessão. O relatório técnico leva a assinatura certificada da Verifact e carimbo de tempo ICP-Brasil. O carimbo de tempo ICP-Brasil, ou *timestamp* utilizado no relatório gera imutabilidade dos dados, registrando o exato dia e horário que o conteúdo foi acessado na internet e impedindo que os dados sejam apagados ou alterados após o registro (Verifact, 2022).

5.8.3 Blockchain

Derivado das palavras em inglês *block* (bloco) e *chain* (corrente), essa tecnologia sugere uma imagem mental de seu funcionamento: blocos de registros de informações conectados em uma rede. Dessa forma, chega-se à ideia de uma "cadeia de blocos" ou "encadeamento de blocos", o que oferece uma referência inicial sobre como essa tecnologia opera. Ela permite a transmissão de qualquer tipo de informação por meio de criptochaves, que, quando utilizadas, formam um bloco, funcionando como um livro contábil de registros de maneira pública, compartilhada e universal. Isso cria consenso e confiança entre todos os participantes e sobre todas as informações, nas quais as transações de cada registro são armazenadas (Engelmann, 2023).

Didier Júnior, Braga e Oliveira (2019) explicam que esse termo designa, ao mesmo tempo, a) uma base de dados distribuída e b) a tecnologia que mantém as múltiplas cópias dessa base de dados, operando em sincronia umas com as outras. A noção de descentralização da base de dados fica mais clara com o exemplo de bases de dados concentradas não distribuídas. Imagine que se pretenda obter informações sobre determinado imóvel. Essa informação estará disponível no Registro de Imóveis, de maneira centralizada, não distribuída. O mesmo ocorre, quando buscamos informações sobre antecedentes criminais. Devemos nos socorrer da base de dados das Justiças Estadual e Federal. O banco centraliza as informações financeiras do indivíduo. Por fim, há os buscadores de internet. Quando fazemos uma pesquisa por meio dessas ferramentas, utilizamos o site do Google ou do *Bing*, que são ferramentas que centralizam uma quantidade enorme de informações sobre vários assuntos, cujo acesso está disponível na internet (Didier Júnior; Braga; Oliveira, 2019, p. 261).

Por demasiado importante, transcrevemos o escólio dos autores:

> A ideia subjacente à blockchain é a de que a informação deve ser registrada em *múltiplos servidores*, de modo que é desnecessário existir um intermediário - o Registro de Imóveis, o Setor de Distribuição, o banco, o *google* - para que possamos acessar essa informação. Essa ideia se concretiza por meio do compartilhamento (distribuição) da informação – também chamada de *consenso distribuído*.
> Uma informação registrada na blockchain não fica em apenas um lugar, nem depende de um intermediário para ser acessada. Ela é distribuída entre os inúmeros computadores que compõem a rede (denominados "nós"), de modo que fica registrada em todos eles.
> Isso assegura a plena acessibilidade das informações registradas na blockchain, que podem ser consultadas 24 horas por dia, 365 dias por ano. Se um "nó" (computador da rede) estiver desligado ou tiver problemas porque sofreu um ataque *hacker*, haverá outro funcionando e a informação estará lá (Didier Júnior; Braga; Oliveira, 2019, p. 261).

Vale dizer: o que a tecnologia *blockchain* visa a fazer é descentralizar a informação, eliminar a figura do intermediário.

Thamay e Tamer (2022, RB-2.18) explicam tratar-se de uma rede *peer-to-peer*, em que cada usuário, de forma voluntária, disponibiliza seu dispositivo em prol dessa malha descentralizada de dispositivos, apontando para o fato de que a principal característica das redes *peer-to-peer* é a de que cada um dos dispositivos conectados nessa rede descentralizada é, ao mesmo tempo, um cliente ou receptor da informação como um servidor da rede. Cada dispositivo, portanto, exerce essa dupla função. Difere da rede mais comum em que há um servidor concentrando a emissão da informação e todos os demais dispositivos a ele conectados; apenas funcionam como clientes ou receptores dessa informação ou mensagem eletrônica. Cada dispositivo representa, portanto, a imagem de um nó ou um ponto de intersecção dessa rede.

Um sistema *blockchain* ideal busca a combinação de controle descentralizado (nenhuma parte única tem um papel privilegiado a priori), o consenso sobre um único estado ("fonte única de verdade"), registro à prova de falsificação (transações validadas não podem ser excluídas ou atualizadas *ex post,* uma vez adicionadas ao *blockchain*), preservação da privacidade (dados compartilhados publicamente, mas protegidos e privatizados por técnicas criptográficas como *hashing* criptográfico, criptografia de chave pública-privada, compartilhamento secreto para assinaturas digitais, provas de conhecimento zero etc.), e alta disponibilidade (alto grau de replicação em nós controlados por operadores de nós independentes e não

coniventes) em ambientes não confiáveis (Liu *et al*., 2022).

Thamay e Tamer (2022) utilizam a imagem de um "'livro-razão distribuído" para descrever a tecnologia, um

> protocolo seguro no qual uma rede de computadores verifica, de forma coletiva, uma transação antes de registrá-la e aprová-la. A tecnologia que sustenta o *blockchain* cria confiança, permitindo que pessoas que não o conheçam (e, portanto, não têm nenhuma base subjacente de confiança) colaborem, sem ter [sic] de passar por uma autoridade central neutra – ou seja, um depositário ou livro contábil central (Thamay; Tamer, 2022, RB-2.18).

Elegantemente, definem que "em essência, o *blockchain* é um livro contábil compartilhado, programável, criptograficamente seguro e, portanto, confiável; ele não é controlado por nenhum usuário único, mas pode ser inspecionado por todos" (Thamay; Tamer, 2022, RB-2.18).

Vale, ainda, replicar a doutrina dos autores, de modo a facilitar a compreensão do funcionamento do instituto:

> No blockchain, de forma diversa, as informações ficarão salvas de forma descentralizada e integral em cada terminal conectado na rede. Em outras palavras, os arquivos ou movimentações on-line feitas ficarão registradas em toda a rede. Isso significa, em termos práticos, que qualquer terminal integrante do blockchain (computador, dispositivo eletrônico ou estrutura computacional) tem uma cópia integral das informações (arquivo, transações etc.) e pode acessá-las imediatamente. Além disso, cada um dos terminais é responsável por validar ciberneticamente qualquer alteração informacional da rede, de tal modo que qualquer alteração precisa do consenso de toda a estrutura do blockchain (Thamay; Tamer, 2022, RB-2.18).

Então, a partir dessa compreensão, como a tecnologia de *blockchain* pode contribuir para a preservação das provas digitais?

Para Engelmann (2022), é evidente que a tecnologia *blockchain* pode ser utilizada no sistema processual cível, devido à sua conformidade com o núcleo ontológico do "meio de prova". A tecnologia tem o potencial de esclarecer o *thema probandum*, e o fato de a fonte da prova ser um sistema não impede sua admissão, desde que sejam respeitados os limites da legalidade da prova.

Souza, Munhoz e Carvalho (2022, p. 65) apontam que essa tecnologia consiste um uma operação que envolve duas ações, a) a verificação rápida de modificações

nos dados e b) a correção automática com base em replicadores desses dados. “Com isso, gera-se a imutabilidade dos dados, não permitindo a modificação de conteúdo que lhe foi inserido.” Caso seja detectada alguma adulteração nos dados, os replicadores são acionados, a fim de se obter a informação original do bloco, caso em que há uma verificação de consenso, através da qual os replicadores apontarão qual deveria ser a informação no bloco alterado.

É a própria ideia de uma cadeia de blocos, em que uma informação se conecta a outra. “Sempre que um novo bloco é validado consensualmente na rede, é como se todos os blocos que o antecedem fossem novamente validados” (Didier Júnior *et al*., 2019, p. 263).

De forma muito didática, Thamay e Tamer (2022, RB-2.18) ilustram com a imagem de que a compreensão do *blockchain* pode ser visualizada a partir de duas perspectivas: a) uma vertical, em que há uma cadeia de blocos de informação, e cada bloco contém sua própria informação e a de todos os blocos anteriores; e b) outra horizontal, em que o blockchain está em uma malha descentralizada de dispositivos, e cada dispositivo possui uma cópia confiável da cadeia de blocos.

Vale dizer que, para manipular ou apagar uma informação presente em algum dos blocos, é necessário alterar todos os demais. Além disso, “como o armazenamento se dá em malha descentralizada e cada um dos dispositivos dessa malha contém uma cópia simultânea e fidedigna, qualquer alteração em qualquer um dos blocos precisa ser validada tecnicamente por todos os dispositivos da malha” (Thamay; Tamer, 2022, RB-2.18).

Com isso, seria ineficaz o ataque a só um dispositivo. Para alguém infringir dano ao sistema, teria de ter força técnica para vulnerabilizar toda a rede descentralizada.

Thamay e Tamer (2022, RB-2.18) apontam que o Tribunal de Internet de Hangzhou, na China, já implementou um sistema de preservação judicial de provas utilizando *blockchain*, em casos relacionados a direitos autorais digitais, contratos financeiros e contratos de serviços de rede. As partes envolvidas se registram na plataforma, preservam as evidências de seu interesse na rede *blockchain* e as utilizam durante os processos judiciais.

Já há julgados nos tribunais pátrios, indicando a utilidade da tecnologia *blockchain* para a preservação da prova digital.

Tomemos como exemplo sentença publicada em 24 de novembro de 2023 nos autos do processo n. 0001080-82.2023.5.12.0050, da 5ª Vara do Trabalho de Joinville (Brasil, 2024m), em que uma empregada havia pedido indenização por danos morais, alegando que teve a sua vida sexual exposta, inclusive para clientes, o que pretendeu provar por meio de *prints* de *WhatsApp* e áudio.

Estes foram impugnados pela parte contrária, não sendo validados como meios de prova. O juízo fundamentou a não admissão das provas, por entender que para ser admitida, uma prova judicial digital deve reunir os requisitos de integridade, imutabilidade, temporalidade e publicidade, o que não pode ser observado no caso de conversas de *WhatsApp* ou *print screens* de quaisquer outras ferramentas de interlocução, que podem ser alteradas, com a supressão de trechos em prejuízo ao contexto integral das imagens. Revelador para o estudo da tecnologia de *blockchain* como meio de preservação da prova digital é que o juízo entendeu que o só fato de não se poder descartar a hipótese de adulteração do conteúdo produzido, é suficiente para que a prova não tenha a confiabilidade suficiente para ser usada em processo. Sugere com isso que

> [...] uma vez impugnada a autenticidade e a integridade de documento referente a *printscreen* de conversa ou videoconferência, faz-se necessário a juntada do documento integral, por ata notarial ou por meio idôneo de validação difuso, a exemplo plataforma "Verifact" ou de tecnologia em "Blockchain", como "Original My", dentre outros similares disponíveis, que garantem a integridade, imutabilidade, temporalidade e publicidade da prova apresentada e pretendida (Brasil, 2024m).

A 4ª Câmara do Tribunal Regional do Trabalho (TRT) da 12ª Região, em acórdão de relatoria da Desembargadora Maria Beatriz Vieira da Silva Gubert, publicado em 22 de março de 2024, manteve os termos da sentença, com destaque para o seguinte trecho:

> No que se refere aos *prints* de WhatsApp carreados, compartilho do entendimento do Magistrado de origem, notadamente quanto ao modo de produção inviabilizar a fidedignidade, autenticidade e integridade da prova, para fim de efetiva comprovação do alegado.
> Isto porque os *prints* de WhatsApp foram devidamente impugnados pela ré, de forma que cabia à autora exportar inteiramente as mensagens colacionadas ou certificar a sua autenticidade através da plataforma *Verifact*, por exemplo (Brasil, 2024m).

Caso parecido aconteceu no processo n. 1000786-26.2019.8.26.0660, em que a Quinta Câmara de Direito Privado confirmou sentença da vara cível da comarca de Viradouro/SP, em que o juízo *a quo* destacou a tecnologia *blockchain* como hábil a preservar a prova:

> Com efeito, as mensagens publicadas na rede social vieram comprovadas tão somente por capturas de tela. Certamente, haveria maior segurança na prova se os autos viessem instruídos com ata notarial ou por meio de prova preservada pela tecnologia *blockchain* (São Paulo, 2021).

Ainda que indiretamente, o entendimento pela possibilidade de uso da tecnologia *blockchain* para a preservação da prova digital vem ganhando espaço.

Thamay e Tamer (2022, RB-2.19), ao explicarem o funcionamento da tecnologia para a preservação do conteúdo fático, destacam duas funcionalidades principais. Na primeira, salva-se um documento eletrônico na rede *blockchain* - normalmente um PDF –, ou se produz o documento na própria rede. Assim, “a rede funciona como qualquer dispositivo eletrônico de salvamento ou armazenamento, a diferença é que a informação é inserida em uma rede descentralizada e o conteúdo será, em regra, imutável”.

Na segunda, a rede *blockchain* permite a verificação da existência de determinado conteúdo disponível na internet a partir da criação de uma cópia idêntica de seu conteúdo, permitindo a sua verificação, a qualquer momento. O interessado fornece o endereço da página (Uniform Resource Locator - URL) e a *blockchain* verifica se ela está lá. Se estiver, a *blockchain* faz uma cópia exata do conteúdo e a guarda em sua rede. Isso prova que a página estava *on-line* no momento da verificação (2022, RB-2.19).

Ponderam, entretanto, sobre a capacidade de garantir a autenticidade e integridade de um documento na rede de *blockchain.*

Isso porque, quando os documentos são feitos na própria rede, a exemplo dos *smartcontracts*, “eles são criados, elaborados e executados integralmente na rede, os códigos *hash* produzidos e extraídos a cada nova alteração ou movimentação contratual automática asseguram sua autenticidade e integridade, bastando como prova do fato contratual em si considerado” (Thamay; Tamer, 2022, RB-2.19).

Entretanto, em relação aos documentos que são digitalizados ou produzidos eletronicamente, “a rede *blockchai*n, mediante código *hash* extraído no momento do salvamento, assegura tão somente a autenticidade e integridade da versão eletrônica do documento salvo”. Não há garantia de que o documento não tenha sofrido manipulação ou adulteração, até o momento de sua inserção na rede, de modo que a sua autenticidade e integridade devem ser verificadas normalmente em relação ao próprio documento (Thamay; Tamer, 2022, RB-2.19).

Arrematam:

> Na visualização de um passo a passo da cadeia de custódia da prova, o *blockchain* apenas assegura a autenticidade e integridade do documento a partir do momento em que ele é inserido em sua rede, antes disso tal tarefa não lhe compete. No caso do documento eletrônico, terá presunção de autenticidade e integridade mediante a assinatura eletrônica nele aposta. Ou, sem a presunção, se essa ficar demonstrada de outra forma. No caso do documento digitalizado, por sua vez, a autenticidade e a integridade são verificadas quanto à formatação do documento físico original e no processo de digitalização, mediante a comparação do documento digitalizado com sua via física original (Thamay; Tamer, 2022, RB-2.19).

Souza, Munhoz e Carvalho (2022, p. 66) alertam que a tecnologia pode “congelar no tempo” a informação, mas, se utilizada isoladamente, não pode garantir a autenticidade e origem do documento, pois que a inserção de qualquer tipo de informação em sua rede é permitida, seja verdadeira ou falsa. Para tanto, atentam para o fato de que essa tecnologia deve ser utilizada em um processo maior, que gere informações confiáveis quanto ao conteúdo apresentado antecipadamente, para, assim, evitar posteriores manipulações de seu resultado.

Em suma, a rede *blockchain* desempenha um importante papel na preservação de provas digitais, mas seu manuseio deve ser cuidadoso, com a sugestão de que, se necessário, seja empregado o uso de outras tecnologias que permitam a garantia não só da integridade do documento, mas, também, de sua autenticidade e origem.

5.9 Prova digital e privacidade

Machado (2022, p. 166-167) propõe a reflexão de que o instituto da privacidade vem passando por uma grande mutação jurídica que abrange seu próprio sentido e alcance, o que decorre do avanço das tecnologias da informação

Recorda, ainda, o voto do Ministro Gilmar Mendes na Medida Cautelar na Ação Direta de Inconstitucionalidade (ADI) n. 6.389 - Distrito Federal, de relatoria da Ministra Rosa Weber, julgado em maio de 2020, para quem há uma reconceptualização do direito à privacidade, coincidente com o desenvolvimento jurisprudencial do conceito de autodeterminação informacional, termo construído pelo Tribunal Constitucional Alemão, que consiste no poder de o indivíduo decidir sobre:

a) “a divulgação e o uso de seus dados pessoais”; e
b) quando e dentro de quais limites os fatos da sua vida pessoal podem ser revelados e, ainda, de ter conhecimento sobre quem sabe e o que sabe sobre si, quando e em que ocasião” (Machado, 2022, p. 166).

Depois de análises detalhadas sobre os direitos individuais, em relação aos desafios da era da informática, chegamos à conclusão de que os indivíduos têm o direito de determinar como seus dados pessoais são utilizados e compartilhados. Qualquer restrição a esse direito seria aceitável somente em casos de interesse público significativo, ou mediante uma norma clara que respeitasse o princípio da proporcionalidade (Bessa, 2020).

A LGPD consagra a privacidade como fundamento da proteção de dados. Aliás, é notável que a palavra privacidade aparece 28 vezes no texto legal. A primeira vez já no art. 1º, de que se depreende:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, [2022d]).

Bessa (2020) ainda argumenta que

> a expressão ‘o direito à autodeterminação informativa’ é um dos fundamentos expressos da LGPD (artigo 2º), ao lado da ‘privacidade’ e da ‘intimidade’. É fato que o legislador, inseguro com a ausência de amadurecimento e rigor técnico, preferiu ‘pecar por excesso’, ao utilizar vários termos que, em última análise, conduzem à preocupação com o livre desenvolvimento da personalidade (Bessa, 2020).

É imprescindível, ainda, mencionar a Emenda Constitucional (EC) n. 115/2022, promulgada em 10 de fevereiro de 2022 (Brasil, 2022a), que introduziu o inciso LXXIX ao art. 5º da CRFB/1988, estabelecendo que o direito à proteção dos dados pessoais, inclusive nos meios digitais, será assegurado nos termos da lei.

Então, diante da rede de proteção que foi construída em torno do direito à proteção dos dados pessoais e demais direitos que compõem a esfera individual do indivíduo, resta perquirir se essa proteção é absoluta ou se esses dados podem ser utilizados na esfera judicial (Machado, 2022, p. 167).

A primeira noção que surge é a de que os direitos fundamentais não são absolutos. Em decisão paradigmática, no Mandado de Segurança (MS) n. 23.452, de relatoria do Ministro Celso de Melo publicada em 12 de maio de 2000, foi consignado que direitos e garantias fundamentais não possuem caráter absoluto,

> mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição (Brasil, 2000).

Tão reveladora quanto a posição do Ministro Celso de Melo é a do Ministro Alexandre de Morais, que, em seu voto no Referendo na Medida Cautelar na ADI n. 6.387 - Distrito Federal, em decisão de 2020, destacou:

> Em outras palavras, os direitos e garantias fundamentais, especificamente intimidade, vida privada e sigilo de dados, não são absolutos, não são ilimitados, como também bem destacou a eminente Ministra Rosa Weber em seu voto. Encontram, obviamente, limites nos demais direitos consagrados pela nossa Carta Magna. É o denominado, pela doutrina, princípio da relatividade ou da convivência das liberdades públicas (Brasil, 2020e).

No que respeita ao princípio da privacidade, a jurisprudência tem corroborado o enunciado constitucional que preconiza, em seu art. 5º, XII, exceções à inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas.

A Ministra Rosa Weber, em seu voto na ADI n. 4.924 (Brasil, 2022c) - Distrito Federal, de relatoria do Ministro Gilmar Mendes, cujo acórdão foi publicado em 29 de

março de 2022, compartilha esse entendimento, quando assevera que, em casos anteriores, o STF já houvera esclarecido que a proteção mencionada no art. 5º, XII, da CRFB/1988, se refere ao sigilo das comunicações de dados, não aos próprios dados em si. Ressaltou, ainda, que, como acontece com qualquer outro direito fundamental, o direito à privacidade não é absoluto e pode ser flexibilizado para garantir outros direitos constitucionais, conforme a jurisprudência estabelecida pela Corte Constitucional.

O entendimento jurisprudencial abunda e, via de regra, vai ao encontro da CRFB/1988, tornando-se redundante a apresentação de várias decisões similares.

O fato é que sempre deve haver a ponderação entre valores da mesma estatura constitucional quando em conflito, razão pela qual não podem ser tomados por absolutos.

Machado (2022, p. 168) lembra que, na fase de execução, o emprego de ferramentas eletrônicas de pesquisa patrimonial de devedores é uma realidade que ocorre desde 2001, com a criação do *Bacen Jud*, que posteriormente foi sucedido pelo Sistema de Busca de Ativos do Poder Judiciário (SISBAJUD), em 2020, ambos sistemas de comunicação eletrônica entre o Poder Judiciário e as instituições financeiras. Na esteira desse sistema, foram introduzidos outros sistemas de busca patrimonial, como o Sistema de Restrições Judiciais sobre Veículos Automotores (RENAJUD) e o Sistema de Informações ao Judiciário (INFOJUD).

O uso desses sistemas não gerou grandes discussões quanto à eventual violação do direito de privacidade, talvez, por serem de uso exclusivo do Poder Judiciário. Os debates se acentuam no emprego de tecnologias nas fases de conhecimento, intensificação da coleta de provas nas fontes abertas, como as redes sociais, sites e plataformas digitais (Machado, 2022, p. 169).

No Direito do Trabalho, o âmago da discussão fica bem evidente. É possível pensar no uso de geolocalização para identificar o local em que determinado empregado estava em seu horário de trabalho, ou postagens nas redes sociais particulares criticando a empresa.

Na sequência, na subseção pertinente à geolocalização, a discussão sobre conflito de princípios será melhor abordada, especialmente a partir de estudo da jurisprudência do Tribunal Superior do Trabalho.

Reiteramos que não há direito fundamental absoluto e, especialmente no caso da privacidade, a própria CRFB/1988 a relativiza. Caso assim não fosse, o processo constitucional de nada serviria, pois, a impossibilidade de produzir prova ilidiria os princípios constitucionais mais basilares, como o contraditório, a ampla defesa e o devido processo constitucional.

Ademais, vários dispositivos permitem ao juiz requisitar registros de conexão ou de acesso a aplicações da internet, como o art. 22 do MCI (Machado, 2022, p. 170).

De tudo isso, concluímos que, embora o legislador esteja cada vez mais ampliando a proteção aos dados pessoais, especialmente os digitais, como evidenciado pela introdução do inciso LXXIX ao art. 5º da CRFB/1988 e pela jurisprudência nacional, conforme destacado no voto do Ministro Gilmar Mendes na Medida Cautelar na ADI n. 6.389 (Brasil, 2020d), que importa da Alemanha o princípio da autodeterminação informacional, não se pode atribuir primazia absoluta ao direito à privacidade e intimidade em detrimento dos demais princípios fundamentais. Isso poderia resultar em uma violação ao conjunto normativo, tanto sob o aspecto sistemático, quanto no que tange às normas específicas que permitem a busca de provas eletrônicas.

Por fim, tratamos dessa questão novamente, quando da análise de julgamentos do STF, mormente a ADPF n. 403 e a ADI n. 5.527.

5.10 Ônus da prova digital e inversão

Gemignani (2022, p. 115-116) propõe dois critérios para tratar da inversão do ônus da prova, um que afere a aptidão para a produção de provas relacionado à inversão do *onus probandi*, e outro que se orienta pela distribuição dinâmica do ônus da prova. Pelo primeiro critério, a atribuição do encargo probatório é verificada no caso concreto, quando se averigua que sua produção é demasiadamente dificultosa - ou mesmo impossível - para uma das partes e fácil para a outra. Daí se dizer de um critério que afere a aptidão para a produção de provas.

Já o segundo critério, orientado pela distribuição dinâmica do ônus da prova, permite alcançar a conclusão de que a atribuição do encargo probatório não pode ser regida por critério estático. O ônus da prova deve ser imputado àquele que possui

melhores condições para tanto, sejam fáticas, técnicas, econômicas ou quaisquer outras, não chegando ao extremo de que é impossível sua produção por uma das partes.

Feito esse introito, Gemignani (2022, p. 117) passa a pensar o ônus da prova a partir da perspectiva das provas digitais.

Destaca que quando, em um ou outro caso (inversão ou distribuição dinâmica do ônus probatório), estiver envolvido o tratamento de dados pessoais, é imprescindível levar em conta a finalidade, adequação, necessidade, qualidade dos dados, transparência e segurança, conforme a Lei Geral de Proteção de Dados.

O art. 6º da referida Lei define esses institutos como princípios, nos seguintes termos:

a) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
b) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
c) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos, em relação às finalidades do tratamento de dados;
d) qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
e) transparência: garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
f) segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Brasil, [2024d]).

Com isso, Gemignani (2022) destaca que são especialmente sensíveis os princípios da finalidade, adequação, necessidade e segurança, por balizarem a

conduta judicial. Postula uma elegante concatenação de ideias para justificar a especial importância desses institutos:

> [...] o tratamento de dados deve ficar limitado ao mínimo necessário e adequado para atingir a finalidade do ato, com a utilização de medidas aptas a proteger esses dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Gemignani, 2022, p. 118).

A reverência que a autora confere aos princípios que regem o tratamento de dados pessoais tem o condão de harmonizar a utilização de provas com os direitos fundamentais, especialmente o da privacidade.

Exsurge, ainda, a seguinte questão: a distribuição do ônus da prova digital pode se dar no julgamento - regra de julgamento – ou deve ser oportunizada à parte manifestação, de tal modo que o *onus probandi* seja regra de procedimento?

De certa maneira, ao se adotar as lentes do processo constitucional, cotejando-se a CRFB/1988 com os dispositivos processuais em vigência, a resposta surge de forma natural.

Como abordado anteriormente, Nunes, Bahia e Pedron (2021) destacam que um modelo democrático de processo visa a ampliar a participação do cidadão no provimento jurisdicional, e isso é feito estimulando a comparticipação. Nesse modelo cooperativo de processo, as normas de distribuição do ônus da prova devem ser tidas como regras de procedimento, sendo imprescindível comunicar às partes que determinado fato não está devidamente aclarado, oportunizando à parte se desincumbir de seu encargo probatório.

Alexandre Freitas Câmara (2006, p. 233) possui idêntico raciocínio, quando afirma, de forma peremptória, que a redistribuição do ônus da prova não pode se dar em sentença, o que contrariaria os princípios que regem o processo constitucional, especialmente o contraditório, acarretando decisão surpresa.

Diante da sistemática processual vigente, não é possível alcançar outra conclusão senão a de que a distribuição do ônus da prova digital constitui regra de procedimento, assim como nas provas típicas.

Gemignani (2022), em linha com o quanto exposto, assevera:

> O contraditório e a ampla defesa devem atuar para proteger os direitos fundamentais postos pelo art. 5º da Constituição Federal em sua

> integralidade, como uma unidade de valor, bússola de navegação neste momento de ressignificação de conceitos e transição para a construção de um novo modelo probatório, por constituírem pilares de sustentação também do devido processo legal digital, assim norteando a fixação de critérios para a imputação do ônus, quanto à produção de provas digitais (Gemignani, 2022, p. 120).

Assim, a regra é a de que quem pretende provar seu direito apresenta a prova, nos termos do art. 373, *caput*, do CPC, mas discussões relevantes sobre a distribuição do ônus da prova surgem de análise mais detida.

5.11 Metadados

São dados adicionais sobre determinado conteúdo, ou operação digital, que podem ajudar no processamento da informação pelos softwares, além de identificar recursos e manter históricos. No mais das vezes, estão ocultos do usuário, sendo de pouca utilidade na utilização cotidiana da aplicação, ainda que tenham diversas funcionalidades relevantes para seu funcionamento. “Cada situação no meio digital pode eventualmente coletar e gravar determinados metadados com base no seu objetivo”, sendo importantes no que respeita ao direito probatório, na medida em que podem revelar detalhes cruciais sobre determinadas provas, permitindo um maior grau de confiança sobre a autenticidade e integridade da prova (Souza; Munhoz; Carvalho 2023, p. 47).

O Decreto Federal n. 10.278, de 18 de março de 2020, sucintamente os descreve como “dados estruturados que permitem classificar, descrever e gerenciar documentos” (Brasil, 2020a).

O termo se refere a uma vasta gama de diferentes tipos de dados, que o Tribunal Distrital dos Estados Unidos para o distrito de Maryland agrupou em três categorias em seu protocolo sugerido, para a descoberta de informações armazenadas eletronicamente:

a) metadados do sistema: dados automaticamente gerados a partir do computador e incluem “autor, data e hora de criação, e a data em que documento foi modificado”,
b) metadados substantivos: dados que refletem alterações em um documento feitas por um usuário, por exemplo, mudanças rastreadas, e

c) metadados incorporados: dados inseridos em um documento ou arquivo, mas normalmente não visível, por exemplo, fórmulas em células em uma planilha do Excel (Simpson; Williams, 2017).

Os metadados são anexados a todos os arquivos eletrônicos e podem ser uma excelente fonte de informação, fornecendo detalhes sobre quem, o quê, por que, quando, onde e como um arquivo foi criado ou modificado. Diferentes formatos de arquivo possuem diferentes tipos de metadados. Algumas informações de metadados são facilmente visíveis para o usuário, enquanto outras requerem métodos avançados para serem acessadas, como os programas de recuperação de metadados. Além disso, alguns metadados são incorporados ou criptografados (Simpsons; Williams, 2017.

Exemplos de metadados são o número IP, o GPS (Global Positioning System) (localização), a data e hora de criação de um arquivo e o remetente e destinatário de um IP (Datacertify, 2023).

Capanema (2024) traz dois exemplos interessantes para ilustrar a importância dos metadados: um é o de John McAfee, fundador do antivírus que leva seu nome.

McAfee “ficou rico, ficou maluco e foi morar na América Central”, onde resolveu virar traficante. A revista Vice enviou dois jornalistas para desvendar seu paradeiro, os quais o localizaram e enviaram uma foto para o *site* da revista. Ocorre que o GPS estava ativo, de modo que a foto chegou com localização, o que levou John McAfee a fugir novamente.

O segundo exemplo é o *serial killer* americano BTK, que atuou dos anos 1970 aos anos 1990, ficando desaparecido por muito tempo. Um dia resolveu enviar um disquete para um jornal que estava publicando uma matéria sobre ele, com um arquivo de *Word*, o qual tinha metadados, com um nome e endereço. Ocorre que eram seu nome e o endereço de seu trabalho, o que levou à sua prisão (Datacertify, 2023).

Os metadados também são de grande relevância para a análise de imagens fotográficas digitais. As fotografias digitais, além da própria imagem, contêm dados adicionais conhecidos como Exchangeable Image File Format (*exif*), um padrão usado para armazenar metadados em arquivos de imagens ou vídeos capturados por câmeras digitais, smartphones e outros dispositivos de captura. Esses metadados podem fornecer informações sobre o tipo de aparelho utilizado, o local, a data e o

horário em que a foto foi tirada, entre outras funções.

Bazzel (2021, p. 443) traz relevantes *insights* sobre os metadados em imagens, quando explica que cada fotografia digital capturada com uma câmera digital possui metadados conhecidos como dados *exif*, uma camada de código que fornece informações sobre a foto e a câmera. Todas as câmeras digitais gravam esses dados em cada imagem, mas a quantidade e o tipo de dados podem variar. Esses dados, incorporados em cada foto "por trás das cenas", não é visível ao visualizarmos a imagem capturada. Para fazermos isto é necessário um leitor de *exif*, como o Jeffrey's *Exif Viewer* **.**

Os dados *exif* de uma fotografia digital podem incluir uma miniatura da imagem original. Câmeras digitais geram essa versão menor e a armazenam nos dados *exif,* adicionando pouco ao tamanho total do arquivo. Quando a imagem é cortada, essa miniatura pode ou não ser substituída. Programas como *Photoshop* ou *Microsoft Photo Editor* geralmente substituem a miniatura, mantendo ambas as versões idênticas. No entanto, outros programas e algumas ferramentas de corte *on-line* não fazem essa substituição, o que resulta na presença da imagem original não cortada nos dados *exif* da foto recortada.

Por exemplo, ao examinar uma foto recortada com o visualizador *exif* do Jeffrey's, é possível ver a versão original não cortada nos dados *exif*, permitindo visualizar a imagem como era antes do corte. Essa técnica tem sido usada pela polícia para identificar produtores de pornografia infantil, que recortam imagens ilegais para evitar a identificação. Quando a polícia encontra essas fotos, a versão original não cortada pode ser suficiente para identificar e processar o criminoso (Bazzel, 2021, p. 444).

Bazzell (2021, p. 447) indica o *site* fotoforensics.com para descobrir imagens manipuladas. O FotoForensics permite que alguém carregue uma imagem digital. Após o *upload* bem-sucedido, ele exibirá a imagem normal. Abaixo desta imagem haverá uma imagem duplicada escurecida. Quaisquer áreas destacadas da imagem indicam uma possível manipulação. Embora este *site* não deva ser usado para declarar definitivamente o *status* da imagem, se manipulada ou não, os investigadores podem querer realizar uma análise apenas para fins de inteligência.

Muitas vezes, a obtenção de metadados ainda é difícil, vez que as empresas os apagam ou não os disponibilizam, alegando cumprimento da legislação, seja a

LGPD no Brasil ou a GDPR na Europa.

O Portal do *WhatsApp* informa que os metadados são utilizados para transmitir comunicações, operar os serviços, garantir a segurança e proteção dos serviços, além de prevenção, detecção, investigação e correção de incidentes de segurança, *spams*, vulnerabilidades, *malware* e usos ou acessos não autorizados, faturar e cumprir com obrigações legais, conforme a lei vigente.

Entretanto, também se pode ler no Portal que os metadados de mensagens são apagados ou anonimizados, quando deixam de ser necessários para a transmissão de dados, operar os serviços do comunicador, garantir a segurança e a proteção dos serviços, faturar ou cumprir as obrigações legais, de acordo com a lei aplicável (WhatsApp, 2024).

Outras mídias, como o *Instagram* e o *Facebook*, não disponibilizam metadados de fotos, também sob a alegação de privacidade do usuário, o que não implica sua inexistência, entretanto. Uma possibilidade é demandar no Judiciário uma tutela antecipada ou produção antecipada de prova, para requisitar ao provedor de aplicação os metadados, inclusive o IP do autor da postagem que se pretende utilizar como prova (Lima, 2022, p. 267-268).

5.12 Fontes das provas digitais

No contexto do atual universo digital em que a sociedade está imersa, a comunicação ocorre por meio de diversas plataformas. Assim, é essencial examinar os principais meios por onde essas interações acontecem, bem como a jurisprudência em torno do debate sobre a validade dos documentos produzidos a partir desses ambientes.

5.12.1 O e-mail

A história do *e-mail* está intrinsecamente associada à da internet, destacando-se como uma das principais formas de comunicação, persistindo ainda hoje, mais de 50 anos após ser dotado da configuração atual, concebida pelo engenheiro Ray Tomlinson, a quem é atribuído o envio do primeiro e-mail, em 1971. (Ray [...], 2016)

Para que um e-mail seja enviado e chegue ao destinatário, é necessário que alguns protocolos trabalhem juntos para garantir a entrega correta da mensagem.

Ao enviar um *e-mail,* o Simple Mail Transfer Protocol (SMTP) é responsável por encaminhar a mensagem do computador de quem a envia para o servidor de saída de *e-mails* do seu provedor. Este protocolo cuida de todos os dados necessários para a transmissão da mensagem ao servidor de saída.

No lado do destinatário, os protocolos Post Office Protocol (POP) ou *Internet* Messaging Access Protocol (IMAP) são responsáveis por receber a mensagem no servidor para que o usuário final possa acessá-la. POP e IMAP são protocolos de recebimento que operam em portas diferentes e podem ser configurados, conforme as necessidades do usuário. Enquanto o POP, ou sua versão mais recente o POP3, baixa o e-mail para o computador do usuário, e pode excluir a mensagem do servidor, e dependendo da configuração, o IMAP mantém a mensagem no servidor, permitindo a sincronização dos *e-mails* em diferentes dispositivos (Serra, 2024).

Souza, Munhoz e Carvalho (2023, p. 133) explicam que, quando um e-mail é enviado, os servidores trocam informações e mantêm registro sobre essa interação. “O caminho tomado pelo e-mail, da sua origem até seu destino, fica gravado em seu cabeçalho técnico, permitindo rastrear sua existência a partir dos registros mantidos nos servidores envolvidos”

Capanema (2024, p. 271-272) esclarece que a natureza do cabeçalho é de metadados “que informam, por meio de campos, o remetente e o destinatário da mensagem, a data do envio, o trajeto percorrido, entre outros, ” lecionando que, para a produção de prova de *e-mail* em juízo, este deverá ser levado em toda a sua estrutura, com cabeçalho e corpo, sob o risco de ser avaliado como mero indício.

O STJ, em virtude do julgamento do Recurso Especial (REsp) n. 1.381.603/MS (Brasil, 2016b), de relatoria do Ministro Luis Felipe Salomão, já decidiu que o correio eletrônico pode servir de base para uma ação monitória, desde que o juiz esteja convencido da verossimilhança das alegações e da autenticidade das declarações. Isso permite ao réu contestá-las através do processo adequado. A validade do e-mail deve ser avaliada no caso específico, juntamente com os demais elementos de prova trazidos pela parte interessada.

Thamay e Tamer (2022) destacam, ainda, que o STJ já decidiu que a notificação por *e-mail* é juridicamente válida para o exercício do direito de preferência

(STJ, REsp nº 1.545.965/RJ, 3ª Turma, Relator Ministro Ricardo Villas Bôas Cueva, julgado em 22.09.2015,) e que um e-mail pode ser usado para iniciar, de forma anônima, um procedimento investigatório (STJ, HC nº 191.797/PA, 5ª Turma, Relator Ministro Napoleão Nunes Mais Filho, julgado em 21.06.2011). Também já foi decidido que conversas por e-mail podem confirmar o aperfeiçoamento de um ajuste negocial (TJSP, Apel. nº 1004322-89.2018.8.26.0100, 38ª Câmara de Direito Privado, Relator Desembargador Mario de Oliveira, julgado em 23.10.2019) (Tamay; Thamer, 2022, RB-2.2).

Stopanovski (2015) argumenta que, para ser válido como prova judicial, o e-mail deve obedecer a alguns critérios: autenticidade, que exige a possibilidade de validação da chave geradora com base em uma chave pública; confidencialidade, assegurada pelo emissor possuir uma chave pessoal registrada em uma cadeia de autenticação; integridade, garantindo que a alteração de um único *bit* na mensagem resulte em incompatibilidade com as chaves; e irretratabilidade, impedindo o emissor de negar que aplicou a assinatura à mensagem.

Na já referida decisão no recurso em HC n. 186.138/SP (Brasil, 2024f), o STJ decidiu exatamente nesse sentido, dando provimento a HC, dada a ausência de confiabilidade e garantia de integridade da cópia do e-mail carreado aos autos, tendo sido registrado que é responsabilidade do Estado demonstrar que os elementos e informações recolhidos são exatamente aqueles utilizados na ação penal. No caso, nem os provedores, nem a autoridade policial, nem o Ministério Público trouxeram provas que tivessem garantido a integridade das mensagens de e-mail apresentadas.

5.12.2 A geolocalização

A geolocalização consiste no uso de dados de posição geográfica para determinar a existência de dado dispositivo ou indivíduo em alguma localidade.

Existem várias maneiras de obter a geolocalização, incluindo sinais de internet, Global Positioning System (GPS), Assisted Global Positioning System (AGPS), Estação Rádio Base (ERB), radiofrequência e outros sinais de posicionamento. A geolocalização é frequentemente encontrada em dispositivos móveis, como *smartphones, laptops e tablets*, e é fundamental para aplicativos como o *Google Maps* e o *Waze*. Devido ao amplo uso dessa funcionalidade, ela está sendo cada vez mais

utilizada como prova em processos judiciais (Azevedo; Munhoz; Carvalho, 2023, p. 149).

A utilização da geolocalização como prova está intimamente relacionada à falibilidade da prova testemunhal.

Fortes (2022), refletindo sobre seus anos de Magistratura, compartilha a perspectiva de que o que temos no processo são narrativas, e não fatos. Essas narrativas, por sua vez, são tingidas por interesses, preconceitos, preceitos, valorações e influências. São impregnadas de emoções e imprecisões. Mesmo que não tenham o intuito deliberado de favorecer ou prejudicar alguém, por vezes acabam se distanciando da verdade (Fortes, 2022, p. 236).

As testemunhas muitas vezes se lembram de eventos de maneira imprecisa ou distorcida, pois podem deixar de mencionar detalhes, mentir sobre certos aspectos, mudar suas narrativas ao longo do tempo, apresentar informações conflitantes em diversos depoimentos, exagerar ou agir por motivos pessoais. Devido a essas limitações inerentes ao testemunho e com o avanço da tecnologia, advogados estão cada vez mais recorrendo a dados de geolocalização.

A coleta de dados pode ser efetuada por meio de consulta de servidores vinculados ao IP, por triangulações de captações de satélites, *Wi-fi* ou radiofrequência. Seu acesso pode ser feito pelo próprio usuário do dispositivo eletrônico, ou por meio de ordem judicial ao administrador da rede ou aplicativo (Fortes, 2022, p. 241).

A geolocalização pode ser utilizada como prova na área cível, criminal ou trabalhista.

Exemplo emblemático de seu uso ocorreu por ventura das investigações do homicídio da então vereadora do Município do Rio de Janeiro, Marielle Franco, e seu motorista, Anderson Gomes.

Após instauração do inquérito policial, o Ministério Público do Estado do Rio de Janeiro (MPRJ) requereu ao Juízo da 4ª Vara Criminal da Comarca do Rio de Janeiro, a quebra de sigilo telemático, determinando que o *Google* identificasse os IPs ou *Device IDs* de usuários que tivessem utilizado o *Google Maps* e/ou plataformas *Waze* no período compreendido entre 10/3/2018 e 14/3/2018, para realizar consulta de alguns endereços em que a vereadora esteve, o que foi deferido (Brasil, 2020b).

Alegando que o pedido não encontrava amparo no ordenamento jurídico brasileiro, que não admite quebras de sigilo e interceptações genéricas desprovidas

de individualização razoável dos investigados, a empresa recorreu ao STJ, que consignou que o juízo agiu corretamente, nos seguintes termos:

> 1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. No Brasil, a Constituição Federal, no art. 5º, X, estabelece que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital.
>
> 2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública (Brasil, 2020b).

Após interposição do Recurso Extraordinário (RE) n. 1.301.250/RJ (Brasil, 2021d), a Ministra Relatora Rosa Weber votou pelo provimento do apelo do *Google*, destacando que inexiste dispositivo legal com suficiente densidade normativa para legitimar emprego de medida tão ampla. Atualmente, o processo encontra-se sobrestado, após pedido de vista do Ministro Alexandre de Moraes.

O STJ tem entendido em decisões recentes que a quebra de sigilo de dados de geolocalização é adequada, necessária e proporcional, em casos nos quais não há outra maneira de elucidar o crime (Recurso em Mandado de Segurança - RMS 68.487/PE) (Brasil, 2023f), "sendo considerada menos invasiva que a interceptação telefônica, modalidade que dá acesso ao fluxo de comunicações de dados e o conhecimento integral da conversa".

Essa posição não é unânime, entretanto.

A Quinta Turma do STJ recentemente decidiu não ser possível a quebra de sigilo de dados informáticos estáticos (registros de geolocalização), nos casos em que haja a possibilidade de violação da intimidade e da vida privada de pessoas não

diretamente relacionadas à investigação criminal (Brasil, 2021b).

A Sexta Turma já esposou entendimento parecido: dados que refletem informações íntimas (como o acesso irrestrito a fotos e conteúdo de conversas), quando a ordem de quebra de sigilo se voltar a universo indeterminado de pessoas, devem ser afastados desta possibilidade (Brasil, 2021a).

Na seara trabalhista, o TRT da 3ª Região já decidiu nesse sentido. Em julgamento do MS n. 0012565-21.2022.5.03.0000, de Relatoria da Desembargadora Paula Oliveira Cantelli publicado em 24 de março de 2023 (Brasil, 2023i), a 1ª Seção de Dissídios Individuais ordenou a suspensão da decisão que determinou a realização da prova digital (geolocalização) no telefone celular do autor, sob a alegação de que tal autorização deve levar em conta os direitos à privacidade e intimidade, de modo que os meios ordinários de prova devem ser esgotados, revelando-se inoportuna a realização da prova digital, que deve ser adotada em caráter excepcional.

Entretanto, o mesmo TRT-3 já decidiu que a tecnologia atual permite saber a geolocalização das pessoas em tempo real, tornando-a prova digital crucial, em casos em que se discute a prestação de horas extras pelo reclamante. Foi ressaltado, ainda, que a utilização da prova digital visa, principalmente, a dar efetividade ao princípio lógico do terceiro excluído, no qual para qualquer proposição existem duas possibilidades: ou ela é verdadeira ou a sua negação é verdadeira. Portanto, se há duas proposições contraditórias, uma delas é verdadeira e a outra é falsa. Assim, a prova digital neste contexto busca verificar a veracidade das alegações das partes em relação à prestação de horas extras, ou seja, por meio da prova digital, realiza-se a "prova dos 9", eliminando qualquer dúvida sobre a matéria controvertida (Brasil, 2024l).

É possível observar que a prova de geolocalização envolve não apenas a necessidade de que seja íntegra e autêntica, mas o sopesamento de valores constitucionais, como privacidade e intimidade.

Fortes (2022) entende ser plenamente possível a utilização da prova de geolocalização, afirmando que a alegada invasão de privacidade da parte ou testemunha não justificaria o indeferimento da prova. Isso, porque a parte, ao ingressar em juízo, se submete a todas as provas admitidas em direito que podem ser produzidas pela parte contrária, a pedido desta ou por determinação do juízo. A testemunha, por sua vez, ao depor, se compromete a dizer a verdade, sob pena de

incorrer no crime de falso testemunho, estando, assim, sujeita à verificação da veracidade de seu depoimento por todos os meios de prova admitidos em direito. Se o relatório de geolocalização demandar sigilo ou segredo de justiça, excepcionando o princípio da publicidade, caberá ao julgador esse juízo (Fortes, 2022, p. 242).

Aliás, consta o permissivo para o emprego da prova de geolocalização da Lei Geral de Proteção de Dados:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral [...]
> [...]
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral [...] (Brasil, [2022d]).

Silva (2022), Juiz Titular da Vara de Trabalho de Teófilo Otoni/MG, traz interessante ponto de vista, em capítulo de livro intitulado *Do panoptismo ao pós-panoptismo: controle da geolocalização dos trabalhadores pelo empregado*. Postula o autor que é fundamental tratar da prova de geolocalização no processo trabalhista, pois que suscita muitas discussões acerca do confronto de direitos como a intimidade, a privacidade, o poder empregatício, o devido processo constitucional e a liberdade probatória.

Assim, introduz seu texto com a noção de que o poder empregatício decorre da lei e do contrato de trabalho, mas que esse poder não é absoluto, encontrando limites na CRFB/1988, leis, normas coletivas e o contrato, por exemplo.

Passa, então, a desenvolver uma reflexão sobre o exercício do poder fiscalizatório do empregador, considerando o uso de novas tecnologias, especialmente a geolocalização, confrontando-a com direitos fundamentais, especialmente o à privacidade.

Evocando Teresa Coelho Alexandra Moreira, Silva (2022) faz referência ao denominado “trabalhador transparente” ou “trabalhador de vidro”, na medida em que a possibilidade de captura de dados do empregado incide diretamente sobre aspectos de sua privacidade, a qual é merecedora de proteção, não só na CRFB/1988, mas em todo o ordenamento jurídico infraconstitucional.

Dada a dinâmica da relação entre empregado e empregador, essas práticas assumem especial relevância, uma vez que acentuam, ainda mais, o desequilíbrio de forças entre empregado e empregador.

Explica o supracitado autor que o direito à privacidade teve uma concepção negativa em seu nascedouro, na jurisprudência norte-americana, no sentido de que o direito estava resguardado, na medida em que a pessoa não era violada em sua intimidade/privacidade (Silva, 2022).

Com o avanço das tecnologias e o surgimento de novos riscos, os conceitos de proteção à intimidade da vida privada foram sendo ampliados. Agora, essa proteção é vista como parte integrante do direito da personalidade, aplicável a todos (*erga omnes*), e assumiu uma nova dimensão positiva, impondo um dever geral de respeito, o que implica a proibição de acessar informações privadas e divulgar dados pessoais.

Silva demonstra essa evolução, ao se socorrer da já referida decisão da Corte Constitucional da República Federal da Alemanha de 1983, em que é reconhecido o direito à autodeterminação informativa.

Assim, a privacidade acaba tomando essa nova feição, podendo ser considerada como o direito ao controle sobre as informações que dizem respeito aos cidadãos, bem como de determinar a construção de sua própria esfera particular, apontando para uma estrutura tridimensional da privacidade, formada por um aspecto decisional, outro informacional e um terceiro espacial, a) o primeiro relacionado às suas escolhas, gostos, projetos e características, b) o segundo preocupado com a coleta, processamento e disseminação de dados pessoais e c) o último relativo ao espaço físico, literalmente. A privacidade de um lar, de uma casa, de um espaço qualquer.

Ao fim, após apontar para a realidade da tecnologia em face do direito à privacidade, Silva (2022, p. 247-258) sugere ser imprescindível o estabelecimento de parâmetros éticos e limites para a utilização de ferramentas de geolocalização, especialmente em virtude da dimensão positiva de intimidade, que ganha contornos nítidos com a autodeterminação informativa.

A razão pela qual se faz mister trazer o escólio de Silva (2022) é que a discussão fulcral em torno das provas de geolocalização é o confronto entre privacidade e o direito à produção de provas.

Como já comentado, o STJ ainda se debruça sobre o tema, optando, por ora, pela solução no caso concreto.

Voltando à Justiça do Trabalho, em recente decisão, publicada em 14 de junho de 2024, na Subseção II Especializada em Dissídios Individuais, nos autos do processo n. Tribunal Superior do Trabalho (TST) / Recurso Ordinário Trabalhista (ROT) 23218-21.2023.5.04.0000 (Brasil, 2024n), de relatoria do Ministro Amaury Rodrigues Pinto Júnior, foi validada a geolocalização como prova digital de jornada de bancário.

Da leitura da ementa, podemos depreender especialmente que:

a) no sistema constitucional brasileiro, nenhum direito é absoluto. Em caso de conflito de princípios, deve-se realizar a concordância prática, ajustando proporcionalmente o alcance de cada um para atingir sua finalidade;
b) tribunais internacionais aceitam provas digitais com previsão legal, objetivos legítimos e necessários em uma sociedade democrática, atendendo aos critérios de validade;
c) A LGPD (Lei nº 13.709/2018, 7º, VI), a Lei de Acesso à Informação (Lei nº 12.527/2011, 21 c/c 31, § 4º) e o MCI (Lei nº 12.965/2014, 22) permitem acesso a dados pessoais e informações para a defesa de interesses em juízo;
d) provas digitais devem ser adequadas, necessárias e proporcionais, conforme o grau de afetação de um princípio à importância do outro;
e) o princípio da “primazia da realidade” favorece o conteúdo sobre a forma e pode ser usado por empregados e empregadores;
f) a admissibilidade de provas deve seguir um regime de inclusão, aumentando as chances de obter a verdade real, conforme a Corte Interamericana de Direitos Humanos;
g) a geolocalização do trabalhador só invade a intimidade, se ele não cooperar com a exposição da verdade em juízo (CPC, 6º e 77, I);
h) não há violação ao sigilo telemático e de comunicações na prova por geolocalização, pois a proteção constitucional se refere à comunicação dos dados, não aos dados em si;
i) a quebra do sigilo de dados por geolocalização é adequada, necessária e proporcional, segundo o STJ;

j) desenvolver sistemas e treinar magistrados em tecnologias essenciais é coerente com a promessa constitucional de uma sociedade justa (CF, 3º, I); e
k) a prova de geolocalização deve ser limitada aos períodos indicados na petição inicial e o processo mantido em segredo de justiça (Brasil, 2024n).

Entretanto, não podemos olvidar do voto vencido, do Ministro Aloysio Corrêa de Veiga, para quem a utilização de prova digital de geolocalização leva em conta de um lado, o direito à privacidade (art. 5º, X, da CRFB/1988) e, de outro, o direito à realização de prova, encarnada nos princípios da ampla defesa e do contraditório (art. 5º, LV, da CRFB/1988), e deve ser resolvida através da aplicação do preceito da proporcionalidade.

Arguiu que deveria ter havido esgotamento das provas típicas antes do uso da "prova excepcional", uma vez que esse tipo de prova deve se dar em caráter subsidiário, na medida em que violaria o direito à intimidade. Em suas palavras, "as vantagens que o ato promove - eventual busca da verdade processual quanto ao horário de labor - não superam as desvantagens que provoca, qual seja, a violação do direito à privacidade" (Brasil, 2024n).

A propósito, a Escola Judicial do TRT da 4ª Região, por meio dos Grupos de Estudos, Análise Normativa e Análise Jurisprudencial, elaborou o Enunciado n. 27, de que depreendemos que "a prova digital por geolocalização é legal, moralmente legítima (art. 369 do CPC) e está genericamente autorizada nos arts. 22 da Lei 12.695/2014 (MCI) e 7º da Lei 13.709/2019 (LGPD)" (Brasil, 2023j). Também se consignou que os requisitos de autenticidade, integridade e cadeia de custódia necessariamente devem ser obedecidos.

Além disso, é interessante notar o registro de que a prova por localização não é infalível, nem substitutiva da prova testemunhal. Assim, na decisão de sua produção, "cabe à (ao) juiz (íza) do trabalho efetuar avaliação de verossimilhança. Em sentença, será analisada conjuntamente com demais meios de prova produzidos" (Brasil, 2023j).

Em suma, a prova digital de geolocalização, evidentemente, possui os mesmos requisitos de validade que as outras provas digitais, exigência de autenticidade e integridade, além de envolver, de forma muito acentuada, o direito de privacidade, matéria ainda em discussão nos tribunais brasileiros.

5.12.3 Prova de mensagens instantâneas

5.12.3.1 Mensageiros instantâneos e privacidade

Mensagens instantâneas ou IM (instant messaging) são aplicativos que permitem a troca de informações em tempo real, como o próprio nome sugere, de textos, áudios, vídeos e toda a sorte de mídias.

Talvez, o mais conhecido mensageiro instantâneo seja o *WhatsApp*, razão pela qual o abordamos nesta subseção como paradigmático. Entretanto, o que vale para o *WhatsApp* também é cabível para as demais plataformas e os aplicativos, como o *Telegram, Facebook Messenger, Microsoft Teams, Slack, Discord, Skype, Signal, Viber e WeChat -,* como leciona Feliciano (2022, p. 212). É que os entendimentos judiciais em torno desses aplicativos ainda são raros no Brasil, mas, em relação ao *WhatsApp,* já é possível identificar julgados que permitem extrair entendimentos sobre a validade da prova coletada a partir desse dispositivo.

Conforme Castro e Vieira (2020, p. 47) explicam, o aplicativo de mensagem *WhatsApp* foi criado em 2009, por Brian Acton e Jan Koum, que se tratava de uma aplicação inicialmente concebida para a troca de mensagens via Short Message Service (SMS), posteriormente tendo evoluído para uma plataforma que permite a transmissão de arquivos de mídia, como fotografias, áudios, documentos e vídeos. Ensinam ainda, que os princípios que o regem são a privacidade e a segurança, por meio da criptografia de ponta a ponta.

No Portal do *WhatsApp* podemos ler a seguinte informação:

> A privacidade e a segurança estão no nosso DNA e, por isso, utilizamos a criptografia de ponta a ponta no WhatsApp. Com a criptografia de ponta a ponta, suas mensagens, fotos, vídeos, mensagens de voz, documentos, atualizações de status e chamadas ficam protegidas para não caírem em mãos erradas (Whatsapp, 2024).

Brian Acton, cofundador do *WhatsApp,* participou pessoalmente de uma audiência pública no STF, por ventura do processamento da Ação de Descumprimento de Preceito Fundamental n. 403, para defender a criptografia ponta a ponta do aplicativo, destacando que ela é fundamental para a segurança e acessibilidade dos seus usuários (Acton *apud* STF Criptografia [...], 2016). Ele enfatizou

que a criptografia torna as comunicações invioláveis, até mesmo para o *WhatsApp*, e que as chaves de segurança são exclusivas dos interlocutores e mudam a cada mensagem:

> Todas as mensagens enviadas pelo WhatsApp são garantidas com um cadeado e uma chave. Só o emissor e o receptor é que têm as chaves necessárias para destrancar e ler as mensagens de WhatsApp, e ninguém mais. Ninguém acessa, nem o WhatsApp, nem o Facebook [dono do aplicativo], nem os hackers (Acton *apud* STF Criptografia [...], 2016).

O tema é relevante, pois o objeto ADPF n. 403 é a suspensão de decisões judiciais que determinaram o bloqueio do serviço de mensagens *WhatsApp* no Brasil. A ADPF n. 403 foi ajuizada pelo Partido Popular Socialista (PPS) junto ao STF, alegando que essas decisões violam preceitos fundamentais, como a liberdade de comunicação, o direito à privacidade e à segurança das comunicações.

O partido argumentou que a suspensão do *WhatsApp* causava transtornos significativos aos milhões de usuários e às atividades econômicas que dependiam do serviço, além de não ser uma medida proporcional aos objetivos pretendidos pelas decisões judiciais de quebra de sigilo das comunicações (Brasil, 2016c).

Do voto do Ministro Relator, Edson Fachin, podemos extrair que, por entender que o risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional ou outras medidas que diminuam a proteção garantida por uma criptografia forte, ele considera que não há como obrigar que as aplicações de internet que oferecem criptografia de ponta a ponta quebrem o sigilo do conteúdo das comunicações, à luz do consenso científico atual sobre o assunto.

Assim sendo, o Ministro se mostrou convencido de que a sanção de suspensão só deve ocorrer, quando os aplicativos de internet tiverem violado os direitos de privacidade dos usuários.

Em síntese, no atual estágio de desenvolvimento da internet, a criptografia forte é, conforme as principais evidências científicas, o mecanismo por excelência para garantir o relevante direito à privacidade, sendo forçoso reconhecer que fragilizar a criptografia é enfraquecer o direito de todos a uma internet segura (Brasil, 2021c).

A Ministra Rosa Weber, Relatora da ADI n. 5.527, que também discutiu a possibilidade de decisões judiciais autorizarem o bloqueio de serviços de mensagens

pela internet, participa do entendimento de que tais bloqueios violam direitos fundamentais, como a liberdade de comunicação e expressão, a privacidade e a segurança das comunicações, além de serem desproporcionais em relação aos objetivos buscados.

Ela destacou que o bloqueio de um serviço de comunicação utilizado por milhões de pessoas no país causa transtornos significativos e desproporcionais, afetando tanto a vida pessoal quanto a econômica dos cidadãos. Rosa Weber enfatizou que existem outros meios menos drásticos para se obter as informações necessárias para investigações, sem prejudicar o direito coletivo à comunicação.

Assim, o voto da Ministra foi no sentido de preservar a continuidade do serviço do *WhatsApp*, reconhecendo a importância do aplicativo na vida cotidiana e na economia digital, ao mesmo tempo em que se devem buscar formas alternativas e proporcionais para atender às demandas judiciais de quebra de sigilo, quando necessário.

De seu voto se pode depreender que a tecnologia utilizada pelo mensageiro instantâneo concretiza a garantia de preservação do sigilo das comunicações, conforme o art. 5º, XII, da CRFB/1988. Um entendimento contrário implicaria submeter a regra, que é a proteção do sigilo das comunicações, à exceção, que é o acesso do Estado ao conteúdo da comunicação privada durante a persecução criminal (Brasil, 2020c).

Ambas as ações ainda estão em curso e é necessário aguardar para que seja definido o caminho que será adotado, mas os primeiros votos sugerem, no caso concreto, a prevalência da segurança, privacidade, intimidade e proporcionalidade, quando de determinações judiciais para obtenção de dados criptografados em mensageiros instantâneos.

5.13.3.2 A polêmica envolvendo o print screen

Importante questão atinente à temática probatória diz respeito aos dados estanques, ou seja, aqueles armazenados em determinado dispositivo e que podem ser acessados por qualquer usuário. É o caso de a própria parte levar aos autos a prova digital, como um *print* de tela coletado do mensageiro, a partir da troca de dados com outro usuário.

Antigamente, o sistema operacional dos computadores era o DOS, e a função do *print* era imprimir o que estava na tela. Com o passar do tempo e o advento de novos sistemas operacionais com recursos gráficos, sua função passou a ser a de enviar para a memória, ou arquivo, o conteúdo exibido na tela, de modo que o *print* pode ser considerado uma prova documental que registra um conteúdo exibido em tela em dado um momento (Datacertify, 2023).

Partindo desse raciocínio, Capanema (2024) entende ser perfeitamente admissível o *print* como prova judicial. Primeiro, que não há requisito de admissibilidade de prova documental, segundo que o argumento de que ele pode ser facilmente adulterado vale para toda e qualquer prova documental. Há, por exemplo, uma chance de uma testemunha mentir, porém, isso não retira a validade da prova testemunhal (Datacertify, 2023).

Ponderamos, entretanto, que essas cópias de tela podem ser facilmente manipuladas, dadas as várias tecnologias capazes de editar mensagens e simular uma conversa. Há uma fragilidade ínsita à cópia de tela, diante da baixa complexidade desse material.

Com uma simples pesquisa jurisprudencial no *site* do Tribunal de Justiça de Minas Gerais (TJMG), é possível encontrar decisões que evidenciam essa fragilidade, como a que se segue:

> Incumbe ao réu o ônus de provar a existência de relação jurídica válida, ensejadora da obrigação de pagar, e, obviamente, o seu crédito, quando sustentado pelo autor desconhecimento de ambos, ante a inviabilidade de impor-lhe prova de fato negativo. Os *prints* de telas eletrônicas, sem assinatura ou cópia dos documentos pessoais do autor, não comprovam contratação válida e débito (Minas Gerais, 2022).

Também é possível localizar julgados parecidos em outros tribunais, a saber:

> Caso em que o único meio de prova apresentado para demonstrar que a ré fez comentário difamatório contra a autora em rede social é um *print screen* de tela de celular extraído do aplicativo Facebook, sem ata notarial ou indicação de link da publicação. Prova frágil que, tendo sido impugnada pela ré e estando desacompanhada de outros elementos, não possui valor probatório para, por si só, convencer pela procedência do pedido de indenização de danos morais. Aplicação do art. 422 do CPC. Improcedência mantida. APELAÇÃO DESPROVIDA (Rio Grande do Sul, 2023).

Não obstante, há vários julgados que consideram os *prints* válidos, mesmo sem os devidos acautelamentos da parte que os leva aos autos.

Cabe, a esta altura, menção ao art. 422 do CPC, de que se extrai que qualquer reprodução mecânica tem aptidão para fazer prova dos fatos ou das coisas representadas, se a sua conformidade com o documento original não for impugnada por aquele contra quem foi produzida.

Já o §1º desse dispositivo aponta que as fotografias digitais e as extraídas da rede mundial de computadores fazem prova das imagens que reproduzem, devendo, se impugnadas, ser apresentada à respectiva autenticação eletrônica, o que vale para a forma impressa de mensagem eletrônica, nos termos do §3º.

Havendo a impugnação, caberá à parte que trouxe a prova digital aos autos fazer prova de que o documento apresentado é autêntico.

O Portal da empresa *Verifact* (2023) aponta três motivos pelos quais a Justiça pode não aceitar *prints* como prova judicial:

a) a sua limitação como prova, já que são apenas imagens de tela sem informações cruciais como origem, contexto e detalhes técnicos, dificultando a auditoria do conteúdo apresentado;
b) o risco de falsificação, porquanto é fácil alterar imagens com programas de edição avançados ou manipulação de código-fonte, tornando sua credibilidade questionável, especialmente quando os conteúdos originais são excluídos da internet; e
c) a ausência de cadeia de custódia, que impede a documentação precisa da história cronológica da evidência coletada, comprometendo sua validade e confiabilidade.

Surge, então, o questionamento: quais requisitos devem as mensagens instantâneas preencher para que tenham validade como prova judicial?

Souza, Munhoz e Carvalho (2023, p. 86-87) argumentam que os Tribunais têm exigido o cumprimento de três requisitos para o reconhecimento da validade jurídica de conversas trocadas por intermédio dos mensageiros instantâneos:

a) licitude da prova;
b) integridade da prova; e
c) cientificidade da prova, o que vale dizer que as provas devem ser coletadas a partir do emprego de metodologias científicas válidas que atendam a normas e técnicas forenses.

Nesse sentido, sugere-se a garantia da cadeia de custódia, com todos os acautelamentos necessários que confiram força probante à captura de tela levada aos autos, conduzindo o caso a uma maior segurança jurídica.

Essa garantia pode ser alcançada através de ferramentas *on-line*, ata notarial ou de qualquer meio que dote a prova de autenticidade e integridade.

5.12.3.3 O STJ e o WhatsApp Web

Bem reveladoras têm sido as decisões do STJ no que diz respeito à validade de provas obtidas por espelhamento de *WhatsApp*, no processo penal.

O posicionamento do STJ mudou em relação à possibilidade de autorização judicial para espelhamento via *WhatsApp Web* de conversas realizadas pelo investigado com terceiros. O entendimento antes consolidado era o de que a analogia com o instituto da interceptação telefônica não era possível, em vista de disparidades relevantes, o que acarretaria a ilegalidade da medida, redundando em restrição ao direito de privacidade do investigado (Brasil, 2018a).

Em julgamento paradigmático, a Ministra Laurita Vaz, da Sexta Turma do STJ, proferiu voto no Recurso em HC n. 99.735/SC (Brasil, 2018b), no sentido de que, tanto no aplicativo quanto no navegador, é possível enviar novas mensagens e excluir mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), sejam elas enviadas pelo usuário ou recebidas de algum contato, com total liberdade. Isso, porque qualquer exclusão de mensagem enviada ou de mensagem recebida não deixa absolutamente vestígio algum, tanto no aplicativo quanto no computador emparelhado. Consequentemente, essas mensagens jamais podem ser recuperadas para uso como prova em processos penais, uma vez que a empresa fornecedora do serviço, devido à tecnologia de encriptação ponta a ponta, não armazena o conteúdo das conversas dos usuários em servidor algum. Entretanto,

esse posicionamento vem mudando.

Por ventura do julgamento do Agravo em REsp n. 2.309.888/MG (Brasil, 2023d), em julgamento feito pela Quinta Turma, de Relatoria do Ministro Reynaldo Soares da Fonseca, ocorrido em 17 de outubro de 2023, o espelhamento foi considerado lícito.

No caso, após a Polícia ter identificado vestígios de crime, colheu autorização judicial para interceptação telefônica dos aparelhos utilizados pelos investigados.

O Ministério Público requereu que a quebra de sigilo telefônico deferida se estendesse aos dados telemáticos das linhas utilizadas pelos suspeitos, com autorização de espelhamento, em tempo real, das mensagens e áudios de aplicativos de mensagens e redes sociais vinculados aos terminais interceptados, mediante utilização de *WhatsApp Web*, o que foi deferido.

Assim, a Polícia obteve as provas que precisava, a partir do espelhamento do *WhatsApp* e, com base nos elementos informativos, o Ministério Público ofereceu denúncia.

Alegando que a técnica não encontrava respaldo legal, mormente na Lei n. 9.296/1996 (Brasil, [2019a]), os acusados alegaram a nulidade das provas obtidas por meio do espelhamento.

Ocorre que a Lei n. 12.850/2013 (Brasil, [2019b]), que trata de Organizações Criminosas, permite a infiltração de agentes em qualquer fase da persecução penal, mediante autorização judicial sigilosa e fundamentada. Isso possibilita que agentes estaduais penetrem em organizações criminosas para coletar informações e combater essas atividades.

O MCI (Lei n. 12.965/2014) também permite a interferência no fluxo das comunicações na internet por ordem judicial. A Lei n. 13.964 (Brasil, 2019a) ampliou a Lei n. 12.850/2013 para incluir expressamente a figura do agente infiltrado virtual.

Observamos, ainda, que as regras processuais modernas devem respeitar direitos e garantias fundamentais dos investigados. A infiltração, assim como outros métodos que restringem direitos, está sujeita ao controle judicial. Assim, não há impedimento para o uso de ações encobertas ou agentes infiltrados no meio virtual, desde que se observem os critérios de proporcionalidade e subsidiariedade, e que a prova não possa ser obtida por outros meios.

Ao fim, chegou-se ao entendimento de que o espelhamento do *WhatsApp Web* como meio de infiltração investigativa é válido, pois a interceptação direta no aplicativo original é inviável devido à criptografia ponta a ponta, sendo esta uma modalidade de infiltração equivalente e legal para obtenção de prova.

Por tudo isso, concluiu-se ser lícita a coleta da prova (Brasil, 2023d).

Essa jurisprudência reitera entendimento já esposado no julgamento do AGRG no REsp n. 2.318.334/MG (Brasil, 2024d), também de Relatoria do Ministro Reynaldo Soares da Fonseca, em que foi definido ser possível a utilização de ações encobertas e controladas, incluindo agentes infiltrados no ambiente cibernético e o espelhamento do *WhatsApp Web*, desde que a ação controlada na investigação criminal tenha autorização judicial.

5.12.3.4 Mensageiros instantâneos e cadeia de custódia

Em relação à cadeia de custódia, o STJ, por meio de sua Quinta Turma, já decidiu, à unanimidade, serem inadmissíveis, no processo penal, as provas obtidas de celular, quando não forem adotados procedimentos que assegurem a idoneidade e integridade dos dados extraídos.

No julgamento do AGRG no HC n. 828.054-RN (Brasil, 2024e), de relatoria do Ministro Joel Ilan Paciornick, julgado em 23 de abril de 2024, foi assentado que o instituto da cadeia de custódia assegura a integridade e a confiabilidade dos elementos probatórios, de sua coleta à análise judicial, evitando interferências que possam comprometer sua validade.

A volatilidade dos dados telemáticos exige mecanismos que preservem integralmente os vestígios, permitindo a detecção de quaisquer alterações, intencionais ou não, no material coletado.

Assim, foi consignado que, a fim de se garantir a auditabilidade, repetibilidade, reprodutibilidade e justificabilidade das evidências digitais, é essencial utilizar metodologias e procedimentos certificados, como os recomendados pela Associação Brasileira de Normas Técnicas (2013).

Por fim, ainda foi mencionado o princípio da mesmidade, que visa a assegurar que a prova colhida corresponda exatamente ao que foi extraído do substrato digital, o que pode ser garantido pelo uso de algoritmos *hash* em conjunto com *software*

confiável, auditável e certificado, permitindo acesso, interpretação e extração dos dados digitais (Brasil, 2024e).

5.12.4 Redes sociais

A disruptura tecnológica nos leva a uma nova forma de comunicação. Se, há poucos anos, a comunicação era presencial, por telefone ou carta, restrita a algumas poucas pessoas, atualmente, não apenas nos comunicamos pelas redes sociais, mas expomos quem somos, revelamos preferências e rejeições. Reagimos positivamente ou negativamente a postagens. Compartilhamos aquilo que achamos relevante e essas publicações têm potencial de atingir um número volumoso de pessoas.

Assim, as redes sociais assumem um papel primordial na forma como nos socializamos, seja pela substituição das interações físicas pelas virtuais, seja pelo giro linguístico ínsito as design dessas plataformas, que nos faz expressar pensamentos e emoções com recursos diferentes dos da linguagem tradicional, seja ainda pelo alcance que a comunicação passa a ter.

Talvez, as redes sociais mais relevantes da atualidade sejam *Facebook, Instagram, Twitter, LinkedIn e TikTok*, cada qual com seu perfil particular.

Judicialmente, as provas extraídas das redes sociais se tornam relevantes em todas as esferas. Na cível, podemos pensar em uma propaganda enganosa, que poderá levar a uma indenização, na penal em difamação ou injúria. Na trabalhista, não é difícil imaginar um empregado que alega não poder trabalhar por estar doente, mas posta em perfil de rede social sua imagem em uma praia.

Alie-se a isso o problema do anonimato, que permite a perpetração de atos discriminatórios, ofensas que podem levar o ofendido a desenvolver distúrbios mentais e a difusão de inverdades (*fake news*) com o intuito de promoção política em detrimento do outro espectro político.

Obviamente, a Justiça não pode se tornar simplesmente alheia ao que acontece no mundo virtual, pois o que ocorre neste espaço encontra correspondência no mundo real.

Assim, as provas produzidas a partir de dados coletados nas redes sociais ganham, cada vez mais, destaque:

Exemplo de como as relações sociais e suas dinâmicas mudaram pode ser extraído da apelação criminal n. 0002074-05.2018.4.03.6102, processado pela Quinta Turma do Tribunal Regional Federal da 3ª Região, de Relatoria do Desembargador Federal Maurício Kato (Brasil, 2020f).

No dia 19 de setembro de 2019, o réu, por meio de seu perfil no *Facebook*, publicou comentários discriminatórios sobre a população negra em uma publicação da página “Pense, é grátis”, ao sugerir haver distinções de raça entre pessoas de diferentes tons de pele, alegando que determinados atributos são ínsitos aos negros e outros aos brancos.

Do voto do Relator se pode ler que, apesar da negativa do acusado e do depoimento das testemunhas de defesa, os demais elementos dos autos deixam claro que o acusado tinha a intenção de praticar a discriminação de raça, ao postar seu comentário na página "Pense, é grátis", da rede social *Facebook*.

O notável desse caso é como uma opinião particular toma grandes proporções com a utilização da tecnologia para sua expressão.

Outro caso notório, e que tem se tornado cada vez mais comum, é o do empregado que alega doença para se ausentar do trabalho, mas é flagrado em redes sociais realizando atividades incompatíveis com a doença que ensejou o atestado médico.

Segundo informações do TRT da 21ª Região (TRT-RN), de 24 de abril de 2023, sua Segunda Turma manteve a demissão por justa causa de recepcionista que publicou no Instagram imagens dançando em festa residencial, uma semana após apresentar atestado médico de 30 dias por trauma no tornozelo (Rio Grande do Norte, 2023).

No processo, a empresa juntou cópias de postagens de vídeos gravados no evento social, em que a recepcionista dançava normalmente.

A trabalhadora alegou em sua defesa que "não compareceu a nenhum evento público ou frequentou ambiente que não fosse propício à sua condição de saúde, especialmente, porque não tinha capacidade física de permanecer em pé por muito tempo"(Rio Grande do Norte, 2023).

Em seu voto, o Relator Desembargador Bento Herculano Duarte Neto destacou que o fato de a empregada se ausentar do serviço por um extenso período, devido a uma enfermidade que a impediria de ficar de pé por muito tempo, e, “no início do

afastamento, se apresentar publicamente dançando em uma festa, sem qualquer tipo de cuidado ortopédico, configura mau procedimento", permitindo a dispensa por justa causa, nos termos do art. 482, 'b', da Consolidação das Leis do Trabalho (CLT) (Rio Grande do Norte, 2023).

A partir desses exemplos, podemos perceber que as provas digitais erigem com enorme destaque, seja pelo fato de os conteúdos relacionados à nossa vida real estarem expostos em plataformas virtuais, seja pela sua característica de possuir grande força probante.

Devemos lembrar neste ponto, a discussão acerca da geolocalização e sua capacidade de fornecer dados objetivos e muito mais confiáveis que aqueles obtidos por meio da coleta de depoimentos testemunhais.

Assim como as demais provas digitais, o mais importante para a parte que junta a prova digital é garantir a autenticidade, integridade e preservação da cadeia de custódia da prova que se pretende coletar e preservar, permitindo o exercício do contraditório substancial e exonerando a parte que juntou a prova digital do ônus de ter de demonstrar a respectiva autenticação eletrônica, nos termos do art. 422 e §§ do CPC. Tudo isso deve ser feito por meio de tecnologias como a ICP-Brasil ou *blockchain*.

Vejamos, a respeito decisão do Tribunal Regional de Pernambuco, no Recurso Eleitoral n. 0600026-47.2020.6.17.0007 (Brasil, 2020g), de Relatoria do Desembargador Rodrigo Cahu Beltrão, cujo acórdão foi publicado em 13 de novembro de 2020, de cuja ementa se pode depreender que "meras capturas de tela (prints) não são provas aptas a demonstrar os fatos alegados", e que é descabido cogitar-se indevida inversão do ônus da prova e cerceamento de defesa, em razão do indeferimento de intimação do deputado Eduardo Bolsonaro para comparecer ao feito, e a impossibilidade técnica do *Twitter* Brasil de localizar a postagem referida.

5.12.5 A integração entre ambiente físico e digital

Esta subseção se dedica a esclarecer, ainda que brevemente, como a sociedade vem avançando tecnologicamente e como cada dado produzido em um ambiente insuspeito pode ser utilizado como prova digital, para muito além dos conteúdos de computador e dos celulares que carregamos conosco, em uma

verdadeira simbiose entre os meios físico e digital.

Atualmente, quando pensamos em espaço digital, devemos ter em conta algo muito mais amplo do que aquilo com o que estamos acostumados a pensar.

Como leciona Christian Perrone[4] sobre desafios e possibilidades das provas digitais na atualidade, nosso dia a dia é pautado pelo que ocorre no mundo digital.

Além das formas mais óbvias, como redes sociais e mensageiros instantâneos, os espaços estão se tornando cada vez mais conectados. A luz se conecta ao *smartphone*, que é capaz de comandá-la, bem como câmeras de segurança, televisão etc. Mesmo um *e-reader* tem aptidão para demonstrar o livro que alguém está lendo, quando e onde ele começou essa leitura e quando e onde ele parou. Esses elementos têm marcações e registros do que aconteceu no mundo físico. Exemplo disso é o ingresso em um ambiente. Talvez não se consiga uma prova direta desse ingresso, mas certamente dados sobre a presença são obteníveis a partir de marcadores de aparelhos digitais com sensores, QR Code, GPS ou reconhecimento facial, por exemplo[5].

Todos esses dados gerados podem ser relevantes para a demonstração da ocorrência de um fato. É dizer que hoje há uma “superdocumentação” dos fatos da vida.

Na urbe mesmo, mas não só nela, há uma série de artefatos que podem ser relevantes para a determinação da ocorrência de um fato, como câmeras, antenas, monitoramento de qualidade do ar e da água, controle de tráfego, identificação de vazamentos de água etc. No campo da saúde também é possível vislumbrar uma miríade de marcadores, como dispositivos conectados para monitoramento da saúde, dispositivos vestíveis e roupas conectadas para a monitoração de exercícios físicos e sinais vitais, dentre outros, tudo isso para demonstrar a integração cada vez maior entre os espaços físicos e o virtual, de modo que é aconselhável estarmos sempre atentos para o fato de que, cada vez mais, estamos lidando com uma multiplicidade de dados[6].

---

[4] Informações extraídas do curso *online Provas digitais: fundamentos e aplicações práticas no direito*', promovido pelo Instituto de Tecnologia e Sociedade, que ocorrerá de 8 de julho a 7 de agosto de 2024.

[5] Informações extraídas do curso *online Provas digitais: fundamentos e aplicações práticas no direito'*, promovido pelo Instituto de Tecnologia e Sociedade, que ocorrerá de 8 de julho a 7 de agosto de 2024.

[6] Informações extraídas do curso *online Provas digitais: fundamentos e aplicações práticas no direito'*, promovido pelo Instituto de Tecnologia e Sociedade, que ocorrerá de 8 de julho a 7 de agosto de

Nessa direção da obtenção de dados, os recursos não se esgotam. Drones já vêm sendo utilizados por advogados em ações litigiosas de divisão de terras e usucapião rural. Nessa esteira, segundo Araujo e Costa (2023) a diretora-geral do Departamento Estadual de Trânsito (Detran-PI) informou que serão instaladas câmeras de videomonitoramento nos locais onde são realizados os exames práticos de direção.

> Entre as outras mudanças, estão previstas, ainda, a instalação de microfones dentro dos carros e sensores ao redor do veículo. A expectativa é que as alterações sejam implementadas até dezembro. Para ela, o novo sistema vai possibilitar que o candidato possa pedir uma revisão em caso de reprovação.
>
> Se o aluno for reprovado durante o exame, e não concordar, ele vai poder solicitar uma revisão do resultado. Isso traz mais segurança. Antes de implementar essas melhorias dialogamos com as autoescolas e com os examinadores. As autoescolas são parceiras do Detran e o nosso diálogo sempre vai existir, explicou a diretora (Araujo; Costa, 2023).

Fato notório também é a recente discussão sobre a utilização de câmeras corporais pela polícia militar de São Paulo, com questionamentos do próprio governador sobre a necessidade de seu uso (Liga [...], 2024).

A partir dessa perspectiva, podemos nos dar conta de que a sociedade, e, por conseguinte, o Direito, especialmente no campo das provas, está na iminência de romper novas fronteiras, se é que já não foram rompidas.

5.12.6 Provas em fontes abertas (OSINT)

Como já delineado em subseção pertinente, a fonte aberta se caracteriza por estar livremente disponível, sem proteção, não havendo necessidade de uso de senha ou intervenção judicial para acessar seu conteúdo. Sua utilização pode decorrer de atividade humana ou automatizada.

Trata-se da inteligência de exploração do mar aberto que é a internet. A advocacia proativa, bem como os juízes, promotores e operadores do direito, tem na rede uma miríade de formas de obter informações, como nomes, bens, qualificação, localizações, datas, horas, endereços IPs, remuneração de servidores públicos,

---

2024.

depoimentos de testemunhas etc.

Nesta subseção, listamos apenas algumas das ferramentas disponíveis livremente, a fim de demonstrar o potencial que a inteligência de fontes abertas oferece para o operador do direito.

Talvez, a ferramenta de pesquisa do *Google* seja a principal forma de se obter provas digitais, sejam daqueles fatos ocorridos *on-line* ou no mundo físico. A página de pesquisa avançada do *Google* permite a customização da atividade de busca, filtrando exatamente termos relevantes às informações a que se pretende ter acesso. O *Google Maps*, por exemplo, é um serviço de mapas que permite a visualização de ruas.

O já citado *exif* tem a função de identificar metadados de fotos digitais. Exif, reiteramos, é a abreviação de *Exchangeable Image File*, um formato padrão para armazenar informações de intercâmbio em arquivos de imagem de fotografia digital, usando compactação Joint Photographic Experts Group (JPEG). Quase todas as novas câmeras digitais usam a anotação exif, armazenando informações sobre a imagem como velocidade do obturador, compensação de exposição, número F, qual sistema de medição foi usado, se foi usado *flash*, número ISO, data e hora em que a imagem foi tirada, balanço de branco, lentes auxiliares que foram utilizadas e resolução. Algumas imagens podem até armazenar informações de GPS, para que se possa facilmente ver de onde as imagens foram tiradas.

O Wayback Machine é outra ferramenta de extrema valia, que conta com um banco de dados digital que armazena bilhões de páginas da *World Wide Web,* desde 1996. Esta permite que os usuários visualizem versões arquivadas de páginas de *websites*, mostrando como eram no passado.

Um exemplo de seu uso ocorreu por ventura de um cumprimento de sentença processado na 2ª Vara do Trabalho de Itapecerica da Serra/SP, no processo n. 1000223-30.2020.5.02.0332 (Brasil, 2021e). A juíza do caso, Thereza Christina Nahas, utilizou de ofício a ferramenta para verificar a existência de grupo econômico, registrando que “a impugnação lançada pela requerida quanto ao documento não se sustenta”, uma vez que ela própria consultou o *site* Wayback Machine, no qual localizou o endereço eletrônico, verificando que a requerida alterou o conteúdo das informações anteriormente transmitidas aos seus consumidores mas, com a consulta acima não se tem dúvidas da veracidade das informações trazidas pela parte autora”.

Ao fim, o requerimento apresentado pelo reclamante de ver declarada a responsabilidade entre a executada e outras duas empresas foi acolhido (Brasil, 2021e).

O Who.is é uma ferramenta de informações sobre dados de nomes de domínios, e o IP *Logger* tem a função de identificar IPs.

O Poder Executivo possui uma grande variedade de ferramentas, como o Portal Transparência, Busca CEP, Beneficiários do Programa Bolsa Família, Comprovante de Regularidade Fiscal, dentre inúmeras funcionalidades que disponibilizam informações públicas e de fácil acesso.

O Poder Judiciário e o Legislativo igualmente dispõem de várias ferramentas abertas de busca de dados, como Situação Eleitoral, Certidão Negativa de Débitos Trabalhistas e Consulta às Contas do Tribunal de Contas da União (TCU).

Poderíamos arrolar um sem-número de aplicações passíveis de uso, mas o intuito foi apenas elencar e ilustrar o potencial que essas ferramentas oferecem atualmente se bem compreendidas.

5.13 O Supremo Tribunal Federal e algumas questões relevantes acerca das provas digitais

5.13.1 Ação Declaratória de Constitucionalidade n. 51

Na Ação Declaratória de Constitucionalidade (ADC) nº 51, a Federação das Associações das Empresas de Tecnologia da Informação (ASSESPRO Nacional) solicitou a confirmação da validade do Acordo de Assistência Judiciária em Matéria Penal (Mutual Legal Assistance Treaty - MLAT, na sigla em inglês), promulgado pelo Decreto Federal 3.810/2001 (Brasil, 2001). Este acordo é utilizado em investigações criminais e instruções penais em curso no Brasil, envolvendo pessoas, bens e ativos localizados nos Estados Unidos. O acordo bilateral aborda a obtenção de conteúdos de comunicações privadas controladas por provedores de aplicativos de internet sediados fora do país (Brasil, 2023h).

Como se depreende do acórdão, a controvérsia judicial envolve o debate sobre a constitucionalidade e a aplicabilidade do Decreto nº 3.810/2001, bem como dos arts. 237, II do CPC, e dos artigos 780 e 783 do CPP, no que diz respeito à obtenção de

conteúdo de comunicações que estão sob controle de empresas de tecnologia localizadas fora do território nacional.

Após ponderar que “a controvérsia constitucional veiculada nesta ADC é, a rigor, mais ampla do que a simples declaração de validade do uso das cartas rogatórias e dos acordos MLAT para fins de investigação criminal”, o Ministro Relator Gilmar Mendes frisou que devem ser considerados o art. 21 do CPC e o art. 11 do MCI, “que atribuem jurisdição e determinam a imperiosa aplicação da lei brasileira sempre que a coleta de dados ocorrer em território nacional e ainda que a empresa responsável seja estrangeira” (Brasil, 2023g).

Assim, o que foi posto a apreciação não foram apenas as normas supracitadas, mas a possibilidade de os Tribunais brasileiros utilizarem o art. 11 do MCI, para determinar o dever das empresas de tecnologia de fornecerem essas informações.

O voto do Ministro Gilmar Mendes foi muito didático, pois, de seu voto, podemos extrair várias considerações.

O Ministro ponderou que a questão crucial era saber até que ponto o Poder Judiciário brasileiro poderia ordenar que provedores de redes sociais, *e-mails* e aplicativos de mensagens instantâneas concedessem acesso a dados e conteúdos de comunicações privadas armazenados em bancos de dados localizados em países estrangeiros. Este debate naturalmente envolve conflitos entre direitos fundamentais, como privacidade e segurança da informação, além de questionar os limites da jurisdição, dado que esses dados muitas vezes não são armazenados nos países onde as comunicações ocorrem (Brasil, 2023g).

Reflete, ainda, que há no mundo todo uma tendência à elaboração de normas domésticas “que impõem aos agentes econômicos que atuam na internet o dever de obedecer às determinações dos Tribunais nacionais, ainda que as operações on-line mediadas por essas empresas não ocorram inteiramente dentro do país” (Brasil, 2023g), tendência solidificada após o caso *Snowden*.

Assim, o objetivo de disposições normativas como a regra do art. 11 do MCI é o de resguardar a soberania nacional, obrigando que certos tipos de dados coletados dentro do país possam ser armazenados e processados nacionalmente.

Observando que o art. 11 do MCI

> é norma específica em relação às regras gerais do MLAT, das cartas rogatórias e da cooperação jurídica internacional, e estabelece a

> aplicação da legislação brasileira e a jurisdição nacional sobre atividades de coleta, armazenamento, guarda e tratamento de registros, dados e comunicações eletrônicas ocorridas em território nacional, desde que, pelo menos, um dos atos ou terminais se encontrem em território nacional (Brasil, 2023g).

O Ministro fundamentou seu voto:

> Destarte, com base em todos esses motivos, concluo pela constitucionalidade dos dispositivos do MLAT, do CPC e do CPP que tratam da cooperação jurídica internacional e da emissão de cartas rogatórias, em especial nos casos em que a atividade de comunicação ou a prestação de tais serviços não tenham ocorrido em território nacional, sem prejuízo da aplicação específica do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste para a solicitação de dados, registros e comunicações eletrônicas relativos a atos praticados no país.
>
> Isso significa que, fora das hipóteses do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste, que tratam de atividades e serviços prestados em território nacional, o único instrumento cabível é o da cooperação previsto pelo tratado bilateral e pelas regras das cartas rogatórias (Brasil, 2023g).

Se é correto que a decisão proferida na ADC n. 51 aponta para a noção de cooperação jurídica internacional, conforme preceituado no art. 26 do CPC, certo é que as empresas detentoras de dados situados no exterior ainda podem dificultar o fornecimento de dados, alegando que devem obediência à legislação do país de origem dos dados, de tal maneira que o Ministro Alexandre de Moraes proferiu voto no sentido de que as autoridades brasileiras devem solicitar informações diretamente às empresas localizadas no exterior, nos termos do art. 11 do MCI e do art. 18 da Convenção de Budapeste, com a ressalva de que o MLAT deve ser aplicado de forma subsidiária, quando não for possível às autoridades judiciais brasileiras a obtenção direta dos dados requeridos.

5.13.2 Arguição de Descumprimento de Preceito Fundamental n. 403

De relatoria do Ministro Edson Fachin, a ADPF n. 403 foi ajuizada pelo PPS, em face de decisão do Juiz de Direito do Estado de Sergipe, em que o magistrado determinou a suspensão do aplicativo de comunicação *WhatsApp* em todo o Brasil, por suposto descumprimento de ordem judicial.

Sustentou o Ministro desrespeito ao art. 5º, IX da CRFB/1988, por ser

> cristalina a violação do direito à comunicação. Afinal, o aplicativo de mensagens WhatsApp realizou algo visto como impensável até a década passada: uniu as mais diversas gerações em uma só plataforma de troca de informações, proporcionando a comunicação de maneira irrestrita para os aderentes [e que] a suspensão da atividade do WhatsApp, baseado em controverso fundamento, viola o direito à comunicação, garantido constitucionalmente ao povo brasileiro (Brasil, 2017).

Assim, requereu provimento da sua arguição, para “reconhecer a existência de violação ao preceito fundamental à comunicação, nos termos do art. 5º, inciso IX, com a finalidade de não mais haver suspensão do aplicativo de mensagens *WhatsApp* por qualquer decisão judicial” (Brasil, 2017).

Posteriormente, notificou outra ocorrência de determinação judicial de bloqueio do *WhatsApp*, da 2ª Vara Criminal da Comarca de Caxias/RJ, de modo que pediu o julgamento liminar em ambas as decisões.

Apontando para o direito fundamental à liberdade de expressão consubstanciado no art. 5º, IX da CRFB/1988 e enunciado no art. 3º, I do MCI, como um dos princípios do uso da internet no país, o Ministro Relator fundamentou sua decisão no sentido de que a concessão da liminar pelo juízo *a quo* viola o princípio fundamental da liberdade de expressão. “Ademais, a extensão do bloqueio a todo o território nacional, afigura-se, quando menos, medida desproporcional ao motivo que lhe deu causa” (Brasil, 2017).

Assim, foi deferida a liminar para suspender a decisão da 2ª Vara Criminal da Comarca de Caxias/RJ, ainda em 2016.

Em sessão realizada em 28 de maio de 2020, foi proferido o voto do Ministro Relator com exauriência cognitiva, do qual se extrai valorosas lições (Brasil, 2021c).

Resumindo a controvérsia acerca da validade constitucional das normas do Marco Civil que amparam a privacidade e preveem a sanção de suspensão, o Ministro Relator colocou como ponto de partida o art. 7º, II do MCI, tratando de investigar os limites da decisão judicial que restringe o direito à privacidade.

Em um tópico denominado “Alegações Mais Relevantes Trazidas na Audiência Pública”, o Relator resume a visão dos representantes da Polícia Federal, para os quais o *iter criminis* hodiernamente é realizado a partir dessas plataformas tecnológicas, alegando que “não há uma investigação da Polícia Federal que em, em

momento oportuno, não se revela que atos de cogitação, porque não atos de preparo, ordens de execução, são feitos por meio de comunicação ” (Brasil, 2017).

Argumentaram, ainda, que “a persecução penal no Brasil não pode se ditar por empresas de informática. Ela tem que se ditar pelo Estado” (Brasil, 2017), indicando que o combate à criminalidade moderna deve se dar por meio de ferramentas que oportunizem a obtenção de autoria e materialidade, ressaltando que a decisão do STF pode ser um ponto de virada, alertando que diversos métodos de investigação atualmente utilizados pela Polícia Federal poderão ser invalidados pelo mesmo argumento de inviabilidade técnica usado pelo *WhatsApp*.

Já a Procuradoria-Geral da República (PGR) defendeu a importância de o STF definir o regime jurídico aplicável às atividades desenvolvidas pelo *WhatsApp* e outros aplicativos de mensagens instantâneas, determinando se essas atividades podem ser consideradas essenciais. Em sua visão, apenas serviços essenciais estão protegidos pelo princípio da continuidade e, portanto, não podem ser suspensos. No mérito, argumentaram pela improcedência da ação, com base em três pontos:

a) o caráter relativo do direito à comunicação e à liberdade de expressão;
b) a ausência de violação desses direitos pela suspensão temporária de um aplicativo; e
c) a submissão do WhatsApp ao MCI, especialmente no que diz respeito à aplicação de sanções por não cumprimento de ordens judiciais (Brasil, 2017).

Demi Getschko, representante do Comitê Gestor da Internet (CGI) no Brasil e do Núcleo de Informação e Coordenação do Ponto BR, afirmou que, quanto mais se busca pressionar a internet para que monitore e intercepte as atividades nela desenvolvidas, mais a internet se protege, criando mecanismos de defesa. Ele destacou que a criptografia não está sujeita a críticas; é uma ferramenta essencial para o desenvolvimento da comunidade, seja na esfera privada, pública ou qualquer outra, e deve ser protegida. A questão não é permitir ou não a criptografia. (Brasil, 2017).

Assim, indicou os perigos de se criarem acessos privilegiados, as chamadas *backdoors*, para permitir a interceptação, na medida em que não se tem como garantir a integridade e a segurança do sistema. Após citar alguns casos em que a estratégia

teve resultados adversos, finalizou seu discurso, mencionando o Decálogo elaborado pelo CGI.br, que dispõe que a criptografia é instrumento aos direitos humanos de privacidade e liberdade de expressão; é uma tecnologia que deve ser estimulada e não restringida; as plataformas que disponibilizam tecnologias de segurança da informação não devem ser penalizadas pelos usos de seus usuários. Concluiu, afirmando que “privacidade e segurança são convergentes e não contrapostos” (Brasil, 2017).

Um dos especialistas acadêmicos presentes na audiência, o Professor Anderson Nascimento, explicou, de maneira geral, o funcionamento da criptografia, destacando que seu objetivo é garantir a integridade, autenticidade e confidencialidade das informações. Ele afirmou que o *WhatsApp* utiliza criptografia de chave pública ou assimétrica, na qual cada usuário possui duas chaves: uma para cifrar e outra para decifrar. O objetivo desses sistemas é criar um túnel criptográfico entre os usuários, permitindo que as mensagens enviadas e recebidas passem por um servidor que estabelece protocolos de sinalização, descobre os endereços IP das partes envolvidas, auxilia na troca de chaves, entre outras funções.

O Professor Anderson Nascimento esclareceu que a interceptação das mensagens criptografadas do *WhatsApp* é impossível, devido à adoção de criptografia forte pelo aplicativo. Ele explicou que esse tipo de criptografia utiliza o Protocolo *Signal*, que, segundo a comunidade científica, é considerado seguro e não apresenta vulnerabilidades, sendo assim impenetrável.

Finalizou, citando trecho do Relatório Especial do Conselho de Direitos Humanos da Organização das Nações Unidas (ONU), que diz que “a criptografia possibilita que indivíduos exerçam seus direitos à liberdade de opinião e expressão na era digital e, como tal, merece nossa proteção” (Brasil, 2017).

Vale a pena, por fim, trazer a exposição do cofundador do *WhatsApp*, Brian Acton, que participou da audiência pública. Para ele, desde o princípio da criação do aplicativo, a privacidade e a segurança foram essenciais e que a criptografia protege os usuários contra ataques de *hackers* e ajuda a transmitir a sensação de segurança para que os usuários realizem suas comunicações (Brasil, 2017).

Asseverou que a criptografia ponta a ponta adotada pelo *WhatsApp* torna impossível alguém, que não o próprio usuário, ter acesso ao conteúdo das mensagens. A única maneira de desabilitar a criptografia para um usuário específico

seria desabilitá-la para todos os usuários. Em relação à criação de uma *backdoor* no aplicativo ou à implementação de uma chave-mestra, sustentou que o sistema ficaria vulnerável, permitindo que, se um *hacker* obtivesse acesso a essa chave, ele poderia acessar qualquer mensagem ou arquivo de qualquer usuário do aplicativo, em todo o mundo (Brasil, 2017).

Registrou, ao fim de sua exposição, que os metadados coletados pelos servidores do *WhatsApp* são disponibilizados para as forças de segurança e justiça do Brasil, de acordo com as ordens judiciais, mas o conteúdo em si das mensagens e/ou dados são sempre encriptados, não podendo ser lidos ou interceptados.

Com base na oitiva desses diversos atores, percebemos, claramente, um conflito entre princípios fundamentais, como segurança pública, privacidade e liberdade de expressão. É a partir dessa constatação, que /o Ministro Fachin construiu sua argumentação, e para /ele, os pontos de vista apresentados nas audiências foram essenciais para esclarecer, plenamente, as questões controvertidas desta arguição.

Colacionou, ainda, trecho da manifestação do Ministro Gilmar Mendes na ADI n. 6.389/DF, cuja transcrição vale a pena ler, dada a sua profundidade:

> O direito fundamental à igualdade – enquanto núcleo de qualquer ordem constitucional – é submetido a graves riscos diante da evolução tecnológica. A elevada concentração de coleta, tratamento e análise de dados possibilita que governos e empresas utilizem algoritmos e ferramentas de *data analytics*, que promovem classificações e esteriotipações discriminatórias de grupos sociais para a tomada de decisões estratégias para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por viesses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham.
> (...)
> Todo esse contexto nos indica que decisões críticas para o Estado de Direito estão sendo cada vez mais substituídas por mecanismos automatizados. Em outras palavras, de forma bem direta: vivemos na era das escolhas de Sofia automatizadas. Independente do acerto ou desacerto dessas decisões automatizadas, é inequívoco que a proteção dos valores estruturante da nossa democracia constitucional requer que o Direito atribua elementos de transparência e controle que preservem o exercício da cidadania. É por isso que, para muito além do mero debate sobre o sigilo comunicacional, este Tribunal deve reconhecer que a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo (Brasil, 2021c).

Então, após refletir sobre os desafios que a modernidade traz ao Direito, o Ministro Fachin tratou de delimitar o objeto da arguição, que é:

a) determinar se é constitucional a ordem judicial que permite aos órgãos do Estado acesso ao conteúdo de comunicações protegidas por criptografia, conforme previsto no art. 7º, II, MCI; e, caso seja considerada constitucional;
b) verificar se a sanção prevista no inciso III do art. 12, III do mesmo diploma legal pode ser aplicada pelo Poder Judiciário.

Ao fim, é esse o objeto da ADPF n. 403.

Vale dizer: o art. 7º, II garante a inviolabilidade do fluxo de comunicações pela internet, salvo por ordem judicial. Entretanto, se a ordem judicial de apresentação de dados for negada, o art. 12, III permite a suspensão das atividades do provedor de aplicação (Brasil, [2021b]).

Então, o Ministro assenta três premissas para prolatar seu voto:

a) a criptografia é um meio de se assegurar a proteção de direitos essenciais para a vida pública;
b) a internet segura é direito de todos; e
c) há dificuldades técnicas na apuração de crimes que violam direitos fundamentais, como, por exemplo, os casos de pornografia infantil e de condutas antidemocráticas, como manifestações xenófobas, racistas e intolerantes, que ameaçam o Estado de Direito, muitas vezes privando os órgãos de segurança do Estado de instrumentos para a consecução do seu objetivo de garantir a segurança pública.

Dessa forma, a questão central para abordar o mérito da arguição é determinar se o risco público representado pelo uso da criptografia justifica a restrição desse direito, por meio da imposição de soluções de *software*, como a proibição da criptografia, a criação de canais excepcionais de acesso, ou a redução do nível de proteção.

“O guia de interpretação deve ser o seguinte: os direitos que as pessoas têm *offline* devem também ser protegidos *online*. Direitos digitais são direitos

fundamentais", uma orientação do Conselho de Direitos Humanos das Nações Unidas (A/HRC/RES/32/13) (Brasil, 2021c).

Após apanhar diretrizes internacionais de conduta, tratados internacionais, legislação e jurisprudência de outros países e do próprio STF, o Ministro chega à compreensão de que a proteção de privacidade não é apenas proteção individual, mas garantia instrumental do direito à liberdade de expressão, a qual é assegurada pela criptografia, como meio de garantir a privacidade das pessoas no âmbito digital.

Argumentou, ainda, que

> a proteção dada pela criptografia e pelo anonimato também são extremamente úteis em locais e cenários em que predominam atividades censórias. A rejeição absoluta à censura feita pela Constituição de 1988 ganha, pois, força com esses mecanismos de proteção. Além disso, porque o direito à liberdade de expressão tem uma dimensão transnacional, a criptografia e o anonimato poderiam ser utilizados para promover a prevalência dos direitos humanos (Brasil, 2021c).

Conquanto compreenda que a criptografia engaje um fortalecimento da proteção da expressão de liberdade e da privacidade, reconhece o referido Ministro que se cria um risco para a segurança pública, porém, valendo-se da sustentação do Professor Diego Aranha, Fachin insiste que o benefício obtido pela redução da proteção criptográfica é negativo. Não há interesse algum de segurança de rede na concessão de um acesso excepcional: ele só aumentará a insegurança para os usuários. "Não existe acesso apenas para as pessoas boas. *Backdoor* apenas para *good guys* não funciona. Dito de outro modo, de nada adianta deixar a chave debaixo do tapete". (Brasil, 2021c).

Ao fim, diante dessas ponderações, restou assentada a procedência da ADPF n. 403

> para declarar a inconstitucionalidade parcial sem redução de texto tanto do inciso II do art. 7º, quanto do inciso III do art. 12 da Lei 12.965/2014, de modo a afastar qualquer interpretação do dispositivo que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta a ponta ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet (Brasil, 2021c).

Por ora, esse é o único voto proferido nos autos da ADPF n. 403, mas, é fundamental para entendermos o dilema que envolve o antagonismo de princípios

fundamentais em torno da necessária segurança pública e das igualmente necessárias privacidade e liberdade de expressão.

5.13.3 Ação Direta de Inconstitucionalidade n. 5.527

A ADI n. 5.527 aborda a mesma questão que a ADPF n. 403: a possibilidade de suspensão dos serviços de mensagens pela internet, como o *WhatsApp*, devido ao suposto descumprimento de ordens judiciais que exigem a quebra de sigilo das comunicações.

Trata-se de ADI proposta pelo Partido da República, tendo por objeto os arts. 10, § 2°; e 12, incisos III e IV do MCI – Lei n. 12.965, de 23 de abril de 2014.

O primeiro dispositivo impugnado estabelece que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º" (Brasil, 2021b).

Já o art. 12, III prevê a suspensão temporária das atividades dos provedores de conexão e de aplicações como sanção, enquanto o art. 12, IV cuida da proibição de exercício das atividades desses provedores.

Com isso, inferimos que o objetivo da ação movida pelo Partido da República é o reconhecimento da inconstitucionalidade das sanções que impõem a suspensão temporária das atividades e a proibição do exercício da empresa responsável por uma plataforma de comunicação via internet, devido ao descumprimento de ordem judicial para disponibilização do conteúdo de mensagens privadas dos usuários.

A Ministra Relatora, Rosa Weber, foi a única a proferir voto até então, do qual podemos extrair subsídio para a compreensão do que está em jogo nessa discussão (Brasil, 2022d).

De saída indica ela que o debate é salutar, uma vez que as questões enfrentadas "dizem respeito a valores fundacionais da ordem jurídica pátria, conforme consagra o próprio preâmbulo da Carta Política: liberdade e segurança, desenvolvimento e justiça" (Brasil, 2022d).

Pondera que nossos celulares guardam muito mais de nossa vida privada e íntima que nossas paredes, porém, não temos dificuldade para reconhecer a inviolabilidade do domicílio.

Citando vários casos de ordem de suspensão das atividades do *WhatsApp* em um curto período de tempo, entre 2015 e 2016, lamentamos que o Brasil figure ao lado de outros países “que não compartilham das mesmas tradições e valores democráticos caros à nossa sociedade, em listas de países pouco comprometidos com a preservação das liberdades individuais na Internet” (Brasil, 2022d).

A Ministra Rosa Weber reflete que o pleno exercício das liberdades de expressão e de comunicação inclui a capacidade de as pessoas escolherem livremente as informações que desejam compartilhar, as ideias que desejam discutir, o estilo de linguagem utilizado e o meio de comunicação de que quer fazer uso. A consciência de que a comunicação está sendo monitorada por terceiros interfere em todos esses aspectos da liberdade de informação: os cidadãos podem alterar sua forma de expressão, ou até mesmo evitar falar sobre determinados assuntos, o que a doutrina denomina efeito inibitório (*chilling effect*) sobre a liberdade de expressão, o que levaria “desde a desconfiança em relação às instituições sociais à apatia generalizada e a debilitação da vida intelectual, fazendo de um ambiente em que as atividades de comunicação ocorrem de modo inibido ou tímido, por si só, uma grave restrição à liberdade de expressão” (Brasil, 2022d).

Rosa Weber sugere que uma característica estrutural das sociedades democráticas é justamente a proteção da privacidade, razão pela qual tanto o reconhecimento de uma esfera de privacidade imune à ingerência quanto a garantia de proteção à palavra proferida surgiram, na história do constitucionalismo moderno, como fatores que limitam o poder das autoridades sobre os cidadãos.

Referindo-se a uma “corrida armamentista” entre tecnologias que facilitam a vigilância e tecnologias de proteção da privacidade que vem ocorrendo nas últimas décadas, alega que a hermenêutica constitucional não pode ficar alheia a essas mudanças, “em vista da manutenção do equilíbrio entre proteção da privacidade e os limites da atuação do Estado” (Brasil, 2022d).

A cada avanço tecnológico que possibilita a imposição de níveis crescentes de controle sobre diversos aspectos da vida das pessoas, surge novamente a questão a ser decidida pelas Cortes: permitir o aumento do poder estatal ou fortalecer as proteções à privacidade individual.

É evidente a elevada importância que a Ministra atribui à proteção da privacidade e da intimidade.

Assim é que em importante trecho de seu voto, cita o art. 5º, XII da CRFB/1988, interpretando-o no sentido de que a lei somente pode autorizar a suspensão do sigilo de comunicações privadas para fins de investigação criminal ou instrução processual penal.

Apontando para o art. 21 da Convenção de Budapeste sobre o Cibercrime, registra Rosa Weber que o uso legítimo de medidas que obriguem um fornecedor a recolher ou registrar esse conteúdo deve seguir três diretrizes:

a) a definição, no direito interno, de um conjunto prévio de infrações consideradas especialmente graves, a ponto de justificar a natureza da medida;
b) que a exigência não ultrapasse a capacidade técnica do fornecedor; e
c) que a medida tenha como objeto o conteúdo de comunicações específicas (Brasil, 2022d).

Tratando sobre a tecnologia empregada por algumas plataformas, especialmente a criptografia, mostra-se contrária ao entendimento de que o Estado poderia obrigar tais plataformas a criarem uma brecha que possibilitasse a extração de dados, que, de outro modo, seria impossível.

Isso, porque o poder do Estado de exigir a disponibilização do conteúdo de mensagens em investigações criminais ou instruções processuais penais não implica que seja ilegal oferecer um serviço que utilize tecnologia que torne esse conteúdo inacessível ao próprio provedor da plataforma. Uma vez que um particular desenvolve e adota uma tecnologia voltada a garantir a segurança e a privacidade das comunicações, oferecendo-a como valor agregado a outros particulares que contratam seus serviços, o Estado não pode compelir esse provedor a oferecer um serviço menos seguro e mais vulnerável (como forçá-lo à implementação de *backdoors*), sob o pretexto de que poderia, eventualmente, utilizar essa vulnerabilidade artificial para cumprir uma ordem judicial. Isso significaria tornar a criptografia, ou pelo menos alguns de seus usos, ilegal.

Acertadamente, em nossa opinião, Rosa Weber indica que a criptografia não traz um embate entre segurança pública e privacidade,

> pois a pretensão que ameaça a privacidade, ainda que fundada no combate a uma ameaça imediata à segurança, vulnera no longo prazo, também a segurança das redes e de seus usuários como um todo,

> expondo-os a maiores riscos de ciberataques, fraudes, roubos de identidade, invasão da intimidade extorsão etc. (Brasil, 2022d).

A tecnologia que facilitaria o acesso das autoridades de segurança pública ao conteúdo armazenado também pode ser utilizada por criminosos para acessar informações privadas de futuras vítimas.

Quanto às sanções previstas no art. 12, III e IV, do MCI, concluiu que eles não facultam a suspensão ou proibição do exercício de atividades pelos provedores de conexão e aplicação. A partir de interpretação sistemática dos dispositivos, concluiu que "a *mens legis* das sanções previstas no art. 12 da Lei nº 12.965/2014 é voltada à proteção da privacidade, e não o contrário". Em suas palavras:

> O art. 12, III e IV, da Lei nº 12.965/2014 permite a suspensão ou proibição, repito, das atividades que envolvem a "operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações" justamente para salvaguardar a integridades desses elementos em face de provedor que venha a vulnerá-los.
> Trata-se de uma norma protetiva dos direitos dos usuários, que de modo algum configura suporte jurídico à imposição de sanções em decorrência do descumprimento de ordem judicial (Brasil, 2022d).

Ao fim, a Ministra entendeu:

a) pela improcedência do pedido de declaração de inconstitucionalidade do art. 12, III e IV, da Lei nº 12.965/2014;
b) pela procedência do pedido de interpretação, conforme a CRFB/1988 do art. 10, § 2º, da Lei nº 12.965/2014, no sentido de que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º, e para fins de investigação criminal ou instrução processual penal",
c) improcedente o pedido sucessivo de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei nº 12.965/2014 e d) parcialmente procedente o pedido sucessivo de interpretação, conforme a Constituição do art. 12, III e IV, da Lei nº 12.965/2014, assentando que as penalidades de suspensão e proibição do exercício de atividades só podem ser aplicadas aos provedores de conexão e aplicações de internet "nos casos de descumprimento

> da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros", afastando qualquer interpretação de que "o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação" não pode ser objeto de exegese dos artigos questionados nem mesmo do art. 7º, II e III do MCI (Brasil, 2022d).

O que vale destacar do voto da Ministra é que a criptografia é vista como uma tecnologia concretizadora do direito fundamental à privacidade, à intimidade e à liberdade de expressão. Assim, medidas que visem a restringi-la não coadunam com o Estado Democrático de Direito.

Assim, em face da inviabilidade técnica do cumprimento da ordem judicial, os dispositivos do MCI não se prestam a forçar esse cumprimento. Sendo viável, lado outro, sem fragilização dos mecanismos de proteção de privacidade dos usuários, por óbvio que se deve cumprir a ordem judicial.

Assim como na ADPF n. 403, o voto é de maio de 2020 e, atualmente, encontra-se destacado pelo Ministro Alexandre de Morais.

5.13.4 Ação Direta de Inconstitucionalidade n. 5.642

Trata-se de ADI movida pela Associação Nacional das Operadoras Celulares (ACEL), que pretendia ver declaradas inconstitucionais as regras insculpidas nos arts. 13-A e 13-B do CPP, sob a alegação de que eles esvaziariam a proteção constitucional à privacidade e ao sigilo das comunicações, dando "verdadeira carta em branco", para que as autoridades possam acessar todos os dados de cidadãos tidos como suspeitos (Brasil, 2024b).

O art. 13-A cuida da possibilidade de requisição direta a quaisquer órgãos do poder público ou de empresas da iniciativa privada, pelo membro do Ministério Público ou pelo delegado de polícia, de dados e informações cadastrais de vítimas e suspeitos da prática de determinados tipos penais, sem a necessidade de ordem judicial.

A requisição deve ser atendida em 24 horas e os tipos penais se cingem a cárcere privado, a redução a condição análoga à de escravo, o tráfico de pessoas, o sequestro relâmpago, a extorsão mediante sequestro e o envio ilegal de criança ao exterior, crimes especialmente graves.

Já o art. 13-B trata da obtenção de informações que auxiliem na localização de vítimas ou suspeitos de crimes relacionados ao tráfico de pessoas, a partir da disponibilização de meios técnicos adequados, como sinal de celular ou de internet. Esses dados só podem ser fornecidos às autoridades investigadoras, mediante ordem judicial. No entanto, se o juiz não analisar o pedido de acesso aos dados em até 12 horas, a Polícia ou o Ministério Público podem exigir sua entrega diretamente. O juiz deverá ser informado imediatamente e poderá analisar a questão posteriormente.

A ação foi protocolada em 17 de janeiro de 2017 e julgada em 18 de abril de 2024, pela improcedência dos pedidos, 7 anos após seu ajuizamento e por uma maioria de 6x5.

O voto prevalente foi o do Ministro Relator Edson Fachin, que destacou que a ação desafiava a atualização da cláusula constitucional de proteção à privacidade na era digital, já adiantando no começo de seu voto que a ação era improcedente

Afirmou que a CRFB/1988, especialmente por meio do art. 5º, XI e XII, dá corpo ao princípio fundamental da privacidade e à vida privada consagrado no art. 11 do Pacto de São José da Costa Rica, discorrendo sobre o necessário sigilo que ampara uma legítima expectativa de privacidade.

Ocorre que esse direito não é absoluto, mas qualificado, com a lei podendo restringi-lo, ao prever hipóteses em que o Poder Judiciário poderá afastá-lo.

Recordou-se, ainda, dos precedentes da Corte Constitucional, de acordo com os quais “as informações de registros públicos e os dados cadastrais, de posse das empresas de telefonia, também poderiam ser requisitados, sem que se falasse em ofensa ao direito à privacidade” (Brasil, 2022d).

Em reveladora passagem, consignou que, no Brasil, similarmente ao direito norte-americano, desenvolveu-se uma doutrina de terceiros (*third-party doctrine*) que elimina a expectativa de privacidade dos dados mantidos por terceiros, ou seja, agentes privados que possuem a custódia de informações voluntariamente fornecidas a bancos, provedores de internet e companhias telefônicas.

Aduziu que o ponto fulcral do debate consistia em “saber se a expressão ‘dados cadastrais’ ampara a proteção constitucional da privacidade à luz das inovações trazidas pelo desenvolvimento tecnológico”. (Brasil, 2022d).

Ponderou sobre vários óbices colocados pela doutrina, conquanto à restrição do direito à privacidade trazida por esses dispositivos legais, como a de que

> sem a restrição de quais aparelhos podem ser usados, sem indicação dos dados a serem mapeados, sem a determinação da intensidade, da profundidade, da continuidade e da duração da requisição, o mero recurso à expressão ‘dados cadastrais’ é insuficiente para a promoção da privacidade na era digital (Brasil, 2022d).

No entanto, o Ministro Relator partiu da compreensão de que, apesar das considerações apresentadas pela doutrina, a norma contestada não concedia um poder irrestrito de requisição. Pelo contrário, ela oferecia um poder instrumentalmente necessário para reprimir violações de crimes graves que ameaçam a liberdade pessoal, visando a permitir o resgate das vítimas dessas infrações, enquanto elas ainda estão ocorrendo.

> Os pedidos deduzidos pela requerente, no sentido de restringir os dados que podem ser requisitados, conquanto possam comportar discussões mais aprofundas em outras ações diretas, não merecem trânsito relativamente aos poderes de requisição para os crimes que atentam contra a liberdade pessoal, tal como os disciplinados pela redação do art. 13-A do Código de Processo Penal, quer por sua notável gravidade, quer porque foram objeto de especial seleção por parte do legislador, o que permitiu restringir tanto as autoridades públicas que têm poder de requisição, quanto as hipóteses em que esse poder se manifesta. Por isso, não há inconstitucionalidade na disposição normativa atacada (Brasil, 2022d).

Ao fim, ficou consignado que a expressão "dados cadastrais" não incluía a interceptação de voz, a interceptação telemática, os dados cadastrais de usuários de IP, os serviços de agenda virtual oferecidos por empresas de telefonia, os dados cadastrais de *e-mails* e os extratos de conexão a partir de linha ou IP. Para esses dados, era necessário obter autorização judicial.

No entanto, podem ser requisitados sem controle judicial prévio, mas, estarão sempre sujeitos a controle judicial posterior:

a) a localização de terminal ou IMEI de cidadão em tempo real, por meio de ERB, por um período determinado, desde que necessário para reprimir os crimes contra a liberdade pessoal descritos no art. 13-A do CPP; o extrato de ERB;
b) os dados cadastrais de terminais fixos não listados em listas telefônicas divulgáveis e de terminais móveis; o extrato de chamadas telefônicas;
c) o extrato de mensagens de texto (SMS ou Multimedia Messaging Service MMS); e
d) os sinais para localização de vítimas ou suspeitos, após o prazo de 12 horas estabelecido no § 4º do art. 13-B do CPP (Brasil, 2024g).

5.13.5 Arguição de Descumprimento de Preceito Fundamental n. 1.143

Outra ação de suma importância é a ADPF n. 1.143 (Brasil, 2024h) que se originou da Ação Direta de Inconstitucionalidade por Omissão (ADO) n. 84.

Na ADO em questão, proposta em 13 de dezembro de 2023, a Procuradoria-Geral da República (PGR) pediu ao STF o reconhecimento de omissão legislativa do Congresso Nacional quanto à regulamentação do uso de ferramentas de monitoramento secreto (*softwares* espiões) de aparelhos de comunicação pessoal, como celulares e *tablets,* por órgãos e agentes públicos.

A PGR argumentou que, com os atuais avanços tecnológicos, houve uma proliferação global de ferramentas de intrusão virtual e que esses dispositivos tecnológicos eram capazes de interceptar comunicações telefônicas e telemáticas, ao infectar dispositivos eletrônicos com programas espiões (*spyware*), o que permitia aos intrusos monitorar conversas, escutar o som ambiente pelo microfone do dispositivo, captar imagens pelas câmeras frontal e traseira, determinar a localização em tempo real via GPS, capturar imagens da tela e acompanhar tudo o que é digitado (*keylogger*) ou visualizado pelo usuário em tempo real.

Ponderou o Órgão que os impactos nos direitos fundamentais resultantes do uso desregulado e ilegítimo dessas ferramentas pelo poder público haviam sido destacados em um relatório elaborado pelo Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos, que aponta não apenas violações à garantia do sigilo de dados e de comunicações, mas também às garantias da intimidade, da vida privada, do devido processo legal, e à liberdade de expressão, de

manifestação do pensamento e a de imprensa.

Dessa forma, indicou que a questão principal da controvérsia era o uso secreto e abusivo de softwares e ferramentas de intrusão virtual, sem autorização judicial e sem limites ou salvaguardas, em contrariedade à tutela do interesse público e aos deveres de proteção dos direitos fundamentais que se impõem em um Estado de Direito (Brasil, 2024h).

E é justamente a ausência de regulamentação para o uso, por órgãos e agentes públicos, de programas para a intrusão virtual remota e ferramentas de monitoramento secreto e invasivo de dispositivos digitais de comunicação pessoal que representa uma omissão legislativa, contrária às exigências do art. 5º, X e XII, da CRFB/1988, resultando em uma redução arbitrária e injustificada da proteção das garantias fundamentais previstas nas normas constitucionais.

Após manifestação da própria PGR pelo processamento da ADO como ADPF, “dada a necessidade que se percebe de uma visão holística da questão – que não se reduz apenas ao domínio da falta normas, mas também da qualidade das que têm sido pressupostas para as ações de investigação”, a ADO n. 84 (Brasil, 2024i) passou a ser processada como a ADPF n. 1.143.

A ação é recente e muita discussão ainda será travada em torno desse tema, mas já foi realizada uma audiência pública sobre o tema, em 11 de junho de 2024, de tal modo que podemos extrair dela alguns pontos levantados (Brasil, 2024i).

O representante do Ministério da Justiça e Segurança Pública (MJSP), Victor Epitácio Cravo Teixeira, destacou que o sigilo de comunicações pessoais conta com proteção constitucional, o qual só pode ser levantado mediante ordem judicial.

A segunda representante do MJSP, Lilian Cinta de Melo, destacou que “a atividade de inteligência não se confunde com práticas de vigilantismo e espionagem”, no que foi secundada por Rodrigo Morais Fernandes, representante da Polícia Federal.

Os riscos cibernéticos também foram levantados e apontados.

O defensor público-geral federal, Leonardo Magalhães, enfatizou a importância do debate sobre as consequências do uso de aplicativos de invasão e monitoramento digital, especialmente em relação ao direito à privacidade e à intimidade.

Gustavo Santana Borges, representante da Agência Nacional de Telecomunicações (ANATEL), informou que o órgão regulador possui poder legal para

editar dispositivos e regulamentos visando a garantir a segurança cibernética e evitar a quebra do fluxo de comunicações na camada da infraestrutura, o que exige rigorosos padrões de segurança para mitigação de riscos e vulnerabilidades, o que vem sendo realizado por meio de resoluções e atualizações normativas da ANATEL.

Tereza Gimenes, representante da Associação Brasileira de Indústria Elétrica e Eletrônica (ABINEE), destacou que a indústria de telefonia investe significativamente em ferramentas de controle para manter os produtos mais seguros, especialmente contra ferramentas de intrusão na rede.

Os integrantes das FFAA se mostraram adeptos ao uso de novas tecnologias de monitoramento remoto. Foi destacado que ferramentas de inteligência são utilizadas para a ajuda humanitária, como busca e salvamento, e que as atividades de inteligência e contrainteligência já contam com adequado controle, de modo que qualquer desvio de finalidade deve ser investigado pela Comissão Mista de Controle das Atividades de Inteligência (CCAI), órgão permanente do Congresso Nacional.

Lado outro, os perigos da permissão do uso de tais dispositivos também foram lembrados por Ana Bárbara Gomes, diretora do Instituto de Referência em Internet e Sociedade (IRIS), para quem as ferramentas intrusivas podem ser classificadas como “armas digitais que ameaçam a liberdade de expressão, o respeito ao sigilo dos dados e a própria democracia”, significando risco à soberania nacional, uma vez que envolvem o acesso a informações sensíveis (Brasil, 2024h).

Atualmente, dois projetos de lei sobre o regulamento de ferramentas de monitoramento remoto estão em tramitação, o PL n. 58/2024, de autoria do deputado federal Alberto Fraga e o PL n. 402/2024, de autoria do senador Alessandro Vieira.

Outros países já estão mais avançados no tratamento do tema, como é o caso da Alemanha.

Décadas após o célebre julgamento do caso do censo demográfico de 1983 pelo Tribunal Constitucional Federal, em que foi reconhecido o direito à autodeterminação informativa, o Tribunal Constitucional Federal postulou um novo direito fundamental: o denominado direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais, proclamado no contexto de uma reclamação constitucional ajuizada contra dispositivos de lei do Estado de Nordrhein-Westfalen, que regulamentavam e permitiam a denominada busca ou investigação remota de computadores de pessoas suspeitas de cometerem ilícitos criminais. Esta

lei permitia que a polícia daquela unidade da federação realizasse busca ou investigação secreta e remota de computadores de pessoas suspeitas de cometerem ilícitos criminais, autorizando ainda o monitoramento de todas as atividades do suspeito na internet, sendo declarada posteriormente inconstitucional. (Menke, 2019, p. 782).

O Tribunal Constitucional Federal considerou que a proteção existente para o direito fundamental à autodeterminação informativa não era suficiente para garantir a confiança na funcionalidade dos sistemas de tecnologia e informação usados para a comunicação. Esta confiança é crucial para o exercício do direito da personalidade. Uma proteção apenas antes da coleta e após a utilização de dados pessoais é insuficiente, se não incluir a proteção contra o acesso ao próprio sistema informático usado para a comunicação. Confiamos na operação correta, contínua e ininterrupta desse sistema, e sua infiltração ou manipulação geram comprometimentos e perigos à proteção da personalidade que não podem ser totalmente prevenidos apenas com a proteção dos dados coletados.

A infiltração de um sistema informático complexo, com a possibilidade de manipular seu funcionamento ou instalar *software* para modificar dados pessoais e processos de comunicação, cria fontes independentes de perigo, gerando riscos e comprometimento para os dados disponíveis no sistema. Uma defesa eficaz contra essas ameaças à personalidade exige uma proteção que vá além, focando também a infraestrutura, garantindo a autodeterminação com os dados, assim como a liberdade e integridade da comunicação. Infiltrações expõem esses sistemas a controle e manipulações externas (Hoffmann-Riem, 2020, p. 347-348, 2020).

Obviamente, a garantia de confidencialidade e integridade dos sistemas técnico-informacionais não é um direito absoluto, de modo que uma lei específica pode restringir esse direito, desde que respeitados certos limites, como a obediência à proporcionalidade e adequação do método empregado. O monitoramento de sistema informático deve ser submetido a um rigoroso controle de proporcionalidade, podendo ser efetivado por um órgão investigativo apenas como *ultima ratio* (Menke, 2019, p. 801).

Importante é notar como já se fazem discussões ao redor do mundo sobre a proteção da privacidade em face de dispositivos remotos.

Na Austrália, por exemplo, já existem leis em cada estado e território para regulamentar o uso de dispositivos de vigilância. Estas leis regem o uso de equipamentos para a realização de vigilância e atividades relacionadas, em particular para comunicar informações obtidas sob vigilância. As leis também preveem a emissão de mandados para conduzir vigilância por parte dos agentes da lei; mecanismos de monitoramento e fiscalização; exceções de interesse público; condições de admissibilidade das informações obtidas sob vigilância como prova; e restrições à fabricação e ao fornecimento de dispositivos de vigilância (Australian Law Reform Commission, 2014).

A *Emenda à Legislação de Vigilância* (Identificar e Perturbar) (Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act) introduziu três novos poderes para a Polícia Federal Australiana e a Comissão Australiana de Inteligência Criminal, para identificar e interromper atividades criminosas graves *on-line.* São os mandados de:

a) interrupção de dados;
b) controle de conta; e
c) atividade de rede.

Mandados (a) de interrupção de dados permitem a modificação e exclusão de dados para prevenir o cometimento de crimes graves, como a distribuição de material de abuso infantil; os (b) de controle de conta permitem o controle da conta on-line de uma pessoa para reunir evidências sobre atividades criminosas e avançar uma investigação criminal; e os (c) de atividade de rede permitem a coleta de inteligência sobre atividades criminais graves realizadas por redes criminosas que operam on-line (Australian Government, 2021).

No Reino Unido, há o *Ato de Poderes Investigativos* (*Investigatory Powers Act*), que entrou em vigor em novembro de 2016. A partir de 27 de junho de 2018, as operações de interceptação de comunicações passaram a ser autorizadas por ele, com a restrição de que mandados que autorizam a interceptação só podem ser emitidos por um Secretário de Estado, e devem ser aprovados por um Comissário Judicial independente do Escritório do Comissário de Poderes de Investigação (Investigatory Powers Act, 2016).

O Parlamento Europeu, por sua vez, aprovou a Recomendação P9_TA (2023)0244, que trata de investigação sobre a utilização do *software* espião de vigilância Pegasus e equivalentes, de que depreendemos que:

> 2. manifesta a firme convicção de que as violações destes direitos e liberdades fundamentais revestem-se de uma importância decisiva para o respeito pelos princípios jurídicos comuns estabelecidos nos Tratados e noutras fontes, e observa que a própria democracia está em jogo, uma vez que a utilização de software espião em políticos, na sociedade civil e nos jornalistas tem um efeito dissuasor e afeta gravemente o direito de reunião pacífica, a liberdade de expressão e a participação pública;
> 3. Condena veementemente a utilização de software espião pelos governos dos Estados-Membros, ou por membros de autoridades ou instituições do Estado, para monitorizar, chantagear, intimidar, manipular e descredibilizar membros da oposição, críticos e a sociedade civil, e assim eliminar o controlo democrático e a liberdade de imprensa, manipular as eleições e comprometer o Estado de direito, tomando como alvo juízes, procuradores do Ministério Público e advogados para fins políticos; (União Europeia , 2023).

Em editorial do Instituto Brasileiro de Ciências Criminais (IBCCRIM), em que se discorreu sobre a utilização de equipamentos de monitoramento remoto e espionagem, foi assinalado que

> desde 2021, o assunto ganhou notoriedade, quando veículos de imprensa revelaram que governos em vinte e quatro países teriam adquirido e utilizado o software espião Pegasus, da empresa israelense NSO Group, para hackear e vigiar secretamente jornalistas, advogados, ativistas e opositores políticos, incorrendo em violações gravíssimas de direitos humanos (Os Riscos, [...], 2024).

No Brasil, seguimos aguardando o pronunciamento da Suprema Corte e a atividade legiferante do Congresso Nacional, mas com a recomendação de que os princípios constitucionais sejam sempre levados em consideração, antes da autorização do uso de equipamentos potencialmente fragilizadores de princípios fundamentais, o que acaba por enfraquecer o próprio Estado Democrático de Direito.

5.14 Síntese do capítulo

As provas digitais são uma realidade jurídica, não só inexorável, mas, também, cada vez mais onipresente, atraindo crescente atenção de juristas e legisladores que discutem temas multidisciplinares, que, por vezes, colocam frente a frente valores constitucionais.

Assim é que foram apresentados e discutidos alguns conceitos tecnológicos essenciais para a devida compreensão da matéria, como endereços IP, servidores, registros e rede de criptografia.

Também, procuramos conceituar as provas digitais, indicar sua natureza jurídica e discorrer suas características essenciais.

Apontamos a diferença entre fontes abertas e fechadas, cada qual importante para o operador do direito saber qual procedimento adotar diante de cada caso, bem como demonstramos que há em curso um giro do sistema de provas típicas para um de provas atípicas no direito probatório.

Também, discutimos a legislação relacionada à matéria, como o MCI, Lei n. 12.965, de 23 de abril de 2014, considerado por muitos como a “Constituição da Internet”, a Lei Geral de Proteção de Dados, Lei n. 13.709, de 14 de agosto de 2018, que cuida da proteção de dados no Brasil, a Medida Provisória n. 2.200-2, de 24 de agosto de 2001, que Institui a ICP-Brasil, destrinchando sua estrutura, a fim de demonstrarmos sua importância, para conferir autenticidade e integridade aos documentos digitais.

Além disso, diversas outras leis foram citadas e discutidas, uma vez que a legislação sobre a matéria ainda se encontra dispersa e não consolidada. Em virtude dessa lacuna, foi apresentado o PL n. 4.939/20, de autoria do deputado federal Hugo Leal, do PSD/RJ, em 15 de outubro de 2020.

O PL “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” (Leal, 2020) e, esperamos, irá consolidar a matéria, a fim de que as diretrizes sobre o tratamento da matéria se tornem mais uniformes.

Os pressupostos de validade e utilidade das provas digitais foram expostos a partir da noção de confiabilidade da prova, especialmente levando em conta o suporte

em que esta é coletada e preservada. Com isso, aparece a necessária garantia de autenticidade e integridade da prova, estes pressupostos intrínsecos da prova digital, bem como a preservação da cadeia de custódia, que visa justamente a garantir a autenticidade e integridade da prova digital.

Fizemos alguns apontamentos sobre a produção e preservação das provas digitais, com a exposição de algumas tecnologias utilizadas com esse condão.

Tratamos, em subseção própria, do binômio prova digital e privacidade. Entretanto, como a leitura deste capítulo comprova ter esse tema sido nele, onipresente, e deixando claro que uma das maiores preocupações hodiernas quanto ao referido tema é justamente pelo equilíbrio entre privacidade e provas digitais.

Ainda foi objeto de estudo deste capítulo o ônus da prova digital, que mereceu especial destaque dadas as peculiaridades da matéria.

Os metadados, em virtude de sua importância para o estudo do tema, foram abordados em subseção própria, tendo sido de extrema utilidade para a elucidação de alguns fatos. Isso, porquanto, é aquilo que “não se vê, mas que muito revela” que conta, e se encontram presentes em fotografias, arquivos de texto, planilhas, vídeos, mensagens, e tudo mais que possamos imaginar.

Provas digitais em espécie foram apontadas, cada qual com sua peculiaridade, quando não várias, a exemplo dos mensageiros instantâneos que suscitam controvérsias sobre vários aspectos, alguns deles atualmente em discussão no STF.

Aliás, discussões no STF compõem a última subseção do capítulo, no qual demonstramos os princípios em jogo na discussão de provas digitais, como soberania nacional, cooperação internacional, privacidade, intimidade, liberdade de expressão, autodeterminação informativa e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais, dentre outros.

6 CONSIDERAÇÕES FINAIS

A pesquisa, que começou com o condão de averiguar a compatibilidade entre o instituto das provas digitais e o modelo de processo constitucional atualmente vigente no Brasil, demonstrou que não só há plena compatibilidade, como também é desejável que assim o seja.

Em uma sociedade que muda - arriscamos dizer – como nunca antes, o Direito deve ser instrumento ativo a conduzir os cursos pelos quais a sociedade seguirá, de modo que a realidade impõe a proatividade do Direito. Não se trata de meras palavras, mas de uma constatação baseada no que já foi, é e continuará sendo observado com crescente evidência.

Assim, foi feita uma breve introdução à Teoria Geral das Provas, de modo a destacar os elementos essenciais do que viria a conduzir o estudo.

Em seguida, foi feita a apresentação da perspectiva sobre a qual a pesquisa foi desenvolvida, a do processo constitucional, com destaque para os princípios fundamentais que norteiam a produção probatória, úteis ao estudo da matéria que é o objeto desta pesquisa: as provas digitais.

A fim de concatenar o estudo das provas tradicionais com o das provas digitais, incluímos um capítulo dedicado às transformações tecnológicas que culminaram em um giro linguístico, resultando no uso crescente de provas digitais nos processos judiciais.

No capítulo em que, efetivamente, as provas digitais foram abordadas e discutidas, pudemos constatar a notável diferença que apresentam em relação às provas típicas, muito em virtude do suporte em que foram coletadas, manuseadas e preservadas: o digital. Definitivamente, um fato que ocorre no mundo virtual, ou mesmo no físico, e é preservado em ambiente virtual, está sujeito a todo tipo de adulterações e manipulações, de modo que a melhor forma de permitir seu ingresso nos autos é por meio de um rígido processo que garanta a autenticidade e a integridade das provas, com a preservação da cadeia de custódia. Isso fica muito claro no processo penal, que envolve o direito fundamental à liberdade do acusado, já havendo várias decisões sobre a necessária observância desses elementos, sob pena de nulidade dessas provas. Obviamente, tratando-se de direitos disponíveis, a parte poderá apresentar a prova sem garantir sua autenticidade e a integridade, mas,

correrá o risco de ter a prova impugnada e não conseguir se desincumbir do ônus de atestar a veracidade da prova levada aos autos.

Ademais, notamos que o tema das provas digitais sempre suscita discussão sobre outros temas da maior relevância jurídica, como a soberania, caso da ADC n. 51, apreciada pelo STF, privacidade, tema comum a vários julgados de todos os tribunais, intimidade, liberdade de expressão e segurança pública.

Concluímos, portanto, que as provas digitais se tornaram uma realidade incontornável, devendo ser analisadas à luz do modelo processual constitucional, e sempre respeitar os princípios que regem a atividade probatória.

Ponderamos, entretanto, que a discussão e análise não se exaure neste texto. A revolução tecnológica, que abrange todas as esferas, coloca em jogo diversos princípios fundamentais. Diante disso, o Estado Democrático de Direito deve mobilizar todas as suas estruturas de Poder – Executivo, Legislativo e Judiciário – para assegurar a prevalência dos direitos fundamentais mais preciosos para essa sociedade, os quais, em última instância, formam sua base estruturante.

REFERÊNCIAS

ABELLÁN, Marina Gascón. **Os fatos no direito:** bases argumentativas da prova. Tradução de Ravi Peixoto. São Paulo: Juspodivm, 2022

ALMEIDA, Cleber Lúcio. **Elementos da teoria geral da prova:** a prova como direito humano e fundamental das partes do processo judicial. São Paulo: LTr, 2013.

AMENDOEIRA JÚNIOR, Sidnei. **Manual de direito processual civil:** teoria geral do processo e fase de conhecimento em primeiro grau de jurisdição. 2. ed. São Paulo: Saraiva, 2012. v. 1.

ARAUJO, Ezequiel; COSTA, Glayson. **Com câmeras, sensores e microfone, alunos poderão pedir revisão da prova prática, diz Detran**. Teresina: Portal o Dia, 24 ago. 2023. Disponível em: https://portalodia.com/noticias/teresina/com-cameras-sensores-e-microfone-alunos-poderao-pedir-revisao-da-prova-pratica-diz-detran-400253.html. Acesso em: 22 jul. 2024.

ARISTÓTELES. **Metafísica.** Tradução de Leonel Vallandro. Porto Alegre: Globo, 1969.

ASCENSI, Felipe. **Sociedade caminha cada vez mais rápido que o direito**. [São Paulo: Consultor Jurídico, 10 nov. 2013. Disponível em: https://www.conjur.com.br/2013-nov-10/felipe-asensi-sociedade-caminha-cada-vez-rapido-direito. Acesso em: 31 mar. 2023.

ASSANGE, Julian *et al*. **Cypherpunks:** liberdade e o futuro da internet. Tradução de Cristina Yamagami. São Paulo: Boitempo, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27037/2013:** tecnologia da informação: técnicas de segurança - diretrizes para identificação, coleta, aquisição e preservação de evidências digitais. Rio de Janeiro: ABNT, 2014.

AUSTRALIAN LAW REFORM COMMISSION**.** Surveillance devices. *In*: AUSTRALIAN LAW REFORM COMMISSION**. Serious invasions of privacy in the digital era.** Sydney: ALRC, 2014. Disponível em: https://www.alrc.gov.au/wp-content/uploads/2019/08/fr123_14._surveillance_devices.pdf. Acesso em: 7 jul. 2024.

AUSTRALIAN GOVERNMENT. S**urveillance Legislation Amendment (Identify and Disrupt) Act 2021**. [Áustria]: Affairs, 2021. Disponível em: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/surveillance-legislation-amendment-identify-and-disrupt-act-2021. Acesso em: 7 jul. 2024.

BARACHO, José Alfredo de Oliveira. **Direito processual constitucional:** aspectos contemporâneos. Belo Horizonte: Fórum, 2008.

BARACHO JÚNIOR, José Alfredo de Oliveira. **Processo e Jurisdição Constitucional**. **Revista Meritum**, Belo Horizonte, v. 18, n. 4, p. 10-26, 2023. DOI: https://doi.org/10.46560/meritum.v18i4.9059.

BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELLI, Guilherme. **Investigação digital em fontes abertas.** Rio de Janeiro: Brasport, 2017.

BARRETO JUNIOR, Irineu Francisco; LEITE, Beatriz Salles Ferreira. Responsabilidade civil dos provedores de aplicações por ato de terceiro na lei 12.965/14 (marco civil da internet). **Revista Meritum,** Belo Horizonte, v. 18, n. 4, p. 10-26, 2023. DOI: https://doi.org/10.46560/meritum.v18i4.9059.

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo:** os conceitos fundamentais e a construção do novo modelo. 11. ed. São Paulo: Saraiva, 2023.

BARZOTTO, Luciane Cardoso. A prova digital como meio de prova atípica: aspectos teóricos e um caso prático. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle; AZEVEDO NETO, Platon Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 95-106.

BAZZELL, Michael. **Open source intelligence techniques:** resources for searching and analyzing online information. 8. ed. Nevada: CCI Publishing, 2021.

BERTACHINI, Danielle. **Provas digitais:** fontes restritas. [*S. l.*]: TRT, 2021. Disponível em: https://portal.trt12.jus.br/sites/default/files/2021-08/Ju%C3%ADza%20Danielle%20Bertachini.pdf. Acesso em: 5 jun. 2024.

BESSA, Leonardo Roscoe. **A Lei Geral de Proteção de Dados e o direito à autodeterminação informativa**. [São Paulo]: Consultor Jurídico, 26 out. 2020. Disponível em https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa/. Acesso em 11 de junho de 2024.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e a proteção dos dados do consumidor.** São Paulo: Grupo Almedina, 2022. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556277066/. Acesso em 11 de junho de 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988:** Brasília, DF: Presidência da República, [2024a]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 15 dez. 2024.

BRASIL. **Decreto nº 3.810, de 2 de maio de 2001**. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997, corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001. Brasília, DF: Presidência da República, 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm. Acesso em: 1 abr. 2024.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para dispor sobre a proteção de dados pessoais e a segurança da informação na Internet. Brasília, DF: Presidência da República, 2016a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 1 abr. 2024.

BRASIL. **Decreto nº 10.278, de 18 de março de 2020.** Dispõe sobre o Comitê Interministerial de Governança de Dados e sobre o compartilhamento de bases de dados no âmbito da administração pública federal. Brasília, DF: Presidência da República, 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10278.htm. Acesso em: 10 abr. 2024.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023a. Disponível em https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 2 abr. 2024.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Brasília, DF: Presidência da República, [2024b]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 12 maio 2024.

BRASIL. **Emenda Constitucional nº 115, de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022a. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 20 mar. 2024.

BRASIL. Instituto Nacional de Tecnologia da Informação. **Estrutura**. Brasília: ITI, 2024. Disponível em: https://estrutura.iti.gov.br/. Acesso em: 20 abr. 2024a.

BRASIL. **Lei nº 5.869, de 11 de janeiro de 1973**. Código de Processo Civil de 1973. Brasília, DF: Presidência da República, [2015]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L5869compilado.htm. Acesso em: 27 mar. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, [2022a]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 20 abr. 2024.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regula a interceptação de comunicações telefônicas, de informática e telemática. Brasília, DF: Presidência da República, [2019a]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 28 dez. 2023.

BRASIL. **Lei nº 9.472, de 16 de julho de 1997**. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Brasília, DF: Presidência da República, [2021a]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 5 fev. 2023.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei. Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 1 mar. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, [2024c]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 18 fev. 2024.

BRASIL. **Lei nº 11.419, de 19 de dezembro de 2006**. Brasília, DF: Presidência da República, [2022b].Dispõe sobre a informatização do processo judicial. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 30 mar. 2024.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Brasília, DF: Presidência da República, [2022c]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 fev. 2024.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Brasília, DF: Presidência da República, [2019b]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 3 jun. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2021b]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 abr. 2024.

BRASIL. **Lei nº 13.105, de 16 de março de 2015.** Código de Processo Civil. Brasília, DF: Presidência da República, [2024d]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm.htm. Acesso em: 9 dez. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, [2022d]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 dez. 2023.

BRASIL. **Lei nº 13.964**, de 24 de dezembro de 2019. Altera a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 30 maio 2024.

BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm. Acesso em: 24 maio 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Instituto Nacional de Tecnologia da Informação. **ICP-Brasil**. Brasília: ITI, 4 mar. 2024b. Disponível em: https://www.gov.br/iti/pt-br/assuntos/icp-brasil. Acesso em: 7 abr. 2024.

BRASIL. Serviços e Informações do Brasil. Finanças, Impostos e Gestão Pública. Brasília: Serviços, 16 set. 2024c. Disponível em: https://www.gov.br/pt-br/servicos/contratar-emissao-de-carimbo-do-tempo#:~:text=O%20que%20%C3%A9%3F,validade%20de%20sua%20assinatura%20digital. Acesso em: 7 abr. 2024.

BRASIL. Superior Tribunal de Justiça. (5ª Turma). Agravo em Recurso Especial n. 2.318.334/MG. Relator: Ministro Reynaldo Soares da Fonseca. **Diário da Justiça Eletrônico**, Brasília, 23 abr. 2024d. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?termo=2318334&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO. Acesso em: 20 jun. 2024.

BRASIL. Superior Tribunal de Justiça. (5ª Turma). Agravo Regimental no Habeas Corpus n. 828.054/RN. Relator: Ministro Joel Ilan Paciornick. **Diário da Justiça Eletrônico**, Brasília, 29 abr. 2024e. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301896150&dt_publicacao=29/04/2024. Acesso em: 15 jul. 2024.

BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso em Mandado de Segurança n. 59.716/RS. Relator: Ministro Sebastião Reis Júnior. Sexta Turma. **Diário da Justiça Eletrônico**, Brasília, 17 ago. 2021a. Disponível em:https://processo.stj.jus.br/jurisprudencia/externo/informativo/?aplicacao=informativo&acao=pesquisar&livre=interceptacao+telefonica+&refinar=S.DISP.&&b=INFJ&p=true&t=null&l=20&i=1. Acesso em: 25 jun. 2024.

BRASIL. Superior Tribunal de Justiça. (5ª Turma). Agravo Regimental no Recurso em Mandado de Segurança n. 68.119/RS. Relator: Ministro Jesuíno Rissato. **Diário da Justiça Eletrônico**, Brasília, 28 mar. 2022b. Disponível em: https://processo.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28%28AROMS.clas.+ou+%22AgRg+no+RMS%22.clap.%29+e+%40num%3D%2268119%22%29+ou+%28%28AROMS+ou+%22AgRg+no+RMS%22%29+adj+%2268119%22%29.suce. Acesso em: 12 jul. 2024.

BRASIL. Superior Tribunal de Justiça. (5ª Turma). Agravo Regimental no Recurso Ordinário em Habeas Corpus n. 143.169/RJ. Relator: Ministro Ribeiro Dantas. **Diário da Justiça**, Brasília, 2 mar. 2023b. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?termo=2021%2F0057395-6&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO. Acesso em: 2 maio 2024.

BRASIL. Superior Tribunal de Justiça. (5ª Turma). Agravo Regimental no Recurso Especial n. 2.052.180/MG. Relator: Ministro Ribeiro Dantas. **Diário da Justiça Eletrônico**, Brasília, 16 out. 2023c. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301787886&dt_publicacao=16/10/2023. Acesso em: 20 jun. 2024.

BRASIL. Superior Tribunal de Justiça. (5ª Turma). Agravo em Recurso Especial n. 2.309.888/MG. Relator: Ministro Reynaldo Soares da Fonseca. **Diário da Justiça Eletrônico**, Brasília, 30 out. 2023d. Disponível em https://processo.stj.jus.br/processo/pesquisa/?termo=2309888&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO. Acesso em: 24 jul. 2024.

BRASIL. Superior Tribunal de Justiça. (5ª Turma). Recurso em Habeas Corpus n. 77.836/PA. Relator: Ministro Ribeiro Dantas. **Diário da Justiça**, Brasília, DF, 12 fev. 2019b. Disponível em https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=92078000&num_registro=201602865444&data=20190212&tipo=5&formato=PDF. Acesso em: 15 maio 2024.

BRASIL. Superior Tribunal de Justiça (5ª Turma). Recurso em Habeas Corpus n. 186.138/SP. Relatora: Ministra Daniela Teixeira. **Diário da Justiça**, Brasília, 22 mar. 2024f. Disponível em: https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=236166044&tipo_documento=documento&num_registro=202303047252&data=20240403&formato=PDF. Acesso em: 6 jun. 2024.

BRASIL. Superior Tribunal de Justiça. (6ª Turma). Habeas Corpus n. 749.817/PR. Relator: Ministro Antonio Saldanha Palheiro. **Diário da Justiça Eletrônico**, Brasília, 14 abr. 2023e. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202200716193&totalRegistrosPorPagina=40&aplicacao=processos.ea. Acesso em: 26 jun. 2024.

BRASIL. Superior Tribunal de Justiça. (6ª Turma). Habeas Corpus n. 454.228/SC. Relatora: Ministra Laurita Vaz. **Diário da Justiça Eletrônico**, Brasília, 19 out. 2018a. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?termo=2018%2F0141168-0&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO. Acesso em: 22 jul. 2024.

BRASIL. Superior Tribunal de Justiça (6ª Turma). Recurso em Mandado de Segurança nº 68.119/RJ. Relator: Ministro Vice-Presidente do STJ. Brasília: STJ, 17 dez. 2021b. Disponível em:

hhttps://processo.stj.jus.br/processo/pesquisa/?src=1.1.2&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_processo=RMS68119. Acesso em: 12 jul. 2024.

BRASIL. Superior Tribunal de Justiça (6ª Turma). Recurso em Mandado de Segurança nº 68.487/PE. Relator: Ministro Vice-Presidente do STJ. Brasília: STJ, 15 mar. 2023f. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202200716193&totalRegistrosPorPagina=40&aplicacao=processos.ea. Acesso em: 26 jun. 2024.

BRASIL. Superior Tribunal de Justiça. (6ª Turma). Recurso em Habeas Corpus n. 99.735/SC. Relatora: Ministra Laurita Vaz. **Diário da Justiça Eletrônico**, Brasília, 12 dez. 2018b. Diáhttps://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1777437&num_registro=201801533498&data=20181212&peticao_numero=-1&formato=PDF. Acesso em: 6 jul. 2024.

BRASIL. Superior Tribunal de Justiça. Recurso em Mandado de Segurança n. 61.302/RJ. Recurso em Mandado de Segurança. Direito à Privacidade e à Intimidade. [...] Relator: Ministro Rogerio Schietti Cruz, 26 ago. 2020. **Diário da Justiça**, Brasília, 26 ago. 2020b. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201901991320&dt_pu. Acesso em: 25 jun. 2024.

BRASIL. Superior Tribunal de Justiça (4ª Turma). Recurso Especial n. 1.381.603/MS. Relator: Ministro Luis Felipe Salomão. **Diário da Justiça**, Brasília, 11 nov. 2016b. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=201300578761&totalRegistrosPorPagina=40&aplicacao=processos.ea. Acesso em: 11 jun. 2024.

BRASIL. Supremo Tribunal Federal. Ação Declaratória de Constitucionalidade nº 51. Ação Declaratória de Constitucionalidade. Normas de Cooperação Jurídica Internacional. [...]. Relator: Ministro Gilmar Mendes, 23 fev. 2023g. **Diário de Justiça Eletrônico,** Brasília, 28 abr. 2023. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15357625435&ext=.pdf. Acesso em: 4 jul. 2024.

BRASIL. Supremo Tribunal Federal. Ação Direita de Inconstitucionalidade n. 4.924/DF. Ação direta de inconstitucionalidade. Constitucional. Administrativo. Direitos fundamentais [...] Relator: Min. Gilmar Mendes, 4 nov. 2021. **Diário de Justiça Eletrônico**, Brasília, 29 mar. 2022c. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4382183. Acesso em: 5 jul. 2024.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 5.527. Relatora: Min. Rosa Weber, 8 abr. 2022. **Diário de Justiça Eletrônico**, Brasília, 12 abr. 2022d. Disponível em https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Acesso em: 15 dez. 2024.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 5.527/Distrito Federal. **Voto**. Brasília: STF, 2020c. Disponível em https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf. Acesso em 26 de junho de 2024.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Ação Direta de Inconstitucionalidade nº 5.642. Ação Direta de Inconstitucionalidade Direito Constitucional. Ação Direta De Inconstitucionalidade. [...]. Relator: Min. Edson Fachin, 18 abr. 2024. **Diário de Justiça Eletrônico**, Brasília, 22 ago. 2024g. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5117846. Acesso em: 30 jun. 2024.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 403/SE. Relator: Min. Edson Fachin, 20 abr. 2017. **Diário de Justiça Eletrônico**, Brasília, 25 abr. 2017. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acesso em: 20 dez. 2024.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 403/SE. **Voto**: síntese do voto. Brasília: STF, 2021c. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf. Acesso em: 19 jun. 2024.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental nº 1.143. Relator: Ministro Cristiano Zanin, 28 jun. 2024. **Diário de Justiça Eletrônico**, Brasília, 2 jul. 2024h. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814. Acesso em: 7 jun. 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade por Omissão** 84/Distrito Federal. Relator: Ministro Cristiano Zanin. Brasília: STF, 16 abr. 2024i. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15366173525&ext=.pdf. Acesso em: 7 jun. 2024.

BRASIL. Supremo Tribunal Federal. **Autoridades nacionais podem requisitar dados diretamente a provedores no exterior, decide STF**. Brasília: STF, 23 fev. 2023h. Disponível em https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=502922&ori=1. Acesso em: 1 jul. 2024.

BRASIL. Supremo Tribunal Federal. Mandado de Segurança nº 23.452. Comissão Parlamentar de Inquérito - Poderes de Investigação (Cf, art. 58, §3º) - Limitações Constitucionais [...] Relator: Min. Celso de Mello, 16 set. 1999. **Diário de Justiça Eletrônico**, Brasília, 12 maio 2000. Disponível em https://portal.stf.jus.br/processos/detalhe.asp?incidente=1763585. Acesso em: 20 maio 2024.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade n. 6.389**.** Ementa Medida Cautelar em Ação Direta de

Inconstitucionalidade [...]. Relatora: Min. Rosa Weber, 7 maio 2020. **Diário de Justiça Eletrônico**, Brasília, 12 nov. 2020d. Disponível em https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895168. Acesso em: 8 jul. 2024.

BRASIL. Supremo Tribunal Federal. **Processo:** ADPF/403. Brasília: STF, 2016c. Disponível em: https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarp rocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=4975500. Acesso em: 16 jun. 2024.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade n. 6.387.** Medida Cautelar em Ação Direta de Inconstitucionalidade [...] Relatora: Min. Rosa Weber. Brasília, DF: STF, 12 nov. 2020e. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente= 5895165. Acesso em: 4 jul. 2024.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n. 1.301.250/RJ. Direito Constitucional. Direito Processual Penal. Quebra de Sigilo de Dados Pessoais [...]. Relatora: Ministra Rosa Weber, 27 maio 2021. **Diário de Justiça Eletrônico**, Brasília, 8 jun. 2021d. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6059876. Acesso em: 29 jul. 2024.

BRASIL. Supremo Tribunal Federal. **STF encerra audiência pública com diversidade de visões sobre as ferramentas de monitoramento**. Brasília: STF, 11 jun. 2024j. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?id Conteudo=547319&ori=1. Acesso em: 29 jul. 2024.

BRASIL. Supremo Tribunal Federal. **STF valida repasse de dados telefônicos, sem autorização judicial, para investigação de crimes graves**. Brasília: STF, 18 abr. 2024k. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.a sp?idConteudo=532701&ori=1. Acesso em: 29 jul. 2024.

BRASIL. Tribunal Regional do Trabalho (2ª Região). **CumSen 1000223-30.2020.5.02.0332.** 2ª Vara do Trabalho de Itapecerica da Serra. São Paulo: TRT2, 2021e. Disponível em: https://pje.trt2.jus.br/consultaprocessual/detalhe-processo/1000223-30.2020.5.02.0332/1#811eb16. Acesso em: 4 abr. 2024.

BRASIL. Tribunal Regional Federal (3ª Região). **Apelação Criminal n. 0002074-05.2018.4.03.6102**. Relator Desembargador: Maurício Kato. São Paulo, TRF3, 4 ago. 2020f. Disponível em https://pje1g.trf3.jus.br/pje/ConsultaPublica/Detalhe ProcessoConsultaPublica/listView.seam?ca=8a683befeb90231b3b05c2e16438c4af1 e23c0256679d961. Acesso em: 9 jun. 2024.

BRASIL. Tribunal Regional do Trabalho (3ª Região). **Processo nº 0012565-21.2022.5.03.0000 (MSCiv).** Relatora: Paula Oliveira Cantelli. Belo Horizonte: TRT-3, 23 mar. 2023i. Disponível em: https://pje-consulta.trt3.jus.br/consultaprocessual/detalhe-processo/0012565-21.2022.5.03.0000/2#2fd061b. Acesso em: 12 maio 2024.

BRASIL. Tribunal Regional do Trabalho (3ª Região). **ROT n. 0010419-81.2022.5.03.0137.** Relator: Desembargador Ricardo Marcelo Silva. Belo Horizonte: TRT-3, 11 jun. 2024l. https://pje-consulta.trt3.jus.br/consultaprocessual/detalhe-processo/0010419-81.2022.5.03.0137/2#216afcc. Acesso em: 18 jul. 2024.

BRASIL. Tribunal Regional do Trabalho. (4ª Região). Enunciado n. 27 da Escola Judicial. *In*: BRASIL. Tribunal Regional do Trabalho. **Grupos de estudos análise normativa e análise jurisprudencial**. Porto Alegre: TRT-4, 2023j. Disponível em: https://www.trt4.jus.br/portais/escola/grupo-de-estudos-analise-normativa. Acesso em: 29 maio 2024.

BRASIL. Tribunal Regional do Trabalho (12ª Região). **ATSum 0001080-82.2023.5.12.0050.** Relatora Des.: Maria Beatriz Vieira da Silva Gubert. Florianópolis: TRT-12, 9 maio 2024m. Disponível em: https://pje.trt12.jus.br/consultaprocessual/detalhe-processo/0001080-82.2023.5.12.0050/2#94fdb0b . Acesso em: 14 out. 2024.

BRASIL. Tribunal Regional Eleitoral de Pernambuco. **Recurso Eleitoral n. 0600026-47.2020.6.17.0007.** Relator Des.: Rodrigo Cahu Beltrão. Eleições 2020. Recurso Eleitoral. Representação. Ônus da Prova. Cerceamento de Defesa [...]. Recife: TER-PE, 13 nov. 2020g. Disponível em https://jurisprudencia.tre-pe.jus.br/#/jurisprudencia/pesquisa?expressaoLivre=0600026-47.2020.6.17.0007&tipoDecisao=Ac%25C3%25B3rd%25C3%25A3o%252CResolu%25C3%25A7%25C3%25A3o%252CDecis%25C3%25A3o%2520sem%2520resolu%25C3%25A7%25C3%25A3o&params=s. Acesso em 16 de julho de 2024.

BRASIL. Tribunal Superior do Trabalho. **Recurso Ordinário nº 23218-21.2023.5.04.0000.** Relator: Ministro Amaury Rodrigues Pinto Junior. Subseção II Especializada em Dissídios Individuais. Brasília, DF: TST, 14 jun. 2024n. Disponível em: https://consultaprocessual.tst.jus.br/consultaProcessual/resumoForm.do?consulta=1&anoInt=2023&numeroInt=503923. Acesso em: 16 jul. 2024.

BRENOL, Marlise. **Saiba o que é um hash criptográfico**. [Brasília]: SERASA, 20 mar. 2024. Disponível em https://www.serasa.com.br/premium/blog/saiba-o-que-e-hash-criptografico/. Acesso em: 17 maio 2024.

BREVE história da Internet. [*S. l.*]: Repositorium, 2024. Disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/3396/1/INTERNET.pdf. Acesso em: 17 maio 2024.

CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). **Comentários ao novo código de processo civil**. 2. ed. Rio de Janeiro: Forense, 2016.

CÂMARA, Alexandre Freitas. **Lições de direito processual civil.** 15. ed. Rio de Janeiro: Lumen Juris, 2006.

CAPANEMA, Walter Aranha. **Manual de direito digital:** teoria e prática. São Paulo: JusPodivm, 2024.

CARNELUTTI, Francesco. **As misérias do processo penal**. Tradução de Carlos Eduardo Trevelin Millan. 2. ed. São Paulo: Pilares, 2009.

CARNELUTTI, Francesco. **La prueba civil**. Tradução de Niceto Alcalá-Zamora y Castillo. 2. ed. Buenos Aires: Depalma, 1982.

CASTELLS, Manuel. **A sociedade em rede**. 8. ed. São Paulo: Ed. Paz e Terra, 2000.

CASTRO, Rosane Vieira; VIEIRA, Thaís Patrício. **WhatsApp como meio de prova no processo trabalhista**. Orlando, FL, USA: Ed. Ambra University Press, 2020.

CAVALCANTI, Gustavo Henrique de Vasconcellos. **Validade jurídica das provas digitais no processo administrativo disciplinar**. [*S. l.*]: CGU, 2018. Disponível em https://repositorio.cgu.gov.br/bitstream/1/31038/5/Artigo_Evidencias_digitais_no_PAD.pdf. Acesso em: 5 jul. 2024.

CEROY, Frederico Meinerg. **Os conceitos de provedores no marco civil da Internet.** [Belo Horizonte]: Migalhas 29 set. 2020. Disponível em: https://www.migalhas.com.br/depeso/211753/os-conceitos-de-provedores-no-marco-civil-da-internet. Acesso em: 28 jun. 2024.

COMOGLIO, Luigi Paolo. **Le prove civili**. Torino: UTET, 1999.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime (Convenção de Budapeste)**, adotada em 23 de novembro de 2001. [*S. l.*]: COE, 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso em: 9 jul. 2024.

CONSELHO DA JUSTIÇA FEDERAL. IV Jornada de direito civil: enunciado n. 297. *In*: CONSELHO DA JUSTIÇA FEDERAL. **Jornadas de direito civil I, III, IV e V** : enunciados aprovados. Coordenador: Ministro Ruy Rosado de Aguiar Júnior Brasília, DF: CJF, 2014. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/EnunciadosAprovados-Jornadas-1345.pdf. Acesso em: 6 fev. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Metas nacionais do poder Judiciário para 2023**. Brasília, DF: CNJ, 2023. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2023/01/metas-nacionais-aprovadas-no-16o-enpj.pdf. Acesso em: 20 nov. 2023.

COUTURE, Eduardo Juan. **Fundamentos do direito processual civil**. Tradução de Henrique Carvalho. Florianópolis: Conceito. 2008

DELLEPIANE, Antonio. **Nova teoria da prova**. Tradução de Érico Maciel. Rio de Janeiro: José Konfino, 1958.

DIAS, Ronaldo Brêtas de Carvalho. Las pruebas en el nuevo código de processo civil brasileño y procedimiento probatorio. *In*: SOARES, Carlos Henrique *et al*. (org**).**

Proceso democrático y garantismo procesal. Belo Horizonte: Arraes Editores, 2015. p. 152-163.

DIAS, Ronaldo Brêtas de Carvalho. **Processo constitucional e estado democrático de direito.** Belo Horizonte: Del Rey, 2022.

DICIONÁRIO de informática. ICP Brasil. Palestrante: Rodrigo Schaeffer. [São Paulo]: ICP, 18 jul. 2023. 1 vídeo (14 min.) Disponível em: https://www.youtube.com/watch?v=7d5EHYjYkQA. Acesso em: 12 abr. 2024.

DIDIER JÚNIOR, Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. **Curso de direito processual civil:** teoria da prova, direito probatório, decisão, precedente, coisa julgada e tutela provisória. 14. ed. Salvador: Jus Podivm, 2019.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.); MUCELIN, Guilherme (org.). **Direito digital:** direito privado e internet. 5. ed. Indaiatuba, SP: Foco, 2024. Cap. 2. 33-50. *E-book*.

ENGELMANN, Alana Gabriela. Blockchain e processo civil: a tecnologia como meio (a)típico de produção probatória. *In*: PINHO, Anna Carolina *et al*. (coord.). **Manual de direito na era digital.** Indaiatuba: Foco, 2023. p. 33-66.

EUROPEAN COUNCIL FOR NUCLEAR RESEARCH. **A short history of the web**. [*S. l.*]: CERN, 2024. Disponível em: https://home.cern/science/computing/birth-web/short-history-web. Acesso em: 12 dez. 2024.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. **Electronic evidence - a basic guide for first responders**. [*S. l.*]: ENISA, 2015. Disponível em: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders. Acesso em: 8 fev. 2024.

FACHINETTI, Aline Fuke; CAMARGO, Guilherme. **Convenção 108+**: o tratado de proteção de dados e a relevância do tema para o Brasil. [São Paulo]: Consultor Jurídico, 4 jul. 2021. Disponível em https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados/. Acesso em: 1 ago. 2024.

FELICIANO, Guilherme Guimarães. Prova oral obtida por meio de WhasApp e aplicativos similares: uma breve análise. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle; AZEVEDO NETO, Platon Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 212-218.

FERRARI, Pollyana. A hipermídia entrelaça a sociedade. *In:* FERRARI, Pollyana (org.). **Hipertexto, hipermídia:** as novas ferramentas da comunicação digital. 2. ed. São Paulo: Contexto, 2014. p. 35-39.

FERREIRA, Estevão. **O Neoprocessualismo e o Novo CPC**. [São Paulo]: Jusbrasil, 2015. Disponível em https://www.jusbrasil.com.br/artigos/o-neoprocessualismo-e-o-novo-cpc/316080045. Acesso em: 3 fev. 2024.

FERRER-BELTRÁN, Jordi. **Prova sem convicção:** standards de prova e devido processo legal. Tradução de Vitor de Paula Ramos. 2. ed. São Paulo: Jus Podivm, 2023a.

FERRER-BELTRÁN, Jordi. **Valoração racional da prova**. Tradução de Vitor de Paula Ramos. 3. ed. São Paulo: Jus Podivm, 2023b.

FIUZA, César Augusto de Castro; SÁ, Maria de Fátima Freire; DIAS, Ronaldo Brêtas de Carvalho. **Temas atuais de direito processual civil**. Belo Horizonte: Del Rey, 2011.

FORGIONI, Paula A.; MIURA, Maira Yuriko Rocha. O princípio da neutralidade e o Marco Civil da Internet no Brasil. **Revista Jurídica Luso-Brasileira**, v. 1, n. 4, p. 1269-1301, 2015. Disponível em: https://www.cidp.pt/revistas/rjlb/2015/4/2015_04_1269_1301.pdf. Acesso em: 3 fev. 2024.

FORTES, Olga Vishnevsky. Novos meios de busca da verdade: a geolocalização. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle; AZEVEDO NETO, Platon Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 235-246.

FÓRUM PERMANENTE DE PROCESSUALISTAS CIVIS**.** Enunciado n. 50. *In*: DIDIER Junior, Fredie *et al*. (coord.). **Rol de enunciados e repertório de boas práticas processuais do FPPC - Fórum Permanente de Processualistas Civis (2024)**. Brasília: Academia Edu, 16 mar. 2024. Disponível em: https://www.academia.edu/116460831/Rol_de_enunciados_e_repert%C3%B3rio_de_boas_pr%C3%A1ticas_processuais_do_FPPC_F%C3%B3rum_Permanente_de_Processualistas_Civis_2024_. Acesso em: 4 dez. 2024.

FRAGA, Alberto. **Projeto de Lei nº 58, de 2024**. Dispõe sobre a utilização, para fins de atividades de inteligência estatal, de investigação criminal, de controle ou de fiscalização fazendária federais, de programas informáticos de intrusão virtual remota ou ferramentas de monitoramento sigiloso de aparelhos digitais de comunicação pessoal, define crimes, e dá outras providências. Brasília: Câmara, 2024. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2416950. Acesso em: 8 jul. 2024.

FREITAS, Alexandre Câmara. **O novo processo civil brasileiro.** São Paulo: Atlas, 2015.

FURLANETO NETO, Mário Furlaneto; SANTOS, José Eduardo Lourenço dos. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. **Revista Em Tempo**, v. 20, n. 1, nov. 2020. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 12 jul. 2024.

FUX, Luiz. **Curso de direito processual civil.** 6. ed. Rio de Janeiro: Forense, 2023.

GEMIGNANI, Teresa Aparecida Asta. Ônus da prova digital no processo do trabalho. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle; AZEVEDO NETO, Platon

Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 107-120.

GILL, Lex; ISRAEL, Tamir; PARSONS, Christopher**. Shining a light on the encryption debate:** a canadian field guide. Ottawa: Tspace, 2018. Disponível em https://tspace.library.utoronto.ca/bitstream/1807/94803/1/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf. Acesso em: 28 jun. 2024.

GOLDMAN, Alvin. **Knowledge in a social world**. Oxford: Oxford University Press, 1999.

GUIMARÃES, Natália Chernicharo. **Processo coletivo em rede**. Belo Horizonte: D'Plácido, 2023.

HARAWAY, Donna; KUNZRU, Hari**. Antropologia do ciborgue:** as vertigens do pós-humano. Organização e tradução de Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica Editora, 2009.

HAACK, Susan. **Filosofia das lógicas**. Tradução de Cezar Augusto Mortari e Luiz Henrique de Araújo Dutra. São Paulo: UNESP, 2002.

HARTMANN, Rodolfo Kronemberg. **Curso completo de processo civil.** 8. ed. São Paulo: Rideel, 2023.

HERNANDEZ, Ary César. **Sem revisão**: o contraditório e a ampla defesa no processo administrativo. São Paulo: MPSP, 2024. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_publicacao_divulgacao/doc_gra_doutrina_civel/civel%2052.pdf. Acesso em 15 de março de 2024.

HOFFMANN-RIEM, Wolfgang. A proteção de direitos fundamentais da confidencialidade e da integridade de sistemas próprios de tecnologia da informação. **Revista de Direito Civil Contemporâneo,** São Paulo, v. 7, n. 23. p. 329-365, abr./jun. 2020.

INVESTIGATORY POWERS ACT. **GCHQ's mission is predominantly governed by the Investigatory Powers Act 2016**. [*S. l.*]: GCHQ, 2016. Disponível em https://www.gchq.gov.uk/information/investigatory-powers-act#:~:text=The%20act%20does%20three%20things,to%20them%20clear%20and%20understandable. Acesso em: 16 abr. 2024.

LAGIER, Daniel González. **Quaestio facti:** ensaios sobre a prova, causalidade e ação**.** Tradução de Luis Felipe Kircher. São Paulo: Juspodivm, 2022.

LEAL, Hugo. **Projeto de Lei nº 4.939, de 2020**. 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. Brasília: Câmara, 2020. Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264324. Acesso em: 16 abr. 2024.

LEAL, Rosemiro Pereira. **Processo e eticidade familiar constitucionalizada**. [Belo Horizonte]: IBDFAM, 2023. Disponível em: https://ibdfam.org.br/_img/congressos/anais/151.pdf. Acesso em: 6 jan. 2023.

LEAL, Rosemiro Pereira. **Teoria geral do processo**: primeiros estudos. 14. ed. Belo Horizonte: Fórum, 2018.

LEINER, Barry M. *et al*. **Brief history of the Internet**. [*S. l*.]: Internet Society. 1997. Disponível em: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf. Acesso em: 22 jul. 2024.

LÉVY, Pierre. **As tecnologias da inteligência:** o futuro do pensamento na era da informática. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1993.

"LIGA e desliga" em câmeras de policiais seguirá regras rígidas e desvios serão penalizados, diz governo de SP. Brasília: CNN Brasil, 25 maio 2024. Disponível em https://www.cnnbrasil.com.br/nacional/liga-e-desliga-em-cameras-de-policiais-seguira-regras-rigidas-e-desvios-serao-penalizados-diz-governo-de-sp/. Acesso em 23 de julho de 2024.

LIGUORI, Carlos. **Direito e criptografia.** São Paulo: Saraiva, 2022.

LIMA, Ana Cláudia Pires Ferreira de. Muito além da imagem da fotografia digital: a utilização dos metadados como prova judicial. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle; AZEVEDO NETO, Platon Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 259-276.

LIU, Yizhong *et al*. Building blocks of sharding blockchain systems: concepts, approaches, and open problems. **Computer Science Review**, v. 46, 100513, 2022.

LONGHI, João Victor Rozatti. Marco civil da internet no brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. *In*: SOUZA, Allan Rocha de *et al*. (coord.); MUCELIN, Guilherme (org.). **Direito digital**: direito privado e internet. 5. ed. Indaiatuba, SP: Foco, 2024. Cap. 6. 121-152. *E-book*.

LOPES, Bráulio Lisboa. Uma visão do direito processual segundo a teoria neoinstitucionalista do processo. **Revista Jus Navigandi**, Teresina, ano 8, n. 159, dez. 2003. Disponível em: https://jus.com.br/artigos/4519. Acesso em: 5 jan. 2023.

LUCON, Paulo Henrique dos Santos. Capítulo XII – Das provas. Seção I - Das disposições gerais (arts. 369 a 380). *In*: CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). **Comentários ao novo código de processo civil**. 2. ed. Rio de Janeiro: Forense, 2016.

LUDGERO, Paulo, MEDEIROS, Patrícia; RIBEIRO, Valéria. Meios de Validação da Prova Digital: Verifact; HTTrack; Wayback Machine; Ata Notarial; OriginalMy; Arquivos em Nuvem. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle;

AZEVEDO NETO, Platon Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 219-234.

LYNCH, Michael. **The nature of truth:** classic and contemporary perspectives. Cambridge: The MIT Press, 2001.

MACHADO, Herminegilda Leite. Prova digital e privacidade. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle; AZEVEDO NETO, Platon Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 158-174.

MACIEL JÚNIOR, Vicente de Paula. A liberdade da informação na rede, o modelo de processo coletivo participativo em ambiente protegido e a luta contra a escravidão digital. **Virtuajus**, v. 3, n. 5, p. 11-33, jan. 2019.

MAGALHÃES, Maria Cristina Faria. **A evolução da avaliação processual das provas ilícitas.** Revista do Ministério Público, Rio de Janeiro, n. 23, p. 179-193, jan./jun. 2006.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Prova e convicção**. 6. ed. São Paulo: Thomson Reuters Brasil, 2022.

MARQUES, José Frederico. **Instituições de direito processual civil**. Rio de Janeiro: Forense, 1959. v. 3.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira**, v. 5, n. 1, 2019. Disponível em: https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf. Acesso em: 10 dez. 2024.

MINAS GERAIS. Tribunal de Justiça (4ª Câmara). **Apelação Cível n. 1.0000.21.203611-5/001**. Rel.: Des.: Roberto Apolinário de Castro. Belo Horizonte, 9 mar. 2022. Disponível em: https://encurtador.com.br/YizBN. Acesso em: 2 jun. 2024.

MIRANDA, Pontes de. **Comentários ao código de processo civil.** São Paulo: Forense, 1974. t. 4.

MÜLLER, Julio Guilherme. **Negócios processuais e desjudicialização da produção da prova: Análise econômica e jurídica.** São Paulo: RT, 2017. *E-book*.

NEVES, Daniel Amorim Assumpção. **Manual de direito processual civil**. 7. ed. Rio de Janeiro: Forense, 2015.

NEVES, Flávia. **Sinônimo de ônus**. [*S. l.*]: Dicionário online de sinônimos, 2024. Disponível em https://www.sinonimos.com.br/onus/. Acesso em: 2 mar. 2024.

NUNES, Dierle. **Por que a reforma do código civil merece ser aprovada? A defesa dos nossos neurodireitos.** [São Paulo]: Consultor Jurídico, 24 abr. 2024. Disponível em: https://www.conjur.com.br/2024-abr-24/por-que-a-reforma-do-codigo-civil-merece-ser-aprovada-defesa-dos-nossos-neurodireitos/. Acesso em: 3 jun. 2024.

NUNES, Dierle; BAHIA, Alexandre; PEDRON, Flávio. **Teoria geral do processo.** 2. ed. Salvador: JusPodivm, 2021.

OMMATI, José Emílio Medauar. **Uma teoria dos direitos fundamentais.** 8. ed. Belo Horizonte: Conhecimento Livraria e Distribuidora, 2021. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 25 jun. 2024.

O QUE é Sistema Autônomo. [*S. l.*]: Dendrites Studio, 2024. Disponível em https://dendrites.io/glossario/o-que-e-sistema-autonomo/. Acesso em: 20 mar. 2024.

OS RISCOS de um açodado uso de softwares espiões na persecução penal. **Boletim IBCCRIM,** v. 32, n. 380, p. 2-4, 2024. Disponível em https://publicacoes.ibccrim.org.br/index.php/boletim_1993/issue/view/55/40. Acesso em: 9 jul. 2024.

PAOLINELLI, Camilla Mattos. **O ônus da prova no processo democrático**. Rio de Janeiro: Lumen Juris, 2014.

PAOLINELLI, Camilla Mattos. O que é processo constitucional? **Revista Eletrônica do Curso de Direito - PUC Minas Serro,** n. 13. jan./jul. 2016. Disponível em: http://periodicos.pucminas.br/index.php/DireitoSerro/article/view/12043/10152. Acesso em: 9 jul. 2023.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. **Revista Brasileira de Direito Civil**, Belo Horizonte, n. 16, p. 35-56, abr./jun. 2018.

PINHEIRO, Patrícia Peck. **Direito digital**. São Paulo: Saraiva, 2021. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 9 jul. 2023.

PASTORE, Guilherme de Siqueira. Considerações sobre a autenticidade e a integridade da prova digital. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 63-79, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/i_5_considera%C3%A7%C3%B5es_autenticidade.pdf?d=637250343071305756. Acesso em: 5 fev.2024.

PONZONI, Christian. **Standards de prova no processo civil brasileiro.** Porto Alegre: PUC/RS, 2020. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/9175/5/DIS_CHRISTIAN_PONZONI_COMPLETO.pdf. Acesso em: 4 maio 2023.

POPPER, Karl. **Conhecimento objetivo:** uma abordagem evolucionária. Tradução de Bruno Mendes dos Santos. Petrópolis: Vozes, 2022.

PRAYUDI, Yudi; AZHARI, SN. Digital Chain of Custody: State of the Art. **International Journal of Computer Applications**, v. 114, n. n. 5, March 2015. Disponível em https://www.researchgate.net/profile/Yudi-Prayudi/publication/273694917_Digital_Chain_of_Custody_State_of_The_Art/links/5

508eb510cf2d7a2812b6945/Digital-Chain-of-Custody-State-of-The-Art.pdf. Acesso em: 20 nov. 2024.

PROVAS digitais e crimes na era da tecnologia. Datacertify**.** 28 set. 2023. 1 vídeo (1:30 min.). Disponível em: https://www.youtube.com/watch?v=VvWRo_Ofg88. Acesso em: 20 nov. 2024.

PROVAS digitais. Palestrante: Dierle Nunes. Rio de Janeiro: Congresso Inovações Tecnológicas na EMERJ, 15 dez. 2013. 1 vídeo (18:12 min.) Disponível em: https://www.youtube.com/watch?v=WLg5djoqqZ0. Acesso em: 30 jan. 2024.

PROVA no direito digital. Palestrante: TAMER, Maurício. [São Paulo]: Vimeo, 2020. 1 vídeo (4min.). Disponível em: https://vimeo.com/390716558. Acesso em: 29 mar. 2024.

RAMOS, Vitor de Paula. **Ônus da prova no processo civil**. Do ônus ao dever de provar. 3. ed. São Paulo: JusPodivm, 2022.

RAY Tomlinson, o criador do e-mail, morre aos 74 anos nos EUA. **Correio Braziliense**, 7 mar. 2016. Disponível em: https://www.correiobraziliense.com.br/app/noticia/tecnologia/2016/03/07/interna_tecnologia,520910/ray-tomlinson-o-criador-do-e-mail-morre-aos-74-anos-nos-eua.shtml. Acesso em: 12 jul. 2024.

REALE, Miguel. **Verdade e conjetura**. 3 ed. Rio de Janeiro: Nova Fronteira, 2001.

RIO GRANDE DO NORTE (21ª Região). **TRT-RN**: justa causa para trabalhadora com atestado que publicou imagens dançando em festa. Natal: TRT, 24 abr. 2023. Disponível em: https://www.trt21.jus.br/noticias/noticia/trt-rn-justa-causa-para-trabalhadora-com-atestado-que-publicou-imagens-dancando-em. Acesso em: 22 jul. 2024.

RIO GRANDE DO SUL. (Décima Câmara Cível.). Tribunal de Justiça. **Apelação Cível, Nº 50009577720228210132.** Relator: Min.: Túlio de Oliveira Martins. Porto Alegre: TJRS, 30 nov. 2023. Disponível em https://www.tjrs.jus.br/buscas/jurisprudencia/exibe_html.php. Acesso em: 2 jun 2024.

SAMPIETRO, Luiz Roberto Hijo**. O direito à prova, os poderes de instrução do juiz e a boa-fé objetiva no CPC/15.** [São Paulo]: Consultor Jurídico, 5 jan. 2022. Disponível em: https://www.conjur.com.br/2022-jan-05/opiniao-direito-prova-poderes-juiz-boa-fe-cpc15/. Acesso em: 28 fev. 2024.

SANTOS, Moacyr Amaral. **Primeiras linhas de direito processual civil**. 13. ed. São Paulo: Saraiva, 1990. v. 2.

SANTOS, Moacyr Amaral. **Prova judiciária no cível e comercial**. 2. ed. São Paulo: Max Limonad, 1952. v. 1.

SÃO PAULO. Tribunal de Justiça. **Apelação Cível n. 1000786-26.2019.8.26.0660.** Relatora: Des.: Maria de Lourdes Lopez Gil. São Paulo, 29 jul. 2021. Disponível em: https://tj-sp.jusbrasil.com.br/jurisprudencia/1255497249/apelacaocivel-ac-

10007862620198260660-sp-1000786-2620198260660/inteiro-teor1255497269. Acesso em: 23 jun. 2024.

SAPIR, Edward. The status of linguistics as a science. **Language,** Chicago, v. 5, n. 4, dec. 1929. Disponível em: https://doi.org/10.2307/409588. Acesso em: 9 jan. 2024.

SAUSSURE, Ferdinand. **Curso de linguística geral**. 27. ed. São Paulo: Cultrix, 2006.

SERASA EXPERIAN. **ICP-Brasil:** saiba o que é, como funciona e como obter um certificado ICP-Brasil. [Brasília]: SERASA, 19 jun. 2024. Disponível em: https://serasa.certificadodigital.com.br/blog/certificado-digital/icp-brasil-2/#:~:text=A%20ICP%2DBrasil%20%C3%A9%20a,no%20padr%C3%A3o%20da%20ICP%2DBrasil. Acesso em: 31 jan. 2024.

SERRA, Pedro. **Como funciona o e-mail?** [*S. l.*]: Linkedin, 4 mar. 2024. Disponível em: https://pt.linkedin.com/pulse/como-funciona-o-e-mail-pedro-serra-zhdqf. Acesso em: 15 jun. 2024.

SILVA, Fabrício Lima. Do panoptismo ao pós-panoptismo: controle da geolocalização dos trabalhadores pelo empregador. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle; AZEVEDO NETO, Platon Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 247-258

SILVA, José Antônio Ribeiro de Oliveira. A prova digital: um breve estudo sobre seu conceito, natureza jurídica, requisitos e regras de ônus da prova. **Revista do Tribunal Superior do Trabalho**, São Paulo, v. 88, n. 2, jan./mar. 2022.

SILVA, Louise S. H. Thomaz da *et al.* **Direito Digital.** Porto Alegre: SAGAH, 2021. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556902814/. Acesso em: 30 jun. 2024.

SIMPSON, Maryssa; WILLIAMS, Bentom. **Insurance Symposium 2017**: use of metadata in litigation. Dallas: Cooperscully, 2017. Disponível em: https://www.cooperscully.com/uploads/file/MJS%20&%20BW%20-%20Use%20of%20Metadata%20in%20Litigation.pdf. Acesso em: 2 jul. 2024.

SMITH, Brad; BROWNE, Carol Ann. **Armas e ferramentas:** o futuro e o perigo da era digital. Rio de Janeiro: Alta Books, 2020.

SOARES, Carlos Henrique *et al*. (org**). Proceso democrático y garantismo procesal**. Belo Horizonte: Arraes Editores, 2015.

SOARES, Saulo Cerqueira de Aguiar; EÇA, Vitor Salino de Moura; SOARES, Ivna Maria Mello (coord.). **Afirmação de direitos em tempos líquidos**. Curitiba: CRV, 2020.

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

STF - CRIPTOGRAFIA de ponta a ponta é inviolável, afirma co-fundador do WhatsApp. [*S. l.*]: Jusbrasil, 2016. Disponível em https://www.jusbrasil.com.br/noticias/stf-criptografia-de-ponta-a-ponta-e-inviolavel-afirma-co-fundador-do-whatsapp/466067715. Acesso em: 19 jun. 2019.

STOPANOVSKI, Marcelo. **E-mails exigem cuidados específicos para que sirvam como prova.** São Paulo: Consultor Jurídico, 2 set. 2015. Disponível em https://www.conjur.com.br/2015-set-02/suporte-litigios-servir-prova-acoes-mail-passar-pericia/. Acesso em: 15 jun. 2019.

SWAINE, Michael R.; FREIBERGER, Paul A. **Eniac**. Chicago: Encyclopedia Britannica, 11 Dec. 2024. Disponível em: https://www.britannica.com/technology/ENIAC. 2023. Acesso em: 14 dez. 2024.

TAMER, Maurício. **LGPD:** comentada artigo por artigo. 2. ed. São Paulo: Rideel, 2022. *E-book*. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 1 ago. 2024.

TANEBAUM, Andrew; WETHERALL, David J. **Computer networks**. 5. ed. Boston: Pearson Education, 2010.

TARUFFO, Michele. **Uma simples verdade:** o juiz e a construção dos fatos. São Paulo: Marcial Pons, 2016.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico**. São Paulo: Saraiva, 2024. *E-book.* Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553622344/. Acesso em: 14 dez. 2024.

TEIXEIRA, Tarcisio. Wi-Fi - Riscos e limites da responsabilidade pelo compartilhamento. **Revista dos Tribunais**, v. 961, nov. 2015. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.961.02.PDF. Acesso em: 18 jul. 2024.

THAMAY, Rennan; TAMER, Maurício. **Provas no direito digital**: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2022. *E-book*.

THEODORO JÚNIOR, Humberto. **Curso de direito processual civil.** 64. ed. Rio de Janeiro: Forense, 2023. v. 1.

TERCEIRO NETO, João Otávio**. Interpretação dos atos processuais.** Coordenação de Leonardo Carneiro da Cunha. Rio de Janeiro: Forense, 2019.

TURMA, Eduardo. **Trabalho, tecnologia e desemprego**. 2. ed. São Paulo: Grupo Almedina, 2022.

UNIÃO EUROPEIA. **Recomendação do Parlamento Europeu P9_TA(2023)0244:** investigação sobre a utilização do software espião de vigilância Pegasus e equivalentes. Estrasburgo: Europart, 15 jun. 2023. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_PT.html. Acesso em: 9 jul. 2024.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016: relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia,** L 119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 28 jan. 2024.

UNITED KINGDOM. **Investigatory Powers Act 2016**. London: The Stationery Office Limited, 2016. Disponível em: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted. Acesso em 05 de julho de 2024.

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN. **NSCA Mosaic**. [*S. l.*]: NCSA, 2023. Disponível em: https://www.ncsa.illinois.edu/research/project-highlights/ncsa-mosaic/. Acesso em: 12 dez. 2023.

U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, NATIONAL INSTITUTE OF JUSTICE. **Electronic crime scene investigation:** a guide for first responders. 2. ed. [*S. l.*]: OJP, 2008. Disponível em: https://www.ojp.gov/pdffiles1/nij/219941.pdf. Acesso em: 8 fev. 2024.

VAZ, Denise Provazi. **Provas digitais no processo penal:** formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

VERIFACT. **Dúvidas frequentes.** [*S. l.*]: Do Autor, 2022. Disponível em: https://www.verifact.com.br/duvidas-frequentes/#:~:text=Os%20c%C3%B3digos%20HASH%20s%C3%A3o%20%22impress%C3%B5es,Carimbo%20de%20Tempo%20ICP%2FBR. Acesso em: 18 maio 2024.

VERIFACT. **Print não serve:** 3 motivos pelos quais a justiça pode rejeitar prints em processos judiciais. [*S. l.*]: Do Autor, 10 maio 2023. Disponível em https://www.verifact.com.br/print-nao-serve-3-motivos-de-rejeicao-de-prints-em-processos/. Acesso em: 20 jun. 2024.

VERIFACT. **Saiba mais.** [*S. l.*]: Do Autor, 10 maio 2024. Disponível em https://www.verifact.com.br/saiba-mais/. Acesso em: 14 jun. 2024.

VIEIRA, Alessandro. **Projeto de Lei n° 402, de 2024**. Disciplina a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares. Brasília: Câmara dos Deputados, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 15 jul. 2024.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy:** originalmente publicado em 4 Harvard Law Review 193 (1890). [*S. l.*]: University of Louisville, 2024. Disponível em: https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/the-right-to-privacy. Acesso em: 1 ago. 2024.

WHATSAPP. **Política de privacidade do WhatsApp**. [*S. l.*]: Do Autor, 4 jan. 2023. Disponível em: https://www.whatsapp.com/legal/privacy-policy-eea/revisions/20210104?lang=pt_PT. Acesso em: 3 jul. 2024.

WHATSAPP. **Sobre a criptografia de ponta a ponta**. [*S. l.*]: Do Autor, 2024. Disponível em: https://faq.whatsapp.com/820124435853543/?locale=pt_BR. Acesso em: 19 jun. 2024.

YAMADA. Vitor Leandro. **Prova digital:** um novo paradigma probatório. [*S. l.*]: Portal TRT, 2021. Disponível em: https://portal.trt12.jus.br/sites/default/files/2021-05/Material%20Dr.%20Vitor%20Yamanda.pdf. Acesso em: 14 abr. 2024.

YAMADA, Vitor Leandro. Requisitos legais da prova digital: autenticidade, integridade e cadeia de custódia. *In*: MISKULIN, Ana Paula Silva; BERTACHINI, Danielle; AZEVEDO NETO, Platon Teixeira de (coord.). **Provas digitais no processo do trabalho:** realidade e futuro. Campinas: Lacier Editora, 2022. p. 121-157.