

JOSÉ ANTÔNIO RIBEIRO
DE OLIVEIRA SILVA

MANUAL
DAS PROVAS
NO PROCESSO
DO TRABALHO

2025

 EDITORA
*Jus*PODIVM
www.editorajuspodivm.com.br

7

PROVAS DIGITAIS: POR UMA TEORIA GERAL

7.1. CONSIDERAÇÕES INICIAIS SOBRE A PROVA DIGITAL

Não é incomum ouvir que a prova digital será a nova “rainha das provas”, ou seja, será o meio de prova hegemônico no processo do trabalho, que desbancará meios recorrentes como o depoimento pessoal e principalmente o depoimento testemunhal. Também, não é incomum encontrar quem defenda que as provas digitais podem acabar com as mentiras contadas nas audiências trabalhistas. No entanto, é importante reconhecer que as provas digitais, assim como qualquer evidência advinda do meio digital, podem ser sujeitas a fraudes. Presentes nas mais diversas áreas do cotidiano humano, as fraudes, infelizmente, também ocorrem no processo judicial, e as provas digitais, por mais que “endeusadas” por parte da doutrina e da jurisprudência, não estão imunes às práticas fraudulentas.

Portanto, a ideia de que as provas digitais trarão a verdade absoluta deve ser vista com a máxima cautela. Guilherme G. Feliciano, em uma palestra sobre provas digitais proferida em curso oferecido pela Escola Nacional Associativa dos Magistrados da Justiça do Trabalho (ENAMATRA), destacou que o que temos no processo é *a verdade processual*, não necessariamente a verdade real ou material. Embora as provas digitais possam oferecer mais segurança e confiabilidade em certos casos, não podemos abandonar os meios tradicionais de prova, como a prova documental, a prova pericial e até mesmo a prova testemunhal.

Com efeito, Marinoni e Arenhart asseveram que “a noção de verdade é, hoje, algo meramente utópico e ideal (enquanto absoluto)”. E não apenas no campo do processo, mas também “em outros campos científicos”, pois “*jamais se poderá afirmar, com segurança absoluta, que o produto encontrado efetivamente corresponde à verdade*” – destaques dos autores. “Realmente, a

essência da verdade é intangível (ou ao menos o é a certeza da aquisição desta” (MARINONI, ARENHART, 2008, p. 255).

De modo que nem mesmo as provas digitais nos oferecerão a verdade absoluta, tampouco a chamada verdade real. A prova digital nos trará – como qualquer outro meio de prova – *apenas a verdade processual*.

Agora, é preciso reconhecer que nos últimos anos, especialmente desde o final da década de 1990, houve uma revolução tecnológica significativa, com o surgimento, posteriormente, do que se convencionou chamar de *quarta revolução industrial* ou *indústria 4.0*. Na década de 1990, os celulares estavam apenas começando a se popularizar, e os primeiros modelos eram grandes e pesados, usados basicamente para fazer e receber chamadas. Hoje, os celulares contêm praticamente toda a nossa vida, como calendários, conversações e informações financeiras. Perder um aparelho celular, atualmente, pode ser desastroso, pois ele armazena muitas das nossas informações pessoais e profissionais. Este avanço tecnológico descomunal transformou a maneira como lidamos com as informações e, conseqüentemente, com as provas, no mundo digital.

As provas digitais estão cada vez mais presentes também no campo processual. O uso do PJe (Processo Judicial Eletrônico) exemplifica essa realidade. Nos anos 90, era impensável – ou um sonho visionário de estudiosos avançados –, que um dia teríamos autos de processos totalmente digitais. Naquela época, eu carregava grandes quantidades de autos de processos físicos para casa, empilhando-os para redigir sentenças, sem imaginar que um dia tudo isso se tornaria digital. Mas aconteceu. Desde 2014, todos os processos que tramitam na Justiça do Trabalho brasileira se tornaram “digitais”, tendo sido, posteriormente, digitalizados até mesmo autos de processos físicos.

No entanto, embora os fatos digitais estejam cada vez mais integrados às nossas vidas, devemos lembrar que bilhões de pessoas, no mundo, ainda não têm acesso a essa tecnologia. Muitas pessoas, no nosso planeta, não possuem aparelhos celulares ou acesso à internet, o que nos revela que a vida da maioria das pessoas não é tão “digital” como alguns pretendem fazer parecer. As provas digitais são importantes e precisam ser estudadas, mas ainda existem muitos trabalhadores humildes e simples, bem como pequenos empresários, que não têm acesso (amplo) a essas tecnologias. Embora quase todos possuam um aparelho celular, o acesso digital completo ainda não é uma realidade para muitos, principalmente em nosso país de dimensões continentais.

Por outro lado, e até como expressão da desigualdade social, há muitos fatos digitais no ambiente de trabalho, especialmente entre os chamados “altos empregados”, cujas atividades são praticamente todas na forma digital. Hoje, para falar com um gerente de banco, geralmente é pelo *WhatsApp* ou por

outros canais de comunicação digital. E as reuniões de trabalho da gerência das agências bancárias são praticamente todas virtuais.

Ademais, os contratos se tornaram digitais, substituindo o papel tradicional. Atualmente, ao abrir uma conta em um banco, o contrato é digital, e o cliente o assina com uma senha ou impressão digital. As transações bancárias e entre empresas também são digitais. O PIX, por exemplo, revolucionou a forma como fazemos transferências ou pagamentos, tornando-os extremamente simples e rápidos, e todos pelo meio digital.

Além disso, temos moedas digitais, criptomoedas e a *geolocalização*, que é uma das *vedetes* das provas digitais. A geolocalização pode rastrear onde uma pessoa esteve em determinado momento, o que levanta questões sobre a aceitação e a aplicação dessa tecnologia pelos juízes do trabalho, especialmente em matéria de horas extras. A ideia de ser rastreado por geolocalização é um tanto assustadora, mas essa tecnologia está cada vez mais presente e pode se tornar uma ferramenta importante, na coleta de provas no processo judicial.

E, por isso, diante da extensão, inovação contínua e do grande impacto que as provas digitais geram e podem gerar, não podemos simplesmente focar em como elas funcionam, como podem ser utilizadas e como fazer a verificação de sua validade nos autos de um processo. Precisamos sempre nos apoiar na *teoria geral da prova* para termos solidez na compreensão dos diversos problemas de produção probatória – e de contraprova – que as provas digitais já proporcionam.

Assim, antes de abordarmos o “como fazer” – como juntar uma prova digital –, é importante considerarmos alguns pilares fundamentais da teoria geral das provas: (i) pode ser feito? (ii) Em que medida pode ser feito? (iii) E como podem ser impugnadas? Essas questões são essenciais para a aplicação adequada das provas digitais no processo civil e no processo do trabalho.

Primeiramente, devemos questionar se a utilização das provas digitais é permitida dentro do arcabouço legal existente. Isso envolve avaliar a *natureza jurídica das provas digitais* e assegurar que sua admissão respeite os princípios fundamentais do direito processual. Em seguida, é necessário determinar a extensão em que essas provas podem ser utilizadas, incluindo a avaliação dos (i) critérios de admissibilidade, a (ii) relevância das provas para o caso específico e as (iii) limitações impostas pela legislação vigente. Por fim, a *possibilidade de impugnação das provas digitais* deve ser rigorosamente considerada. É essencial definir os procedimentos e as condições sob as quais uma parte pode impugnar a autenticidade e/ou a integridade dessas provas, garantindo que ambas as partes tenham a oportunidade de apresentar suas alegações e contraposições de maneira adequada e equitativa.

As provas digitais *transcendem* a simples utilização e disponibilização de dados eletrônicos. Elas requerem uma abordagem cuidadosamente estruturada que considere sua (i) admissibilidade, (ii) alcance e (iii) impugnabilidade, assegurando que seu uso no processo judicial seja efetivo e justo. E aqui se faz necessário trazer à baila uma outra questão de elevada importância e devida complexidade: *o ônus da prova em matéria de provas digitais*.

O ônus da prova, em particular, não tem sido amplamente analisado por estudiosos, doutrinadores e professores quando tratam de provas digitais, mas nessa temática específica temos várias questões a serem solucionadas, como as seguintes: (i) *de quem será o ônus da prova em circunstâncias envolvendo provas digitais?* (ii) Se o reclamante se recusar a exibir o aparelho celular para o juiz, na audiência trabalhista, ele tem esse direito? (iii) E se uma testemunha desejar exibir seu celular para o juiz, para comprovar que está dizendo a verdade, como isso deve ser tratado? (iv) Pode o juiz, de maneira arbitrária, “confiscar” o celular da parte ou da testemunha para averiguações, ou ele deve seguir medidas processuais específicas? (v) Além disso, *se a parte adversa não impugnar a prova digital*, ainda será necessário apresentar toda a cadeia de custódia e verificar a autenticidade da prova? (vi) Quando houver impugnação, quem deve provar a validade – ou invalidade – da prova: *a parte que apresentou a prova digital ou a parte que a impugnou?*

Analisar com profundidade essas questões – e tantas outras –, é essencial para que se possa desenvolver uma *teoria da prova digital*, na qual o procedimento probatório esteja bem claro, evitando-se as indesejáveis surpresas no curso do processo. Estabelecer diretrizes claras e procedimentos específicos para lidar com essas situações ajudará a evitar abusos e a assegurar que as provas digitais sejam tratadas com a devida seriedade e rigor processual, em observância ao *pilar do devido processo legal*.

Pois bem, o intuito deste capítulo do Manual consiste em esclarecer estas questões levantadas – e outras –, com vistas à correta utilização das provas digitais no processo do trabalho.

7.2. O QUE É UMA PROVA DIGITAL: CARACTERIZAÇÃO E DESDOBRAMENTOS

De início, é importante notar que ainda há poucos escritos específicos sobre a prova digital, especialmente quando comparados ao elevado número de livros, monografias e artigos doutrinários publicados sobre a prova “convencional”. Porém, certamente, na teoria geral da prova – uma temática estudada há séculos – temos muitos aportes que podem servir como *bússola* na investigação do que seria exatamente a prova digital.

Antes disso, acredito ser relevante registrar a mudança de paradigma que tem ocorrido na sociedade, refletindo-se na atividade probatória, em juízo.

Essas mudanças são intensas e abrangentes, impulsionadas pela utilização cada vez mais frequente dos recursos tecnológicos disponíveis, por pessoas físicas e jurídicas.

A integração da tecnologia em diversos aspectos da vida tem transformado profundamente as interações humanas e a organização da sociedade. Isso tem alterado *desde a comunicação*, na qual as cartas foram substituídas por e-mails e os telefonemas por mensagens instantâneas de texto, áudio ou vídeo, *até os registros de fatos* – públicos ou privados –, que antes eram feitos em papel, com várias precauções, e hoje são amplamente substituídos por sistemas de informática.

Além disso, toda a sorte de atividades, que antes exigiam contato presencial ou que criaram novas possibilidades, agora utilizam a internet. Por meio dela, acessa-se e transmite-se um volume imenso de informação, celebram-se negócios jurídicos e também se cometem atos ilícitos (PASTORE, 2020, p. 64).

Precisamos, portanto, identificar *o que é exatamente uma prova digital*, haja vista que os meios probatórios, aparentemente, permanecem os mesmos, porém, *as fontes de prova* se alteram e reclamam a elaboração de novos critérios para o seu adequado exame (PASTORE, 2020, p. 64). Se o rito probatório não se altera, mantendo-se as formalidades sobre a juntada de documentos e a produção de outras provas correlatas, as fontes acessadas por meios tecnológicos, “que é o traço verdadeiramente distintivo do que se chama de prova digital, ostenta peculiaridades merecedoras de tratamento diferenciado” (PASTORE, 2020, p. 64).

Rennan Thamay e Mauricio Tamer, em uma excelente monografia sobre o tema, *definem a prova digital* como um instrumento jurídico destinado a demonstrar a ocorrência ou não de um determinado fato e suas circunstâncias, seja ele ocorrido total ou parcialmente em meios digitais ou, se ocorrido fora deles, que esses meios sirvam como instrumento de sua demonstração. A prova digital é *o meio de demonstrar a ocorrência de um fato existente em meio digital* ou que utilize o meio digital como instrumento de demonstração de determinado fato e de seu conteúdo (THAMAY; TAMER, 2020, p. 33).

7.2.1. Provas digitais de primeiro grau x provas digitais de segundo grau

Existem duas abordagens principais ao se tratar de provas digitais: a primeira está relacionada aos (i) *fatos ou atos jurídicos que ocorrem diretamente em meios digitais*, utilizando-se destes últimos como suporte. Exemplos disso incluem: (A) envio de *e-mails* ou mensagens por aplicativos de mensageria, como *WhatsApp*, *Telegram* e outros; (B) publicação de vídeos na internet, como

no *YouTube*; (C) cópia de *software* ou da base de dados de um computador, entre outros. Assim, temos fatos ou atos que ocorreram diretamente nos meios digitais, utilizando tecnologias da comunicação e da informação, tratando-se da *prova digital em sentido estrito* (THAMAY; TAMER, 2020, p. 32-33).

A segunda abordagem trata de (ii) situações nas quais, embora o fato ou ato jurídico tenha ocorrido em meios “convencionais”, ele *pode ser comprovado por meio de ferramentas digitais disponíveis*. Dessa forma, o fato ocorre no mundo real ou físico, no mundo convencional, e utilizamos a prova digital apenas para demonstrá-lo. Nesse caso, a prova digital é um meio opcional de prova, pois podemos provar o mesmo fato por outras maneiras. Se existe a possibilidade de provar o fato por outros mecanismos, então não se trata de uma prova digital em sentido estrito, ou de primeiro grau, mas de uma *prova digital de segundo grau*, opcional (THAMAY; TAMER, 2020, p. 32-33).

Por exemplo, em uma ata notarial, o tabelião certifica que fotografias publicadas em redes sociais como *Facebook* e *Instagram* demonstram encontros, viagens e até intimidades entre determinadas pessoas. Posteriormente, a critério do juiz, esses registros podem caracterizar uma amizade íntima ou um conluio entre um empregado de determinada empresa e o diretor de uma empresa concorrente, entre outros. Aqui, os fatos – como encontros, viagens, abraços e beijos – não são digitais em si, mas *os suportes digitais servem como mecanismos de demonstração* (THAMAY; TAMER, 2020, p. 32-33).

Para facilitar a compreensão dessa dicotomia, poderíamos sugerir que, na primeira vertente, temos (i) *prova digital de primeiro grau* – fatos digitais –, ao passo que, na segunda vertente, temos uma (ii) *prova digital de segundo grau*, pois, nesse caso, apenas a prova em si é produzida a partir de meios ou suportes digitais.

A distinção entre *provas digitais de primeiro grau* e *provas digitais de segundo grau* é de grande valia para o presente tópico, visto que, desta classificação, desdobram-se uma série de consequências. A *prova digital de primeiro grau* tem origem no meio digital, sendo mais complexa e tecnológica. Já a *prova digital de segundo grau* surge como um instrumento de prova, utilizada para demonstrar algo por intermédio de suportes digitais, embora pudesse ser comprovada por outros meios, como depoimentos de testemunhas, confissões ou documentos (SILVA, 2021, p. 95).

Consequentemente, as restrições e a *rigidez do procedimento* para a prova digital de primeiro grau não se aplicam com a mesma severidade à prova digital de segundo grau. A *prova digital de segundo grau* pode ser usada apenas como mecanismo de prova complementar, já que outros meios de prova

poderiam ser utilizados. A título de exemplo, uma conversa por *e-mail*, que é uma *prova digital de primeiro grau*, não pode ser totalmente reproduzida por uma testemunha, que só poderia relatar ter visto (ou lido) a conversa, mas não recordar todas as palavras exatas. Assim, essa prova é genuinamente digital e sua autenticidade depende do meio digital em que foi produzida.

Desta classificação, ou seja, da distinção entre a prova digital de primeiro grau e a prova digital de segundo grau, surgem *duas questões importantes*: (i) a violação da intimidade e (ii) a cadeia de custódia/sistema de verificação. Evidentemente, se distintas em suas classificações, distintas também serão em seus desdobramentos.

Na primeira questão – a possibilidade de violação da intimidade pelo uso das provas digitais –, a centralidade do debate reside em até que ponto uma parte pode utilizar como prova informações retiradas de instrumentos digitais privados, como perfis de redes sociais fechados no *Instagram* ou *Facebook*. Essa preocupação é especialmente relevante quando se trata de *provas digitais de primeiro grau*, que envolvem diretamente conteúdos privados ou semiprivados, suscetíveis à invasão de privacidade. A violação da intimidade, portanto, emerge como uma questão crítica quando tais provas são apresentadas, pois a obtenção dessas informações pode envolver o acesso não autorizado a espaços digitais pessoais, o que tornaria a prova nula, por se tratar de uma *prova ilícita*.

Em contraste, quando lidamos com *provas digitais de segundo grau*, nas quais os suportes digitais são utilizados apenas como intermediários para o registro de algo que pode ser comprovado por outros meios, a violação da intimidade não se apresenta com a mesma intensidade. Exemplificando, um registro digital que documenta a existência de um contrato físico ou uma transação que pode ser corroborada por outros documentos ou testemunhas não suscita as mesmas preocupações de privacidade.

Contudo, a complexidade aumenta significativamente quando estamos lidando com *provas digitais de primeiro grau*, como contratos digitais ou e-mails trocados entre duas pessoas. Nesses casos, a forma como a prova foi obtida torna-se um aspecto importante, frequentemente levantando questões sobre invasão de privacidade e possíveis violações da intimidade. A obtenção de tais provas pode envolver desafios legais e éticos, especialmente se o acesso a esses documentos não foi autorizado por uma das partes envolvidas.

Além disso, o acesso público à informação também é um aspecto essencial a ser considerado, ao se discutir a possível violação da intimidade na obtenção de provas digitais. Se a informação em questão foi disponibilizada publicamente pelo próprio titular, não se pode alegar ofensa à privacidade. Por exemplo, se uma foto foi publicada pela própria pessoa em uma rede social

aberta, como *Instagram* ou *Facebook*, não há violação da intimidade na sua utilização no processo judicial, pois essas informações estavam acessíveis a qualquer pessoa. Em contrapartida, perfis “fechados” ou informações retiradas de conversas privadas em aplicativos de mensageria carregam um potencial muito maior de ofensa à intimidade.

A segunda questão a ser considerada é a relativa à *cadeia de custódia* e ao sistema de verificação da idoneidade da prova digital. Como introdução, visto que abordaremos esse assunto com maior profundidade ao longo deste capítulo, é importante entender que, no contexto jurídico, a ferramenta *Verifact* refere-se ao serviço de autenticação e validação de provas digitais. Esse serviço é ofertado ao público pela empresa que criou a ferramenta digital de certificação, a um custo relativamente acessível, sendo muito utilizada para garantir a preservação da cadeia de custódia na produção da prova digital, assegurando que a prova em questão não foi adulterada, desde a sua obtenção até a sua apresentação em juízo.

Assim, as exigências de verificação da autenticidade e da integridade, mediante a preservação da cadeia de custódia, podem variar, dependendo do tipo de prova digital em questão. Melhor dizendo, ao tratarmos, por exemplo, das *provas digitais de segundo grau*, estes requisitos e as observações pertinentes à cadeia de custódia podem ser mais flexíveis. O motivo encontra-se na constatação de que a demonstração dos fatos pode ser feita por outros meios de prova, ou seja, eles podem ser demonstrados por documentos, prova testemunhal etc.

Por sua vez, a preservação da cadeia de custódia e, conseqüentemente, a obrigatoriedade de recurso aos sistemas de verificação, são pontos bem mais complexos e rigorosos quando estamos diante de *provas digitais de primeiro grau*. Ora, se estamos falando de fatos ou atos jurídicos que ocorrem *diretamente* nos meios digitais, a garantia de sua autenticidade e integridade é *imprescindível*. A prova digital de primeiro grau só existe no meio digital, sendo impossível sua manifestação em outros meios de prova, não sendo possível, portanto, que seja “substituída” por documentos ou prova testemunhal.

7.2.2. Fatos que ocorrem em meios digitais e podem configurar ilícitos

Ainda para uma maior compreensão do que são as provas digitais, Thamay e Tamer, na referida monografia, fazem menção a ilícitos civis, trabalhistas e criminais que envolvem a temática das provas digitais, em seu cerne. Ou seja, são ilícitos que tem sua origem na utilização de provas digitais – em sua maioria nas provas digitais de primeiro grau – e clarificam o que constitui a manifestação destes meios de provas (THAMAY; TAMER, 2020, p. 34-39).

Quanto aos ilícitos de *natureza civil*, merecem destaque os seguintes exemplos:

- I. Uma pessoa realiza uma postagem inverídica, desatualizada ou desonrosa sobre outra pessoa em mídias sociais (como Facebook, Instagram, Twitter) ou faz isso por meio de um vídeo no YouTube. Nesse caso, o autor do dano usa meios digitais amplamente conhecidos, especificamente os serviços dos respectivos provedores de aplicação. A pessoa prejudicada, seja natural ou jurídica (conforme artigo 52 do Código Civil e Súmula n. 227 do STJ), pode buscar uma indenização por dano moral em juízo (arts. 186 e 927 do Código Civil). Para demonstrar esse fato em juízo, o autor da demanda deve agir rapidamente para preservar o conteúdo e identificar tecnicamente o usuário responsável (obtenção dos registros eletrônicos e dados cadastrais), por meio da produção antecipada de prova ou obtenção de uma tutela de urgência na própria ação indenizatória (THAMAY; TAMER, 2020, p. 34-39);
- II. Alguém cria sites utilizando marcas de outras organizações sem a devida autorização, gerando benefício ilícito e confundindo o público consumidor. Isso viola o direito de propriedade intelectual de terceiros, seja no âmbito da propriedade industrial (marcas, *trade dress*, etc.) conforme a Lei nº 9.279/1996, seja no âmbito do direito autoral ou dos direitos sobre o software. Esses atos, praticados exclusivamente em meio digital, geralmente são demonstrados por prova pericial (THAMAY; TAMER, 2020, p. 34-39);
- III. A prática ilícita comum de compartilhamento não autorizado de materiais ou cursos por *e-mail* e outros meios digitais, que atenta contra os direitos autorais (Lei n. 9.610/98);
- IV. As práticas de concorrência desleal, dentre tantas, a utilização de páginas ou *blogs* anônimos vocacionados à propagação de conteúdo ilícito (inverídico ou desatualizado) para levar o concorrente ao descrédito, bem como a contratação da palavra-chave de busca da empresa concorrente em sites de busca, como o *Google*, de modo que, quando o usuário faz a busca pelos termos que normalmente identificariam o concorrente, aparecem para si apenas os resultados patrocinados, diante da “contratação dos chamados anúncios ou *links* patrocinados” (THAMAY; TAMER, 2020, p. 34-39).

Na *seara trabalhista* – a que mais nos interessa –, os autores afirmam que são muitos os exemplos de ilícitos cometidos nas *relações de trabalho*, com a utilização dos meios digitais, tanto pelo empregado quanto pelo empregador (THAMAY; TAMER, 2020, p. 36-37).

Por parte do *empregado*, podem ser citados os seguintes exemplos:

- I. O desvio de informações ou de documentos sigilosos e de propriedade das organizações empregadoras para terceiros – essa prática pode ser empreendida por cópias enviadas por um simples *e-mail*, mas geralmente é bem sofisticada, com a extração de cópia de arquivos digitais (*pen drive*, HD externo etc.), posteriormente entregue ao concorrente; e caracteriza, sem sombra de dúvidas, *justa causa* para o despedimento do empregado, não somente pela quebra de confiança, mas por haver previsão expressa na CLT, a esse respeito: constitui figura de *justa causa* a violação de segredo da empresa (alínea “g” do art. 482);
- II. Um empregado, responsável pela condução de uma RFP – *Request for Proposal* (um documento de solicitação de proposta, “muitas vezes feita por meio de um processo de licitação, por uma agência ou empresa interessada na aquisição de uma mercadoria, serviço ou ativo valioso, a potenciais fornecedores para apresentar propostas comerciais” (Disponível em: <https://en.wikipedia.org/wiki/Request_for_proposal>; acesso em: 03 jun. 2024) – que, *numa licitação*, “negocie vantagens a determinado concorrente por e-mail ou celular corporativo”; de se notar que essa prática também está tipificada como *justa causa* no art. 482, alínea “c”, da CLT: “negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço” (THAMAY; TAMER, 2020, p. 36-37);
- III. Ato de empregado que, em grupo de *WhatsApp* da empresa faz publicação de conteúdos desonrosos ou profere xingamentos a outro empregado, tumultuando o ambiente corporativo – aliás, tem sido muito mais comum que empregados desanquem a honra objetiva da própria empresa ou a subjetiva de proprietários e diretores nesses canais internos de comunicação – grupo de *WhatsApp* corporativo –, mas principalmente em *mídias sociais*, como *Facebook*, *Instagram*, *Twitter* e outras (THAMAY; TAMER, 2020, p. 36-37). Em todos esses casos teremos ilícitos praticados em suporte digital, que desafiam a argúcia dos advogados para a produção da prova a respeito dos fatos; novamente, o que se tem aqui é outra figura de *justa causa*, tipificada no art. 482, alínea “k”, da CLT, a saber: “ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima defesa, própria ou de outrem”;
- IV. Os autores citam, ainda, o exemplo de empregado que alega doença para não comparecer em serviço e depois reste provado, a partir de

postagens em mídias sociais que, na verdade, mentiu – embora se trate de hipótese cada vez mais frequente nas audiências trabalhistas, por coerência, tenho de ressaltar que essa situação não é de prova digital em sentido estrito, ou seja, daquela que demonstra fatos ocorridos em meio digital. Aqui, temos *prova digital da segunda vertente* anteriormente analisada, porque os fatos – viagens, festas, jogos etc. – ocorreram em ambiente “físico”, não nas plataformas digitais; apenas as provas dos fatos que revelam a mentira do empregado – em regra, fotografias publicadas por ele próprio em suas páginas e perfis, nas redes sociais – é que serão consideradas *digitais*. Mais uma vez, temos, no caso, uma figura de *justa causa*, pois é inadmissível que o empregado apresente atestado médico para não trabalhar em razão de sua doença e, no lugar de permanecer em casa se recuperando, faça suas viagens, compareça em festas, bares ou vá praticar esportes. Essa conduta propicia a quebra da confiança que deve ser depositada em todo empregado, estando prevista, ainda que não expressamente, na alínea “b” do art. 482 da CLT: (ato de) “incontinência de conduta ou mau procedimento” (THAMAY; TAMER, 2020, p. 36-37).

Contudo, o *empregador* também pode cometer, contra o empregado, ilícitos com o uso dos *meios digitais*, dando ocasião a uma prova digital de sua conduta reprovável. Citam-se, como exemplos, os seguintes (THAMAY; TAMER, 2020, p. 36-37):

- I. Prática de *assédio sexual* pelo empregador, que aborda o(a) empregado(a) por meio de mensagens privadas no *WhatsApp* com tom indecoroso, sexual, inclusive com envio de imagens – ou de coação. Há de se registrar, novamente, que, em regra, o empregador ou gerente da empresa que procede à prática atos de assédio sexual “a portas fechadas”, sem qualquer registro em meio digital, dificultando sobremaneira a produção da prova por parte do(a) empregado(a) vítima desse tipo de assédio. Se houver uma *prova digital* dessas investidas, como gravação em áudio no aparelho celular, temos, aqui, uma situação em que *apenas a prova é digital*; agora, no exemplo dado (pelos autores citados), temos, sem dúvida, um caso em que o próprio fato ilícito foi cometido por intermédio de aplicativo de mensageria instantânea (*WhatsApp*, *Telegram* e outros). Aqui, *a prova é digital por excelência*, desafiando a demonstração da autoria das mensagens, da integridade destas e até da preservação da tal

- cadeia de custódia, requisitos da prova digital que serão analisados mais adiante (THAMAY; TAMER, 2020, p. 36-37);
- II. Desrespeito ao direito de férias do empregado, pelo envio (constante) de mensagens por aplicativos e exigência de respostas (e trabalho, portanto) durante o período em que o trabalhador se dedica à sagrada *desconexão do trabalho* – temos, aqui, um gravíssimo ilícito trabalhista porque o direito ao gozo de férias se trata de um dos mais importantes direitos sociais dos trabalhadores, erigido ao patamar de *direito fundamental* (art. 7º, inciso XVII, da CF/88). A hipótese revela uma situação de *prova digital de primeiro grau*, por assim dizer, porque o fato – trabalho durante o período de férias – ocorreu com a utilização dos meios digitais: cobrança de respostas e informações por *e-mail* ou aplicativo de mensagens instantâneas, com o trabalho prestado também por esses mecanismos digitais (THAMAY; TAMER, 2020, p. 36-37);
 - III. Realização de horas extras pela comunicação feita por *WhatsApp* fora do horário de trabalho – do mesmo modo que no exemplo anterior, aqui se constata outro grave ilícito trabalhista, haja vista que o *direito à limitação da jornada de trabalho* se trata de um direito social histórico (Convenção n. 1 da OIT, de 1919), também consagrado como *direito fundamental* na Constituição brasileira (art. 7º, incisos XIII e XIV, da CF/88). Também aqui a hipótese – tão frequente nas relações de trabalho – é de uma *prova digital de primeiro grau*, porque as horas extras, consubstanciadas nas respostas e informações prestadas por *WhatsApp*, foram praticadas com a utilização desse mecanismo digital. A juntada de cópia dessas mensagens – de preferência na íntegra – irá demonstrar que o meio digital foi o utilizado para a própria prestação dos serviços (THAMAY; TAMER, 2020, p. 36-37);
 - IV. Posso citar, ainda, dentre tantos outros exemplos que já começam a fazer parte da jurisprudência trabalhista, o caso de *assédio moral* praticado por gerentes e outros gestores das empresas contra seus empregados, por intermédio de canais de comunicação internos, dentre eles, grupos de *e-mail* corporativo, de *WhatsApp*, *Telegram* e outros; nessa situação, as mensagens agressivas, em regra exigindo o cumprimento de metas ou de outras imposições do empregador, são constantes, por vezes tomando algum empregado como “exemplo” de baixa produtividade ou não comprometimento com as diretrizes da empresa; essas mensagens abusivas, reveladoras do *assédio moral*, quando praticadas com a utilização dos recursos tecnológicos de comunicação – *e-mail* corporativo, grupos de *WhatsApp* e/ou

Telegram – vão caracterizar a prova como sendo digital, pois os fatos, aí, ocorrem todos no suporte digital.

Quanto à prova digital na esfera criminal, são citados pela doutrina vários exemplos de fatos criminosos praticados com a utilização dos meios digitais, como os crimes de furto mediante fraude, estelionato, extorsão, calúnia, difamação e até de estupro virtual (THAMAY; TAMER, 2020, p. 37-39). Contudo, trata-se de temática que foge por completo à investigação proposta neste Manual.

7.2.3. A problemática da geolocalização

A *geolocalização* é “um recurso que permite determinar a posição geográfica de um dispositivo com base em um sistema de coordenadas”, as quais “podem ser obtidas por meio de diferentes tipos de sinais”, como os seguintes: GPS, Radiofrequência, AGPS, Wifi (Disponível em: <<https://maplink.global/blog/como-funciona-geolocalizacao/>>. Acesso em: 03 jun. 2024).

Há de se notar que os dados produzidos e armazenados como prova digital de primeiro grau podem ser encontrados em fontes abertas (de livre acesso, como pesquisas no Google, sites de transparência, redes sociais) ou fontes fechadas (de acesso restrito, por meio de solicitação judicial), das quais sejam titulares empresas públicas ou privadas.

É importante destacar que os dados utilizados como provas digitais não se restringem a postagens em redes sociais. Ao utilizar fontes de dados fechadas, como de uma empresa de telefonia, operadora de celular ou rede social, é possível acessar dados de geolocalização, biometria, metadados de fotos e até rastreamento de IP.

Segundo o Promotor de Justiça Fabrício Rabelo Patury, um dos maiores especialistas nessa temática, é possível, a partir de *posts* com *geolocalização* do aparelho celular, até mesmo localizar pessoas em insolvência. Além disso, esses dados podem ser usados para verificar situações de formação de vínculos trabalhistas, horas extras, prestação de serviço e até para justificar uma demissão por justa causa. (Disponível em: <<http://www.tst.jus.br/provas-digitais>>. Acesso em: 03 jun. 2024).

Contudo, diante da complexidade da prova digital, surgem questões importantes relacionadas à geolocalização que devem ser examinadas com cautela. A geolocalização, embora poderosa, não deve ser vista como a solução definitiva para todas as disputas legais. Embora ofereça uma ferramenta valiosa para se determinar a localização e a movimentação de pessoas e dispositivos, *essa tecnologia não é infalível*.