A prova por geolocalização no Processo do Trabalho: limites constitucionais e a jurisprudência recente do Tribunal Superior do Trabalho

Clovis Andrade Goulart
Advogado da CAIXA no Rio Grande do Sul.

RESUMO

A prova por geolocalização, viabilizada por tecnologias como GPS, Estações Rádio-Base (ERBs) e registros de aplicativos, tem se consolidado como instrumento relevante na apuração de jornada e horas extras no Processo do Trabalho. Contudo, seu uso intensifica a tensão entre o direito fundamental à prova e os direitos à intimidade, vida privada e sigilo de dados, especialmente diante do reconhecimento expresso da proteção de dados pessoais como direito fundamental pela EC 115/2022, em diálogo com o regime estabelecido pela LGPD. Analisa-se a orientação do STF e do STJ quanto à vedação de medidas genéricas e à exigência de fundamentação reforçada. Por fim, examina-se a jurisprudência recente do TST acerca da admissibilidade da geolocalização, com ênfase nos requisitos de delimitação temporal, necessidade e sigilo judicial.

Palavras-chave: Geolocalização. Prova digital. Tribunal Superior do Trabalho. Proteção de dados pessoais.

ABSTRACT

Geolocation evidence, enabled by technologies such as GPS, cell tower records (CSLI), and application logs, has become a relevant instrument for verifying working hours and overtime in Brazilian labor litigation. However, its use intensifies the tension between the fundamental right to evidence and the rights to privacy, private life, and data secrecy, especially in light of the express recognition of personal data protection as a fundamental right by Constitutional Amendment No. 115/2022, in dialogue with the legal framework established by the LGPD (Brazilian General Data Protection Law). This paper analyzes the guidelines set by the Brazilian Supreme Court (STF) and the

Superior Court of Justice (STJ) regarding the prohibition of blanket measures and the requirement of enhanced judicial reasoning. Finally, it examines recent case law of the Superior Labor Court (TST) on the admissibility of geolocation evidence, with emphasis on the requirements of temporal delimitation, necessity, and judicial secrecy.

Keywords: Geolocation. Digital evidence. Brazilian Superior Labour Court. Personal data protection.

Introdução

No final do século XVIII, o filósofo e jurista inglês Jeremy Bentham concebeu uma estrutura arquitetônica destinada a revolucionar os mecanismos de controle social: o Panóptico. Em sua obra seminal, intitulada "O Panóptico" (BENTHAM, 2008), o autor descreveu um modelo de inspeção circular que permitia a um único observador monitorar todos os indivíduos sem que estes pudessem identificar o momento exato da fiscalização. Para Bentham, a eficácia do poder não residia na força física, mas na onipresença da vigilância e na consequente autodisciplina do indivíduo diante da incerteza do olhar constante.

Essa premissa foi profundamente esmiuçada por Michel Foucault em *Vigiar e Punir* (FOUCAULT, 2014), obra na qual o filósofo francês elevou o projeto *benthamiano* à categoria de diagrama de poder da sociedade moderna. Para Foucault, a disciplina panóptica não se restringe aos muros das prisões; ela se infiltra nas fábricas, nas escolas e nos hospitais, transformando o espaço social em um campo de visibilidade permanente, onde o indivíduo interioriza a vigilância, tornando-se o próprio guardião de sua conduta.

Nos tempos atuais, a lógica foucaultiana sofre uma metamorfose profunda sob a égide da revolução digital. O "Panóptico tecnológico" reside no fluxo de dados gerados ininterruptamente por dispositivos móveis.

O direito fundamental à privacidade (art. 5º, X, da CF/88) — entendido como "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (RODOTÁ, 2008, p. 15) — está no centro das discussões constitucionais. Isso ocorre porque as tecnologias da informação, ao induzirem a "hiperdocumentação" do cotidiano, têm deixado vulneráveis aspectos sensíveis da vida íntima, desde pequenos atos domésticos até movimentações físicas e manifestações em redes sociais.

Nesse cenário, os dados de geolocalização consolidam-se como elementos disruptivos no Direito Processual do Trabalho. A possibilidade de reconstruir a jornada laboral com precisão matemática confronta o Direito com um dilema axiológico: de um lado, a busca pela verdade; de outro, os direitos fundamentais à intimidade, à vida privada, ao sigilo de dados e à proteção de dados pessoais. O Tribunal Superior do Trabalho constitui espaço privilegiado para observar a colisão entre modernização probatória e direitos fundamentais.

1 A limitação do direito à prova no uso da geolocalização no processo do trabalho

O direito à prova constitui garantia fundamental do processo justo e instrumento indispensável para a efetividade do acesso à Justiça e para uma ordem jurídica justa. No ordenamento jurídico brasileiro, encontra fundamento nos arts. 369 e 371 do Código de Processo Civil, os quais asseguram às partes a possibilidade de empregar todos os meios legais e moralmente legítimos para demonstrar a verdade dos fatos, bem como no art. 765 da Consolidação das Leis do Trabalho, que confere ao magistrado ampla liberdade na condução do processo e na apreciação das provas necessárias ao esclarecimento da controvérsia.

Todavia, o direito à prova não possui caráter absoluto. Seu exercício encontra limites materiais nos direitos e garantias fundamentais assegurados pela Constituição Federal, especialmente na proteção à intimidade, à vida privada, à honra e à imagem (art. 5º, X), no sigilo de dados (art. 5º, XII), bem como no direito à proteção de dados pessoais (art. 5º, LXXIX). Assim, a atividade probatória deve ser exercida de forma compatível com a proteção da esfera privada do indivíduo.

Verifica-se aqui, no contexto da sociedade digital, uma tensão: de um lado, o direito à prova, enquanto garantia essencial à efetividade da tutela jurisdicional e à formação do convencimento judicial; de outro, situam-se os direitos fundamentais, diretamente afetados pela utilização de tecnologias capazes de reconstruir rotinas, deslocamentos e padrões comportamentais do trabalhador, revelando hábitos de vida e dinâmicas pessoais dotadas de elevado potencial invasivo. Diante desse cenário, impõe-se questionar: até que ponto a busca pela verdade processual pode legitimar a ingerência na esfera privada do trabalhador? Em que medida o direito à prova autoriza a reconstrução de rotinas pessoais e deslocamentos individuais, sem comprometer o núcleo essencial dos direitos à intimidade, à vida privada e à proteção de dados?

A admissibilidade da geolocalização como meio probatório não comporta soluções apriorísticas ou absolutas, exigindo análise casuística e criteriosa. Em contextos nos quais existam controles de ponto regulares ou outros meios probatórios idôneos, igualmente aptos ao esclarecimento dos fatos controvertidos, a utilização da geolocalização tende a ser compreendida como medida excessiva, por ampliar a ingerência na esfera privada do empregado sem acréscimo proporcional de utilidade probatória.

A doutrina processual trabalhista reconhece que o direito à prova constitui garantia fundamental da cidadania, mas ressalta que sua admissibilidade está condicionada à compatibilidade com os direitos fundamentais (SCHIAVI, 2017, p. 672). Nessa linha, a jurisprudência tem afirmado que a busca pela verdade processual não legitima, por si só, restrições desproporcionais à privacidade e ao sigilo de dados, exigindo-se fundamentação robusta para qualquer medida restritiva.

O mero interesse probatório não constitui fundamento jurídico suficiente para legitimar a coleta e o uso de dados de geolocalização, sendo imprescindível a demonstração de sua indispensabilidade e da inexistência de meios alternativos menos invasivos.

Nesse prisma, os princípios da proporcionalidade e da necessidade assumem papel central como parâmetros de controle da admissibilidade da prova de geolocalização. Conforme leciona Gilmar Ferreira Mendes, qualquer restrição a direitos fundamentais deve ser adequada, necessária e não excessiva em relação à finalidade pretendida, funcionando a proporcionalidade como mecanismo de equilíbrio entre interesses em conflito (MENDES, 2021, p. 663). Essa leitura é reforçada pela compreensão da dignidade da pessoa humana como eixo estruturante do sistema constitucional, na medida em que, conforme sustenta Sarlet, ela é valor-fonte e critério hermenêutico dos direitos fundamentais, funcionando como parâmetro de legitimação e de limitação de toda atuação estatal e privada que interfira na esfera jurídica do indivíduo, especialmente quando envolvidas restrições à liberdade, à intimidade e à autonomia pessoal (SARLET, 2019, p. 232).

2 A prova digital no processo do trabalho e seu regime legal: da LGPD à EC 115/2022

No cenário contemporâneo, a prova digital emergiu como elemento fundamental para a instrução processual, especialmente no âmbito trabalhista. Conforme conceitua Patrícia Peck Pi-

nheiro (2021), trata-se do "conjunto de evidências e arquivos eletrônicos que representam a relação e/ou obrigação gerada, acordada ou contratada por uma via digital". Sua relevância no processo do trabalho é dupla: serve tanto para comprovar fatos ocorridos integralmente no mundo virtual quanto para documentar, por meio de rastros digitais, acontecimentos do mundo físico. Isso ocorre porque a rotina laboral está cada vez mais permeada por ferramentas tecnológicas, englobando desde comunicações realizadas por aplicativos de mensagens, como WhatsApp e Telegram, até registros em redes sociais, que podem evidenciar vínculos empregatícios, atividades desempenhadas ou condutas inadequadas. Além disso, comprovantes de transações eletrônicas, *logs* de acesso a sistemas corporativos e trocas de e-mails formam um conjunto probatório robusto e, frequentemente, decisivo.

Já em 2011, quando os smartphones começavam a se popularizar e o debate sobre privacidade digital ainda engatinhava, o Parecer 13/2011 do *Article 29 Data Protection Working Part*y (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2011) — órgão consultivo europeu precursor do atual Comitê Europeu para a Proteção de Dados (EDPB) — sistematizava, com notável visão de futuro, as principais infraestruturas de geolocalização em dispositivos móveis. O parecer alertava, já naquela ocasião, para os riscos à privacidade decorrentes da coleta massiva e, muitas vezes, despercebida desses dados, que podem revelar padrões íntimos da vida dos titulares.

Esse movimento demandou uma nova postura jurídica, a qual passou a tratar a informação como um bem jurídico relevante e sua proteção como prioridade. Nesse contexto, a União Europeia impulsionou o debate internacional com o *General Data Protection Regulation* – GDPR (UNIÃO EUROPEIA, 2016), servindo como paradigma para diversos ordenamentos — inclusive o brasileiro, que editou a sua Lei Geral de Proteção de Dados (LGPD — Lei nº 13.709/2018), com o objetivo de aprimorar a governança de dados pessoais e garantir a proteção dos direitos fundamentais na era digital.

É imperativo ressaltar, contudo, que a proteção de dados no Brasil não se originou com a LGPD, possuindo raízes em diversos diplomas legais preexistentes. A matéria já era contemplada, em diferentes graus, pelo Código de Defesa do Consumidor (1990), ao disciplinar os bancos de dados de consumo, e pela Lei do Habeas Data (1997). Posteriormente, a Lei de Acesso à Informação (2011) e o Marco Civil da Internet (2014) pavimenta-

ram, definitivamente, o caminho para a tutela da esfera privada do cidadão no ambiente digital.

Dessa forma, a LGPD sistematizou princípios que já permeavam o ordenamento jurídico e estabeleceu um marco infraconstitucional sólido. É relevante notar que, mesmo antes da Emenda Constitucional nº 115/2022, o Supremo Tribunal Federal — notadamente no julgamento das ADIs relativas à MP 954 em 2020, que será detalhado adiante — já reconhecia a proteção de dados pessoais como um direito fundamental implícito. Para a Corte, tal direito é corolário da dignidade da pessoa humana, do livre desenvolvimento da personalidade e das garantias de privacidade e intimidade (SARLET, 2022).

O advento da Emenda Constitucional 115/2022 promoveu uma mudança de paradigma ao inserir no art. 5º, LXXIX, da CF, a garantia de que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Essa positivação formal, como destaca Ingo Sarlet, confere ao direito uma carga positiva adicional e consequências jurídicas profundas: (i) consolida sua autonomia como direito fundamental com âmbito de proteção próprio; (ii) submete-o a uma reserva legal simples, tornando a LGPD sua lei regulamentadora específica; e, de modo crucial, (iii) elimina qualquer 'zona livre' de proteção, assegurando que setores excluídos do âmbito material da LGPD também devam respeitar seu núcleo essencial (SARLET, 2022).

Este robusto regime legal, portanto, projeta-se diretamente sobre o processo do trabalho, gerando uma tensão processual concreta. De um lado, o artigo 765 da Consolidação das Leis do Trabalho confere ao juiz ampla liberdade na condução da instrução e na produção da prova, princípio que favorece a admissão de novos meios probatórios como a geolocalização. De outro, essa liberdade instrutória esbarra nos limites materiais impostos pela Constituição e pela LGPD. A requisição judicial de dados de geolocalização, nesse cenário, não é um mero ato processual, mas um ato de tratamento de dados pessoais que deve observar as bases legais do artigo 7º da LGPD – notadamente o inciso VI, que autoriza o tratamento para o "exercício regular de direitos em processo judicial" – e, acima de tudo, respeitar o direito fundamental à proteção de dados agora explicitado pela EC 115/2022.

Em síntese, a EC 115 não inaugurou, mas constitucionalizou plenamente a proteção de dados. Ela elevou a LGPD ao patamar de lei regulamentadora de um direito fundamental expresso e transformou qualquer tratamento de dados pessoais no

processo – inclusive, a requisição de geolocalização – em um ato que deve ser confrontado com o rigoroso regime das garantias constitucionais. É nesse terreno, entre a busca da verdade material (amparada pelo art. 765 da CLT) e a vedação ao excesso (imposta pela EC 115/2022 e pela LGPD), que se situa o debate sobre a necessária proporcionalidade na admissão da prova digital.

2.1 Principais tecnologias para realizar a geolocalização e suas implicações probatórias

Em termos técnico-operacionais, a geolocalização corresponde ao conjunto de técnicas digitais destinadas a inferir a localização de uma pessoa ou dispositivo, a partir de coordenadas geográficas, sinais de satélite, rede de telefonia ou registros de aplicativos. No âmbito jurídico e probatório, essa tecnologia permite a localização em tempo real ou a reconstrução histórica de deslocamentos e permanências, com maior ou menor granularidade conforme a técnica utilizada, possibilitando a verificação de rotas, pontos de parada, intervalos de permanência e compatibilidade entre alegações processuais e dinâmicas reais de deslocamento. Beltramini (2024, p. 36) ressalta, ainda, que, embora a LGPD não mencione expressamente os dados de localização, é "fácil inferir que os dados de localização integram o conceito de dado pessoal, tendo em conta que de acordo com a referida Lei são informações de pessoa natural, que possam identificá-la". De fato, pela exegese do art. 5º da LGPD, dados de localização são dados pessoais, pois identificam ou tornam identificável o indivíduo, sujeitando-se às regras gerais de proteção de dados. Diferentemente dos dados sensíveis, os quais se submetem a regime jurídico reforçado nos termos do art. 11, a geolocalização não integra, por si, o rol taxativo de categorias sensíveis, sem prejuízo de que, em hipóteses concretas, o cruzamento de dados de localização com padrões de permanência e deslocamento possa revelar informações sensíveis por inferência.

Do ponto de vista tecnológico, a prova por geolocalização não constitui uma categoria única, mas um conjunto de métodos distintos de inferência de localização, cuja confiabilidade, precisão e potencial invasivo variam significativamente conforme a fonte dos dados. Assim, a eficácia da geolocalização como prova depende da tecnologia empregada, cada uma apresentando diferentes níveis de precisão e intrusão na privacidade.

A forma mais conhecida de geolocalização é a realizada por GPS (*Global Positioning System*) [1] , na qual o dispositivo móvel capta sinais de satélites e calcula sua posição geográfica. Trata-se de tecnologia geralmente dotada de alta precisão, capaz de identificar rotas, permanências e deslocamentos com elevado grau de detalhamento. Em termos probatórios, isso pode favorecer a reconstrução objetiva da jornada, especialmente em atividades externas (como propagandistas, vendedores, motoristas, técnicos de campo e trabalhadores em rota), mas também amplia o risco de devassa da vida privada quando os dados são obtidos de maneira contínua, sem recorte temporal ou sem delimitação estrita do objeto da prova. A depender do modo de coleta, pode haver rastreamento de alta granularidade, revelando não apenas deslocamentos, mas também padrões de rotina que extrapolam o vínculo laboral, alcançando o núcleo protegido pelos direitos fundamentais à intimidade e à vida privada.

Outro método relevante é o uso de registros de Estações Rádio-Base (ERBs), também denominados CSLI (*Cell Site Location Information*), que decorrem da conexão do aparelho às antenas de telefonia. Nessa modalidade, a localização é inferida a partir do ponto de conexão e da intensidade do sinal, com precisão variável conforme densidade urbana, infraestrutura de rede e condições geográficas. Embora em muitos casos seja menos precisa do que o GPS, essa tecnologia é frequentemente utilizada em requisições judiciais por estar sob custódia das operadoras e por permitir a indicação de presença em determinadas áreas e intervalos temporais, o que pode ser suficiente para aferir deslocamentos relevantes à controvérsia trabalhista. Essa modalidade tende a ser particularmente útil para demonstrar a plausibilidade de rotas, o tempo de permanência aproximado em determinados municípios e a compatibilidade (ou incompatibilidade) entre a jornada alegada e a dinâmica real de deslocamentos.

Há, ainda, a geolocalização obtida por logs de aplicativos e serviços digitais, como Google, Apple e plataformas de mobilida-

[1] Tecnicamente, o termo correto para o sistema global de posicionamento por satélites é GNSS (*Global Navigation Satellite System*), que abrange constelações como GPS (EUA), GLONASS (Rússia), Galileo (União Europeia) e BeiDou (China). A popularização do termo "GPS" como sinônimo segue o mesmo fenômeno de "xerox" para fotocópias ou "gilete" para lâminas de barbear. Os dispositivos modernos utilizam múltiplos sistemas GNSS simultaneamente para maior precisão. Para mais detalhes, ver o Manual Técnico de Posicionamento do INCRA (2013, p. 10).

de, que armazenam históricos de localização em nuvem e permitem exportação de dados (por exemplo, por meio do Google Takeout). Nesses casos, os registros podem combinar múltiplas fontes simultâneas, como GPS, Wi-Fi, Bluetooth e dados de rede, formando uma base informacional ainda mais detalhada. Essa modalidade, em regra, é a mais intrusiva, pois frequentemente permite reconstrução minuciosa de rotas, permanências, horários e padrões comportamentais, com elevado potencial de inferência de dados sensíveis, exigindo rigor máximo na aplicação dos princípios da minimização, necessidade e proporcionalidade.

Por fim, deve-se mencionar que a geolocalização também pode ser inferida por redes Wi-Fi e Bluetooth, sobretudo em ambientes urbanos densos e em locais internos, nos quais o GPS apresenta limitações. A identificação de redes próximas e dispositivos conectados pode fornecer informações relevantes sobre permanência em determinado local (como dependências empresariais, agências bancárias ou pontos de atendimento). Nessa modalidade, torna-se ainda mais importante assegurar auditabilidade técnica e contraditório efetivo, pois a valoração judicial do dado depende da possibilidade de verificação independente e da transparência sobre o método de coleta e armazenamento.

Compreendida essa pluralidade técnica, torna-se possível analisar, com maior rigor, as balizas fixadas pela jurisprudência do Supremo Tribunal Federal e do Superior Tribunal de Justiça quanto à vedação de medidas genéricas e à necessidade de fundamentação reforçada para o acesso a dados digitais. A partir dessas premissas, será possível examinar como o Tribunal Superior do Trabalho vem assimilando tais parâmetros no âmbito das controvérsias trabalhistas, especialmente na apuração de jornada, horas extras e atividades externas.

3 A prova digital e a proteção da intimidade nos Tribunais Superiores (STF e STJ)

Antes de adentrar na jurisprudência trabalhista, é imperativo analisar a visão do Supremo Tribunal Federal e do Superior Tribunal de Justiça sobre o tema. As instâncias extraordinárias têm enfrentado o desafio de mediar o conflito entre a busca pela verdade real, facilitada pelas novas tecnologias, e a preservação do núcleo essencial dos direitos da personalidade. Nesse cenário, o STF estabeleceu que os poderes investigativos, embora amplos, encontram limites intransponíveis nos princípios da proporcionalidade e da dignidade da pessoa humana.

O Supremo Tribunal Federal exarou importante pronunciamento acerca da utilização de dados de geolocalização no cenário da Covid-19. Trata-se de medida cautelar deferida em 24 de abril de 2020, sob a relatoria da Min. Rosa Weber, no bojo das ADIs 6.387, 6.388, 6.389, 6.390 e 6.393. O cerne das ações residia na impugnação da Medida Provisória 954/2020, a qual disciplinava o compartilhamento de registros de usuários de telefonia com o IBGE. Em suma, o diploma legal autorizava o acesso a dados cadastrais e registros de usuários para monitorar a adesão populacional às políticas de isolamento social.

Segue trecho da ementa do julgado, *verbis*:

> EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 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. 2º, I e II, da Lei nº 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 dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, 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.

Nesse contexto, a decisão é considerada paradigmática por reconhecer, de forma expressa, a autodeterminação informativa como um direito fundamental extraído diretamente da Constituição Federal. Segundo Beltramini (2024, p. 41), ao analisar o esco-

po desse conceito, o autor destaca que tal direito "assegura ao cidadão o exercício da liberdade de decisão sobre seus dados pessoais, ou seja, confere ao indivíduo o poder de decidir por só mesmo sobre a divulgação ou uso, ou não, de seus dados pessoais". Para fundamentar esse entendimento, o acórdão remete a marcos históricos, como o artigo *The Right to Privacy*, de Warren e Brandeis, e a decisão do Tribunal Constitucional Alemão relativa à Lei do Censo de 1983. Tais referências foram essenciais para que a Corte superasse o entendimento fixado no RE n. 418.416-8/SC e estabelecesse que existe uma proteção autônoma aos dados em si.

Ao suspender a eficácia da Medida Provisória 954/2020, o Plenário da Corte identificou vícios graves que comprometiam a constitucionalidade do tratamento de dados. De acordo com a análise de Beltramini (2024, p. 42), destacou-se a ausência de finalidade específica, visto que a MP não definia de maneira clara como e para que os dados seriam utilizados, além da inexistência de mecanismos de controle para avaliar a adequação do tratamento ou garantir a segurança contra vazamentos.

Por fim, o Tribunal reconheceu a desproporcionalidade temporal da medida, entendendo ser excessiva a manutenção dos dados por até 30 dias após o fim da emergência de saúde pública. Como bem observa Beltramini (2024, p. 42), é relevante notar que este marco histórico ocorreu enquanto a LGPD ainda estava em período de vacância e antes da aprovação da Emenda Constitucional n. 115, que incluiu formalmente a proteção de dados no rol de direitos fundamentais.

Essa sedimentação teórica promovida pelo Plenário nas citadas ADIs permitiu que a Corte, em momentos subsequentes, passasse a tutelar o cidadão contra incursões estatais desmedidas em sua esfera privada. Exemplo proeminente dessa aplicação prática ocorreu no julgamento do Mandado de Segurança (MS) 38.061/DF, sob a relatoria do Ministro Ricardo Lewandowski (decisão monocrática de 25/10/2021), no qual a Corte enfrentou diretamente a tensão entre o poder investigatório e a preservação da intimidade digital. O caso, originado contra ato da CPI da Pandemia, questionava a quebra ampla de sigilos telemáticos de um Assessor Especial da Presidência. O impetrante alegava que a medida era "invasiva ao extremo", avançando sobre conteúdos de comunicações e, primordialmente, dados de geolocalização alheios ao objeto da investigação parlamentar.

Ao decidir a questão, a Corte consolidou o entendimento de que as prerrogativas investigatórias não são absolutas e não podem se converter em uma *"fishing expedition"* (expedição

de pesca) — uma procura genérica e indiscriminada por provas sem fundamentação idônea ou correlação clara com o fato investigado. O relator destacou que a geolocalização é uma prova de natureza excepcional e altamente invasiva. Isso ocorre porque o rastreamento por GPS ou sinais de rede não revela apenas o deslocamento físico, mas também permite a inferência de dados sensíveis, como hábitos religiosos, condições de saúde e inclinações políticas, conforme prevê a Lei Geral de Proteção de Dados (LGPD).

Na mesma linha intelectiva, importante analisar a decisão monocrática proferida pelo Ministro Nunes Marques no Mandado de Segurança (MS) 38.070/DF. Nesse julgado, o Supremo Tribunal Federal aprofundou o debate sobre os limites da "devassa digital". O relator enfatizou que a quebra de sigilos telefônico e telemático deve ser medida excepcionalíssima, exigindo fundamentação que aponte a "causa provável" e indícios concretos de ilicitude, sob pena de nulidade. O STF, ao suspender o ato da CPI da Pandemia, fundamentou sua decisão no fenômeno da "hiperdocumentação" do cotidiano. Observou que, na sociedade contemporânea, o modo de vida das pessoas está intrinsecamente ligado ao uso de smartphones, os quais registram desde atos domésticos e opiniões políticas até deslocamentos físicos minuciosos. Diante dessa realidade, a decisão ressaltou que dados de geolocalização e metadados de comunicações não podem ser acessados de forma genérica, pois isso permitiria ao Estado vasculhar aspectos sensíveis da vida íntima, que nenhum interesse possuem para o objeto da investigação. O Ministro enfatizou que a produção de provas digitais deve ser regida pelo "princípio da minimização", um pilar da Lei Geral de Proteção de Dados (LGPD). Segundo esse entendimento, o tratamento de dados pessoais em investigações deve ser proporcional e estritamente necessário, limitando o acesso ao mínimo indispensável para o interesse público, preservando-se, inclusive, a privacidade de terceiros que possam ser atingidos colateralmente pela medida.

Sob uma ótica complementar, enquanto o Supremo Tribunal Federal delimitou as balizas constitucionais contra o arbítrio estatal, o Superior Tribunal de Justiça avançou na definição de critérios operacionais para a validade da prova tecnológica. No julgamento do RMS 71.032/PE (Rel. Des. Conv. Carlos Cini Marchionatti, 17/06/2025), a Corte enfrentou a legalidade de ordens judiciais de geolocalização coletiva, analisando o fornecimento, por parte do Google, de registros de localização de

usuários que transitaram em perímetro urbano específico. A empresa insurgiu-se contra a medida, classificando-a como uma *fishing expedition*, que sacrificaria a privacidade de uma coletividade indeterminada de pessoas insuspeitas em favor de uma investigação criminal.

O STJ estabeleceu uma distinção fundamental entre a interceptação de comunicações e a quebra de sigilo de dados informacionais estáticos. Com amparo no Marco Civil da Internet (Lei 12.965/2014), a Corte entendeu que a geolocalização, quando delimitada por coordenadas geográficas e um lapso temporal restrito, possui a necessária proporcionalidade. Argumentou-se que o Artigo 22 da referida Lei autoriza a requisição de registros justamente para possibilitar a identificação de utilizadores, tornando dispensável a individualização prévia dos "alvos" quando a finalidade da prova é, primordialmente, descobrir quem estava presente na cena de um ilícito. A decisão também trouxe uma crítica contundente à postura das empresas de tecnologia, sustentando que aquelas que monitoram os passos dos utilizadores para fins comerciais não podem invocar o direito à privacidade para obstruir o acesso judicial a esses mesmos dados. O acórdão concluiu que a geolocalização é um meio de prova legítimo e eficaz, desde que o interesse público e a utilidade da investigação sejam demonstrados.

4 A geolocalização na jurisprudência do Tribunal Superior do Trabalho

Em duas decisões recentes, órgãos colegiados do Tribunal Superior do Trabalho consideraram válido o uso da geolocalização como prova digital para verificar a realização de horas extras. O entendimento foi de que a medida não viola o direito fundamental à privacidade, previsto na Constituição Federal, nem as garantias previstas na Lei Geral de Proteção de Dados (LGPD).

No julgamento do Recurso Ordinário em Mandado de Segurança nº TST-ROT-23369-84.2023.5.04.0000, pela SDI-2, acórdão publicado em 17/10/2025, da relatoria do Ministro Douglas Alencar Rodrigues, discutiu-se a legalidade da determinação judicial que ordenou às operadoras de telefonia o fornecimento de dados de geolocalização de empregado que exercia a função de propagandista vendedor. O trabalhador alegava jornada média superior a 11 horas diárias, enquanto a empregadora sustentava a necessidade da prova digital para aferição objetiva da jornada efetivamente cumprida. A controvérsia ganhou relevo cons-

titucional ao envolver, de um lado, o direito fundamental à prova e, de outro, os direitos à intimidade, à privacidade e à proteção de dados pessoais. Na fase instrutória, a Vara do Trabalho de Santo Ângelo (RS) mandou oficiar as operadoras Vivo S.A. e Claro S.A para que fornecessem dados de geolocalização dos números telefônicos particular e profissional do vendedor. Contra a determinação, o trabalhador impetrou Mandado de Segurança alegando, entre outros pontos, violação de privacidade. O Tribunal Regional do Trabalho da 4ª Região entendeu que a ordem judicial violava direitos fundamentais à intimidade e era desproporcional e desnecessária, pois a jornada poderia ser comprovada por outros meios, sem violar seus dados pessoais. A empresa, então, recorreu ao TST.

O Tribunal Superior do Trabalho afastou a tese de ilicitude da prova, assentando que a requisição de dados de geolocalização não se confunde com interceptação de comunicações telefônicas ou telemáticas, regulada pela Lei nº 9.296/1996, tampouco implica acesso ao conteúdo de mensagens, ligações ou comunicações privadas. Trata-se, segundo o entendimento firmado, de dados técnicos de conexão, capazes de indicar deslocamentos espaciais do aparelho, sem revelar o conteúdo da vida comunicacional do indivíduo.

Sob a perspectiva constitucional e infraconstitucional, o TST destacou que a proteção de dados pessoais, elevada a direito fundamental pela Emenda Constitucional nº 115/2022, não possui caráter absoluto. A própria Lei Geral de Proteção de Dados autoriza expressamente o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, assim como o Marco Civil da Internet permite a requisição judicial de registros e dados armazenados. Nessa linha, a Corte reafirmou que a tutela da privacidade deve ser harmonizada com a garantia do contraditório, da ampla defesa e da busca da verdade real.

Todavia, o Tribunal não adotou uma postura de admissão irrestrita da prova digital. Ao contrário, reconheceu que a decisão de primeiro grau carecia de delimitação adequada, na medida em que autorizava o fornecimento de dados de geolocalização de maneira ampla e contínua, potencialmente revelando aspectos da vida privada alheios à relação de trabalho. Por essa razão, concedeu-se parcialmente a segurança para restringir a produção probatória aos horários de trabalho indicados na petição inicial e ao período contratual controvertido, além de determinar a imposição de sigilo judicial sobre as informações obtidas.

O voto condutor enfatizou que a validade da geolocalização como prova está condicionada à observância dos princípios da necessidade e da proporcionalidade, bem como à adoção de medidas concretas de minimização de dados. Não há interesse processual — nem constitucionalmente legítimo — na investigação de deslocamentos estranhos à prestação laboral, sendo vedada qualquer utilização que extrapole a finalidade estritamente probatória. Ressaltou-se que a utilização de dados de geolocalização é prova digital válida e precisa para apurar jornadas e vínculos trabalhistas, especialmente de quem desenvolve atividades externas e o processo judicial não pode ficar imune às mudanças trazidas pelas novas tecnologias.

Quanto à questão da privacidade e do sigilo, o relator observou que o direito à prova de geolocalização pode ser exercido sem sacrificar a proteção de dados. "Basta que sejam solicitadas informações estritamente necessárias e que elas fiquem, por determinação do juiz, disponíveis apenas para as partes do processo", avaliou. "Não há necessidade nem interesse de averiguar e fazer referências aos locais visitados fora do ambiente de trabalho." O Min. Douglas Alencar lembrou que a LGPD admite a utilização de dados pessoais para o exercício regular do direito em processo judicial. No mesmo sentido, o Marco Civil da Internet (Lei 12.965/2014) permite a requisição de registros e dados armazenados.

Apesar da validade da geolocalização, o Ministro ressaltou que a Vara do Trabalho não delimitou de forma adequada a medida. Por isso, o colegiado restringiu a prova aos horários de trabalho indicados pelo trabalhador e ao período firmado no contrato de trabalho. Determinou, ainda, o sigilo das informações obtidas.

No julgamento do Recurso de Revista nº 0010538-78.2023.5.03.0049, também de relatoria do Ministro Douglas Alencar Rodrigues, apreciado pela Quinta Turma, o TST, seguiu a mesma linha intelectiva, reforçando sua jurisprudência sobre tal temática.

O caso apresenta especial relevância por enfrentar, de modo direto, a tensão entre o poder instrutório do magistrado, a proteção de dados pessoais e o direito fundamental à ampla defesa, em contexto em que a prova digital havia sido expressamente indeferida pelas instâncias ordinárias.

A controvérsia teve origem em reclamação trabalhista ajuizada por bancária do Itaú Unibanco S.A., na qual se discutia a validade dos controles de jornada e o consequente deferimento de horas extras. Embora o banco tenha requerido, de forma es-

pecífica, a produção de prova digital de geolocalização — com o objetivo de demonstrar a permanência (ou não) da empregada nas dependências da instituição nos horários alegados —, o pedido foi indeferido pelo juízo de primeiro grau e mantido pelo Tribunal Regional, sob o argumento de que a medida seria inútil, invasiva da intimidade e desnecessária diante da existência de outros meios probatórios.

O Tribunal Superior do Trabalho, ao reexaminar a matéria, adotou posição diametralmente oposta. Destacou, inicialmente, a contradição lógica do acórdão regional: ao mesmo tempo em que reconheceu a divergência entre a prova oral e a prova documental produzida pelo empregador, concluiu pela condenação ao pagamento de horas extras, sem permitir à parte ré a produção de meio probatório tecnicamente apto a elucidar a controvérsia. Para o TST, tal circunstância evidenciou inequívoco cerceamento do direito de defesa, em afronta direta ao artigo 5º, inciso LV, da Constituição Federal.

O voto condutor avançou além da simples análise de admissibilidade da prova, atribuindo à geolocalização papel central na reconstrução da verdade real. Segundo o relator, trata-se de prova digital dotada de elevada precisão técnica, capaz de superar as limitações inerentes à prova testemunhal, a qual, embora tradicional no processo do trabalho, mostra-se cada vez mais vulnerável a imprecisões, subjetivismos e contradições. A geolocalização, nesse contexto, não deve ser vista como prova subsidiária ou excepcional, mas como instrumento plenamente compatível com o moderno processo trabalhista.

No plano constitucional, o acórdão promoveu ponderação expressa entre direitos fundamentais. Reconheceu-se que a proteção de dados pessoais, alçada à condição de direito fundamental pela Emenda Constitucional nº 115/2022, não possui caráter absoluto e deve ser harmonizada com outras garantias de igual hierarquia, como o contraditório, a ampla defesa e o devido processo legal. A própria LGPD, em seus artigos 7º, inciso VI, e 11, inciso II, alínea "d", autoriza o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, desde que observados os princípios da necessidade, adequação e proporcionalidade.

O Tribunal também afastou, de maneira categórica, a aplicação da Lei nº 9.296/1996 ao caso, esclarecendo que a requisição de dados de geolocalização não se confunde com interceptação telefônica ou telemática. Não há acesso ao conteúdo de comunicações, tampouco à identificação de interlocutores ou mensagens

trocadas, mas apenas a dados técnicos de conexão, aptos a indicar a presença ou ausência do trabalhador em determinado local, em intervalo temporal delimitado.

Elemento particularmente relevante do julgado é a defesa explícita da paridade de armas. O TST advertiu que restringir o uso da geolocalização apenas quando requerida pelo empregado — sob o argumento de consentimento — implicaria grave desequilíbrio processual, esvaziando o direito de defesa do empregador e criando assimetria incompatível com o processo justo. A prova digital, segundo a Corte, deve estar igualmente disponível a ambas as partes, desde que observados os limites legais e constitucionais.

Ainda assim, o Tribunal não admitiu a prova de forma irrestrita. Reafirmou-se a necessidade de delimitação rigorosa do objeto da diligência, restringindo-a aos dias e horários indicados pelas partes como de efetiva prestação laboral, bem como ao período contratual controvertido. Ademais, determinou-se a tramitação do feito sob segredo de justiça, como medida indispensável à preservação da intimidade e à prevenção de usos indevidos das informações coletadas.

Ao final, a Quinta Turma reconheceu a transcendência política da causa, declarou a nulidade dos atos processuais praticados a partir do indeferimento da prova digital e determinou o retorno dos autos ao juízo de origem para reabertura da instrução processual, com a efetiva produção da prova de geolocalização, nos limites fixados.

Conclusão

A prova por geolocalização consolidou-se como um dos instrumentos mais relevantes da modernização probatória no Processo do Trabalho, especialmente na apuração de jornada, horas extras e atividades externas. Entretanto, sua utilização não pode ser analisada como mero avanço tecnológico neutro, pois envolve a tensão estrutural que atravessa todo este estudo: de um lado, o direito fundamental à prova e à efetividade do processo; de outro, os direitos fundamentais à intimidade, à vida privada, ao sigilo de dados e, mais recentemente, à proteção de dados pessoais como direito fundamental expresso, nos termos da EC 115/2022.

Nesse cenário, a LGPD (Lei nº 13.709/2018) opera como eixo normativo central. Não apenas porque disciplina o tratamento de dados pessoais, mas também porque desloca a discussão para um

patamar mais sofisticado: a geolocalização não é somente "prova", mas também um ato de tratamento de dados, que deve obedecer à finalidade, adequação, necessidade e minimização. Assim, o processo judicial trabalhista passa a ser, ainda, um espaço de governança de dados, em que a atividade instrutória deve respeitar o núcleo essencial da personalidade informacional do trabalhador, sem inviabilizar o exercício regular do direito de defesa.

A jurisprudência do STF foi decisiva para construir esse marco constitucional. Ao enfrentar o compartilhamento massivo de dados na pandemia (ADIs da MP 954/2020) e, posteriormente, ao reprimir quebras amplas e genéricas em contexto de CPI (MS 38.061/DF e MS 38.070/DF), a Corte assentou premissas fundamentais ao reconhecer a autodeterminação informativa como dimensão constitucionalmente protegida, o que exige fundamentação reforçada para a obtenção de dados digitais. Nesse sentido, consolidou-se a vedação a medidas genéricas e indiscriminadas, típicas de *fishing expedition*, por representarem devassa incompatível com o Estado Democrático de Direito. O STF, portanto, firmou a ideia de que a prova digital é admissível, mas somente quando compatível com os critérios de proporcionalidade, delimitação e finalidade estritamente vinculada ao objeto do processo.

O STJ, por sua vez, complementou esse desenho ao estabelecer critérios operacionais e pragmáticos para o acesso a dados de localização. Ao admitir, em contexto criminal, a geolocalização delimitada por perímetro e lapso temporal (RMS 71.032/PE), a Corte reforçou que o elemento decisivo não é a natureza tecnológica do dado, mas a estrutura da medida: quanto mais restrita, finalística e necessária, maior sua legitimidade; quanto mais ampla e exploratória, maior sua ilicitude. Ainda que a controvérsia se situe fora do processo do trabalho, o raciocínio é inteiramente transplantável, pois se baseia no mesmo núcleo constitucional: privacidade, sigilo e proteção de dados.

No campo trabalhista, soma-se a essa discussão um fator decisivo: a fragilidade inerente da prova testemunhal na reconstrução da jornada, especialmente em atividades externas, em regimes de confiança ou em contextos nos quais a rotina laboral se confunde com deslocamentos. A prova oral, embora historicamente central no processo do trabalho, está sujeita a limitações estruturais — subjetivismo, lapsos de memória, contradições, vínculos pessoais, além da natural dificuldade humana em reconstruir horários e rotas com precisão. É precisamente nesse ponto que a geolocalização se apresenta como elemento de racionalização da verdade processual, oferecendo maior objetivi-

dade e auditabilidade, desde que submetida ao contraditório e a recortes legítimos.

É nesse ambiente, marcado pelo diálogo entre Constituição, LGPD e precedentes do STF e do STJ, que se insere a jurisprudência recente do Tribunal Superior do Trabalho. E é justamente aqui que se encontra a síntese final do trabalho: o TST não tem tratado a geolocalização como prova proibida, nem como prova irrestrita, mas como prova digital legítima, condicionada a requisitos rigorosos de proporcionalidade, delimitação e proteção procedimental.

Nos julgamentos recentes analisados, o TST assentou premissas centrais. Primeiro, diferenciou a geolocalização da interceptação telefônica (Lei nº 9.296/1996), afirmando que não se trata de acesso ao conteúdo de comunicações, mas de dados técnicos de conexão. Segundo, reconheceu expressamente que a proteção de dados pessoais, embora fundamental, não possui caráter absoluto, devendo ser ponderada com o contraditório, a ampla defesa e a busca da verdade real. Terceiro, condicionou a validade da prova à minimização concreta: delimitação temporal (restrita aos horários alegados), delimitação do período contratual controvertido, restrição da finalidade probatória e imposição de sigilo judicial.

Mais do que admitir a prova, o TST passou a utilizá-la como parâmetro de devido processo legal, especialmente quando a controvérsia envolve jornada e há divergência entre prova documental e oral. Nesse contexto, o indeferimento imotivado da geolocalização pode configurar cerceamento de defesa, pois impede que a parte produza meio tecnicamente apto a esclarecer a controvérsia. Assim, o Tribunal transforma a prova digital em instrumento de paridade de armas, evitando que o processo do trabalho permaneça preso exclusivamente a modelos probatórios tradicionais, por vezes insuficientes diante da complexidade do trabalho contemporâneo.

Conclui-se, portanto, que a jurisprudência do TST tem caminhado para uma solução de equilíbrio: a geolocalização é admissível e compatível com o processo do trabalho, inclusive sob a égide da LGPD e da EC 115/2022, desde que não se converta em devassa indiscriminada. A Corte trabalhista, ao absorver as balizas do STF (vedação ao excesso e rejeição da *fishing expedition*) e ao dialogar com a racionalidade do STJ (delimitação e finalidade), constrói um modelo de prova digital constitucionalmente orientado: útil à reconstrução objetiva da jornada, mas limitado pela necessidade, pela proporcionalidade e pela proteção procedimental dos dados pessoais.

Dessa forma, a geolocalização deixa de ser símbolo de um "panóptico" processual e passa a ser, quando corretamente utilizada, instrumento de justiça probatória, capaz de conciliar tecnologia e direitos fundamentais, assegurando que o avanço da prova digital não signifique retrocesso na dignidade, na intimidade e na proteção de dados do trabalhador.

Referências

ARTICLE 29 DATA PROTECTION WORKING PARTY (WP29). **Opinion 13/2011 on Geolocation Services on Smart Mobile Devices.** Adopted on 16 May 2011. Brussels: European Commission, 2011. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf. Acesso em: 10 fev. 2026.

BELTRAMINI, Franciano. **A geolocalização no Supremo Tribunal Federal: uma análise a partir da decisão da medida cautelar da ADI n. 6387-DF.** Revista Eletrônica do TRT-PR, Curitiba: TRT-9ª Região, v. 14, n. 137, p. 33-45, nov. 2024.

BENTHAM, Jeremy. **O Panóptico.** Tradução de Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica, 2008.

BRASIL. Instituto Nacional de Colonização e Reforma Agrária (INCRA). **Manual Técnico de Posicionamento: georreferenciamento de imóveis rurais.** 1. ed. Brasília: INCRA, 2013. Disponível em: https://sigef.incra.gov.br/static/documentos/manual_tecnico_posicionamento_1ed.pdf. Acesso em: 24 fev. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 abr. 2026.

BRASIL. Superior Tribunal de Justiça (Primeira Turma). **Recurso em Mandado de Segurança 71.032/PE.** Relator: Paulo Sérgio Domingues. Julgado em: 15 ago. 2023. Disponível em: https://www.stj.jus.br. Acesso em: 15 fev. 2026.

BRASIL. Supremo Tribunal Federal (Pleno). **Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387/DF.** Relatora: Min. Rosa Weber. Julgado em: 7 maio 2020. Disponível em: https://portal.stf.jus.br. Acesso em: 15 fev. 2026.

BRASIL. Supremo Tribunal Federal (Segunda Turma). **Mandado de Segurança 38.061/DF.** Relator: Min. Gilmar Mendes. Julgado em: 13 ago. 2021. Disponível em: https://portal.stf.jus.br. Acesso em: 15 fev. 2026.

BRASIL. Tribunal Superior do Trabalho (Sétima Turma). **Recurso de Revista 0010538-78.2023.5.03.**

0049. Relator: Min. Cláudio Brandão. Julgado em: 13 dez. 2023. Disponível em: https://www.tst.jus.br. Acesso em: 15 fev. 2026.

BRASIL. Tribunal Superior do Trabalho (Subseção II Especializada em Dissídios Individuais). **Recurso Ordinário Trabalhista 23369-84.2023.5.04.0000.** Relator: Min. Amaury Rodrigues Pinto Junior. Julgado em: 28 nov. 2023. Disponível em: https://www.tst.jus.br. Acesso em: 15 fev. 2026.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão.** Tradução de Raquel Ramalhete. 42. ed. Petrópolis: Vozes, 2014.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 16. ed. rev. e atual. São Paulo: Saraiva Educação, 2021.

PINHEIRO, Patrícia Peck. **Direito Digital.** 7. ed. São Paulo: Saraiva Educação, 2021. E-book.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I.** Consultor Jurídico, 11 mar. 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental/. Acesso em: 9 fev. 2026.

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988.** 10. ed. Porto Alegre: Livraria do Advogado, 2019.

SCHIAVI, Ricardo. **Manual de Direito Processual do Trabalho.** 14. ed. São Paulo: LTr, 2017.

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 (General Data Protection Regulation – GDPR).** Jornal Oficial da União Europeia, L 119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 10 fev. 2026.

VEGAS JUNIOR, Walter Rossati. **A geolocalização como panaceia no processo do trabalho.** Revista do Tribunal do Trabalho da 2ª Região, São Paulo, v. 15, n. 30, p. 182-202, jul./dez. 2023.