ISSN 1679-8694

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO

REVISTA DO TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO CAMPINAS/SP

Direção e coordenação da Escola Judicial
Repositório Oficial de Jurisprudência

Campinas n. 62 p. 1 - 344 jan./jun. 2023

O COMPLEXO DE ARGOS: os limites da prova digital de geolocalização

THE ARGOS COMPLEX: the limits of digital proof of geolocation

JANON, Renato da Fonseca[*]

Quis custodiet ipsos custodes?
Quem vigiará os vigilantes?
(Juvenal, Sátira, Livro VI, versos 346-348).

Resumo: A produção indiscriminada da prova digital de geolocalização, quando não observados os requisitos da imprescindibilidade e da proporcionalidade, será manifestamente inconstitucional, inconvencional e ilegal. Inconstitucional por violar o art. 5º, incisos X e XII, da Constituição Federal. Inconvencional por estar em desacordo com o art. 11 da Convenção Americana de Direitos Humanos. E ilegal por colidir com o art. 6º da Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei n. 13.709/2018 - e com o art. 22 do Marco Civil da Internet (Lei n. 12.965/2014). Precedentes do Direito Comparado. Tribunal Constitucional de Portugal. Tribunal de Relação do Porto. Tribunal Constitucional da Alemanha. Tribunal Federal do Trabalho da Alemanha. Suprema Corte da Áustria. Tribunal Supremo da Espanha. A proliferação de decisões judiciais que quebram o sigilo telemático pode vir a normalizar e até mesmo a oficializar uma Sociedade de Vigilância, transformando a internet em um gigantesco panóptico digital que, à semelhança do exemplo de Foucault, controla a tudo e a todos o tempo inteiro, como se fôssemos prisioneiros de uma cela invisível. Nessa sociedade de vigilância, ninguém teria mais qualquer privacidade ou intimidade, e seríamos todos condenados a uma superexposição da nossa vida particular.

[*]Juiz do Trabalho e Mestrando em Ciências do Trabalho e Relações Laborais no Instituto Universitário de Lisboa.

Palavras-chave: Prova digital. Constituição Federal. Convenção Americana de Direitos Humanos. Lei Geral de Proteção de Dados Pessoais. Marco Civil da Internet.

Abstract: The indiscriminate production of digital proof of geolocation, when the requirements of indispensability and proportionality are not observed, will be manifestly unconstitutional, unconventional and illegal. Unconstitutional for violating art. 5, items X and XII, of the Brazilian Federal Constitution. Unconventional for being in disagreement with art. 11 of the American Convention on Human Rights. It is illegal because it conflicts with art. 6 of the General Personal Data Protection Law (GDPL) - Law 13.709/2018 - and article 22 of the Civil Rights Framework for the Internet (Law 12.965/2014). Precedents of Comparative Law. Constitutional Court of Portugal. Court of Appeal of Porto. German Constitutional Court. Federal Labor Court of Germany. Supreme Court of Austria. Supreme Court of Spain. The proliferation of judicial decisions that break telematic secrecy may continue to normalize and even formalize a Surveillance Society, transforming the internet into a gigantic digital panopticon which, like Foucault's example, controls everything and everyone full time, as if we were prisoners of an invisible cell. In this surveillance society, no one would have any privacy or intimacy anymore, and we would all be condemned to an overexposure of our private lives.

Keywords: Digital proof. Brazilian Federal Constitution. American Convention on Human Rights. General Personal Data Protection Law. Civil Rights Framework for the Internet.

A revolução cibernética, resultante dos avanços na área da tecnologia da informação, fez com que, nos últimos anos, aumentassem, de forma exponencial, os requerimentos para a produção de provas digitais em todas as áreas do Direito. No âmbito do Processo do Trabalho, vem ganhando especial destaque a proliferação de pedidos para a quebra do sigilo telemático dos trabalhadores e expedição de ofícios a operadoras de telefonia, provedores e empresas responsáveis pela administração das redes sociais, a fim de se extraírem os dados de geolocalização, principalmente com o intuito de se obter uma prova sobre a jornada de trabalho que, supostamente, seria mais fidedigna do que a prova documental e/ou a prova testemunhal.

Não se ignora que, em casos específicos, a prova digital pode ser útil e até necessária para o esclarecimento do fato controvertido, sobretudo naquelas hipóteses em que estiverem demonstrados os requisitos da proporcionalidade e da imprescindibilidade, ou seja, quando não

houver outra forma, menos invasiva, de se investigar a verdade factual e quando a relevância do bem jurídico que se pretende tutelar for de tal ordem que justifique, excepcionalmente, a relativização do direito constitucional à privacidade. Contudo, o que temos visto, com frequência, é a banalização e o uso indiscriminado desse meio de prova, ignorando-se as restrições constitucionais e legais, assim como o perigo de se permitir a invasão da vida privada dos indivíduos, sobretudo quando é o próprio Poder Judiciário a autorizar uma medida de exceção típica de uma "sociedade da vigilância", na qual todos são vigiados o tempo inteiro por um panóptico digital. Tentaremos, a seguir, expor, ainda que de forma resumida, algumas das razões para que tenhamos cautela e parcimônia no emprego desse meio de prova.

O primeiro - e principal - argumento é que a medida será **inconstitucional**, por violação do art. 5º, incisos X e XII, da Constituição Federal (CF/1988), se não houver uma justificativa que demonstre, de forma clara e inequívoca, que a extração dos dados de geolocalização é imprescindível para a tutela de um bem jurídico que se revele mais relevante do que a proteção do direito fundamental à privacidade.

O segundo ponto é que também será **inconvencional** por contrariar o art. 11 da Convenção Americana de Direitos Humanos. O terceiro é que será manifestamente **ilegal** por afrontar o art. 6º da Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei n. 13.709/2018 - e o art. 22 do Marco Civil da Internet (Lei n. 12.965/2014).

O quarto ponto é que a quebra do sigilo telemático será **desproporcional** se ficar demonstrado que os litigantes detinham outros meios de prova menos invasivos e igualmente eficientes para eles comprovarem suas alegações, sem precisar atentar contra o direito fundamental à privacidade. Por exemplo, no caso da jornada de trabalho, a prova pode ser feita por documentos e testemunhas, sendo que a lei estabelece que, nos estabelecimentos com mais de 20 (vinte) trabalhadores, é obrigação do empregador manter registros de ponto fidedignos, nos termos do art. 74, § 2º, da Consolidação das Leis do Trabalho (CLT).

O quinto argumento é o de que a experiência internacional revela que os dados de geolocalização também estão sujeitos a diversos erros e a imprecisões, de modo que não se pode nem mesmo dizer que seria uma prova mais confiável ou mais precisa. Logo, salvo circunstâncias excepcionais, as quais precisam ser devidamente justificadas, não há adequação, necessidade nem razoabilidade no requerimento de quebra do sigilo telemático para se comprovar a jornada de trabalho cumprida por um trabalhador, uma vez que até mesmo a **confiabilidade** das informações é bastante questionável, conforme veremos a seguir quando analisarmos o precedente do Tribunal Superior Ocidental da Dinamarca (*Vestre Landsret*), o qual determinou a libertação de 32 (trinta e dois) presos

e a suspensão da utilização de dados de geolocalização em um processo criminal porque apresentavam erros relevantes que poderiam comprometer a integridade do julgamento.

O sexto argumento, mas não menos importante, é que, ao restringir o direito fundamental à privacidade, o Poder Judiciário pode estar contribuindo para normalizar ou até oficializar a chamada "**sociedade de vigilância**" (Foucault), na qual todos são vigiados o tempo inteiro e a esfera íntima de cada indivíduo se sujeita ao escrutínio público, abrindo caminho para o autoritarismo e o abuso de poder. A diferença é que, agora, o panóptico seria digital e a prisão pode ser o telefone celular ou a tela do computador. Daí se falar em **complexo de Argos**, em referência a Argos Panoptes, o gigante que, segundo a mitologia grega, tinha o corpo coberto por olhos para que nunca deixasse de vigiar, vendo a tudo e a todos o tempo inteiro.

Na sequência, tentaremos desenvolver esses argumentos de forma mais analítica, inclusive com o auxílio do direito comparado, sem, contudo, jamais ter a pretensão de exaurir a matéria e sempre respeitando todas as divergências.

De início, é de bom alvitre lembrar que a inviolabilidade dos dados de geolocalização, assim como ocorre com o sigilo telemático e com as comunicações telefônicas, também é a regra no ordenamento constitucional, constituindo direito fundamental previsto no art. 5º da Carta Magna:

> [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...] (BRASIL, 1988).

Ademais, sendo o processo uma relação dialética, a prova digital não pode servir de pretexto para o Poder Judiciário suprir a lacuna da prova documental e da prova testemunhal que devem ser produzidas pelos litigantes, dentro das regras do devido processo legal, com respeito ao contraditório e à ampla defesa - art. 5º, LIV, da CF/1988.

Em casos semelhantes, a jurisprudência vem entendendo:

> 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. 5º da CR. (TRT 3 - MS 0011155-59.2021.5.03.0000, Relator Marco Antonio Paulinelli Carvalho, julgamento 27.10.2021, 1ª SDI, publicação 4.11.2021).

MANDADO DE SEGURANÇA. SIGILOS TELEFÔNICO E TELEMÁTICO. GARANTIA INDIVIDUAL PREVISTA NO INCISO XII DO ART. 5º DA CF. QUEBRA DOS SIGILOS PELO JUÍZO TRABALHISTA. ABUSO DE PODER. VIOLAÇÃO A DIREITO LÍQUIDO E CERTO. LIMITE À JURISDIÇÃO TRABALHISTA. DESRESPEITO AO PRINCÍPIO DA LEGALIDADE. A quebra de sigilos telefônico e telemático por Juízo trabalhista em sede de ação trabalhista configura abuso de poder e ofensa ao direito líquido e certo insculpido no inciso XII do art. 5º da CF c/c art. 1º da Lei n. 9.296/1996. Afronta ao princípio da legalidade previsto no inciso II do art. 5º da CF. A quebra dos sigilos telefônico e telemático somente é possível para apuração de infração penal. Por corolário lógico somente o Juízo investido de jurisdição criminal poderá decretar a quebra de sigilo telefônico e telemático, pois somente este oficia em processo penal e exerce o controle de legalidade em sede de inquérito policial. (TRT 2 - MS 1002600-63.2021.5.02.0000, Relator Marcelo Freire Gonçalves, julgamento 28.9.2021, DEJT 30.9.2021).

AGRAVO REGIMENTAL. MANDADO DE SEGURANÇA. QUEBRA DE SIGILO DOS DADOS DE LOCALIZAÇÃO DA IMPETRANTE, BEM COMO REQUISIÇÃO DE RELATÓRIOS COM GEOLOCALIZAÇÃO DAS CHAMADAS E MENSAGENS *SMS* REFERENTES ÀS CONTAS DE TELEFONIA MÓVEL. DEFERIMENTO DA LIMINAR EM FAVOR DA TRABALHADORA. MANUTENÇÃO. O Agravante não oferece novos elementos jurídicos hábeis a ensejar juízo de retratação. Na hipótese, os aspectos apontados na Decisão agravada mostram a plausibilidade do direito alegado pela Impetrante e o perigo de dano ou o risco ao resultado útil do processo, justificadores do acerto na concessão da liminar perseguida pela Autora. Os dados colhidos no caderno processual estão a indicar que o ato apontado coator viola frontalmente direitos e garantias fundamentais constitucionais da Impetrante, notadamente os valores caros à dignidade e à cidadania que visam proteger a intimidade e a vida privada das pessoas, além dos

dados pessoais telemáticos sigilosos (artigo 5º, X e XII, da Lei Maior). Nada há a reformar, portanto. Agravo Regimental ao qual se nega provimento. (TRT 6 - AgRT 0000219-54.2022.5.06.0000, Redatora Eneida Melo Correia de Araujo, julgamento 2.5.2022, 1ª SDI, assinatura 3.5.2022).

MANDADO DE SEGURANÇA. DECRETAÇÃO DE QUEBRA DE SIGILOS TELEFÔNICO E TELEMÁTICO PARA FORNECIMENTO DE DADOS E DE REGISTROS DE GEOLOCALIZAÇÃO DO IMPETRANTE PARA FINS DE INSTRUÇÃO PROCESSUAL. ILEGALIDADE. Padece de ilegalidade a decisão judicial que decretou a quebra de sigilos do impetrante e determinou a requisição às operadoras de telefonia e aos provedores de internet o fornecimento de dados e de registros telefônicos e telemáticos, relativos a determinado período. Embora os direitos e as garantias fundamentais não possuam caráter absoluto, a decretação de quebra de sigilos, na amplitude com que foi determinada pela autoridade coatora, configurou violação do direito à intimidade e da garantia de inviolabilidade da comunicação, de patamar constitucional (CF, art. 5º, incisos X e XII). Constatado que a quebra de sigilos ocorreu após ter sido produzida prova documental e depois de terem sido colhidos depoimentos das partes e de quatro testemunhas, que tratam da matéria controvertida. Ponderado que, conquanto o magistrado detenha poderes instrutórios (CLT, art. 765), os quais também não possuem caráter definitivo, as diligências que, de ofício, foram determinadas não estão adequadas às circunstâncias fáticas do caso concreto, pois há substrato fático com base no qual a controvérsia pode ser solucionada, prevendo o ordenamento jurídico critérios de julgamento para casos em que a prova não esclarece suficientemente as alegações das partes (CLT, art. 818; CPC, art. 373). Reconhecido que o ato judicial atacado revela-se desproporcional, não tendo sido sopesados os bens jurídicos colidentes e protegidos pela norma constitucional. A possibilidade de dirimir a questão controvertida e de influenciar na formação do convencimento do magistrado são fatores que, frente ao conjunto probatório já coligido ao feito principal, não justificam o afastamento de direitos e garantias fundamentais do impetrante. Particularidades deste caso concreto a demonstrar que a decretação de quebra de sigilos telefônico e telemático do impetrante para obtenção de dados de geolocalização para fins de instrução processual não foi medida necessária, adequada nem proporcional. Presente, ainda, o comprometimento da garantia à razoável duração do processo (CF, art. 5º, LXXVIII), sobretudo em razão da grande quantidade

> de informações requisitadas e da dificuldade no tratamento delas. Segurança concedida. (TRT 4 - MSCIV 00223813420215040000, Relatora Angela Rosi Almeida Chapper, julgamento 22.3.2022, 1ª SDI).

Outrossim, a **Convenção Americana sobre Direitos Humanos - CADH (Pacto de São José da Costa Rica)** também dispõe acerca do respeito à inviolabilidade da vida privada, familiar, do domicílio e da correspondência. Nesse sentido:

> Artigo 11. Proteção da honra e da dignidade.
> 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
> 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas. (BRASIL, 1992).

Não se está, aqui, a dizer que esse meio de prova será sempre ilícito ou desproporcional. Nem se poderia fazê-lo, porque, afinal, o próprio ordenamento jurídico brasileiro contém normas expressas que autorizam a desconsideração do sigilo telemático em circunstâncias excepcionais. No entanto, essa mesma legislação é bastante clara ao ressaltar que a medida, sempre extraordinária, somente pode ser deferida em caso de necessidade incontornável, devidamente justificada, ou seja, somente quando não houver outro meio de prova disponível para o esclarecimento do fato controvertido, conforme se extrai da exegese do art. 6º da Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) -, em especial do inciso III.

Por sua vez, o art. 22 do Marco Civil da Internet (Lei n. 12.965/2014) condiciona a prova digital de "registros de conexão ou registros de acesso a aplicações de internet" à existência de "fundados indícios da ocorrência do ilícito". Vejamos:

> 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:

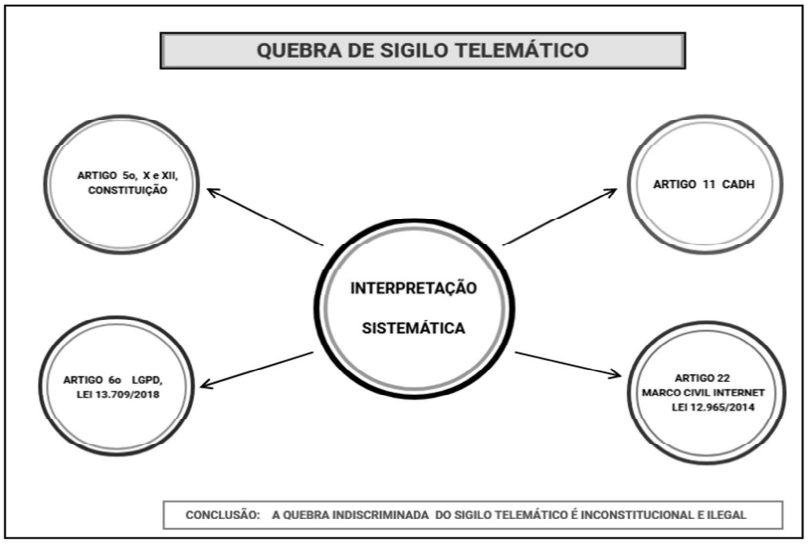
> **I - fundados indícios da ocorrência do ilícito**;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros. (BRASIL, 2014).

Como se percebe da simples leitura da Lei n. 12.965/2014, os requisitos elencados no art. 22 do Marco Civil da Internet são pressupostos cumulativos. Pergunta-se: em uma controvérsia sobre a jornada de trabalho, qual "ato ilícito" um trabalhador teria cometido a ponto de justificar o pedido de quebra do seu sigilo telemático e se devassar a sua privacidade? Ter ingressado com uma reclamatória trabalhista pedindo o pagamento de horas extras? Portanto, é fácil perceber que, se não houver "fundados indícios" de que o trabalhador tenha praticado algum "ato ilícito", não estará presente um dos requisitos legais indispensáveis para se quebrar o seu sigilo telemático.

No mesmo diapasão converge o art. 6º da Lei n. 13.709/2018 (LGPD), ao elencar, em seu inciso III, dentre os princípios para o tratamento de informações de caráter pessoal, o princípio da "necessidade", o qual corresponde ao dever de:

> [...] limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; [...] (BRASIL, 2018).

Quadro 1



Não fosse o bastante, a "prova digital" de geolocalização também será manifestamente **desproporcional** sempre que a parte dispuser de outros meios de prova mais simples e menos invasivos para comprovar suas alegações - por exemplo, no caso da jornada de trabalho cumprida pelo trabalhador, a controvérsia pode ser dirimida por depoimentos pessoais, oitiva de testemunhas e juntada de controles de ponto fidedignos. Assim, se existem outros meios de prova legítimos à disposição da parte, nada justifica invadir a privacidade do indivíduo e violentar o seu direito fundamental ao sigilo telemático. Segundo a Teoria dos Direitos Fundamentais, reelaborada por Robert Alexy, o Princípio da Proporcionalidade ou da Razoabilidade, que também deve ser aplicado no âmbito do direito processual, apresenta três pressupostos: **adequação, necessidade e proporcionalidade** em sentido estrito, vedando-se tanto o excesso quanto a insuficiência de proteção.

Em outras palavras, estamos falando da aplicação da Lei do Balanceamento proposta por **Robert Alexy** para fazermos o adequado sopesamento dos direitos fundamentais em confronto. De forma simplificada, a Lei do Balanceamento é estruturada pela via da ponderação de três dimensões sucessivas e complementares da aplicação do sistema jurídico a um caso concreto, a saber:

> (a) adequação ou sub-princípio da idoneidade, estando a exigir que toda a restrição aos direitos (notadamente aos fundamentais) seja idônea para o atendimento de um fim constitucionalmente legítimo, além do que os meios empregados devem ser instrumentalmente adequados para alcançar o fim almejado;
> (b) necessidade (ou sub-princípio da indispensabilidade, do meio menos restritivo, do direito à menor desvantagem possível), no sentido de que dentre as várias medidas restritivas de direitos igualmente aptas para atingir o fim perseguido, a Constituição impõe que o legislador opte por aquela menos lesiva para os direitos envolvidos (certa proibição de excesso);
> (c) proporcionalidade em sentido estrito, no sentido de que uma restrição aos direitos é constitucional se pode ser justificada pela relevância da satisfação do princípio cuja implementação é buscada por meio da intervenção. (ALEXY, 2000, p. 112).

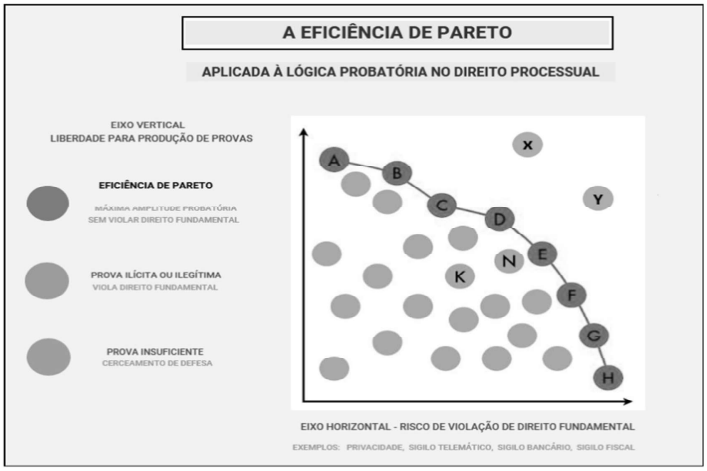
Destarte, é necessário avaliar, em cada caso concreto, se a quebra do sigilo telemático requerida pela parte é proporcional e razoável, ou seja, se há outras formas do litigante produzir as provas que entende necessárias sem violentar o direito constitucional do cidadão à sua privacidade. Releva notar que a doutrina alemã faz um paralelo entre o

princípio jurídico da proporcionalidade e o conceito matemático de **Ótimo de Pareto**. Eficiência ou **Ótimo de Pareto** é um conceito desenvolvido pelo italiano Vilfredo Pareto, que define um estado de alocação de recursos no qual é impossível realocá-los de outra forma tal que a situação de qualquer participante seja melhorada sem piorar a situação individual de outro participante. *Vide*, a propósito, a lição de Robert Alexy em sua versão original:

> The object of the first two sub-principles, the sub-principle of suitability and necessity, is optimization relative to the factual possibilities. In this respect, they are concerned with the question of whether the factual possibilities allow for the avoidance of costs to constitutional rights without bringing about costs contrary to the aims of the legislator. The issue, in other words, is Pareto-optimality. (ALEXY, 2010, p. 10).[1]

Assim, adaptando esse paradigma da proporcionalidade para a delimitação das provas a serem produzidas em um processo judicial, podemos dizer que, no direito processual, o **Ótimo de Pareto** corresponde àquele ponto no qual se garante a cada um dos litigantes a mais extensa amplitude probatória possível sem, contudo, desrespeitar os direitos fundamentais da parte contrária. Essa seria a fronteira intransponível, a linha que não deve ser cruzada nem mesmo pelo Judiciário.

Quadro 2



[1]Em língua portuguesa: "O objeto dos dois primeiros subprincípios, o subprincípio da adequação e o da necessidade, é a otimização relativa às possibilidades factuais. A este respeito, preocupam-se com a questão de saber se as possibilidades factuais permitem evitar custos para os direitos constitucionais sem implicar custos contrários aos objetivos do legislador. A questão, em outras palavras, é a otimização de Pareto".

No gráfico acima fica mais fácil visualizar que, quanto menor for o risco de violação de um direito fundamental protegido por norma constitucional, maior será a liberdade para a produção de uma determinada prova requerida pela parte. Por outro lado, quanto maior for o risco de violação de um direito fundamental, menor será a liberdade para a produção da prova pretendida. O Ótimo de Pareto ou a Eficiência de Pareto corresponde àqueles pontos nos quais é garantida a cada um dos litigantes a mais extensa amplitude probatória possível sem, contudo, violar os direitos fundamentais da parte contrária. Assim, no exemplo acima, os pontos de "A" a "H" correspondem à Eficiência de Pareto, a qual permite assegurar aos contendedores a mais ampla liberdade para a produção de provas sem desrespeitar direitos fundamentais, de modo que não se poderia falar em nulidade por cerceamento de defesa (prova insuficiente) nem por ofensa à garantia constitucional (prova excessiva ou ilícita).

Os pontos "K" e "N" representam hipóteses nas quais houve cerceamento de defesa, uma vez que seria possível produzir a prova negada pelo Juízo sem ofender direito fundamental da parte contrária. De outro lado, os pontos "X" e "Y" representam hipóteses nas quais a prova é nula porque excessiva ou ilícita, na medida em que viola um direito fundamental assegurado pela Constituição Federal. Esses conceitos matemáticos, ainda que como metáfora, ajudam a compreender a aplicação prática do princípio da proporcionalidade no campo da lógica probatória.

No âmbito do **Supremo Tribunal Federal (STF)**, nos autos do Mandado de Segurança MS 38061 MC/DF, com julgamento em 12.7.2021, assim pondera o Ministro Ricardo Lewandowsky, especificamente sobre a utilização de prova digital:

> O tratamento de dados pessoais sensíveis deve ser precedido de cautelas maiores, uma vez que eventual publicização desses tipos de dados pode trazer consequências mais gravosas aos direitos e liberdades de seus titulares. Nesse contexto, o art. 11, II, d, dispõe que o tratamento de dados pessoais sensíveis poderá ocorrer nas hipóteses em que for indispensável para o exercício regular de direitos, inclusive em processo judicial, administrativo e arbitral. A referida lei, embora não se dirija especificamente à disciplina das atividades de investigação, trouxe no art. 4º, § 1º, que tais medidas devem ser 'proporcionais e estritamente necessárias ao atendimento do interesse público'.

Portanto, o Supremo Tribunal Federal ressalta que o requisito da proporcionalidade é decisivo quando se trata de provas digitais, não se podendo deferi-las quando há outros meios de prova que não violem

o direito à privacidade. Na fundamentação da decisão proferida no MS 38061 MC/DF, o Ministro Ricardo Lewandowsky pondera:

> A quebra de sigilo de dados de geolocalização é objeto de debate no RE 1.301.250 RG/RJ, de relatoria da Ministra Rosa Weber, que teve repercussão geral reconhecida (tema 1.148) em 7.6.2021, o qual ainda não foi submetido a julgamento. Assim, a constitucionalidade das medidas discriminadas nos itens b.1, b.4 e b.5, no tocante às localizações determinadas, ainda se encontram sujeitas ao escrutínio definitivo desta Suprema Corte, afigurando-se, portanto, prematura, por enquanto, qualquer decisão nesse sentido, ao menos à vista dos dados que integram os presentes autos. Sob outro vértice, registro, como já assentei em decisões anteriores (*v. g.*, MS 37.963 MC/DF; MS 37.970 MC/DF; MS 37.978 MC/DF, e MS 38.043 MC/DF), minha preocupação com a quebra do sigilo telemático e a consequente exposição de informações e imagens que digam respeito à vida privada de terceiras pessoas e dos próprios impetrantes, razão pela qual advirto que os dados e informações concernentes a estas deverão permanecer sob rigoroso sigilo, sendo peremptoriamente vedada a sua utilização ou divulgação para qualquer fim.

E o Ministro conclui:

> [...] Ante o exposto, defiro em parte o pedido liminar, para permitir o acesso aos dados do impetrante, determinado pela CPI da Covid, com as ressalvas acima declinadas quanto ao trato dos documentos confidenciais, bem como à proteção de elementos de natureza eminentemente privada, estranhos ao objeto da investigação, concernentes ao impetrante ou a terceiras pessoas, os quais deverão permanecer cobertos por rigoroso sigilo, sob as penas da lei. **Suspendo**, contudo, as medidas discriminadas nos itens b.1, b.4 e b.5 do Requerimento 1.037/2021, **quanto aos dados de geolocalização**. (STF MS 38061 DF 0057683-71.2021.1.00.0000, Relator Ricardo Lewandowski, julgamento 12.7.2021, publicação 13.7.2021).

Portanto, nem mesmo uma Comissão Parlamentar de Inquérito (CPI), a despeito de toda a sua importância, pode fazer uma devassa indiscriminada na vida particular dos investigados, por mais graves que sejam as denúncias, sendo que, ao suspender a análise de dados de geolocalização, o Ministro do STF reconheceu que essas são informações sensíveis e protegidas pelo direito fundamental à privacidade.

O direito à privacidade reflete o "direito a estar só" ou o direito "à introspecção" (*right to be let alone*, do direito norte-americano), e de acordo com Celso Lafer é:

> [...] o direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada. (LAFER *apud* AGUIAR JR., 2003, p. 108).

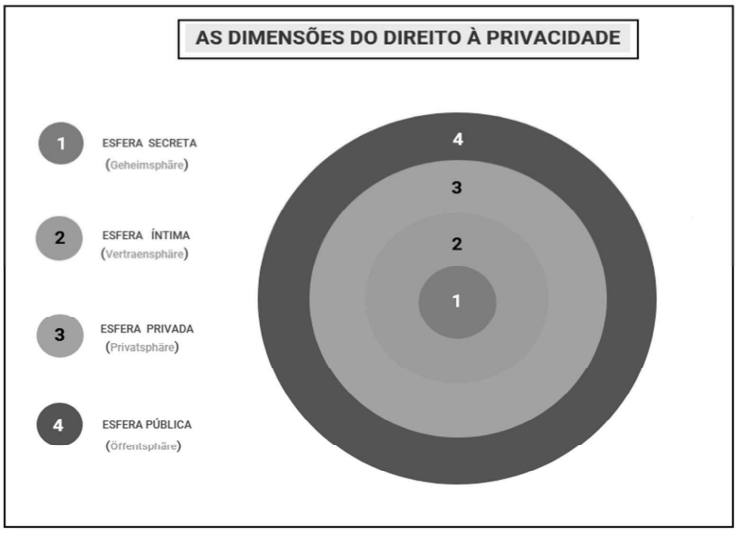
Para desenvolver melhor o conceito de "direito à privacidade", a jurisprudência brasileira tem recorrido à doutrina alemã da denominada "Teoria das Esferas" ou "Teoria dos Círculos Concêntricos", segundo a qual, ressalvando o que é de domínio público, a esfera da "vida privada" é a mais ampla e se refere a fatos que o indivíduo deseja preservar do conhecimento de terceiros que não fazem parte do seu convívio social, mas que são do conhecimento de todos que com ele convivem. A esfera da "vida íntima" ou "confidencial" abrange os fatos que o indivíduo reserva para as pessoas que são de sua estrita confiança, tais como familiares e amigos próximos, excluindo o público em geral. Por fim, a esfera da "vida secreta" é a mais restrita, compreendendo os assuntos que o indivíduo quer guardar somente para si ou, no máximo, para o seu núcleo familiar mais próximo (FARIAS, 2000) (citado no acórdão proferido pelo Superior Tribunal de Justiça, STJ REsp 1929433 PR 2021/0088667-8, Relatora Ministra Nancy Andrighi, publicação DJe 30.8.2021).

Deveras, a doutrina germânica, para explicar as diversas dimensões do direito à privacidade, elaborou a teoria dos quatro círculos concêntricos, diferenciando o público, o privado, o íntimo e o secreto. O círculo mais externo, de maior diâmetro, é a esfera pública, abrangendo fatos e comportamentos que são de conhecimento de todos. O segundo círculo representa a esfera da vida privada (*Privatsphäre*), e corresponde às atitudes que o sujeito deseja excluir do conhecimento público, de modo a preservar sua imagem, seus hábitos e costumes. Dentro da "vida privada" estaria inserido o terceiro círculo, qual seja, o da confidencialidade ou o da intimidade (*Vertraensphäre* ou *Vertralichkeissphäre*). As questões desse terceiro círculo somente são partilhadas com aquelas pessoas em quem o indivíduo deposita estrita confiança, excluindo terceiros em geral e aqueles que não pertencem ao ciclo da vida íntima e familiar.

Dentro desse terceiro círculo da intimidade estariam, por exemplo, a sua situação financeira e a sua vida conjugal. Por fim, o menor e o mais interno dos quatro círculos é o do segredo ou da "vida secreta" (*Geheimsphäre*). São questões cujo conteúdo o indivíduo não deseja dividir com pessoa alguma, reservando-as para si ou compartilhando, no máximo, com seu núcleo familiar mais próximo.

Segundo a "Teoria das Esferas Concêntricas", o Estado não deve avançar nesses círculos interiores sem que exista um motivo muito relevante, o qual justifique relativizar o direito à privacidade do indivíduo, como, por exemplo, no caso de uma investigação criminal sobre um delito grave, que atente contra a ordem pública ou que coloque outras pessoas em risco. E a invasão dessas esferas da privacidade deve ser sempre proporcional e gradativa, avançando-se somente até onde for estritamente necessário, e mesmo assim, desde que não existam outras formas de se obter a prova sobre o fato controvertido que é objeto da investigação.

Quadro 3



No **Direito Comparado**, encontramos na Constituição Espanhola, em seu art. 18.4, a determinação expressa de que:

> [...] 4. A lei deve restringir o uso da informática, a fim de proteger a honra e a privacidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos. (ESPANHA, 2020a, p. 41).

Por sua vez, o art. 8º da Carta dos Direitos Fundamentais da União Europeia estabelece:

> Protecção de dados pessoais
> 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da

> pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. (UNIÃO EUROPEIA, 2020).

O **Tribunal Constitucional de Portugal**, no julgamento que conduziu ao Acórdão n. 268/2022, de 19.4.2022, declarou a inconstitucionalidade, com força obrigatória geral, das normas contidas nos arts. 4º, 6º e 9º da Lei n. 32/2008, de 17.7.2008, conhecida como Lei de Metadados, estatuto que estabelece as condições para o armazenamento e o compartilhamento de dados telemáticos sensíveis. Merece especial destaque a fundamentação do voto conjunto dos Conselheiros Afonso Patrão, Maria da Assunção Raimundo e Mariana Canotilho:

> [...] consideramos que as normas dos artigos 4º e 6º da Lei n. 32/2008, 17 de julho, materializam também uma restrição desproporcionada do direito à inviolabilidade das comunicações, consagrado nos n. 1 e 4 do artigo 34º da Constituição, ao determinarem a conservação generalizada dos dados de tráfego gerados pelas comunicações entre pessoas (ou sua tentativa).
> A garantia de inviolabilidade das comunicações, que vincula as entidades privadas (cfr. Acórdão n. 464/2019), dirige-se à proteção de uma esfera de privacidade e de sigilo no específico domínio das comunicações interpessoais. A Constituição consagra uma garantia constitucional autónoma face àquela que já decorreria do n. 1 do artigo 26º da Constituição; uma **defesa constitucional independente quanto à proteção das comunicações**, com um regime de inviolabilidade mais intenso e cujas exceções são constitucionalmente determinadas. E que abrange não apenas o **conteúdo** da comunicação como os dados de tráfego gerados a seu propósito (Acórdão n. 403/2015).
> Nessa medida, ainda que se considerasse que a agressão ao direito à inviolabilidade das comunicações pudesse ser incluída no âmbito da '**matéria de processo criminal**', tendo especialmente em conta que se procede a uma ingerência nas comunicações entre pessoas que não estão, sequer remotamente, ligadas a qualquer processo criminal, consideramos que deveria ter sido mobilizado como parâmetro do juízo positivo de inconstitucionalidade o direito consagrado nos n. 1 e 4 do artigo 34º da Constituição. (PORTUGAL, 2022a).

A Lei n. 32/2008 regula a:

> [...] conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica portuguesa a Diretiva n. 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações [...]. (PORTUGAL, 2008).

O art. 4º elencava as categorias de dados a conservar pelos fornecedores de serviços de comunicações eletrônicas publicamente disponíveis ou de uma rede pública de comunicações. O art. 6º prescrevia a obrigação da sua conservação pelo período de um ano, a contar da data da conclusão da comunicação. Por sua vez, o art. 9º estabelecia as condições para a transmissão de dados armazenados ao Ministério Público ou à autoridade de polícia criminal competente.

Portanto, os "metadados" abrangem, dentre outros, os dados de geolocalização, pois, como sublinha o Tribunal Constitucional de Portugal no Acórdão 268/2022, "os dados referidos no artigo 4º não abrangem o conteúdo das comunicações, dizendo respeito somente às suas circunstâncias - razão pela qual são usualmente designados por 'metadados' (ou dados sobre dados)", que comportam, segundo categorização feita pelo próprio Tribunal,

> [...] 'dados de base' e 'dados de tráfego'. Os 'dados de base' referem-se à conexão à rede, independentemente de qualquer comunicação, permitindo a identificação do utilizador de certo equipamento - nome, morada, número de telefone [...] Já os 'dados de tráfego' são definidos como 'os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência)' (Acórdão n. 403/2015); 'Constituem, pois, elementos já inerentes à própria comunicação, na medida em que permitem identificar, em tempo real ou *a posteriori*, os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação, devem participar das

> garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações' (Acórdão n. 486/2009, reproduzindo os Pareceres n. 16/94 e 21/2000 do Conselho Consultivo da PGR). (PORTUGAL, 2022a).

Em suma, como pondera Maribel González Pascual, ao analisar o acórdão do Tribunal Constitucional, referindo-se aos dados contemplados na Diretiva n. 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, está a se falar sobre:

> [...] dados relativos às comunicações, que permitem identificar nas comunicações telefônicas e eletrônicas o utilizador do serviço, o destinatário da comunicação, bem como outras circunstâncias básicas da comunicação. Os dados em causa, entre outros, eram os números de telefone ou o *IP* do aparelho emissor e receptor, nome e morada dos utilizadores, data, hora do começo e fim da chamada, dados que identificassem geograficamente o aparelho emissor, tanto nos aparelhos fixos e móveis, bem como o tipo de comunicação (telefone, fixo ou telemóvel, o serviço de Internet utilizado). De maneira que se excluía expressamente o conteúdo da comunicação, mas se incluíam praticamente todas as circunstâncias que a rodearam [...]. (*apud* PORTUGAL, 2022b).

Trata-se de precedente vinculante, com força obrigatória geral em todo o ordenamento jurídico português, tanto que, na sequência, em julgamento realizado no dia 7.9.2022, o **Tribunal de Relação do Porto** confirmou a decisão do Juiz de Instrução Criminal do Porto que havia indeferido o requerimento do Ministério Público para a obtenção de dados de tráfego telefônico com o objetivo de instruir um processo penal, invocando o Acórdão do Tribunal Constitucional n. 268/2022 (TRP, Relator José Antonio Rodrigues da Cunha, Processo n. 877/22.9JAPRT-A. P1, Matéria: Dados de Tráfego e Localização. Inconstitucionalidade. Interpretação conforme o Direito Europeu).

O **Trib. Constitucional da Alemanha** (*Bundesverfassungsgericht*, ou BVerfG), no célebre julgamento proferido em 27.2.2008 (BVerfG, 27.2.2008, BVerfG 1 BvR 370/07, 1 BvR 595/07), ao decidir sobre os limites das investigações *on-line* (*Online-Durchsuchung*) e da consequente alteração do código de processo penal, em seu § 100b StPO, em 2017, concluiu pela existência do direito à privacidade digital e à autodeterminação informativa, reconhecendo o "Direito fundamental da garantia da confidencialidade e integridade dos sistemas de tecnologia

da informação" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)*. Destacamos os trechos mais relevantes:

> 1. O direito geral da personalidade (artigo 2º, n. 1, em conjugação com o artigo 1º, n. 1, da Lei Básica) compreende o direito básico de garantir a confidencialidade e integridade dos sistemas informáticos. (BverfG).
> 2. A infiltração clandestina de um sistema informático, através do qual seja possível monitorizar a utilização do sistema e ler os seus suportes, só é constitucionalmente admissível se houver indícios reais de um perigo concreto para um bem jurídico vital. De suma importância são o corpo, a vida e a liberdade da pessoa ou dos bens do público em geral, cuja ameaça afeta os fundamentos ou a existência do Estado ou os fundamentos da existência humana.
> A medida pode ser justificada se ainda não puder ser determinado com probabilidade suficiente que o perigo ocorrerá em um futuro próximo, desde que certos fatos apontem para um perigo iminente para o ativo jurídico extremamente importante de certas pessoas em um caso individual. (BverfG).
> [...] 5. Se o estado percebe conteúdo de comunicação publicamente disponível na Internet ou participa de processos de comunicação acessíveis ao público, isso não interfere nos direitos fundamentais. (BverfG).
> 6. Se o estado adquire conhecimento do conteúdo da comunicação pela Internet na forma tecnicamente pretendida, isso só infringe o artigo 10, § 1º, da Lei Básica se a autoridade estadual não estiver autorizada a tomar conhecimento dele pelos envolvidos na comunicação.
> 7. O direito geral da personalidade em sua forma especial como um direito fundamental para garantir a confidencialidade e integridade dos sistemas de tecnologia da informação se soma às outras concretizações deste direito fundamental, como o direito à autodeterminação informacional, bem como às garantias de liberdade do art. 10 e art. 13 GG, na medida em que estes não proporcionem proteção alguma ou insuficiente.
> [...] 10. O direito fundamental de garantir a integridade e confidencialidade dos sistemas informáticos aplica-se se a autorização de intervenção abranger sistemas que, isoladamente ou nas suas redes técnicas, possam conter dados pessoais do interessado em certa medida e de forma diversa que permite o acesso ao sistema para obter uma visão das partes essenciais da vida de uma pessoa ou mesmo para obter uma imagem significativa de sua personalidade.

> [...] 12. A proteção dos direitos fundamentais inclui tanto os dados armazenados na memória principal como os dados armazenados temporária ou permanentemente nos meios de armazenamento do sistema. Inclui também a recolha de dados através de meios que são tecnicamente independentes das operações de processamento de dados do sistema de TI em questão, mas que têm por objeto essas operações de processamento de dados.
> 13. A proteção da expectativa de confidencialidade e integridade sob os direitos fundamentais existe independentemente de o acesso ao sistema de tecnologia da informação ser fácil ou somente possível com um esforço considerável.
> 14. O direito fundamental de garantir a confidencialidade e integridade dos sistemas de tecnologia da informação não é ilimitado. As intervenções podem ser justificadas tanto para fins preventivos quanto para processos criminais.
> [...] 18. A autorização legal para uma medida de vigilância que possa afetar a área núcleo da vida privada deve assegurar, tanto quanto possível, que os dados relativos à área núcleo não sejam coletados. Se for praticamente inevitável - como é o caso com o acesso secreto a um sistema de tecnologia da informação - tomar nota das informações antes que sua referência de área central possa ser avaliada, a proteção adequada deve ser fornecida na fase de avaliação. Em particular, os dados que foram encontrados e coletados e relacionados à área central devem ser excluídos imediatamente e seu uso excluído. [...] (ALEMANHA, 2008).

A propósito, no âmbito específico do Direito do Trabalho, na **Alemanha**, o monitoramento por geolocalização durante a jornada laboral somente é possível com conhecimento prévio dos empregados e com aquiescência do Conselho de Trabalhadores da empresa, conforme se extrai da Seção 87 (1), n. 6, da *Betriebsverfassungsgesetz* (BetrVG) - "Lei da Constituição do Trabalho":

> (1) O conselho de trabalhadores tem o direito de codeterminação nas seguintes matérias, desde que não sejam prescritas por legislação ou acordo coletivo:
> 1. questões relativas às regras de funcionamento do estabelecimento e à conduta dos trabalhadores no estabelecimento;
> 2. o início e o término do horário de trabalho diário incluindo pausas e a distribuição do horário de trabalho pelos dias da semana;
> 3. qualquer redução ou extensão temporária das horas normalmente trabalhadas no estabelecimento;

> 4. a hora, o local e a forma de pagamento da remuneração;
> 5. o estabelecimento de princípios gerais para o regime de férias e a preparação do calendário de férias, bem como a fixação da hora em que as férias devem ser gozadas pelos trabalhadores individuais, se não for alcançado um acordo entre o empregador e os trabalhadores em causa;
> 6. a introdução e o uso de dispositivos técnicos destinados a monitorar o comportamento ou desempenho dos funcionários; [...] (ALEMANHA, 2021).

No acórdão proferido no processo BAG 2 AZR 681/16, prolatado em 27.7.2017, o **Tribunal Federal do Trabalho da Alemanha** (*Bundesarbeitsgericht*), ao considerar ilegal o uso de um *software* "*keylogger*" por um empregador, ressaltou que o direito à privacidade dos trabalhadores abrange o sigilo telemático e o direito fundamental à "autodeterminação informativa", não se podendo fazer monitoramento sem o conhecimento prévio da pessoa monitorada e sem a autorização do Conselho de Empregados da Empresa. Destaco trecho da fundamentação:

> [...] A proibição de apresentar material ou de usar evidências devido a uma violação das disposições do artigo 2º, § 1º, em conjunto com o artigo 1º, item n. 1, da Lei Fundamental (A Constituição Alemã) - ver também o artigo 8º, n. 1, da CEDH (a Convenção Europeia dos Direitos Humanos) - pode surgir em processos judiciais do trabalho da necessidade de uma interpretação constitucional do direito processual - por exemplo, do § 138, n. 3, § 286, § 331, § 1º, frase 1, do ZPO (o Código de Processo Civil Alemão).
> Devido à vinculação aos direitos fundamentais relevantes de acordo com o Estado de Direito (BVerfG 13 de fevereiro de 2007 - 1 BvR 421/05 - Rn. 93, BVerfGE 117, 202), o Tribunal deve examinar se o uso de dados pessoais obtidos secretamente e do conhecimento resultante desses dados é compatível com os direitos pessoais gerais da pessoa em questão (BAG 29 de junho de 2017 - 2 AZR 597/16 - Rn. 21; 20 de outubro de 2016 - 2 AZR 395/15 - Rn. 18; 22 de setembro de 2016 - 2 AZR 848/15 - Rn. 2 3, BAGE 156, 370; BGH 15 de maio de 2013 - XII ZB 107/08 - Rn. 21). Além da esfera privada e íntima e sua forma especial como o direito à própria imagem, o direito básico também protege o direito à autodeterminação informativa, o que garante o direito de decidir sobre a divulgação e utilização de dados pessoais.

> Precedentes: BVerfG 11 de março de 2008 - 1 BvR 2074/05 *et al.* - Rn. 67, BVerfGE 120, 378; 23 de fevereiro de 2007 - 1 BvR 2368/06 - Rn. 37, BVerfGK 10, 330; 15 de dezembro de 1983 - 1 BvR 209/83 e outros - sobre C II 1 a das razões, BVerfGE 65, 1. (BAG: 2017: 270717.U.2AZR681.16.0). (ALEMANHA, 2017).

Na **Áustria**, o ordenamento jurídico também consagra, expressamente, o direito à autodeterminação informativa, o qual inclui o direito de decidir sobre a divulgação e utilização de dados pessoais. No âmbito das relações laborais, o § 96, (1) e (3), da *Arbeitsverfassungsgesetz* (Austrian Labour Constitucional Act ou Constituição das Leis do Trabalho) estabelece que uma das condições para o monitoramento pelo empregador é o expresso "consentimento do conselho de trabalhadores" da empresa, lembrando que, por se tratar de uma exceção ao direito à privacidade, não há a menor dúvida de que a medida está diretamente relacionada com a "dignidade humana".

Vejamos o que diz a Consolidação das Leis do Trabalho da Áustria:

> Medidas que requerem aprovação:
> Seção 96. (1) As seguintes medidas por parte do proprietário da empresa requerem o consentimento do conselho de trabalhadores para serem legalmente eficazes:
> [...] a introdução de medidas de controle e sistemas técnicos de controle dos trabalhadores, desde que essas medidas (sistemas) afetem a dignidade humana; [...] (ÁUSTRIA, 2010).

Tanto é assim que a **Suprema Corte da Áustria, o Tribunal Constitucional** (*Oberster Gerichtshof* ou OGH), com sede em Viena, no julgamento do caso OGH 9 Oba 120/19s concluiu que, se um empregador instalar e usar um sistema de posicionamento *GPS* em veículos da empresa sem um acordo coletivo ou sem um acordo individual que indique o expresso consentimento do empregado, essa conduta pode ensejar uma indenização por danos morais em favor do trabalhador por violação do direito à privacidade. A Corte Superior manteve a decisão do Tribunal Regional de Linz, que condenou o empregador a pagar uma indenização por danos morais ao trabalhador, arbitrada em 2.400 euros (dois mil e quatrocentos euros). Na fundamentação do acórdão, o Supremo Tribunal austríaco se baseou na interpretação sistemática do § 96, (1) e (3), da Constituição do Trabalho da Áustria (*Arbeitsverfassungsgesetz* - ArbVG), no § 18 da Lei de Emprego austríaca (*Angestelltengesetz* - AngG), e no § 10 da

Lei do Ajuste do Contrato de Trabalho (*Arbeits-vertrags-Anpassungsgesetz* - AVRAG)[2].

Percebe-se então que, mesmo no curso do contrato de trabalho, os países que admitem o monitoramento dos trabalhadores por geolocalização estabelecem algumas condições inegociáveis, dentre as quais: o conhecimento prévio, pelo trabalhador, de que estará sendo monitorado durante sua jornada de trabalho; o monitoramento deve ficar restrito aos equipamentos eletrônicos ou veículos fornecidos pelo empregador, sem alcançar equipamentos particulares do empregado, e o monitoramento deve ficar limitado ao período no qual o empregado está trabalhando ou sendo remunerado por se encontrar à disposição do seu empregador. O empregado não pode ser monitorado fora da sua atividade laboral porque o que cada pessoa faz em seus momentos de lazer, em sua esfera particular, é uma questão de foro íntimo, que não deve estar sob a supervisão do empregador nem de qualquer autoridade pública.

Outro ponto a ser considerado, para além do direito à privacidade, é que todo ser humano tem o **direito fundamental à desconexão**. *Vide*, por exemplo, os fundamentos da decisão do Supremo Tribunal da Espanha no julgamento do Processo STS 3017/2020, ECLI: ES:TS:2020:3017, em 15 de setembro de 2020, que admitiu o monitoramento de veículos da empresa por geolocalização, "desde que os empregados sejam avisados da instalação" (ESPANHA, 2020b).

Aliás, na **Espanha**, a *Agencia Española de Protección de Dados* (AEPD) afirma, no Guia de Proteção de Dados nas Relações Laborais, com amparo em várias decisões do Supremo Tribunal espanhol (decisão de 26 de outubro de 2017, Rec. 966/2006; de 6 de outubro de 2011, Rec. 4053/2010, e de 21 de junho de 2012, 5259/2012), que se houver monitoramento telemático para o controle do trabalho, devem ser observadas determinadas condições, além de todas as obrigações do Regulamento Geral Sobre a Proteção de Dados - RGPD (UE 2016/679), tais como:

> - Informar previamente os trabalhadores, de forma expressa, clara e inequívoca, nos termos dos artigos 13º e 14º do RGPD, da existência e das características dos dispositivos ou aplicações de geolocalização.
> - Informar sobre o exercício dos direitos de acesso, retificação, restrição de processamento e rasura que os trabalhadores possuem.
> - O controle da geolocalização deve obedecer ao princípio constitucional da proporcionalidade (idoneidade, necessidade e proporcionalidade).

[2]ÁUSTRIA. Suprema Corte. *Oberster Gerichtshof*. OGH - 9 ObA 120/19s. Acórdão 22 jan. 2020. **FLG**, Viena, 2020. Disponível em: https://gdprhub.eu/index.php?title=OGH_-_9_ObA_120/19s. Acesso em: 24 out. 2022.

> - A geolocalização deve ser utilizada exclusivamente durante o horário de trabalho, tendo em consideração o direito ao desligamento digital e, portanto, permitindo a desativação da localização da aplicação de geolocalização.
> - Da mesma forma, os dados armazenados devem ser mantidos apenas pelo tempo estritamente necessário.
> - Por fim, é importante destacar a conveniência de realizar uma Avaliação de Impacto da Proteção de Dados de todo o processo, a fim de garantir a privacidade e a segurança do tratamento de dados pessoais realizado pela empresa, evitando que possam ser acessados por terceiros. (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DADOS, 2022).

Na **França,** o empregador que deseja utilizar um dispositivo de geolocalização deve fazer uma declaração à *Commission nationale de l'informatique et des libertés* (CNIL), a qual é responsável por garantir que a tecnologia da informação continue a serviço dos cidadãos e não coloque em risco a identidade humana ou viole os direitos humanos, a privacidade ou as liberdades individuais ou públicas. A CNIL também verificará se os princípios relativos à proteção de dados pessoais são respeitados. Uma decisão da Corte de Cassação da França, de 3 de novembro de 2011, aponta que um sistema de monitoramento da atividade dos funcionários, como a geolocalização, não pode ser legalmente utilizado (CA Versailles, 17º ch., 17 de setembro de 2010, n. 09/02316, Messaoudi C / SA Sogeres) pelo empregador para quaisquer outros fins que não os declarados à CNIL, e devem ser levados ao conhecimento dos trabalhadores. Além disso, a geolocalização limita a liberdade pessoal dos funcionários, e isso deve ser justificado, como determina o art. L. 1121-1 do Código do Trabalho francês. De acordo com a Corte de Cassação francesa, não existe tal justificativa para controlar a jornada de trabalho de um empregado que tenha liberdade para organizar seu trabalho. Outrossim, o empregado no caso em questão não tinha sido informado de que o dispositivo seria utilizado para esse fim. O Tribunal decidiu que esse uso ilegal é suficiente para justificar uma notificação pelo empregado de uma violação do contrato de trabalho por parte do empregador (equiparada a despedimento sem justa causa ou, no Brasil, a uma rescisão indireta).

Como se vê, a experiência coligida do Direito Comparado recomenda cautela e parcimônia na quebra de sigilo telemático e, em especial, na extração de dados de geolocalização, sobretudo quando, no contrato de trabalho, não havia autorização prévia do empregado consentindo com esse monitoramento.

Não bastassem os argumentos jurídicos sobre a necessidade de serem preservados os direitos fundamentais à privacidade e à

desconexão, há também uma questão de ordem prática, que consiste na dúvida sobre a precisão dos dados de geolocalização. No atual estágio da evolução tecnológica, a confiabilidade dos dados de geolocalização é apenas relativa, podendo apresentar erros significativos que podem induzir a uma interpretação errônea dos fatos controvertidos. Em outras palavras, para ser bastante claro: **os dados de geolocalização podem conter erros e imprecisões**, de modo que não constituem uma prova definitiva, ou seja, não há como se dizer que essa prova digital seria mais confiável do que a prova testemunhal.

Na página da emissora de televisão **CNN Brasil** encontramos a seguinte publicação:

> [...] A **CNN** obteve acesso a um documento encaminhado pelo Google à Justiça do Rio de Janeiro no âmbito das investigações do caso da morte da vereadora Marielle Franco e do motorista Anderson Gomes, em março de 2018. Nele, a empresa aponta problemas no uso do histórico de localização - justamente a tecnologia usada para produção das informações de auxílio para o novo coronavírus. (RESENDE, 2020).

Mais adiante, a notícia prossegue:

> O Google recorreu de decisões do Tribunal de Justiça do Rio que determinaram à empresa o compartilhamento de dados pedido pelo Ministério Público fluminense. No texto, a empresa alega que '[...] a tecnologia não foi desenvolvida para identificar e levantar informações de usuários a partir de coordenadas geográficas, o que conduz a problemas e podem tornar a produção dos dados requisitados severamente randômica'.
> A companhia também afirma que o monitoramento de pessoas está sujeito a erros, porque a localização de pessoas está sujeita a três tipos de fontes: *wifi*, *GPS*, e torres de telefonia. E que isto pode levar à conclusão de que usuários estejam em um lugar, mas, na realidade, estes estão a uma 'distância considerável'. (RESENDE, 2020).

Conforme notícia referente ao Mandado de Segurança impetrado no Processo 547762-5, perante o Tribunal de Justiça de Pernambuco - TJPE (NPU 0000343-50.2020.8.17.0000), a empresa **Google Brasil Internet Ltda**. argumentou que a ordem judicial que determinou a quebra dos sigilos telemáticos:

> [...] feria o princípio da **proporcionalidade**, pois não se tem garantia de que as informações requisitadas levem aos autores do delito investigado, em razão da imprecisão dos dados. Diversos fatores como meio de conexão, qualidade do sinal, horário e local de captação, a geografia do lugar, o modelo de dispositivo (aparelho celular) 'geram aleatoriedade na coleta dos dados de localização e podem tornar a produção dos dados requisitados severamente randômica', daí que 'podem deixar de indicar usuários que estiveram no local ou mesmo apontar pessoas que não estiveram, com potencial de gerar falsos indícios'.
> Essas circunstâncias retiram a **utilidade** da medida e afastam a **confiabilidade** desse meio de obtenção de prova. Para ser válida, a restrição a um direito fundamental necessita ser capaz de satisfazer o fim a que se destina. É preciso que fique demonstrada a **adequação** da medida de quebra do sigilo informacional à finalidade pretendida. Sustentou que, além de ser apta a produzir os objetivos pretendidos, a medida restritiva tem que estar baseada numa situação de **necessidade**, ou seja, é preciso que fique demonstrada a inexistência de outras medidas menos gravosas e igualmente idôneas à produção do resultado pretendido. Alegou existirem outras medidas alternativas e menos invasivas, capazes de levar à individualização dos suspeitos. Afirmou que o art. 2º da Lei n. 9.296/96 exige, para a quebra de sigilo telefônico e de dados telemáticos, não somente a demonstração de indícios de autoria ou participação da pessoa investigada, mas também de que a prova seja necessária, não havendo outros meios menos invasivos. [...] (REINALDO FILHO, 2020).[3]

Como se vê, quem afirma que os dados de geolocalização não são precisos nem totalmente confiáveis é a **Google Brasil**, uma das maiores empresas de tecnologia do mundo. Mas não fiquemos apenas com a palavra da **Google**. Vejamos outro exemplo eloquente, extraído de um caso que teve ampla repercussão na imprensa internacional: o *Teledata Sagen* (Caso Teledata), que teve início em um alerta da autoridade dinamarquesa de proteção de dados e forçou a revisão de investigações criminais naquele país. Transcrevo notícia do jornal britânico **The Guardian**, de 12 de setembro de 2019, informando que, na **Dinamarca,** o Tribunal Superior Ocidental (*Vestre Landsret*), revendo decisão do Tribunal de Aarhus, na Jutlândia, determinou a suspensão da utilização de dados de

[3]Mandado de Segurança, Processo 0547762-5, NPU 0000343-50.2020.8.17.0000, impetrante Google Brasil Internet Ltda., Relator Desembargador Demócrito Reinaldo Filho.

geolocalização em um processo criminal porque apresentavam erros relevantes, os quais poderiam comprometer a integridade do julgamento:

> A Dinamarca libertou 32 prisioneiros como parte de uma revisão em andamento de 10.700 processos criminais após o surgimento de sérias questões sobre a confiabilidade dos dados de geolocalização obtidos de operadoras de telefonia móvel, informou a mídia local. Quase 40 novos casos foram adiados sob uma moratória de dois meses sobre o uso de registros de telefones celulares em julgamentos, que foi imposta depois que a polícia encontrou várias falhas no *software* que converte dados brutos de antenas de telefone em evidências utilizáveis. Entre os erros que a polícia descobriu está uma tendência de o sistema omitir alguns dados durante o processo de conversão, o que significa que apenas as chamadas selecionadas são registradas e a imagem da localização do telefone está materialmente incompleta. O sistema também vinculou telefones a mastros errados, conectou-os a várias torres ao mesmo tempo, às vezes a centenas de quilômetros de distância, registrou a origem de mensagens de texto incorretamente e errou a localização de torres específicas.
>
> Tomados em conjunto, os problemas não significam apenas que pessoas inocentes poderiam ter sido colocadas nas cenas do crime, mas que os criminosos poderiam ter sido erroneamente excluídos das investigações, disse Jan Reckendorff, procurador-geral da Dinamarca. 'Este é um problema muito, muito sério', disse ele à emissora estadual DR. 'Simplesmente não podemos viver com a ideia de que informações imprecisas podem mandar pessoas para a prisão'. Ao anunciar a revisão do caso e a moratória no final do mês passado, Reckendorff admitiu que foi uma 'decisão drástica, mas necessária em um estado de direito'. O ministro da justiça dinamarquês, Nick Haekkerup, saudou a decisão, dizendo que a primeira prioridade deve ser sempre evitar erros judiciais. 'Não devemos correr o risco de que pessoas inocentes sejam condenadas', disse ele. (HENLEY, 2019).

Se esses equívocos ocorreram, em larga escala, na **Dinamarca,** um dos mais países mais desenvolvidos do mundo, que está na vanguarda da revolução tecnológica 4.0, como podemos acreditar que os mesmos erros não aconteceriam também no Brasil? Infelizmente, a "prova digital", embora possa ter a sua utilidade para a instrução processual de casos específicos, está sendo apresentada, equivocadamente, em alguns eventos jurídicos, como se fosse uma panaceia para a "busca da verdade real", uma espécie de exame de DNA cibernético, quando, na verdade, é um meio de prova tão falho e impreciso quanto todos os outros.

Não se trata de uma solução universal para todos os processos, mas sim de um instrumento probatório que deve ser utilizado com bastante parcimônia, justificando-se somente quando não resultar em violação do direito fundamental à privacidade e quando não houver outra forma de se esclarecer o fato controvertido.

Na verdade, a supervalorização da prova digital é uma forma de pensamento mágico que, sob o disfarce de uma suposta modernidade, esconde um raciocínio anacrônico, que remonta ao direito medieval: a prova digital seria uma nova "**ordália**" ("o juízo de Deus"), aquela "prova suprema" que contém uma "revelação divina" e que não pode ser contestada. Aliás, embora as ordálias tenham sido usadas com frequência pelos inquisidores da Idade Média - *vide* o Manual do Inquisidor (*Directorium inquisitorum*) e o Martelo das Bruxas (*Malleus Maleficarum)* -, sua origem histórica é ainda mais antiga, remetendo à passagem bíblica sobre as "Águas da Amargura" (Números, 5:27-28) e, antes disso, à segunda lei do Código de Hamurabi e ao Código de Manu, nos primórdios da civilização Hindu.

A diferença é que hoje, em vez de se mergulhar nas correntes do Rio Jordão ou nas águas do Rio Ganges, mergulha-se nas profundezas da internet, na esperança de ali se encontrar uma resposta definitiva para a "iluminação" do processo. Nada mais incompatível com a evolução da ciência jurídica, a qual, desde a Revolução Francesa, em 1789, vem consagrando o primado da racionalidade. Daí o princípio da persuasão racional, conceito que foi, gradativamente, sendo aperfeiçoado no ordenamento jurídico brasileiro, primeiro no art. 118 do Código de Processo Civil (CPC) de 1939, depois no art. 131 do CPC de 1973, até chegarmos ao art. 371 do CPC de 2015. Verifica-se assim que, por vezes, o que se chama de "moderno" nada mais é do que uma nova embalagem para uma velha ideia reciclada, a qual já estava há muito superada e que, agora, ressurge como se fosse uma novidade. Como dizia o poeta Cazuza, "eu vejo o futuro repetir o passado, eu vejo um museu de grandes novidades. O tempo não para".

Mas se é para falar em "modernidade", devemos observar então o que se passa no país onde ficam sediadas as maiores empresas de tecnologia do mundo. Nos **Estados Unidos**, em outro julgamento histórico, a Suprema Corte Norte-Americana (SCOTUS), no caso Carpenter *v.* Estados Unidos (16-402, 585 US, 2018), também se pronunciou no sentido de que o direito individual à privacidade alcança a proteção do sigilo das informações de geolocalização - rastreamento de localização digital pelo local da célula (*CSLI*) e por dados do sistema de posicionamento global (*GPS*), sendo que este não pode ser o único elemento probatório para uma condenação. O Tribunal considerou que há a violação da Quarta Emenda da Constituição dos Estados Unidos em caso de acesso a registros *CSLI*

contendo as localizações físicas de telefones celulares, sem um mandado de busca e apreensão devidamente fundamentado com uma justificativa razoável - lembrando que o caso em questão era de um processo criminal. A decisão se recusou a estender o caso da doutrina tradicional de terceiros - que foi amplamente aplicada quando a maioria dos americanos dependia de telefones fixos em vez de celulares - para cobrir dados históricos de *CSLI*. Reconhecendo a mudança fundamental que a revolução tecnológica do Século 21 causou no comportamento humano, o Tribunal adotou uma visão ampliada dos direitos constitucionais individuais nesse tipo de dados[4].

Todos os exemplos acima transcritos evidenciam que a regra, no Direito Comparado, é restringir o monitoramento por geolocalização aos casos em que ele for imprescindível, sendo que, no caso específico de uma relação trabalhista, deve-se exigir o conhecimento prévio do trabalhador e limitar o monitoramento somente aos instrumentos de trabalho e à cobertura da jornada laboral, sem jamais invadir a vida privada do cidadão. Não se pode, portanto, pensar em quebrar o sigilo telemático para se obter informações de geolocalização de forma retroativa, a fim de obter dados que seriam extraídos sem o consentimento e sem o conhecimento prévio da pessoa monitorada, sobretudo em se tratando de um processo trabalhista, de natureza civil.

Se não bastassem todos esses argumentos jurídicos, há que se considerar, por fim, a dimensão sociológica do Direito: a construção de uma sociedade de vigilância, sem privacidade, é um futuro distópico que se torna cada dia mais próximo. Será esse o mundo no qual queremos viver e deixar para nossos filhos e netos? O pesquisador e advogado Ronaldo Lemos, em entrevista à **BBC Brasil**, adverte que:

> [...] a banalização de quebra de sigilo na internet pode levar a uma 'sociedade de vigilância'.
> [...] Mais decisões como essa (da Justiça brasileira) [quebra de sigilo telemático] poderiam ter consequência desastrosa para a internet e para os cidadãos brasileiros.
> [...] Caso haja uma banalização crescente do sigilo na internet, podemos estar caminhando, aos poucos, de decisão em decisão, rumo a uma perigosa sociedade de vigilância, em que as pessoas estarão expostas ao controle do que fazem *online*, e isso é inadmissível. [...] (PUFF, 2016).

[4]ESTADOS UNIDOS DA AMÉRICA. Suprema Corte Norte-Americana (SCOTUS). Caso Carpenter *v.* Estados Unidos, n. 16-402, 585 US 2018. Acórdão. **JSC**, Washington, 22 jun. 2018. Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

A advertência do professor Ronaldo Lemos chama a atenção para o perigo de o Poder Judiciário autorizar a quebra do sigilo telemático dos cidadãos, de forma indiscriminada, permitindo uma verdadeira devassa na vida particular dos indivíduos. Lemos mostra como essa onda de decisões judiciais invasivas pode ter um efeito catastrófico, mesmo que os juízes estejam imbuídos das melhores intenções. Primeiro, porque o que mantém uma sociedade coesa e unida é a confiança recíproca e a confiança de que o Estado irá respeitar os direitos individuais. A confiança é uma cláusula inalienável do contrato social em um Estado Democrático de Direito. Logo, o Judiciário, enquanto Estado-Juiz, não pode abusar da confiança depositada pelos cidadãos quando acessaram a rede mundial de computadores crentes de que estariam protegidos pelo direito fundamental à privacidade. Se o indivíduo não cometeu nenhum crime, ele deve ter sua intimidade protegida a qualquer custo. Segundo, porque os juízes, em um regime democrático, devem tomar o cuidado de não criarem precedentes que depois possam ser usados como pretextos para perseguições individuais em um regime autoritário, hipótese que, por mais que tenhamos evoluído, nunca pode ser totalmente descartada, considerando a turbulenta história da América Latina nos últimos quinhentos anos. Nada agrada mais aos regimes totalitários do que ter o controle absoluto sobre a vida das pessoas. Já dizia George Orwell, em **1984**: "Big Brother is watching you" ("O Grande Irmão está observando você").

Afinal, se as decisões judiciais que quebram sigilo telemático continuarem se multiplicando de forma exponencial, estaremos, em breve, em uma **sociedade de vigilância**, transformando a internet em um gigantesco **panóptico digital**, que, à semelhança do exemplo de Foucault, controla a tudo e a todos o tempo inteiro, como se fôssemos prisioneiros de uma cela invisível vigiada por um carcereiro onisciente, que sabe cada clique que damos ao acessar um equipamento conectado à Grande Rede. Nessa sociedade de vigilância, ninguém teria mais qualquer privacidade ou intimidade, e seríamos todos condenados a uma superexposição da nossa vida particular.

O "*Panapticon*" é o modelo de um edifício arquitetônico idealizado por Jeremy Bentham, por meio do qual se poderia vigiar e controlar as ações de todos os presos em uma penitenciária. Foucault, em sua obra **Vigiar e Punir**, assim descreve o panóptico:

> O Panóptico de Bentham é a figura arquitetural dessa composição. O princípio é conhecido: na periferia, uma construção em anel; no centro, uma torre; esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo

> às janelas da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado. Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar [...]. (FOUCAULT, 1999, p. 223).

Essa é a ideia central do panoptismo: controle absoluto. O poder panóptico se basearia na vigilância irrestrita, o que tornaria possível manter a ordem e a disciplina de todos os indivíduos, sem que estes soubessem quem os observava ou quando estavam sendo observados. A visão daqueles que são vigiados é obstruída, ou seja, eles habitam em um território no qual podem ser vistos, mas nada podem ver.

E mais grave do que uma sociedade de vigilância (conceito elaborado por Bentham e Foucault) é a **sociedade de controle**, definida por Deleuze como sendo aquela na qual os indivíduos estão tão adestrados para obedecer que se subordinam, de forma voluntária, à disciplina autoritária que lhes é imposta, na medida em que não têm sequer consciência da privação da sua liberdade. É a "servidão voluntária", da qual falava Étienne de La Boétie. Impossível não fazer um paralelo com os "termos de adesão" ou com a "concordância" que o usuário é obrigado a manifestar para poder utilizar as redes sociais na internet ou os aplicativos de *smartphone*.

Para Gilles Deleuze,

> As sociedades disciplinares são aquilo que estamos deixando pra trás, o que já não somos. Estamos entrando nas sociedades de controles, que funcionam não mais por confinamento, mas por controle contínuo e comunicação instantânea. (DELEUZE, 1992, p. 216).

Nas palavras de Michael Hardt,

> A passagem da sociedade disciplinar à sociedade de controle se caracteriza, inicialmente, pelo desmoronamento dos muros que definiam as instituições. Haverá, portanto, cada vez menos distinções entre o dentro e o fora. (HARDT, 2000).

A negação do direito à "privacidade", consequência da vigilância algorítmica, é o primeiro passo para a transformação de uma sociedade de vigilância em uma sociedade de controle.

Na Era do Dataísmo, na qual toda a nossa vida se encontra exposta em redes sociais e em banco de dados facilmente capturados por ferramentas de *Big Data*, merece especial atenção a advertência do filósofo sul-coreano Byung-Chul Han, em sua obra **No enxame: reflexões sobre**

o digital, quando discorre sobre a "sociedade de vigilância digital". O último capítulo desse livro intitula-se "Psicopolítica". Na última página, podemos ler:

> Sendo assim, o psicopoder é mais eficaz do que o biopoder, uma vez que não é de fora, mas de dentro, que vigia, controla e age sobre os seres humanos. A psicopolítica digital apodera-se do comportamento social das massas, uma vez que se baseia na sua lógica inconsciente. A sociedade de vigilância digital, com o acesso ao inconsciente e aos futuros comportamentos sociais de massa, adquire traços totalitários. Submete-nos à programação e ao controle psicopolíticos. A era biopolítica ficou para atrás. Hoje avançamos rumo à era da psicopolítica digital. (HAN, 2016, p. 92).

Byung-Chul Han argumenta que a potencialidade de processar e agenciar as informações aportadas pelo celular, pelos aplicativos, pelas redes sociais, pelos bancos, pelos *GPS*, pelas câmeras de vigilância, pelos aparelhos conectados à internet, pelos satélites, pelos *drones* etc., converte o panóptico de Bentham em um jogo de crianças. Fazer isso em tempo real com populações inteiras ou com segmentos de populações também é uma possibilidade que supera os dispositivos da biopolítica descritos por Foucault. O *Big Data* não registra apenas características e movimentos associados aos corpos e seus ciclos vitais (biopolítica), ele registra e processa imagens, sons, falas, hábitos, discursos, sentimentos, desejos, impulsos, pulsões, devaneios etc.

A capacidade de desvendar correlações a partir dessa heterogeneidade de informações é o que Han denomina de inconsciente digital (HAN, 2015, p. 72-74). Por meio delas o inconsciente digital revela padrões de comportamento e reações que os próprios agentes ignoram. O potencial para manipular os sujeitos usando esse conhecimento inaugura a passagem da biopolítica à psicopolítica. Daí Domecq indagar, com base nas reflexões de Han:

> Será o *Big Data* realmente capaz não só de vigiar o comportamento humano, mas também de o submeter a um controle psicopolítico?
> [...] o *Big Data* decreta o fim da vontade livre, da privacidade, do segredo e da autonomia. É uma máquina de transparência que oculta suas próprias regras. (DOMECQ, 2020).

Daí se dizer que a sociedade pós-moderna, refém da hiperconexão, sofre do **complexo de Argos**, em referência à mitologia grega.

Argos, ou "aquele tudo vê", seria um gigante cujo corpo era coberto por cem olhos. Ele foi criado pela deusa Hera para ser o vigilante do Olimpo. Enquanto o guardião dormia, metade dos olhos se fechava e descansava enquanto a outra metade vigiava. Certa vez, para acalmar o gigante e escapar de sua vigilância, Hermes tocou uma melodia tão linda com sua lira que todos os olhos se fecharam. Uma vez que Argus Panoptes estava dormindo, Hermes cortou sua cabeça para impedi-lo de reviver e informar Hera (Juno) sobre o que ocorreu. Hera (Juno), para homenagear a morte de seu guardião favorito, colocou os olhos de Argus Panoptes na cauda de seu pássaro favorito, o pavão. Quem diria que, mais de dois mil anos depois, a lenda grega acabaria se tornando realidade com a internet se transformando no Argos redivivo, agora com bilhões de olhos espalhados por todo o planeta, vigiando não mais os deuses do Olimpo, mas sim a vida cotidiana de cada um dos nós, pobres mortais condenados à vigilância eterna.

Se o próprio Judiciário chancelar a vigilância algorítmica, permitindo que cada passo da nossa vida particular seja monitorado por ferramentas de geolocalização, a quem poderemos recorrer para a defesa do direito fundamental à privacidade? Como garantir que, tendo acesso a informações sensíveis obtidas com a quebra do sigilo telemático, o empregador ou o próprio Estado não usarão conhecimento privilegiado para constranger ou intimidar o cidadão que teve a sua intimidade devassada?

Quando Alfred Hitchcock dirigiu o seu célebre filme **Janela Indiscreta** (*Rear Window*), em 1954, o mestre do suspense não poderia imaginar que, algumas décadas depois, ninguém precisaria mais de binóculo para fiscalizar a vida alheia, bastando procurar nas redes sociais, nas quais, depois de uma pesquisa de poucos segundos, os algoritmos tornam visível aquilo que as empresas de tecnologia querem que vejamos. O cuidado com a proteção da intimidade deve ser, portanto, redobrado nesse "admirável mundo novo", no qual os especialistas já falam que a tecnologia *5G* permitirá a interface entre os seres humanos e os objetos inanimados (a chamada "internet das coisas"), de modo que serão armazenados dados até sobre o que as pessoas têm na geladeira, sobre a comida que colocam no micro-ondas, sobre o destino dos carros que dirigem ou até mesmo sobre o que assistem na televisão. E muitos vão além, cogitando que, em alguns poucos anos, poderemos conviver em uma dimensão paralela chamada de "**multiverso**", na qual a realidade factual se confundiria com a realidade virtual, permitindo a interação entre as pessoas por meio de avatares ou hologramas (imaginemos o *home office*), de modo que o sigilo de dados telemáticos se tornará cada vez mais importante, não se tratando apenas de uma questão ligada à privacidade, mas também à própria dignidade do ser humano, na medida em que as informações armazenadas na internet se tornarão cada vez mais vitais.

Cuida-se, assim, mais do que um debate jurídico, de uma reflexão sobre o futuro que estamos a construir diante dessa profunda reformulação do nosso modo de vida, tão bem representada na música **Anjos Tronchos**, de Caetano Veloso (2021):

> Uns anjos tronchos do Vale do Silício
> Desses que vivem no escuro em plena luz
> Disseram vai ser virtuoso no vício
> Das telas dos azuis mais do que azuis
> Agora a minha história é um denso algoritmo
> Que vende venda a vendedores reais
> Neurônios meus ganharam novo outro ritmo
> E mais e mais e mais e mais e mais...

Por conseguinte, para além "dos valores jurídicos abstratos", devemos atentar para as "consequências práticas" de cada decisão judicial, como determina o art. 20 da Lei de Introdução às normas do Direito Brasileiro (LINDB). Em corolário, se não forem observados os requisitos da imprescindibilidade e da proporcionalidade, a produção de prova digital de geolocalização, em um processo trabalhista (que não tem natureza penal), além de ser manifestamente inconstitucional, inconvencional e ilegal, também pode constituir um precedente muito perigoso, normalizando a "Sociedade de Vigilância".

Resta-nos, então, mais uma vez refazer a milenar pergunta de Juvenal, ainda sem resposta: "*Quis custodiet ipsos custodes?*" **-** "Quem vigiará os vigilantes?".

REFERÊNCIAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DADOS. Guias. La protección de datos en las relaciones laborales. **AEPD**, Madrid, 2022. Disponível em: https://www.aepd.es/es/guias-y-herramientas/guias.

AGUIAR JR., Ruy Rosado de (Org.). **Jornada de direito civil**. Brasília: Conselho da Justiça Federal, 2003.

ALEMANHA. *Betriebsverfassungsgesetz* (BetrVG). **FLG**, Berlim, 2021. Disponível em: https://www.gesetze-im-internet.de/englisch_betrvg/index.html.

ALEMANHA. Tribunal Constitucional. *Bundesverfassungsgericht.* BVerfG 1 BvR 370/07, 1 BvR 595/07. Acórdão 27 fev. 2008. **HRRS**, Hamburgo, n. 160, 2008. Disponível em: https://www.hrr-strafrecht.de/hrr/bverfg/07/1-bvr-370-07.php. Acesso em: 24 out. 2022.

ALEMANHA. Tribunal Federal do Trabalho. BAG 2 AZR 681/16 BAG: 2017: 270717.U.2AZR681.16.0. Acórdão 27 jul. 2017. **Bundesarbeitsgericht**, Erfurt, 2017. Disponível em: https://www.bundesarbeitsgericht.de/entscheidung/2-azr-681-16/. Acesso em: 24 out. 2022.

ALEXY, Robert. **Teoría de los derechos fundamentales**. Madrid: Centros de Estudios Constitucionales, 2000.

ALEXY, Robert. The construction of constitutional rights. **Law & Ethics of Human Rights**, Berkeley, v. 4, I. 1, art. 2, 2010.

ÁUSTRIA. *Arbeitsverfassungsgesetz*. Constituição das Leis do Trabalho. **FLG**, Viena, 2010. Disponível em: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008329.

ÁUSTRIA. Suprema Corte. *Oberster Gerichtshof*. OGH - 9 ObA 120/19s. Acórdão 22 jan. 2020. **FLG**, Viena, 2020. Disponível em: https://gdprhub.eu/index.php?title=OGH_-_9_ObA_120/19s. Acesso em: 24 out. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. **DOU**, Brasília, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm.

BRASIL. Decreto n. 678, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. **DOU**, Brasília, 9 nov. 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **DOU**, Brasília, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD) (Redação dada pela Lei n. 13.853, de 2019). **DOU**, Brasília, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.

BRASIL. Supremo Tribunal Federal. MS 38061 DF, Processo 0057683-71.2021.1.00.0000. Acórdão. Relator Ricardo Lewandowski. **DJe**, Brasília, 13 jul. 2021.

BRASIL. Tribunal Regional do Trabalho da 2ª Região. Processo SP 0000219-54.2022.5.06.0000. 1ª Seção Especializada em Dissídio Individual. Redatora Eneida Melo Correia de Araujo. **DEJT**, Brasília, 3 maio 2022.

BRASIL. Tribunal Regional do Trabalho da 3ª Região. Processo MG 0011155-59.2021.5.03.0000. 1ª Seção de Dissídios Individuais. Relator Marco Antonio Paulinelli Carvalho. **DEJT**, Brasília, 4 nov. 2021.

BRASIL. Tribunal Regional do Trabalho da 4ª Região. Processo RS MSCIV 00223813420215040000. 1ª Seção de Dissídios Individuais. Relatora Angela Rosi Almeida Chapper. Julgamento em 22 mar. 2022.

DELEUZE, Gilles. **Conversações**. Tradução de Peter Pál Pelbart. São Paulo: 34, 1992. Coletânea de entrevistas.

DOMECQ, Martin. Sobre a noção de transparência em Byung-Chul Han e a defesa de nossa desacreditada opacidade. **Griot: Revista de Filosofia**, Amargosa, v. 20, n. 3, p. 342-361, out. 2020.

ESPANHA. **Constituição espanhola**. Tradução de Afonso d´Oliveira Martins e Margarida Salema d´Oliveira M. G. Graça. Madri: Agencia Estatal Boletín Oficial del Estado, 2020a.

ESPANHA. Tribunal Supremo da Espanha. Processo STS 3017/2020, ECLI: ES:TS:2020:3017. Acórdão 15 set. 2020. **CENDOJ**, San Sebastián, 2020b. Disponível em: http://www.poderjudicial.es/search/openDocument/8adba1406c95ebc3.

ESTADOS UNIDOS DA AMÉRICA. Suprema Corte Norte-Americana (SCOTUS). Caso Carpenter *v.* Estados Unidos, n. 16-402, 585 US 2018. Acórdão. **JSC**, Washington, 22 jun. 2018. Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

FARIAS, Edilson Pereira de. **Colisão de direitos**: a honra, a intimidade, a vida privada e a imagem *versus* a liberdade de expressão. Porto Alegre: Fabris, 2000.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Raquel Ramalhete. 20. ed. Petrópolis: Vozes, 1999.

HAN, Byung-Chul. **No enxame**: reflexões sobre o digital. Tradução de Miguel Serras Pereira. Lisboa: Relógio D´Água, 2016.

HAN, Byung-Chul. **Sociedade do cansaço**. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2015.

HARDT, Michael. A sociedade mundial de controle. *In*: ALLIEZ, E. (Org.). **Gilles Deleuze**: uma vida filosófica. São Paulo: 34, 2000.

HENLEY, Jon. Dinamarca liberta 32 detentos por falhas em evidências de geolocalização telefônica. **The Guardian**, Londres, 12 set. 2019. Disponível em: https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations.

PORTUGAL. Lei n. 32/2008, de 17 de julho. Transpõe para a ordem jurídica interna a Directiva n. 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações. **DRE**, Lisboa, 17 jul. 2008. Disponível em: https://dre.pt/dre/detalhe/lei/32-2008-456812.

PORTUGAL. Tribunal Constitucional. Processo n. 268/2022. Acórdão. **DRE**, Lisboa, 3 jun. 2022a. Disponível em: https://dre.pt/dre/detalhe/acordao-tribunal-constitucional/268-2022-184356510. Acesso em: 24 out. 2022.

PORTUGAL. Tribunal de Relação do Porto. Processo n. 877/22.9JAPRT-A.P1. Acórdão. **DRE**, Lisboa, 7 set. 2022b. Disponível em: https://vlex.pt/vid/910508041. Acesso em: 24 out. 2022.

PUFF, Jefferson. "Banalização de quebra de sigilo pode levar a sociedade de vigilância", diz pesquisador. **BBC News Brasil**, São Paulo, 1º mar. 2016. Disponível em: https://www.bbc.com/portuguese/noticias/2016/03/160301_entrevista_ronaldo_lemos_facebook_jp.

REINALDO FILHO, Demócrito. Limites e requisitos da ordem judicial para quebra de sigilo de dados armazenados por provedor de serviço na internet: desnecessidade de individualização prévia do(s) investigado(s) e do esgotamento de outros meios de prova. **TJPE Notícias**, Pernambuco, 25 maio 2020. Disponível em: https://www.tjpe.jus.br/agencia-de-noticias/-/asset_publisher/ubhL04hQXv5n/content/limites-e-requisitos-da-ordem-judicial-para-quebra-de-sigilo-de-dados-armazenados-por-provedor-de-servico-na-internet-desnecessidade-de-individualizac.

RESENDE, Leandro. À Justiça, Google admitiu que dados de localização não são precisos. **CNN Brasil**, São Paulo, 10 abr. 2020. Disponível em: https://www.cnnbrasil.com.br/nacional/a-justica-google-admitiu-que-dados-de-localizacao-nao-sao-precisos/.

UNIÃO EUROPEIA. **Carta dos direitos fundamentais da União Europeia**. Luxemburgo: Serviço das Publicações da União Europeia, 2020. Disponível em: https://op.europa.eu/webpub/com/carta-dos-direitos-fundamentais/pt/.

VELOSO, Caetano. Anjos tronchos. *In*: CAETANO VELOSO. **Meu Coco**. Rio de Janeiro, Sony Music Entertainment, 21 out. 2021.