A geolocalização como panaceia no processo do trabalho

The geolocation as a panacea at the labor law procedure

Walter Rosati Vegas Junior *

Submissão: 30 abr. 2023
Aprovação: 16 maio 2023

Resumo: O artigo trata da utilização da geolocalização como meio de prova e apresenta uma crítica de sua ampla admissibilidade como elemento para resolver as controvérsias fáticas no processo do trabalho, particularmente com o enfoque a partir do direito à privacidade e da forma de acesso aos dados digitais oriundos de dispositivos eletrônicos pessoais a partir do papel esperado do juiz. A análise centra-se nos limites constitucionais e legais de acesso indiscriminado por terceiros às movimentações do aparelho celular utilizado por um determinado indivíduo, especialmente quando se esteja diante de uso de equipamento em relação ao qual exista legítima expectativa de proteção da privacidade durante o uso.

Palavras-chave: geolocalização; prova; direito à privacidade.

Abstract: *The article presents the use of geolocation as a evidence and presents a critique of its wide admissibility as an element to resolve factual controversies at the labor law procedure, particularly with a focus on the right to privacy and the form of access to digital data from personal electronic devices based on the expected role of the judge. The analysis focuses on the constitutional and legal limits of indiscriminate access by third parties to the movements of the cell phone used by a given individual, especially when dealing with the use of equipment in relation to which there is a legitimate expectation of privacy protection during use.*

Keywords: *geolocation; evidence; right to privacy.*

---

* Juiz do Trabalho Substituto do Tribunal Regional do Trabalho da 2ª Região. Doutorando, Mestre e Especialista em Direito do Trabalho na Faculdade de Direito da Universidade de São Paulo. Especialista em Direito Processual Civil pela Escola Paulista da Magistratura. Professor universitário.

e infraconstitucional da privacidade dos dados | 3 Acesso aos dados de geolocalização, iniciativa probatória e papel esperado do juiz | 4 Considerações finais

1 Introdução

O presente artigo tem por objeto central uma abordagem crítica sobre a disseminação de um específico meio de prova digital no âmbito do processo do trabalho, ou seja, particularmente a questão do acesso aos dados de geolocalização de usuários de dispositivos eletrônicos a partir de decisão do juiz do trabalho direcionada ao esclarecimento de variadas controvérsias fáticas. Almeja-se apresentar um breve panorama normativo quanto ao tema da proteção da privacidade dos dados, avançando para a análise dos limites e possibilidades de acesso de tais informações e de sua utilização como elemento de prova no âmbito do processo do trabalho pátrio. Para os fins aqui pretendidos será necessário ainda apresentar uma abordagem quanto à iniciativa probatória e papel esperado do juiz ao longo da instrução probatória, a fim de que a partir de todas essas premissas se possam chegar a algumas possíveis conclusões – ainda que parciais e evidentemente não irrefutáveis – sobre a intrincada questão da disseminação do uso da geolocalização para fins probatórios.

2 Uma breve análise da proteção constitucional e infraconstitucional da privacidade dos dados

Ainda que os direitos fundamentais dos cidadãos à inviolabilidade da intimidade e da vida privada (art. 5°, X, da CF/1988) e do sigilo das comunicações telegráficas, de dados e telefônicas (art. 5°, XII, da CF/1988) já estivessem consagrados desde o advento da Constituição Federal de 1988, com claro estabelecimento de verdadeiros limites à atuação estatal e dos agentes privados dentro de um Estado de Direito, múltiplos avanços tecnológicos próprios da sociedade da informação[1] trouxeram novas discussões quanto aos contornos e parâmetros de tais

1 "Embora a informação, em sua acepção ampla de comunicação de conhecimento, já tenha acarretado inovações tecnológicas e verdadeiros rompimentos em um dado modelo de sociedade ao longo da história, o que se verifica no final do século XX é basicamente que o ciclo entre a aquisição de uma informação e a sua utilização em um dado contexto social intensifica-se a tal ponto de tornar aquela a principal "origem do poder dentro da sociedade." (CASTELLS, 1999, p. 69).

garantias, especialmente a partir de aspectos não imaginados à época da definição do rol de direitos fundamentais.

Em relação aos limites relacionados à proteção de dados, cumpre esclarecer que na atualidade avulta a preocupação não apenas com a proteção do processo comunicativo entre os indivíduos em sociedade, na forma da interpretação doutrinária[2] e jurisprudencial[3] construída a partir do art. 5°, XII, da CF/1988, mas também com a efetiva proteção de dados pessoais e amplamente disseminados pelos indivíduos a partir dos múltiplos meios de comunicação social, com possíveis novas conotações relativas ao fenômeno da privacidade.[4] O advento da Lei Geral de Proteção de Dados (LGPD) (Lei n. 13.709/2018) e a promulgação da Emenda Constitucional n. 115/2022, que incluiu a proteção de dados pessoais, inclusive nos meios digitais, entre o rol de direitos fundamentais consagrados no artigo 5° da CF/1988, foram passos legislativos concretos em tal perspectiva de tutela – efetiva - dos dados pessoais, em si, ou seja para além da singela proteção do processo comunicativo.[5]

Particularmente dentro do tema que animou o presente estudo, vale referir que apesar do desenvolvimento da sociedade da informação ter permitido a comunicação cada vez mais simples e rápida entre os

---

2 Em clássico estudo sobre o tema, Ferraz Júnior destaca ao abordar o art. 5°, XII, CF/1988 que "o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação" (FERRAZ JÚNIOR, 1992, p. 86).

3 "Não há violação do art. 5°. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'. 4. A proteção a que se refere o art. 5°, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador." (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270). V - Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2° e 114, II; e Súmula 497 do Supremo Tribunal). (STF, RE 418416, Relator(a): SEPÚLVEDA PERTENCE, Tribunal Pleno, julgado em 10/05/2006, DJ 19-12-2006 PP-00037 EMENT VOL-02261-06 PP-01233).

4 A Suprema Corte estadunidense já teve a oportunidade de firmar premissa no sentido que os "indivíduos têm expectativa razoável de privacidade em todos os seus movimentos físicos" (Carpenter v. United States, No. 16-402, 585 U.S. 12 (2018)), mesmo em se tratando o caso em julgamento de apuração de infração criminal supostamente praticada pelo indivíduo que portava o aparelho celular e compartilhava a respectiva localização com a operadora de telefonia. Entendeu-se na ocasião que o órgão governamental responsável pela investigação (FBI) não possuía um mandado judicial apoiado por causa provável antes de adquirir os registros do dispositivo eletrônico do acusado.

5 Para uma análise desta nova perspectiva de proteção ver, por todos, Doneda (2021).

indivíduos, rompendo barreiras físicas com a adoção de mecanismos tecnológicos que possibilitam comunicação instantânea em áudio e vídeo, com ou sem gravação do conteúdo, isso não significa que não devam existir verdadeiros limites - jurídicos - ao acesso a tais fluxos comunicativos. Não nos parece que exista verdadeiro amparo constitucional ou mesmo legal, por exemplo, para um acesso indiscriminado por terceiros às movimentações do aparelho celular utilizado por um determinado indivíduo, especialmente quando se esteja diante de equipamento de propriedade dele e em relação ao qual exista legítima expectativa de proteção nos contatos mantidos com terceiros ou mesmo da localização - em determinado momento e região - a partir de registros de torres de telefonia, denominadas Estações Rádio Base (ERBs).

Ainda que exista certa controvérsia - doutrinária e jurisprudencial - quanto ao parâmetro constitucional de proteção dos dados digitais a partir dos limites semânticos do inciso XII do artigo 5° da CF/1988, que trata essencialmente da inviolabilidade da comunicação de dados e que, em consonância com interpretação até então pacificada pelo Supremo Tribunal Federal (STF), não englobaria a proteção do dado ou informação em si, parece-nos que desde o advento da Emenda Constitucional n. 115/2022 não há mais dúvidas que a proteção dos dados pessoais ao menos ganhou assento entre os direitos fundamentais (art. 5°, LXXIX, CF/1988) e exige uma nova abordagem da temática, independentemente da inequívoca diferenciação entre os denominados dados estáticos e dinâmicos. Vale aqui pontuar que o próprio STF, na condição de último intérprete da CF/1988 e mesmo durante o caráter excepcional durante a pandemia de covid-19, já teve a oportunidade de fixar nova perspectiva de proteção dos dados pessoais e limitar o compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público, na forma do que se pretendia estabelecer a partir do advento da Medida Provisória n. 954/2020.[6]

---

6 "MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *FUMUS BONI JURIS. PERICULUM IN MORA*. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2°, I e II, da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de

Em relação ao tema dos dados pessoais custodiados por concessionária de serviço público, cumpre pontuar que a Lei n. 9.472/1997 ainda prevê que a prestadora do serviço de telefonia poderá valer-se de informações relativas à utilização individual pelo usuário na execução de sua atividade, ou seja, para o desempenho de seu objeto social, mas claramente limita a divulgação de tais informações a terceiros, ao estabelecer no §2° de seu artigo 72 que ela não poderá ocorrer quando permita "a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade", situação na qual o compartilhamento da informação agregada apenas deveria ocorrer com "anuência expressa e específica do usuário", como estabelece o §1° (BRASIL, 1997). Houve claro cuidado do legislador em tratar do acesso por terceiros de informações relacionadas à utilização pelo usuário – pessoa física ou jurídica - do serviço, o que nos parece que se aplica claramente aos circunstanciais momentos em que ele transita pelas regiões abrangidas pelas denominadas Estações Rádio Base (ERB). Tal raciocínio também pode ser depreendido do direito à inviolabilidade e ao segredo da comunicação previsto no art. 3°, V, do mesmo diploma, que faz a ressalva apenas "nas hipóteses e condições constitucional e legalmente previstas". Aqui nos parece necessário pontuar que a regra é a inviolabilidade do dado ou informação da utilização – individual - de um determinado usuário, a qual poderia ser afastada a partir de hipóteses legalmente previstas, ou seja, quando a ordem jurídica expressamente autorize o acesso a tais dados, como já ocorre, por exemplo, a partir do previsto na Lei de interceptações das comunicações telefônicas (Lei n. 9.296/1996), ou mesmo em outras hipóteses nas quais exista decisão fundamentada a partir de parâmetros legais que admitam expressamente o acesso a tal conteúdo, independentemente da concordância ou não do usuário. Além disso, note-se que por usuário é possível compreender também aquele que adquire e remunere o acesso aos serviços de telecomunicações prestados, ou seja, indicando para a clara possibilidade de uma determinada pessoa física ou jurídica, que custeia o serviço para uso próprio ou por outras pessoas indeterminadas,

---

dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5°, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5°, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados [...]" (ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020).

ter o direito ao acesso aos respectivos dados diretamente na condição de consumidora.

A questão da proteção dos dados digitais ganhou ainda mais densidade e claros contornos a partir do advento do Marco Civil da Internet - MCI (Lei n. 12.965/2014) e da Lei Geral de Proteção de Dados - LGPD (Lei n. 13.709/2018), de modo a indicar verdadeira superação do entendimento até então predominante na jurisprudência quanto a alguns contornos de aplicabilidade dos direitos fundamentais supracitados e trazendo inequívocos deveres jurídicos aos provedores de conexão e de acesso a aplicações de internet, bem como aos que façam o tratamento de dados pessoais na condição de pessoa física ou jurídica. Em que pesem as múltiplas implicações jurídicas e celeumas decorrentes das disposições contidas nos dois marcos normativos acima citados, as quais desbordam para aspectos relacionados à moderação e responsabilidade por conteúdo divulgado por terceiro – perfil ou usuário – em redes sociais[7] e quanto à eventuais discussões sobre o tratamento de dados pessoais sensíveis para o exercício regular de direitos em processo judicial,[8] pelos objetivos e limites do presente estudo nosso foco se limitará à análise dos deveres de guarda e exibição de tais dados a partir de determinação judicial oriunda de processo não penal.

Em tal sentido, cumpre pontuar que o art. 15 do MCI traz regramento

7 Em tal sentido vale realçar que o MCI ainda prevê em seu art. 19 que: "[...] o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. § 1° A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. § 2° A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5° da Constituição Federal. § 3° As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. § 4° O juiz, inclusive no procedimento previsto no § 3°, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação". (BRASIL, 2014).

8 Como já destacamos em outro estudo tratando da publicidade processual, a partir artigo 11, inciso II, alínea b, da LGPD é plenamente possível o tratamento de dados pessoais sensíveis para o exercício regular de direitos em processo judicial, administrativo ou arbitral, independentemente de consentimento do titular e sem exigência expressa da adoção de técnicas de anonimização (CASTRO; VEGAS JUNIOR, 2021, p. 431).

específico no que concerne ao período de guarda de registros de acesso a aplicações de internet, contemplando exclusivamente o dever de guarda "em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses", tempo que inclusive se coaduna com o prazo fixado no art. 38 do Código de Processo Penal (CPP) para fins de exercício do direito de queixa ou de representação pelo ofendido. Como se verifica, tal período é relativamente curto quando cotejado, por exemplo, com o período de prescrição das pretensões condenatórias relativas aos créditos trabalhistas típicos (art. 7°, XXIX, CF/1988), e denota, no mínimo, a duvidosa legalidade de se exigir dos responsáveis por tal guarda a imediata exibição de informações relativas a um período superior a 6 (seis) meses da data da ordem judicial. Vale apenas referir a título de esclarecimento que, apesar do modelo processual civil inequivocamente fixar que "ninguém se exime do dever de colaborar com o Poder Judiciário para o descobrimento da verdade" (art. 378 do CPC/2015), há regramento específico que trata da exibição de documento ou coisa por terceiro ao longo do procedimento, por meio do qual se fixa que o juiz apenas não admitirá a recusa se "o requerido tiver obrigação legal de exibir" o respectivo documento (art. 399, I, do CPC/2015). Assim, eventual recusa por ausência do dever jurídico de guarda dos dados de geolocalização ou de acesso relativos a período superior ao fixado no MCI,[9] parece-nos que não seria manifestamente injustificada a ponto de permitir, por exemplo, a aplicação de medidas indutivas em face do terceiro, na forma do que atualmente admite o art. 139, IV, do CPC/2015.

Ultrapassada tal questão e avançando em relação especificamente

9 "APELAÇÃO CÍVEL. MARCO CIVIL DA INTERNET. FORNECIMENTO DE REGISTROS DE ACESSO A APLICAÇÕES. Ação de obrigação de fazer. Sentença de parcial procedência, a fim de condenar o provedor de aplicação a inviabilizar acesso aos *links* fornecidos pela autora, bem como a fornecer os dados cadastrais dos administradores das contas responsáveis pelas publicações indicadas pela requerente, no prazo de 10 dias, sob pena de multa. Insurgência da ré. Preliminar de nulidade da sentença afastada. Alegação de impossibilidade de cumprir a obrigação quanto a uma das URLs descritas, vez que o perfil foi deletado em setembro de 2020, já tendo sido ultrapassado o prazo a que estava obrigada a armazenar e fornecer registros. Acolhimento. Marco civil da internet que prevê a obrigatoriedade da manutenção dos dados de acesso dos usuários por 06 meses (art. 15 da Lei 12.965/2014). Precedentes. Demanda que foi ajuizada muito após o prazo legal. Caso em que, ademais, o perfil já havia sido excluído pelo próprio usuário na ocasião de citação da ré, momento em tomou ciência da pretensão do usuário no fornecimento do registro. Sentença reformada apenas para afastar a condenação da ré em fornecer os dados cadastrais da mencionada URL. RECURSO PROVIDO." (v. 38577). (TJSP, Apelação Cível 1016907-96.2019.8.26.0477; Relator (a): Viviani Nicolau; Órgão Julgador: 3ª Câmara de Direito Privado; Foro de Praia Grande - 1ª Vara Cível; Data do Julgamento: 15/02/2022; Data de Registro: 15/02/2022).

à requisição ou determinação judicial, vale destacar que ela é minuciosamente prevista nos arts. 22 e 23 do MCI, nos seguintes termos:

> Art. 22. 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. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.
> Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro. (BRASIL, 2014).

A partir do disposto no *caput* do artigo 22 do MCI fica evidente que tal requisição habitualmente será realizada a partir de provocação da "parte interessada" na produção de conjunto probatório em processo judicial, o que em uma interpretação sistemática indica que habitualmente seria medida tomada por aquele que, em tese, foi alvo de alguma espécie de ofensa ou lesão por conteúdo disseminado a partir de conexão ou de registros de acesso a aplicações de internet, o que se reforça a partir da singela e atenta leitura seção anterior do MCI que trata justamente da responsabilidade por danos decorrentes de conteúdo gerado por terceiros, como se verifica dos artigos 18 a 21. Não é incomum que, a partir das características da rede mundial de computadores, ocorra a eventual prática de ofensa à honra ou disseminação de conteúdo lesivo por meio de perfil ou usuário sem a completa possibilidade de imediata identificação, razão pela qual se faria imprescindível o pronto acesso aos respectivos registros para fins de individualização da pessoa – física ou jurídica – para os devidos fins de responsabilização, seja no campo cível ou penal.[10] Por isso, como já afirmamos em outra seara, nos

10 Guardia (2012, p. 117), em estudo sobre os dados digitais no processo penal, pontua nesse particular que "a possibilidade de identificação do responsável por meio dos dados de tráfego é limitada a direção de IP, v.g., permite apenas revelar o computador utilizado, fator que pode

parece adequado que tal requisição possa ser "veiculada no processo do trabalho, já que evidente que o legislador ordinário não pretendeu afastar a possibilidade de tal requisição integrar o acervo probatório daquele de forma incidental" (VEGAS JÚNIOR, 2017, p. 137), valendo referir a título meramente exemplificativo a hipótese de produção antecipada de prova, na forma do art. 381 do CPC/2015, para eventual análise em futura demanda que tenha por objeto a pretensão de reparação por ofensa aos direitos da personalidade, a partir de ato decorrente da relação de trabalho e diante do que prevê o art. 114, VI, da CF/1988.

Todavia, isso não permite que se conclua que tal requisição possa ocorrer de forma indiscriminada e de maneira incidental em todos os processos trabalhistas, o que se reforça a partir do que estabelece o parágrafo único do art. 22 do MCI, quando elenca verdadeiros requisitos para o requerimento de acesso aos respectivos registros, quais sejam:

> "I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros".

Logo, não basta se cogitar da simplória ideia no sentido que a melhor prova de um determinado fato ocorrerá pelo acesso a tais informações. Embora a premissa de busca pelo melhor elemento de prova seja correta em termos epistêmicos,[11] isso não significa que seja sempre admissível juridicamente, especialmente à luz das válidas opções do legislador ordinário no sopesamento de todos os valores envolvidos dentro de determinado modelo de sociedade. Ainda que os dois últimos requisitos legais contidos no parágrafo único do art. 22 do MCI não exijam grandes dificuldades para especificação em uma determinada demanda trabalhista, pois o período dos registros pertinentes é de fácil identificação a partir dos limites da causa de pedir (tempo do contrato de trabalho ou da questão controvertida) e a motivação da utilidade do acesso tenha relação direta com o que se pretende provar (ideias de pertinência e relevância), não se pode ignorar o primeiro e principal requisito da regra aqui analisada, qual seja, a indicação de fundados indícios da ocorrência do ilícito. Tal

não se mostrar suficientemente elucidativo se consideradas as possíveis variações no uso de um número de IP (denominado IP dinâmico) ou o uso de ferramentas de navegação anônima. Ademais, se o identificado for parte de uma rede de acesso à internet, imprescindível a obtenção de dados das pessoas que utilizem a rede local".

11 Para uma análise da perspectiva da melhor prova possível ver, por todos, Nance (1988).

situação fática se apresenta mais evidente, por exemplo, diante de uma publicação ofensiva em rede social, ocasião na qual se faz pertinente apurar a autoria e responsabilidade pelo perfil ou usuário. Todavia, seria de maior dificuldade quando se cogita de uma divergência, por exemplo, quanto ao tempo à disposição em favor do empregador ao longo do contrato de trabalho. Mesmo que se dê ao termo ilícito uma interpretação ampla, no sentido de não se confundir apenas como as infrações penais, cabe se questionar, por exemplo, sobre qual seria a infração do usuário do serviço de telefonia que circunstancialmente é parte em um processo trabalhista no qual postula horas extras, bem como quais seriam os fundados indícios a partir dos quais se justificaria a determinação judicial para acesso a tais informações sobre os exatos locais de registro de conexão e de acesso a aplicações da internet.

3 Acesso aos dados de geolocalização, iniciativa probatória e papel esperado do juiz

A partir do panorama normativo acima fixado e de algumas premissas já alinhavadas dentro do estudo das disposições infraconstitucionais quanto aos dados de uso individual dos serviços de telefonia, registro de conexão e aplicações de internet, cumpre agora avançar para algumas considerações sobre o efetivo acesso a tais informações de maneira incidental no processo do trabalho, com especial enfoque na iniciativa probatória e no papel esperado do juiz em referidos procedimentos.

Como já foi acima especificado, nada impede que o próprio usuário obtenha, por meios próprios, os respectivos dados relacionados ao uso do serviço de telefonia e a sua geolocalização em um determinado período de tempo, sendo que eventual resistência dos responsáveis legais pela guarda e exibição pode validamente ser analisada nas esferas próprias que buscam pacificar eventuais conflitos decorrentes das relações de consumo ou até mesmo com intervenção judicial a partir, por exemplo, do procedimento de produção antecipada de prova. Não é incomum, inclusive, que por meio de seus próprios smartphones os respectivos titulares do bem móvel ou usuários de serviços de aplicativos compartilhem e autorizem – expressa ou tacitamente – o acesso a tais informações relacionadas ao momento e local em que estiveram ao longo de determinado período de tempo do dia. Tais situações denotam a clara possibilidade de que os respectivos dados eventualmente já sejam apresentados voluntariamente nos momentos próprios de produção de provas documentais, aqui entendida a ideia de documento

em sentido amplo e que não necessariamente se vincula a um suporte cartáceo, de modo que invariavelmente caberá ao juiz a respectiva valoração de tais elementos de prova para os fins pretendidos, em cotejo com todos os demais produzidos. Parece-nos assim plenamente pertinente a preocupação e adequação de iniciativas administrativas do Tribunal Superior do Trabalho (TST) e da respectiva Escola Nacional da Magistratura (ENAMAT) para a nova realidade digital de nossa sociedade, pois os efeitos de tal realidade no campo probatório são inexoráveis e demandam constante atualização dos sujeitos processuais e, por conseguinte, do próprio juiz.

De qualquer sorte, tais considerações não autorizam, ao arrepio dos limites constitucionais e legais, principalmente sem o consentimento - expresso - do titular dos dados, que se proceda à verdadeira devassa dos movimentos realizados ao longo da vivência em sociedade de alguém que portava aparelho celular com acesso à internet para fins, por exemplo, de apuração da sua provável jornada de trabalho. Não há dúvida que há uma relação teleológica entre prova e verdade,[12] sendo que a melhor demonstração possível daquilo que ocorreu no mundo fenomênico, por meio das mais diversas provas produzidas em contraditório, permanece sendo um importante fator de legitimação para o próprio Direito enquanto ciência. Todavia, tal premissa não permite que se desconsiderem os meios adotados ou outros valores constitucionais de relevância, sendo de pouca valia um ideal exclusivamente utilitarista, pois os meios utilizados também são importantes para legitimar os fins a serem alcançados. É preciso que o juiz, ao eventualmente ser provocado para a produção de um determinado meio de prova, analise a pertinência, relevância e também a respectiva admissibilidade da prova à luz de todo o ordenamento jurídico. Assim como ocorre no âmbito de pesquisas científicas e também em outros contextos investigativos existem limites decorrentes de outros valores consagrados como de maior relevância em cada campo do conhecimento ou de atuação humana, o que fica ainda mais evidente quando se cogita do exercício de parcela de poder em um Estado Democrático de Direito, como aquele albergado na CF/1988.

Nem mesmo as disposições relacionadas à iniciativa probatória do julgador (art. 765 da Consolidação das Leis do Trabalho - CLT e art. 370 do Código de Processo Civil - CPC/2015), independentemente de

12 "Há uma relação teleológica entre prova e verdade, de modo que a verdade se configura como o objetivo institucional a ser alcançado mediante prova." (FERRER-BELTRÁN, 2022, p. 19).

seu eventual caráter concorrente ou supletivo em relação às partes envolvidas, seriam capazes de justificar o acesso indiscriminado e ao arrepio dos limites legais analisados no tópico anterior. Em que pese o artigo 765 da CLT estabeleça a possibilidade do julgador determinar "qualquer diligência necessária ao esclarecimento" da causa, é evidente que tal regra não pode ser interpretada literalmente, mas sim de forma sistemática e em consonância com o modelo constitucional de processo, o qual, por exemplo, ainda consagra a vedação expressa ao uso da tortura (artigo 5°, III, da CF/1988) e adota a dignidade da pessoa humana com um fundamento central do Estado Democrático de Direito (artigo 1°, III, da CF/1988). O juiz no desempenho de sua iniciativa probatória pode validamente determinar a exibição de documentos ou outras provas pertinentes e relevantes, mas não pode tudo e muito menos tem o condão de transformar um meio inadmissível em prova lícita, apenas por conta de sua iniciativa probatória. Em que pese exista corrente doutrinária que defenda uma necessária diferenciação quanto à denominada inidoneidade do resultado obtido em cotejo com a inadequação do meio adotado, para fins de justificar uma excepcional possibilidade de se admitir, por iniciativa do juiz, o acesso a provas ilícitas no processo civil,[13] não nos parece que esse seja o papel esperado juiz do trabalho em um Estado de Direito. Além disso, vale ressaltar que a CF/1988 não trata de maneira substancialmente diferente a inadmissão de uma prova ilícita (artigo 5°, LVI, da CF/1988) que deriva do uso de tortura (artigo 5°, III, da CF/1988) daquela obtida por meio de interceptação telefônica sem autorização judicial (artigo 5°, XII, da CF/1988), ao menos para fins de condenação em processo penal, o que denota que a iniciativa do juiz, por si só, em nada afeta o tema da admissibilidade.[14]

Nem se cogite aqui de qualquer possível analogia entre as

13 "Se a prova foi obtida por meio ilícito, deveria competir exclusivamente ao magistrado determinar de ofício sua produção, se entender conveniente e necessário para evitar nova violação do ordenamento jurídico." (BEDAQUE, 2009, p. 159).

14 Nem se cogite que o artigo 13 da lei do processo judicial eletrônico (Lei n. 11.419/2006) possa ser interpretado de maneira tão ampla a ponto de vulnerar as garantias fundamentais ou permitir o indiscriminado acesso aos dados digitais. A regra apenas fixa que o juiz "poderá determinar que sejam realizados por meio eletrônico a exibição e o envio de dados e de documentos necessários à instrução do processo", ou seja, trata do meio – digital - de produção da prova e nada dispõem sobre a ideia de ampla admissibilidade. No mesmo sentido é o que se denota da previsão contida no art. 7°, VI, da LGPD, que apenas admite o tratamento de dados pessoais para o "exercício regular de direitos em processo judicial", ou seja, nada dispõe especificamente quanto à forma de acesso e requisição de tais dados, bem como não autoriza qualquer devassa indiscriminada em dados oriundos de equipamento privado.

testemunhas e as respectivas ERBs ou sistemas digitais de acesso a aplicativos, como se esses últimos pudessem atuar na condição de objetos – físicos ou digitais - que presenciam aspectos fáticos pertinentes e relevantes para uma determinada causa, até mesmo pelas distinções muito claras entre elas e as pessoas físicas, mas também pela necessária limitação do uso de provas anômalas, ou seja, das provas típicas sem observância dos requisitos legais. Como a CLT estabelece, por exemplo, que as partes e testemunhas serão inquiridas em audiência (art. 820), não se pode concluir que a apresentação de singela declaração manuscrita assinada pelas partes ou testemunhas presenciais tenha ampla aceitação e idêntica valoração ao de um testemunho em juízo, o que em alguma medida se aplica à informação obtida de uma ERB, que é claramente uma prova digital ou documento em sentido amplo, e não uma espécie de prova testemunhal. Para além disso, parece-nos importante não se olvidar da possível existência de ao menos uma expectativa de privacidade do usuário em relação aos seus movimentos diários com seu respectivo aparelho celular.[15] Parece-nos adequado aqui estabelecer um paralelo com aquilo que há algum tempo já foi utilizado pela jurisprudência para tratar, por exemplo, da admissibilidade do acesso pelo empregador às mensagens encaminhadas por endereço eletrônico (*e-mail*) corporativo.[16] Logo, seria válido apenas se cogitar de inexistência de tal expectativa a partir do uso de ferramentas ou equipamentos fornecidos pelo empregador para o desempenho da função ou execução do contrato de trabalho, como eventual celular corporativo, cartão com acesso a crédito para abastecimento de veículo e outros dispositivos por meios dos quais, a partir da confirmação da existência de tratamento dos dados e ciência do usuário, na forma dos arts. 7, *caput* e inciso V, da LGPD.[17]

---

15 Em sentido contrário ver Duplat Filho (2021) e Albino e Lima (2022).

16 Consoante se depreende do trecho de seguinte ementa extraída de julgado tratando de correio eletrônico corporativo e que foi oriundo da 1ª Turma do TST: "Pode o empregador monitorar e rastrear a atividade do empregado no ambiente de trabalho, em *e-mail* corporativo, isto é, checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a prova assim obtida, visando a demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho. Inexistência de afronta ao art. 5°, incisos X, XII e LVI, da Constituição Federal. 6. Agravo de Instrumento do Reclamante a que se nega provimento" (TST, RR-61300-23.2000.5.10.0013, 1ª Turma, Relator Ministro João Oreste Dalazen, DEJT 10/06/2005).

17 Ainda que em outro contexto, são valiosos os ensinamentos da doutrina quanto aos limites de proteção da cláusula de sigilo das correspondências (Art. 5°, XII, CF/1988), notadamente quando se destaca que "a utilização de meio de comunicação que de antemão se sabe não ser reservado e estar sujeito a fiscalização impede que se invoque a proteção conferida à

O que não se espera, ao menos dentro do campo probatório e do modelo processual vigente, é que se utilize a figura do juiz para se legitimar a vulneração de garantias constitucionais e até mesmo para permitir uma mera conveniência daquele que habitualmente já faz o tratamento de dados pessoais ou tenha a condição de fazê-lo, não sendo incomum na atualidade que as partes obtenham o acesso a tais dados digitais antes do ajuizamento da demanda e subsidiem a suas manifestações com elementos de provas digitais capazes de corroborar as suas afirmativas ou minimamente desconstruir narrativas insinceras da parte contrária. Como se verifica, não se cuida aqui de congelar o processo no tempo ou mesmo se trata de consagrar o mundo analógico em detrimento do mundo digital, mas sim de se adequar importante mecanismo de solução de controvérsias ao devido processo legal, por meio do qual não se legitimam, ao menos em tese, medidas utilitaristas ou sorrateiras que não se coadunam com os limites legais, ainda que por iniciativa do agente político responsável pela condução da instrução processual. O próprio modelo processual já prevê válidos mecanismos para coibir eventuais abusos das partes que apresentarem afirmações manifestamente insinceras, como se depreende, por exemplo, da atual previsão do art. 844, §4°, inciso IV da CLT no sentido que, mesmo diante da revelia, não haverá confissão – ficta – quando "as alegações de fato formuladas pelo reclamante forem inverossímeis ou estiverem em contradição com prova constante dos autos", bem como dos já conhecidos mecanismos de sanção por litigância de má-fé, na forma do atualmente previsto nos arts. 793-B e 793-C da CLT.

O tema é por demais palpitante e ostenta múltiplos desdobramentos para além dos estreitos limites do que aqui se pretendeu destacar sobre o papel do juiz a partir dos limites de admissibilidade de uma espécie de prova digital, qual seja, o acesso à geolocalização de usuários de dispositivos eletrônicos. Já existem, ao menos no âmbito dos Tribunais Regionais do Trabalho, análises jurisprudenciais de tal fenômeno, sendo que já houve o reconhecimento de verdadeira ofensa ao sigilo telemático e privacidade do usuário na requisição de dados de geolocalização para "suprir" prova da jornada de trabalho,[18] como se depreende da seguinte ementa:

---

intimidade. Há consentimento à quebra da intimidade, que atua como pré-excludente de ilicitude, independentemente de prévia autorização judicial. Quem envia mensagem em cartão postal, por exemplo, não pode queixar-se de haver sido ela lida" (MALLET, 2009, p. 205).

18 Em sentido contrário já decidiu a SDI-I do Tribunal Regional do Trabalho da 2ª Região, consoante se depreende da seguinte ementa: "DADOS DE GEOLOCALIZAÇÃO. PROVA DA JORNADA DE TRABALHO. PROPORCIONALIDADE. VALIDADE. A geolocalização é uma prova mais robusta

> DADOS DE GEOLOCALIZAÇÃO. REQUISIÇÃO. OFENSA AO DIREITO AO SIGILO TELEMÁTICO E À PRIVACIDADE. Embora a prova digital da geolocalização possa ser admitida em determinados casos, ofende direito líquido e certo ao sigilo telemático e à privacidade, a decisão que determina a requisição de dados sobre horários, lugares, posições da impetrante, durante largo período de tempo, vinte e quatro horas por dia, com o objetivo de suprir prova da jornada a qual deveria ser trazida aos autos pela empresa. Inteligência dos incisos X e XII do art. 5° da CR (TRT da 3ª Região; PJe: 0011155-59.2021.5.03.0000 (MS); Disponibilização: 04/11/2021, DEJT/TRT3/Cad.Jud, Página 939; Órgão Julgador: 1ª Secao de Dissidios Individuais; Relator: Marco Antonio Paulinelli Carvalho).

O Superior Tribunal de Justiça - STJ, embora já tenha reputado que a "identificação de usuários que operaram em determinada área geográfica, suficientemente fundamentada, não ofende a proteção constitucional à privacidade e à intimidade",[19] a partir da aplicabilidade no caso concreto dos postulados da razoabilidade e da proporcionalidade por parte do juiz condutor da instrução, assim o faz habitualmente em casos de investigação criminal e também condicionando a realização do acesso aos dados digitais à inexistência de "outra medida possível para se desvendar o crime"[20]. Como se nota, parece-nos que a situação fática de elucidação de um crime de homicídio não se equipara ao tratamento processual e amplitude probatória aplicável a um processo trabalhista que trata de discussão sobre jornada de trabalho e data de admissão de um empregado, valendo aqui apenas pontuar que o ordenamento pátria já indica para tal conclusão a partir do que

---

que a prova testemunhal, pois as testemunhas podem se esquecer de fatos ou mesmo alterar a verdade dos fatos de forma deliberada. Frise-se que o ônus de juntar os controles de jornada é da empregadora, enquanto o de comprovar sua inidoneidade é da empregada e a prova seria para esclarecer os fatos, seja confirmando a tese da defesa, seja confirmando a tese da autora, de forma que a medida é adequada e necessária. Outrossim, quanto à exposição da privacidade da autora, o Juízo soube equilibrar os direitos em colisão, pois delimitou a exposição dos dados relativos apenas aos períodos em que a reclamante estaria no local de trabalho e determinou que os dados sejam colhidos por amostragem (três meses para cada ano trabalhado), de forma que a decisão impetrada é proporcional em sentido estrito e, portanto, válida." (TRT da 2ª Região; Processo: 1002734-56.2022.5.02.0000; Data: 26-04-2023; Órgão Julgador: SDI-1 - Cadeira 9 - Seção Especializada em Dissídios Individuais - 1; Relator(a): IVETE BERNARDES VIEIRA DE SOUZA).

19 STJ. RMS n. 61.302/RJ, relator Ministro Rogerio Schietti Cruz, Terceira Seção, julgado em 26/8/2020, DJe de 4/9/2020.

20 STJ, AgRg no RMS n. 68.487/PE, relator Ministro Ribeiro Dantas, Quinta Turma, julgado em 6/9/2022, DJe de 15/9/2022.

está previsto, por exemplo, em relação à interceptação telefônica já referida em tópico acima. A utilização da geolocalização do usuário individualmente identificado como elemento de prova em processos judiciais ainda não foi minuciosamente analisado no pleno do STF,[21] sendo que merece destaque o acompanhamento do julgamento a ser proferido no Recurso Extraordinário n. 1.301.250-RJ, por meio do qual já houve o reconhecimento da "repercussão geral" prevista no §3° do art. 102 da CF/1988 e fixação do tema 1148 sobre os "limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas".

Além de todas as premissas acima fixadas, não se pode olvidar também da devida contextualização e valoração dos respectivos dados digitais a partir de sua eventual disponibilização – de maneira espontânea ou após o cumprimento de requisição judicial – nos autos, a qual deverá ocorrer em conjunto com os demais elementos de prova e atentando-se para as garantias aplicáveis à instrução probatória, sem se cogitar necessariamente de qualquer espécie de primazia, até mesmo por não se tratar de elemento infalível e que justifique todas as ilações construídas a partir de um determinado dado digital. Não é demasiado relembrar que em algumas circunstâncias a decisão judicial fixando o uso do multicitado remédio – acesso à geolocalização – em nada contribuirá sensivelmente para o esclarecimento da discussão fática ou definição do enquadramento jurídico das questões submetidas ao juiz. É o que ocorre, por exemplo, com o acesso aos dados digitais oriundos do celular pessoal a partir do seu contato com uma específica ERB (Estação Rádio Base), indicando, por meios de ângulos de alcance

21 De qualquer sorte, vale referir que existem decisões monocráticas que já abordaram o tema, sendo de grande pertinência para os fins aqui pretendidos a menção aos seguintes trechos de voto do Min. Gilmar Mendes quando da análise de suposta ilegalidade da Comissão Parlamentar de Inquérito do Senado Federal – CPI da Pandemia: "[...] é discutível, ao menos em tese, a extensão do dever jurídico de provedores de aplicações de disponibilizarem o acesso a registros de conexão, dados de comunicação e conteúdos de comunicações privadas dos seus usuários. Ainda que entendamos que as aplicações de internet podem ser compelidas a conceder o acesso a esses dados para fins de instrução criminal quando houver ordem judicial expressa, remanesceria ainda a questão de saber se as Comissões Parlamentares de Inquérito também deteriam o poder investigativo de ordenar essa disponibilização[...]" e "[...] ao menos em um juízo de cognição sumária, parece de fato que o eventual afastamento do sigilo dos dados referenciados no Requerimento teria o potencial de gerar uma exposição bastante alargada da intimidade das pessoas naturais que estão por trás da pessoa jurídica. A partir dos dados colhidos, a CPI poderia acessar uma infinidade de conversas privadas, além de fotos, vídeos e áudios e dados de localizações geográficas, tudo 'de 2018 até o presente', como o próprio Requerimento sugere [...]." (STF, MC em MS n. 38.189/DF, Min. Gilmar Mendes, julgado em 10/09/2021, DJe de 14/9/2021).

da respectiva estação,[22] que o dispositivo permanecia nas proximidades de um determinado estabelecimento do empregador após a jornada de trabalho, o que pode, em tese, acarretar pertinentes discussões quanto à ocorrência concreta de uma das hipóteses em que o empregado estaria "nas dependências da empresa para exercer atividades particulares", na forma das situações contidas no §2° do atual art. 4° da CLT. Além disso, a mera localização do empregado nas proximidades ou mesmo em sua própria residência também não é sempre incompatível com a situação em que ele "esteja à disposição do empregador", o que se verifica, por exemplo, quando exista regime de trabalho híbrido ou na situação de regime de teletrabalho para todos aqueles que não prestam serviços exclusivamente por produção e tarefa, em consonância com os limites da controversa hipótese inserida no inciso III do art. 62 da CLT, por meio da Lei n. 14.442/2022. No mesmo sentido é o que pode ocorrer a partir de questão fática controvertida que se refira a evento ocorrido em data muito superior ao período fixado em lei (art. 15 do MCI), que acaba limitando o dever jurídico de guarda dos registros de acesso a aplicações de internet.

4 Considerações finais

A partir das considerações acima apresentadas e na perspectiva de construção de um debate quanto ao tema central do presente estudo, pode-se concluir que os atuais limites constitucionais e infraconstitucionais indicam para uma verdadeira proteção da privacidade dos dados digitais gerados a partir da mera utilização de um determinado dispositivo eletrônico pessoal, sendo que as operadoras de telefonia e provedores de aplicativo possuem deveres jurídicos bastante limitados para se cogitar de uma tendência de ampla disseminação do uso da geolocalização como meio de prova no processo do trabalho. A previsão contida no atual art. 22 do MCI possui requisitos para franquear o acesso a terceiros dos registros de conexão e de aplicações da internet de um determinado usuário, sendo que não trata especificamente da geolocalização e muito menos de seu uso em processos judiciais. Não se pode olvidar da exigência de indicação na decisão judicial dos "fundados indícios da ocorrência do ilícito" (inciso II do parágrafo único do art. 22),

22 "As antenas ERB podem alcançar até um raio de 1 a 2 km, sendo possível precisar uma região em que o usuário está dentro do ângulo de alcance de uma antena ERB (ângulo chamado de Azimute)." (ALBINO; LIMA, 2022, p. 228).

razão pela qual há ao menos uma elevada carga argumentativa a ser observada pelo juiz do trabalho quando estiver diante de discussão que envolva elucidação da jornada de trabalho ou da data de admissão do empregado, o que seria de grande dificuldade antes da apresentação de elementos capazes de formação ao menos de um juízo indiciário de ilicitude. Tal ilicitude não se pode presumir a partir da mera alegação ou conveniência de uma das partes que optou pela não instituição válida de controle de ponto (art. 74 da CLT), de modo a ser paradoxal que o suposto autor de um ilícito trabalhista possua legitimidade para se valer da própria torpeza em juízo e requisitar dados digitais daquele que, a princípio, não incorreu exatamente na hipótese descrita no parágrafo único do art. 22 do MCI. De qualquer sorte, parece-nos que a atual disposição do MCI acima mencionada tem relação, de fato e a partir de sua análise sistemática, com algo mais próximo de um ilícito de cunho criminal ou equivalente e não se coaduna com a mera divergência de afirmações de partes e testemunhas em um específico processo do trabalho. Não nos parece que o acesso indiscriminado a tais dados digitais de geolocalização de usuários privados seja o papel esperado do juiz, pois, ainda que inequivocamente ele possua iniciativa probatória no processo do trabalho, sua conduta está adstrita aos limites e valores do ordenamento jurídico pátrio, sendo que deve sopesar todas as regras de inadmissibilidade probatória e considerar os exatos limites dos deveres jurídicos impostos às partes e aos terceiros. Já em sede de conclusão, destaque-se que muitas vezes os próprios envolvidos na condição de usuários e titulares de um determinado dispositivo eletrônico já terão amplo acesso ao conteúdo de tais dados e poderão, ao menos em tese, apresentá-los voluntariamente em juízo. Por fim, ainda que se cogite da aplicação dos postulados da razoabilidade e proporcionalidade da medida, em verdadeira e discutível nova ponderação de valores no caso concreto para além dos limites do art. 22 do MCI, cumpre pontuar que nos parece bastante frágil a premissa de existência de proporcionalidade em sentido estrito na decisão do juiz do trabalho que determine a exibição de dados digitais de geolocalização oriundos de dispositivos eletrônicos de uso pessoal das partes e testemunhas.[23]

---

23 "A última etapa da proporcionalidade, que consiste em um sopesamento entre os direitos envolvidos, tem como função principal justamente evitar esse tipo de exagero, ou seja, evitar que medidas estatais, embora adequadas e necessárias, restrinjam direitos fundamentais além daquilo que a realização do objetivo perseguido seja capaz de justificar." (SILVA, 2011, p. 175).

Referências

ALBINO, João Pedro Donaire; LIMA, Ana Cláudia Pires Ferreira de. Técnicas de captura de geolocalização para produção de prova judicial. *Revista Direito das Relações Sociais e Trabalhistas,* São Paulo, v. 8, n. 1, p. 216-233, jan./jun. 2022.

BEDAQUE, José Roberto dos Santos. *Poderes instrutórios do juiz*. 3. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2009.

BRASIL. *Decreto-Lei n. 5.452, de 1 de maio de 1943*. Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro: Presidência da República, [1943]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 12 jul. 2022.

BRASIL. *Lei n. 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 n. 8, de 1995. Brasília, DF: Presidência da República, 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9472.htm. Acesso em: 6 jun. 2023.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 6 jun. 2023.

BRASIL. *Lei n. 13.105, de 16 de março de 2015*. Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 12 jul. 2022.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 jun. 2023.

CASTELLS, Manuel. *A sociedade em rede*. Tradução: Roseneide

Venâncio Majer. 2. ed. São Paulo: Paz e Terra, 1999. (A era da informação: economia, sociedade e cultura, 1).

CASTRO, Ítalo Menezes de; VEGAS JÚNIOR, Walter Rosati. O princípio da publicidade, o direito processual do trabalho e os meios eletrônicos. *In:* NUNES, Dierle José Coelho; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro (org.). *Inteligência artificial e direito processual*: os impactos da virada tecnológica no direito processual. 2. ed. rev., atual. e ampl. Salvador: JusPodivm, 2021. p. 411-438.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2021.

DUPLAT FILHO, Luiz Evandro Vargas. As provas digitais e o operador do Direito do século 21. *Consultor Jurídico*, São Paulo, 8 nov. 2021. Disponível em: https://www.conjur.com.br/2021-nov-08/duplat-filho-provas-digitais-operador-direito-seculo-21. Acesso em: 28 abr. 2022.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Cadernos de Direito Constitucional e Ciência Política*, São Paulo, a. 1, n. 1, p. 77-90, out./dez. 1992.

FERRER-BELTRÁN, Jordi. *Prova sem convicção*: standards de prova e devido processo. Tradução: Vitor de Paula Ramos. São Paulo: JusPodivm, 2022.

GUARDIA, Gregório Edoardo Raphael Selingardi. *Comunicações eletrônicas e dados digitais no processo penal*. 2012. Dissertação (mestrado em direito processual penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

MALLET, Estêvão. Apontamentos sobre o direito à intimidade no âmbito do contrato de trabalho. *Revista da Faculdade de Direito da USP*, São Paulo, v. 104, p. 199-226, 2009.

NANCE, Dale. A. The best evidence principle. *Iowa Law Review*, Iowa City, v. 73, p. 227-297,1988. Paper. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3741500. Acesso em: 7 jun. 2023.

SILVA, Virgílio Afonso da. *Direitos fundamentais*: conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2011.

VEGAS JÚNIOR, Walter Rosati. *Prova no processo do trabalho*: das influências dos avanços tecnológicos e sua utilização no direito trabalhista. Curitiba: Juruá, 2017.