# Prefácio

Um dos efeitos mais marcantes da pandemia que tem assolado o mundo nestes tempos terríveis que atravessamos consiste, sem dúvida, no aumento da presença e na maior visibilidade do tecnológico, do digital, do remoto, do virtual, nas nossas vidas. A todos os níveis, em todos os planos das nossas vidas. E também, claro, no plano da nossa vida profissional. O exemplo mais óbvio constitui, sem dúvida, a centralidade que o teletrabalho, o trabalho prestado à distância, fora da empresa (amiúde, prestado a partir do domicílio do trabalhador), por meio de recurso que as tecnologias de informação e de comunicação, passou a deter. De modalidade contratual com expressão marginal ou residual no plano estatístico, o teletrabalho revelou-se uma peça essencial no combate à propagação do novo coronavírus. A pandemia obrigou ao confinamento, ao distanciamento, ao isolamento, sendo que, em muitas empresas e em muitos setores, a prossecução da atividade laboral foi mantida em novos moldes, à distância, com o precioso e indispensável auxílio das tecnologias hoje disponíveis.

A experiência vivida durante a pandemia desvelou as insuficiências do regime jurídico do teletrabalho para dar resposta a várias questões que a *praxis* veio a colocar: o problema dos custos (quem suporta os custos inerentes ao trabalho à distância?), o problema do tempo (como conciliar vida profissional e vida pessoal e familiar, quando a nossa casa se converte no local de trabalho? como assegurar a separação entre tempo de trabalho e tempo de vida, com a inerente desconexão do trabalhador?), o problema do controlo e vigilância patronal (até onde pode ir o legítimo desejo patronal de vigiar, dirigir e monitorizar a atividade do teletrabalhador? onde começa a inviolável reserva da vida privada deste, para mais quando se encontra na sua casa?), o problema do isolamento (como evitar que o teletrabalho acentue o isolamento, quiçá a solidão, do teletrabalhador, que deixa de ter no trabalho presencial, prestado na empresa tradicional, um espaço de convivência e de sociabilidade? como permanecer solidário, apesar de solitário?), o problema da segurança e saúde no teletrabalho (como adaptar as normas sobre acidentes de trabalho à circunstância de o trabalhador passar a trabalhar a partir da sua própria casa?) etc. Passamos a trabalhar a partir de nossa casa ou, como alguns receiam, passamos a morar no emprego?

A pandemia veio acelerar um processo que já se encontrava em curso, de transição digital, em que o virtual toma o lugar do presencial, em que a comunicação e a interação humana se processam com largo recurso aos dispositivos tecnológicos hoje disponíveis para a generalidade da população (o computador, a internet, o *smartphone* etc.). A inteligência artificial, as *apps* que para tudo servem, a robotização que vai alastrando, tudo sinais de um mundo novo, o mundo 4.0 (quiçá não tão admirável assim…) que já chegou e que vai continuar a surpreender a espécie humana nas próximas décadas.

Os reflexos de tudo isto no plano das relações laborais são óbvios, são incontestáveis, são imparáveis e são irreversíveis. E temos a perfeita consciência de que os problemas suscitados pela inteligência artificial, pelo algoritmo, pelas *apps*, pela robotização, por tudo isto, no terreno laboral, são inúmeros e, quiçá, muitos deles ainda nem sequer os estamos a entrever.

Nesta obra, que temos a honra de prefaciar, um vasto e diversificado lote de autores dedica-se a refletir sobre esta panóplia de temas, todos desafiantes para o Direito do Trabalho, suscitados pelo prodigioso avanço da tecnologia. Desde o desafio representado pela prestação de serviços via *apps*, através de plataformas digitais que permitiram pôr em contacto a oferta e a procura de um determinado serviço (o transporte de um passageiro, a entrega de uma refeição em casa etc.) em moldes inovadores, interpelando o Direito do Trabalho, sobretudo quanto à magna questão de saber se a atividade desses prestadores de serviços poderá ou não ser regulada por este ramo do direito, até ao que poderíamos designar por desafio final, a questão de saber se, a prazo, o trabalho humano não vai perder a sua atual centralidade, se a inteligência artificial e os robôs não irão tornar dispensável que as pessoas humanas trabalhem e se, portanto, o Direito do Trabalho está condenado a desaparecer, acompanhando o inexorável decesso do trabalho humano.

As questões que se colocam são múltiplas e de grande complexidade. O algoritmo, por exemplo, começa a ocupar um lugar crescente nos vários domínios da relação de trabalho (na fase da seleção dos trabalhadores a contratar, na distribuição de tarefas e na monitorização e avaliação da prestação realizada pelos trabalhadores, na seleção dos trabalhadores a despedir etc.), sendo cada vez mais evidentes os riscos de, sob a capa da pretensa cientificidade, neutralidade e objetividade do algoritmo, velhas discriminações serem reproduzidas e relegitimadas. O algoritmo, enquanto sistema computacional de matemática aplicada, não tem coração nem sensibilidade, mas a inteligência artificial pode reproduzir os preconceitos, conscientes ou não, de quem programa o algoritmo, isto é, de quem fornece ao algoritmo os dados (*input*) que irão permitir ao algoritmo tomar as suas decisões (*output*).

Em particular, o trabalho prestado com recurso a plataformas digitais, seja a que nos proporciona uma alternativa de transporte ao clássico táxi, seja a que nos permite encomendar a refeição através de uma cómoda *app*, tem colocado questões delicadas, dir-se-ia que à escala universal, a primeira das quais consiste na qualificação da relação que se estabelece entre a empresa que opera na plataforma digital e os respectivos prestadores de serviços, aqueles que transportam os clientes ao seu destino (os motoristas) ou que lhes levam a casa o produtos (os entregadores). As *apps*, ao permitirem novas formas de prestar serviços, colocando em contacto a oferta e a procura, representam, sem dúvida, um dos desafios emergentes para o Direito do Trabalho. Afinal, os serviços fornecidos *via apps* relevam para o Direito do Trabalho, situando-se dentro das fronteiras deste ramo do ordenamento? Ou, pelo contrário, quem presta tais serviços são trabalhadores independentes, são, quiçá, microempresários, cuja atividade já está para além das fronteiras do direito laboral?

É claro que qualificar o trabalho em plataformas, o trabalho realizado com recurso a *apps*, como autónomo ou dependente sempre dependerá de uma apreciação casuística, que leve em conta os dados resultantes de cada tipo de relação, de cada concreto contrato. E também é claro que estas novas formas de prestar serviços levantam consideráveis dificuldades de enquadramento, até porque, infelizmente, não dispomos de um qualquer "subordinómetro" que nos forneça uma resposta infalível e irrefutável. Não espanta, por isso, que a doutrina e os tribunais, um pouco por toda a parte, se tenham confrontado com esta questão, chegando a resultados nem sempre coincidentes.

De tudo isto e muito mais trata o livro que ora se prefacia. Também do tratamento de dados pessoais dos trabalhadores, da crise pandémica e da insolvência, do cooperativismo, dos testes genéticos, do trabalho intermitente etc. Um livro que, de algum modo, encontra as suas raízes na colaboração estabelecida, há anos, entre o IDET – Instituto de Direito das Empresas e do Trabalho, da Faculdade de Direito da Universidade de Coimbra, e a Plataforma Dialética, graças ao engenho e ao empenho do seu coordenador académico dos cursos internacionais, Prof. Paulo Renato Fernandes da Silva.

Aos autores, os meus parabéns pelo magnífico trabalho realizado! Ao leitor caberá apreciar os méritos do esforço desenvolvido, que agora, em boa hora, se dá à estampa.

Coimbra, fevereiro de 2022

*João Leal Amado*

*Vice-Presidente da Direção do IDET.*
*Professor da Faculdade de Direito da Universidade de Coimbra*

# A Questão do Tratamento de Dados de Localização do Trabalhador em Tempos de Pandemia: Perspectiva Brasileira sobre o Conflito entre a Privacidade e a Saúde Pública e Corporativa

***Paulo Renato Fernandes da Silva***[1]
***Paula Guedes Fernandes da Silva***[2]
***Patrícia Estacio de Lima Corrêa***[3]

## *1. Introdução*

Descoberto em dezembro de 2019 na província chinesa de Wuhan, o novo Coronavírus (COVID-19) espalhou-se mundialmente, declarado pandêmico em março de 2020 pela Organização Mundial de Saúde (OMS).[4] Nesse cenário, além da constante preocupação com a saúde do trabalhador, governos, empresas e outros interessados na luta contra o vírus utilizam tecnologias digitais e análise de dados para lidar com essa nova ameaça.[5]

Nesse sentido, com o intuito de obtenção de respostas eficazes de combate à doença, foram criadas estratégias de saúde pública ao redor do mundo, principalmente baseadas em dados coletados de diferentes fontes, como torres telefônicas, aplicativos de celular, *Bluetooth*, vídeo de vigilância, *feeds* de mídias sociais, termômetros inteligentes, registros de cartão de crédito, *wearables* e diversos outros dispositivos da Internet das Coisas (*Internet of Things* — IoT).[6]

No âmbito privado, as empresas passaram a adotar os protocolos de saúde e prevenção do coronavírus previstos pela legislação brasileira de crise, especialmente com base na Lei Federal n. 13.979, de 6 de fevereiro de 2020, que dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente da rápida proliferação do coronavírus.

Muitos governos e entidades privadas estão buscando tecnologias para ajudar a monitorar e rastrear

(1) Doutor em Direito. Professor Adjunto da UFRRJ e da FGV — Direito Rio. Professor convidado dos cursos de pós-graduação, LLM e MBA da PUC-Rio, da FGV e da EMERJ. Advogado. Presidente da Comissão de Direito Cooperativo do Instituto dos Advogados Brasileiros — IAB Nacional. Diretor da Escola Superior do IAB — ESIAB. Vice-Presidente da Comissão de Direito do Trabalho do IAB. Vice-Presidente da Comissão de Relações Institucionais da OAB/RJ.
(2) Doutoranda em Direito e Mestre em Direito Internacional e Europeu pela Universidade Católica Portuguesa Escola do Porto (UCP Porto). Pesquisadora do grupo de pesquisa em Direito e Tecnologia da PUC-RJ (Legalite). Pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio) em parceria com a Universidade Estadual do Rio de Janeiro (UERJ). Pós-graduada em Direito Digital pela Fundação Escola Superior do Ministério Público (FMP). Formada pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Analista Acadêmica do Data Privacy Brasil. Advogada no Brasil e em Portugal.
(3) Mestranda em Direito Internacional e Europeu pela Universidade Católica Portuguesa — Escola do Porto (UCP Porto); formada pelo Centro Universitário do Distrito Federal (UDF); advogada.
(4) ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). *WHO Director-General's opening remarks at the media briefing on COVID-19.* Março de 2020. Disponível em: <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020>. Acesso em: 5 jun. 2020.
(5) UNIÃO EUROPEIA. Conselho. *Contact Tracing Apps* (Council of Europe Portal). Disponível em: <https://www.coe.int/en/web/data-protection/contact-tracing-apps>. Acesso em: 5 jun. 2020.
(6) IENCA, Marcello *et al. Digital tools against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid*. The Lancet Digital Health 2020, 29 jun. 2020. p. 1. Disponível em: <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30137-0/fulltext>. Acesso em: 12 jun. 2020.

a disseminação da COVID-19.[7] Consequentemente, a coleta e o tratamento de dados de localização e geolocalização (GPS), além de rastreamento de contatos (*contact tracing*), ganharam força nos governos e junto aos empregadores, por vezes em parceria com empresas de tecnologia.[8]

Diante desse cenário, muitos direitos fundamentais são impactados pela pandemia, principalmente no que diz respeito à estratégias de vigilância em massa das populações para identificação de pessoas infectadas a partir da coleta de dados pessoais, com o uso de ferramentas como, por exemplo, drones de reconhecimento facial e de coleta de imagens térmicas, aplicativos de rastreamento, acesso aberto a dados sensíveis de saúde pública e criação de passaportes de imunidade.[9] Algumas dessas iniciativas foram também implementadas em relações de trabalho.

Considerando que os dados coletados para monitoramento, como os de localização, tanto podem ser anônimos quanto dados pessoais e, ainda, potencialmente classificados como dados sensíveis,[10] o objetivo deste trabalho é lançar luz sobre o debate acerca do aparente conflito entre os supracitados direitos fundamentais no contexto da utilização dos dados pessoais no combate à atual pandemia, com foco específico em seu uso no contexto de relações de trabalho.

## *2. Do direito à privacidade dos dados de localização do trabalhador*

Dados podem ser definidos como informação potencial que necessita de processamento para ser utilizada.[11] Metadados, por outro lado, são "dados sobre dados", consistindo em toda a informação sobre quaisquer dados em determinado momento, em qualquer nível de agregação — em outras palavras, é informação estruturada sobre uma fonte de informação de qualquer tipo ou formato de mídia.[12] Já os dados pessoais, nos termos da Lei Geral de Proteção de Dados (LGPD — Lei n. 13.709/2018), constituem informações relacionadas a pessoas naturais, identificadas ou identificáveis.[13] A partir dessa definição, é possível enquadrar diferentes atores de relações de trabalho, sejam empregados, empresários, servidores públicos, estagiários, autônomos, cooperados, trabalhadores em domicílio, informais, estudantes, aposentados etc.

Antes de enquadrarmos a questão específica, ainda é necessário definir a ideia de privacidade de localização. O conceito relaciona-se às informações de localização de um indivíduo, no sentido de impedir que terceiros saibam a sua localização atual ou passada.[14] Nas palavras de Krumm, "essa definição abrange a ideia de que a pessoa cuja localização está sendo mensurada deve controlar quem pode ter conhecimento sobre ela",[15] o que está em consonância com a ideia de autodeterminação informativa prevista como um dos fundamentos da LGPD. O direito à privacidade, previsto em diversos instrumentos internacionais e regionais de proteção de direitos humanos fundamentais, engloba, portanto, o direito à privacidade de localização.[16]

No caso das relações de trabalho, esse monitoramento só pode ocorrer durante a jornada de trabalho do empregado, mesmo que esta se dê fora do estabelecimento empresarial, período no qual os poderes de direção e de fiscalização do empregador

(7) UNIÃO EUROPEIA. Agência dos Direitos Fundamentais da União Europeia (FRA). *Tech answers to COVID-19 should also safeguard fundamental rights*. Viena: FRA Press Release, 28 maio 2020. Disponível em: <https://fra.europa.eu/sites/default/files/fra_uploads/pr-2020-covid-rights-impact-apps_en.pdf>. Acesso em: 6 jun. 2020.

(8) ELECTRONIC FRONTIER FOUNDATION (EFF). *COVID-19 and Digital Rights*. Disponível em: <https://www.eff.org/issues/covid-19>. Acesso em: 11 jun. 2020.

(9) *Idem.*

(10) De acordo com o artigo 5º, inciso II da Lei Geral de Proteção de Dados (LGPD), dado pessoal sensível é todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

(11) POMERANTZ, Jeffrey. *Metadata*. Cambridge: The MIT Press, 2015. p. 21.

(12) BACA, Murtha (ed.). *Introduction to Metadata*. 3. ed. Los Angeles: Getty Research Institute, 2016. p. 2.

(13) BRASIL. Lei n. 13.709, de 14 de agosto de 2018 (LGPD), art. 5º, I.

(14) ATAEI, Mehrnaz; KRAY, Christian. Ephemerality is the New Black: A Novel Perspective on Location Data Management and Location Privacy in LBS. In: GERTNER, Georg; HUANG, Haosheng (ed.). *Progress in Location-Based Services 2016*. Switzerland: Spring, 2017. p. 360.

(15) "*This definition captures the idea that the person whose location is being measured should control who can know it*". KRUMM, John. A survey of computational location privacy. *Pers Ubiquit Comput* 13: p. 391-399, 2009.

(16) Declaração Universal dos Direitos Humanos, art. XII; Pacto Internacional sobre os Direitos Civis e Políticos, art. 17; Carta dos Direitos Fundamentais da União Europeia, art. 7º; Convenção Europeia dos Direitos Humanos, art. 8º.

se protraem sobre a vida profissional daquele. Com efeito, estão afastadas desse raio de projeção patronal os lapsos temporais nos quais o trabalhador encontra-se em intervalo de repouso e alimentação (artigo 71 da Consolidação das Leis do Trabalho — CLT — Decreto-Lei n. 5.452/43)[17] ou em banheiros e vestiários. Isso, entretanto, não afasta o dever do empregado de cumprimento das normas de saúde pública e empresarial de combate à pandemia da COVID-19.

O empregado que esteja, por exemplo, visitando um cliente pode ter sua geolocalização monitorada pelo empregador, caso seja uma medida proporcional previamente estabelecida, expressamente, no âmbito do seu contrato de emprego, em face dos princípios da boa-fé, transparência e lealdade entre as partes.

No ensejo, merece destaque de que o fato de o trabalho ser realizado à distância pelo colaborador não afasta, por si só, a caracterização do vínculo empregatício, segundo o artigo 6º da CLT, assim como não elide, por conseguinte, o poder do empregador de controlar seus trabalhadores, *in verbis:*

> Art. 6º Não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego.
>
> Parágrafo único. Os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio. (Destacamos)

Por outro lado, os dados médicos ou biomédicos do trabalhador são protegidos pelo direito fundamental à intimidade. Ao mesmo tempo, porém, esse direito deve se harmonizar ao poder-dever do empregador de garantir um meio ambiente de trabalho adequado, isto é, seguro, sadio e urbano (artigo 7º da Constituição Federal c/c artigo 157[18] da CLT), para toda a comunidade empresarial.

Nesse sentido, cabe ao empregador exigir de seus colaboradores (empregados ou não) a observância e o efetivo cumprimentos das normas de saúde e proteção contra a pandemia da COVID-19, sejam aquelas previstas na legislação de saúde pública sejam as criadas e regulamentadas pela própria empresa ou até em normas coletivas, em atenção aos princípios da prevenção e da precaução que incidem sobre esta.

A legislação do trabalho brasileira, nesse aspecto, revela-se arrojada, pois já previa o dever do empregador de afastar o empregado do trabalho e encaminhá-lo para a segurança social, diante da mera suspeita de adoecimento deste. Portanto, o controle patronal epidemiológico, no contexto empresarial, deve ser feito preventivamente (com a adoção dos equipamentos de proteção individual — EPIs e dos equipamentos de proteção coletiva — EPCs) e repressivamente no caso do monitoramento da saúde do trabalhador.[19]

A Lei Federal n. 14.128, de 26 de março de 2021[20] prevê que, durante o período da emergência em saúde pública da COVID-19, a imposição de isolamento dispensa o empregado de comprovação de doença por 7 (sete) dias. Se o afastamento for superior a esse período, o trabalhador poderá apresentar como justificativa válida, documento de unidade de saúde do Sistema Único de Saúde (SUS) ou documento eletrônico regulamentado pelo Ministério da Saúde.

Portanto, o controle de dados quanto a saúde do trabalhador é menos invasivo, mas deve ser feito pela empresa, pois a própria CLT estabelece que nenhum interesse individual pode se sobrepujar ao interesse

(17) CLT: "Art. 71. Em qualquer trabalho contínuo, cuja duração exceda de 6 (seis) horas, é obrigatória a concessão de um intervalo para repouso ou alimentação, o qual será, no mínimo, de 1 (uma) hora e, salvo acordo escrito ou contrato coletivo em contrário, não poderá exceder de 2 (duas) horas."

(18) CLT: "Art. 157 — Cabe às empresas: I — cumprir e fazer cumprir as normas de segurança e medicina do trabalho; II — instruir os empregados, através de ordens de serviço, quanto às precauções a tomar no sentido de evitar acidentes do trabalho ou doenças ocupacionais; III — adotar as medidas que lhes sejam determinadas pelo órgão regional competente; IV — facilitar o exercício da fiscalização pela autoridade competente."

(19) É o que pode ser identificado sob a alcunha de Princípio Constitucional da Integridade Psicofisiológica do Trabalhador**.** Esse princípio pode ser localizado no inciso XXII do artigo 7º da CF/88, cujo dispositivo prevê que são direitos dos trabalhadores a redução dos riscos inerentes ao trabalho por meio de normas de saúde, higiene e segurança no trabalho. A expressão "redução dos riscos" deve ser entendida no sentido da adoção de medidas voltadas para a efetiva proscrição dos acidentes de trabalho. A noção de **tolerância zero** para com os acidentes de trabalho é um parâmetro que deve nortear a gestão empresarial, não sendo crível que em pleno século XXI o Brasil ostente índices tão alarmantes de infortúnios.

(20) A referida lei dispõe sobre a compensação financeira a ser paga pela União aos profissionais e trabalhadores de saúde que, durante o período de emergência tenham trabalhado no atendimento direto a pacientes acometidos pela COVID-19.

coletivo (artigo 8º, CLT).[21] Isso é essencial para que o empregador possa redirecionar suas políticas de saúde corporativa para um grau cada vez maior de eficiência e qualidade. A ideia central que pode ser extraída do sistema constitucional de proteção do meio ambiente de trabalho pode ser sintetizada na concepção de tolerância zero com os infortúnios laborais.

Para tanto, uma eficiente política empresarial de monitoramento da saúde e dos problemas epidemiológicos eventualmente existentes é medida de grande importância e está em harmonia com o sentido e o alcance das normas constitucionais. Todavia, tais práticas devem respeitar também as regras estabelecidas pela LGPD no que tange aos dados pessoais dos empregados, já que o regramento é também aplicável a relações trabalhistas. Isso exige que sejam escolhidas bases legais adequadas para o tratamento dos dados pessoais, assim como o cumprimento dos princípios e direitos, além de imposição de salvaguardas técnicas e administrativas que evitem eventuais incidentes de segurança.

A utilização de dados de localização para fins de controle da pandemia evidencia, portanto, um aparente conflito entre o direito à privacidade e a saúde pública, que se traduz no próprio direito à vida. Tal conflito, no entanto, não é absoluto. O direito à privacidade não deve ser entendido como empecilho ao tratamento de dados de localização para fins de controle do surto de coronavírus que, neste momento, assola o mundo, desde que adotadas medidas de segurança dos dados e da informação adequadas, como veremos nos próximos tópicos.

### *3. Tecnologias digitais de saúde e empresarial utilizadas para controle da pandemia*

Pesquisa recente realizada pelo *The Lancet Digital Health*[22] identificou quatro principais categorias funcionais de tecnologias digitais de saúde pública para gerenciamento da pandemia. São elas:

> (i) proximidade e rastreamento de contatos (*contact tracing*) — essas ferramentas medem a proximidade espacial entre os usuários para rastrear sua interação, o que permite identificar quando os usuários são expostos a um indivíduo testado positivo para o Coronavírus;
>
> (ii) monitoramento de sintomas — ferramentas de vigilância de sintomas que coletam, analisam, interpretam e disseminam dados relacionados à saúde de determinado indivíduo. Com o uso dessa tecnologia, os usuários relatam seus sintomas, obtém um diagnóstico inicial e, ainda, podem tomar uma decisão de triagem;
>
> (iii) controle de quarentena — essas ferramentas envolvem o monitoramento, em tempo real, de indivíduos (sintomáticos ou não) que cumprem as regras de isolamento social (quarentena), de acordo com as regras de saúde pública locais; e
>
> (iv) modelagem de fluxo — também são chamadas de relatórios de mobilidade e funcionam a partir da quantificação e rastreamento dos movimentos das pessoas em regiões geográficas específicas. Em regra, essas ferramentas precisam de um conjunto de dados anônimos e agregados de localização geográfica dos usuários, podendo fornecer informações sobre a eficácia das políticas de resposta à doença, como distanciamento físico ou quarentena forçada.

Todas essas medidas podem ser potencialmente adotadas pelos empregadores para aprimorar os processos internos de promoção e proteção da comunidade empresarial como um todo, com especial destaque para os trabalhadores que se relacionam com o público, sejam eles trabalhadores internos ou externos.

Especificamente quanto às ferramentas de rastreamento e proximidade, há dois grandes sistemas. O primeiro baseia-se não em sinal de *Bluetooth* de cada celular, o que é aplicado para as ferramentas de *contact tracing*, ou seja, aquelas capazes de rastrear com quem determinado indivíduo potencialmente infectado com a COVID-19 esteve em contato.[23]

---

(21) CLT: "Art. 8º As autoridades administrativas e a Justiça do Trabalho, na falta de disposições legais ou contratuais, decidirão, conforme o caso, pela jurisprudência, por analogia, por equidade e outros princípios e normas gerais de direito, principalmente do direito do trabalho, e, ainda, de acordo com os usos e costumes, o direito comparado, mas sempre de maneira que nenhum interesse de classe ou particular prevaleça sobre o interesse público. (...)" (Destacamos)

(22) IENCA, Marcello *et al*. *Op. cit*. p. 2.

(23) LANA, Alice de Perdigão; MECABÔ, Alex; SANTOS, Sanalí de Lima. *As tecnologias de geolocalização e crise epidemiológica: reflexões para uma solução conciliatória*. Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná, revisão por Roberto Nelson Brasil Pompeo Filho, junho 2020. Disponível em: <https://www.gedai.com.br/as-tecnologias-de-geolocalização-e-crise-epidemiologica-reflexoes-para-uma-solucao-conciliatoria/>. Acesso em: 7 jun. 2020.

Nesse caso, não é necessária a localização exata do indivíduo alvo, mas apenas a informação acerca da proximidade com outrem. Em outras palavras, aplicativos ou estratégias que utilizam esta tecnologia são capazes de determinar quais dispositivos estiveram próximos, de forma a possibilitar que as próprias pessoas contaminadas possam notificar outras, com quem tiveram proximidade física, de que seus exames deram positivo para a doença, o que também pode ser utilizado para desenvolvimento de políticas públicas.(24)

Já o segundo sistema de rastreamento é configurado, não por *Bluetooth*, mas a partir de dados de geolocalização, isto é, informações precisas de coordenadas geográficas de onde um dispositivo móvel, normalmente celular, está ou esteve em determinado momento, detectadas por triangulação de antenas, a partir de dados coletados por empresas de telecomunicações ou provedores de serviços de internet.(25)

No que se refere às tecnologias de rastreamento no contexto da atual pandemia, os dados de geolocalização dos indivíduos podem ser utilizados de forma agregada ou individualizada. No primeiro caso, são vistos como um conjunto de dados para fins estatísticos apenas, o que é eficiente para o monitoramento de concentrações para avaliação da efetividade das medidas de isolamento social. Já na forma individualizada, é possível averiguar o trajeto individual de cada pessoa.(26)

No entanto, isoladamente, os dados de localização não são suficientes para rastrear com quem um indivíduo infectado com o Coronavírus esteve em contato por meio do *contact tracing*, já que o contágio pressupõe uma proximidade de 2 metros. Para realizar tal análise, seria necessário o tratamento conjunto com um volume de dados muito maior, como dados de mídias sociais e informações sobre contas de cartão de crédito, o que teria potencial violador da privacidade e das regras acerca da proteção de dados pessoais. Sendo assim, para além da coleta de dados pessoais diversos e combinados, há algumas iniciativas de *contact tracing* por meio de rastreio do sinal de Bluetooth de cada celular.(27)

De forma simplificada, as técnicas digitais de *contract tracing* funcionam da seguinte maneira: diante da premissa de que aparelhos de celular registram suas próprias localizações, quando o proprietário de um desses aparelhos testa positivo para COVID-19, um registro de seus movimentos recentes é compartilhado com as autoridades de saúde e, no caso de relações trabalhistas, com o seu empregador.

Os donos de quaisquer outros dispositivos móveis que tenham tido contato próximo recente com o celular do indivíduo infectado (especialmente colegas de trabalho e clientes da empresa) são notificados do potencial risco de contágio e recomendados a seguir medidas de auto isolamento. Desta forma, para que o sistema seja eficiente, os desenvolvedores da tecnologia precisam de informações mínimas acerca da proximidade dos indivíduos e seus respectivos *status* de saúde, além da necessidade de definição de onde essas informações serão armazenadas, quem terá acesso e em qual formato.(28)

Nesse cenário, não há dúvidas de que a forma como os dados são tratados pode causar grandes violações aos direitos fundamentais dos trabalhadores (e das pessoas em geral), especialmente a privacidade, proteção de dados pessoais e o direito a não discriminação, principalmente quando não há transparência e salvaguardas mínimas.

Caso as informações pessoais sejam tratadas em modelo centralizado, quando o Estado tem acesso aos dados e a quem eles pertencem, é fundamental que as autoridades emitam notificações para os indivíduos que entraram em contato com a pessoa infectada para alertá-la da situação. Contudo, o conhecimento desses dados, considerados sensíveis pelo conceito da LGPD, pode significar e dar ensejo a demissões discriminatórias ou até indicar outros aspectos sensíveis da vida do trabalhador para além da saúde, como participação em sindicatos, em determinado

(24) LANA, Alice de Perdigão, *et al. Op. cit.*
(25) *Idem.*
(26) *Idem.*
(27) *Idem.*
(28) SERVICK, Kelly. *Cellphone Tracking Could Help Stem the Spread of Coronavirus. Is privacy the Price?* Science Magazine, mar. 2020. Disponível em: <https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-of-coronavirus-privacy-price>. Acesso em: 8 jul. 2020.

grupo político, religioso ou minoria, principalmente em governos autoritários.(29)

Apesar dos riscos potenciais para a privacidade e proteção de dados dos trabalhadores, muitos argumentam que essas tecnologias, ao analisarem os registros de localização armazenados nos celulares dos pacientes e cruzá-los com dados de outras fontes, tenderiam a ser muito mais eficientes para determinar quem pode ser contaminado e, assim, combater a doença do que a identificação tradicional por agentes de saúde. A adoção de tais medidas em alguns países, a exemplo da Coreia do Sul, foi considerada essencial no combate local da COVID-19.

Diante da propagação mundial do vírus, o governo sul coreano utilizou um sistema que, ao detectar um indivíduo contaminado pelo Coronavírus, possibilitava que a cidade ou distrito no qual a pessoa residia enviasse um alerta para outros cidadãos residentes da mesma região, inclusive com o compartilhamento de informações sobre locais onde o paciente positivo esteve, com detalhes a respeito de sua idade, gênero e movimentação. Tais dados eram coletados a partir de um circuito fechado que incluía, dentre outras, informações de televisão e até de cartão de crédito para proceder à identificação dos locais por onde o indivíduo contaminado passou.(30)

Apesar dos aparentes resultados positivos do sistema implementado na Coreia do Sul, que obteve achatamento da curva de novos casos de forma eficiente, a Comissão Nacional de Direitos Humanos do país classificou a coleta massiva de dados pelas autoridades coreanas como uma violação dos direitos humanos. Para o presidente da Comissão, o uso da tecnologia de rastreamento e alerta foi uma situação clara de exposição pública de informação privada já que, em alguns casos, foram liberadas informações demasiadamente detalhadas, o que possibilitou a identificação nas mídias sociais das pessoas infectadas, que acabaram por ser sujeitas a críticas, constrangimento e mensagens de ódio online.(31) Ainda, a coleta injustificada e desproporcional de dados sensíveis, como informações sobre gênero, poderia ensejar situações de discriminação ou até reforçar preconceitos socialmente enraizados na sociedade em razão da não testagem da tecnologia para *bias*.

A exemplo da Coreia do Sul, grandes volumes de dados para controle e monitoramento do Coronavírus já estão sendo analisados no Brasil. A partir do objetivo de um controle efetivo da disseminação da COVID-19, os Estados de São Paulo e do Rio de Janeiro elaboraram parcerias governamentais com as operadoras de telefonia para acesso aos dados de geolocalização anonimizados de seus usuários para auxiliar no enfrentamento da doença. Nesse caso específico, o rastreamento dos indivíduos é realizado por meio de sinais emitidos pelos celulares que irão representar "mapas de calor" para indicação de locais e períodos de maior ou menor concentração de pessoas. A partir desse sistema, seria possível identificar áreas de maior tendência à aglomeração, mapear o fluxo de pessoas e, em consequência, comprovar a eficácia (ou não) das medidas de distanciamento e isolamento social, com o intuito de prevenção de disseminação da doença.(32)

Outro exemplo de utilização de ferramenta de monitoramento para combate da COVID-19 foi implementado pela prefeitura do Recife, que passou a monitorar 700 mil aparelhos para coordenar ações de incentivo ao isolamento social.(33) A tecnologia utilizada baseia-se em triangulação de redes de Wi-Fi e sensores de bússola dos *smartphones* para a coleta de dados, a partir de aplicativos de terceiros que dispõem, em suas políticas de privacidade e termos de uso, a autorização de transmissão de dados a parceiros comerciais para fins de *marketing* direcionado, principalmente.(34)(35)

(29) LANA, Alice de Perdigão, *et al. Op. cit.*
(30) CLEMENTE, Rachel Ellmann; JUNI, Amanda. Contact Tracing e Privacidade em Tempos de Pandemia. *Migalhas*, 31 mar. 2020. Disponível em: <https://www.migalhas.com.br/depeso/323077/contact-tracing-e-privacidade-em-tempos-de-pandemia>. Acesso em: 8 jul. 2020.
(31) MAH, Luís. O Modelo Sul-coreano na Luta Contra a COVID-19: *Estado, Transparência e Direitos Individuais*. Público Portugal, 15 maio 2020. Disponível em: <https://www.publico.pt/2020/05/15/opiniao/modelo-sulcoreano-luta-covid19-estado-transparencia-direitos-individuais-1916540/amp>. Acesso em 8 jul. 2020.
(32) LANA, Alice de Perdigão, *et al. Op. cit.*
(33) G1. *Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra Coronavírus*. 24 mar. 2020. Disponível em: <https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-rastreia-700-mil-celulares-para-monitorar-isolamento-social-e-direcionar-acoes-contra-coronavirus.ghtml>. Acesso em 9 jul. 2020.
(34) G1. *Op. cit*.
(35) AMARAL, Bruno do. Prefeitura do Recife Coleta Localização dos Celulares para Mapear Isolamento Social. *Teletime*, 25 mar. 2020. Disponível em: <https://teletime.com.br/25/03/2020/prefeitura-do-recife-coleta-localizacao-dos-celulares-para-mapear-isolamento-social/>. Acesso em 9 jul. 2020.

Nesse exemplo, diferente do que ocorre na iniciativa de São Paulo e Rio de Janeiro, que baseava a utilização dos dados em sua suposta anonimização pelas empresas de telecomunicação, a tecnologia implementada em Recife teria por base o consentimento do usuário obtido indiretamente pelas políticas de privacidade dos aplicativos vinculados.(36) Tal aplicação é uma clara utilização ilegal de dados pessoais já que, diante da maneira como o sistema foi implementado, não era possível comprovar o consentimento livre, informado e inequívoco exigido pela LGPD, além não ser razoável que dados pessoais, inicialmente tratados para controle de crise de saúde pública, fossem compartilhados com parceiros comerciais para fins de marketing direcionado.

Diante do exposto, é de grande importância que, em um momento de pandemia mundial, as entidades do mundo do trabalho não se inspirem nos exemplos desproporcionais de tratamento de dados de localização de seus trabalhadores para fins diversos do inicialmente previsto, garantindo proporcionalidade e respeito aos ditames da lei. Por isso, é essencial que os empregadores convirjam seus interesses e seus esforços para a criação de um sistema de proteção da pessoa humana que conecte e processe os dados epidemiológicos com rapidez, segurança e eficiência, com respeito aos direitos fundamentais, principalmente a privacidade dos trabalhadores, e, ao mesmo tempo, salvando vidas.

### *4. Da utilização de dados de localização no combate à pandemia: conflito entre privacidade e saúde da comunidade empresarial?*

Há muito se discute a existência de uma dicotomia absoluta entre a utilização de dados pessoais e o direito à privacidade. No entanto, a privacidade, especialmente no mundo digital, é um conceito fluido que não se encaixa em nenhum dos dois extremos: de um lado aqueles que se posicionam contra qualquer divulgação de informações pessoais e, do outro, os que entendem que todas as informações já foram divulgadas e, portanto, não haveria que se falar em privacidade.(37) Com o desenvolvimento exponencial de novas tecnologias e a rápida construção de uma sociedade da informação, o direito à privacidade ganhou novos contornos, para além do direito à vida privada, a partir a ideia de proteção de dados pessoais, baseada no estabelecimento de proteções mínimas e controle dos indivíduos sobre os seus dados.(38)

No contexto da segurança pública, Daniel Solove(39) argumenta que entendê-la como diametralmente oposta à privacidade não é o caminho para lidar com a questão, já que, para ele, o direito à privacidade sairia "perdendo" em termos de importância. De acordo com o autor, os argumentos de oposição absoluta entre privacidade e segurança são baseados em visões equivocadas sobre os custos e benefícios da proteção da privacidade, o que acarretou um enquadramento incorreto do debate, como se o equilíbrio entre tais valores fosse uma proposição absoluta de tudo ou nada. No entanto, argumenta que a proteção da privacidade não precisa ser fatal para as medidas de segurança, mas demanda fiscalização e regulamentação adequadas. Em regra, a privacidade pode ser protegida sem prejuízos à segurança e, quando isso não seja possível, o equilíbrio deve ser buscado da maneira mais justa para os dois lados.

O mesmo raciocínio pode ser aplicado ao aparente conflito entre a privacidade e a saúde de todos aqueles que laboram ou prestam serviços no âmbito das empresas. A utilização de dados dos empregados para o combate à atual pandemia não precisa — e não deve — necessariamente violar o direito à proteção dos dados pessoais. Para tanto, deve haver controle legislativo, judicial e da sociedade organizada com a participação dos sindicatos profissionais e econômicos, além de efetivação de medidas técnicas e um robusto quadro legal-regulatório, combinado com medidas efetivas e eficazes de controle de aplicação das regras mínimas previstas nos diplomas normativos.

Desta forma, o controle legislativo-social deve incluir a previsão de padrões mínimos obrigatórios de medidas tecnológicas que garantam a segurança das informações tratadas e efetivação das regras dispostas na legislação de proteção de dados pessoais

(36) LANA, Alice de Perdigão, *et al. Op. cit.*
(37) CREMONINI, Marco *et al.* Privacy on the Internet. *In* VACCA, John R. (ed.). *Computer and Information Security Handbook*. 2. ed. Waltham, EUA: Morgan Kaufmann Publishers, 2013. p. 739-740.
(38) RODOTÀ, Stefano. *A vida na sociedade da vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 381; MAGRANI, Eduardo. *Entre dados e robôs:* ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p. 99-101.
(39) SOLOVE, Daniel J. *Nothing to Hide:* The False Tradeoff between Privacy and Security. New Haven: Yale University Press, 2011.

vigente, bem como penalidades para aqueles que não os cumpram. A CLT confere ao empregador o poder-dever de garantir a higidez das normas de saúde e segurança no trabalho, podendo valer-se do seu poder disciplinar para tal.(40)

Aliado ao controle legislativo, o judicial deve cuidar dos casos em que tais medidas não são cumpridas, de modo a garantir a efetiva aplicação das medidas legais-regulatórias e, em consequência, a segurança jurídica.

### 4.1. Métodos para segurança do tratamento de dados (controle tecnológico)

A privacidade dos dados de localização pode ser dividida em três categorias.(41) A primeira é a privacidade de identidade, que se relaciona à proteção da identidade associada à informação sobre a localização. Quanto a essa categoria, as medidas de proteção da privacidade objetivam minimizar a revelação de informações que possibilitem que seja inferida a identidade do indivíduo relacionado à localização — ou mesmo sua errônea identificação. Tais medidas podem ser adotadas em aplicativos ou programas que não demandem a autenticação/identificação do utilizador.

Também existe a dimensão da privacidade da posição do indivíduo. Nesse caso, as medidas de proteção visam acrescentar "barulho" às informações, reduzindo a precisão da informação de localização. É aplicável às situações em que a identificação do utilizador é necessária à prestação do serviço. Uma técnica de proteção bastante usada consiste no aumento da granularidade (de metros para centenas de metros, de um bairro para uma cidade e assim por diante).

Existe, ainda, a privacidade do trajeto, associada à movimentação do indivíduo, o caminho percorrido por ele. Com relação a essa dimensão, a mera desidentificação dos indivíduos pode não ser suficiente para garantir a privacidade, dado que as informações de trajeto podem ser rastreadas a ponto de serem encontradas as suas residências, locais de trabalho etc. Nesse contexto, existem outros métodos de proteção, tal como algoritmos que "perturbam" a informação, cruzando os trajetos de indivíduos onde eles se encontram, a fim de minimizar as chances de rastreio.(42)

Existem diferentes técnicas para garantia de privacidade em cada uma das dimensões relacionadas à privacidade dos dados de localização do trabalhador. Há diversos esquemas de proteção, que podem ser classificados de acordo com suas propriedades arquitetônicas (como, por exemplo, se são baseadas em servidores ou em dispositivos móveis) e métricas de privacidade (como, por exemplo, k-anonimato, entropia da localização etc.)(43) Em breve resumo, podem ser citadas as abordagens abaixo elencadas.

A abordagem de camuflagem (*cloaking*) pode ser espacial ou temporal. A primeira consiste numa chamada área camuflada que engloba o utilizador e pelo menos todos os outros utilizadores de um grupo com os mesmos parâmetros. Já a temporal consiste em camuflar o momento em que a localidade do utilizador é acessada pelo serviço de localização.(44)

A abordagem de áreas misturadas (*mix zones*) consiste, grosso modo, na anonimização da identidade do utilizador pela restrição das posições onde os utilizadores podem ser localizados por meio do uso de "pseudônimos múltiplos" (*multiple pseudonyms*).(45) A abordagem de utilização de localizações "falsas" (*dummy locations*) também pode ser empregada: o programa recupera a verdadeira localização do utilizador juntamente com dados falsos de localização.(46) Além disso, a fim de evitar a necessidade de um servidor de localização que armazene os referi-

(40) O artigo 482 da CLT estabelece os tipos de condutas infracionárias do contrato de emprego que o trabalhador pode incorrer, dentre elas estão as figuras da indisciplina (desentendimento a ordens gerais emanadas do empregador ou seus prepostos) e insubordinação (descumprimentos de ordens especificamente dirigidas a certo ou certos empregados).

(41) CREMONINI, Marco *et al*. *Op. cit*., p. 746.

(42) HOH, Baik; GRUTESER, M. *Protecting Location Privacy Through Path Confusion*. First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Atenas, 2005. p. 194-205.

(43) XIN, Kang G. *et al.* Privacy protection for users of location-based services. *IEEE Wireless Communications*, v. 19, n. 1, p. 30-39, fev. 2012.

(44) TAN, Rong; SI, Wen; WANG, Jian. A privacy protection model for location-based social networking services. *In:* SHAO, Fun; SHU, Wise; TIAN, Tracy (eds.). *Engineering Technology and Applications*. Londres: CRC Press, 2014. p. 142.

(45) FREUDIGER, Julien; SHOKRI, Reza; HUBAUX, Jean-Pierre. On the optimal placement of Mix Zones. *In:* GOLDBERG, Ian; ATALLAH, Mikhail J. (eds.). *Privacy Enhancing Technologies*. Berlim, Springer, 2009. p. 217.

(46) QU, Youyang *et al.* Privacy Preservation in Smart Cities. *In:* RAWAT, Danda B.; GHAFOOR, Kayhan Zrar (eds.). *Smart Cities Cybersecurity and Privacy*. Amsterdã: Elsevier, 2019. p. 83.

dos dados dos utilizadores, foram criados sistemas ponto-a-ponto (*peer-to-peer systems*), que possibilitam requisições de localização anónimas. Por fim, podem ser citados os protocolos de recuperação de informações privadas baseados em criptografia.(47)

Quanto a privacidade e proteção de dados pessoais, é fundamental que as empresas e os órgãos públicos que desenvolvam e utilizem tecnologias inteligentes baseadas em dados, como a Inteligência Artificial, apliquem o *privacy by design and default*. Em outras palavras, é essencial que apliquem as regras e princípios da proteção de dados durante todo o ciclo de vida dos dados (coleta, tratamento, utilização e descarte) e durante todo o processo de desenvolvimento da tecnologia aplicada, a partir da adoção de medidas técnicas e organizativas adequadas para garantia de uma proteção de dados adequada e eficiente.(48) Para além da privacidade, recomenda-se que a construção de tecnologias seja orientada por princípios éticos e direitos humanos desde a sua concepção e por padrão.

Apesar de não haver um plano fixo para implementação do *privacy by design*, há algumas estratégias sugeridas, a exemplo de: (i) minimização — o sistema deve ser programado para coletar e processar apenas as quantidades mínimas de dados necessários; (ii) ocultação — os dados pessoais devem ser ocultados da *plain view*; (iii) separação — dados pessoais devem ser processados e armazenados em compartimentos separados dos demais, sempre que possível; (iv) agregação — os dados pessoais devem sempre ser processados do nível mais alto de agregação possível, em um estado em que esteja protegido, mas ainda útil; (v) estratégias orientadas — sempre que os dados pessoais forem utilizados, a tecnologia deve informar deste uso; (vi) controle — os titulares de dados pessoais devem ter autonomia e agência sobre seus dados tratados, podendo interferir quando desejarem; (vii) imposição — garantia de políticas de privacidade adequadas à legislação e que sejam, de fato, aplicáveis pelos sistemas baseados em dados; (viii) demonstração — as empresas e órgãos devem ser capazes de demonstrar cumprimento de todos os requisitos legais.(49);(50)

Esses são apenas alguns exemplos das metodologias utilizadas para garantir a privacidade dos trabalhadores, baseados em localização (em inglês, *Location based services*: *LBS*). No entanto, é necessário que haja um quadro legal e regulatório eficaz a fim de determinar as diretrizes mínimas de proteção no nível de controle tecnológico da privacidade do trabalhador, além de um controle judicial, arbitral e corporativo-sindical quanto ao cumprimento da legislação e regulações aplicáveis.

### 4.2. Regulação e fiscalização (controle legislativo, judicial e coletivo)

O controle legislativo é imprescindível para a imposição do controle tecnológico. A legislação deve definir níveis mínimos de segurança aceitáveis a fim de minimizar as chances de violação. O controle judicial, por sua vez, é igualmente imprescindível para a efetiva aplicação e observância da legislação.

Nesse contexto, registra-se que a Constituição brasileira resguarda o direito à privacidade.(51) Contudo, diante dos avanços tecnológicos e da ascensão da sociedade e economia de dados, a privacidade como o "direito de ser deixado só" já não era suficiente, o que tornou necessário o desdobramento da proteção em seu viés positivo, a partir da proteção de dados pessoais.(52) Nesse contexto, o direito à proteção dos dados pessoais é atualmente considerado direito fundamental autônomo(53) que, apesar de não estar expressamente previsto na Constituição,(54) já foi

(47) KHOSHGOZARAN, Ali; SHAHABI, Cyrus; SHIRANI-MEHR, Houtan. Location privacy: Going beyond K-anonymity, cloaking and anonymizers. *Knowledge and Information Systems*, v. 26, p. 435-465, mar. 2011.
(48) MAGRANI, Eduardo. *Entre Dados e Robôs:* Ética e Privacidade na Era da Hiperconectividade. Porto Alegre: Arquipélago Editorial, 2019. p. 129.
(49) HOEPMAN, Jaap-Henk. Privacy design strategies. *In:* CUPPENS-BOULAHIA, Nora *et al.* (ed.). *ICT Systems and Privacy Protection*. Nova Iorque: Springer, 2014. p. 452-457.
(50) MAGRANI, Eduardo. *Op. cit*. p. 129-130.
(51) Como um direito negativo, a exemplo da inviolabilidade da intimidade e da vida privada prevista no art. 5º, X.
(52) RODOTÁ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 24.
(53) RODOTÁ, Stefano. *Op. cit*. p. 17.
(54) Atualmente, a Proposta de Emenda à Constituição (PEC) 17/19 está em tramitação no Congresso Nacional do Brasil e busca inserir a proteção de dados pessoais no rol expresso de direitos fundamentais e garantias individuais da Constituição Federal de 1988. A O objetivo é conferir competência privativa à União para legislar sobre o assunto. Agência Câmara de Notícias. *PEC Transforma*

reconhecido pelo Supremo Tribunal Federal (STF) como direito fundamental do ordenamento jurídico brasileiro.(55)

No âmbito infraconstitucional, a LGPD determina níveis mínimos de segurança e princípios orientados à proteção dos dados pessoais. Tais garantias incluem, por exemplo, o cumprimento de princípios, bases legais, direito dos titulares e regras específicas sobre boas práticas em termos de segurança da informação. O tratamento dos dados pessoais, principalmente os de localização e de saúde, sendo este último considerado sensível, pode ocorrer quando presente uma das bases legais dispostas no art. 7º para dados pessoais em geral e art. 11 para dados sensíveis. Neste âmbito, podemos citar o consentimento do titular, que deve ser sempre livre, informado e inequívoco, considerado a base legal mais conhecida e utilizada para se permitir o uso de dados pessoais por terceiros,(56) apesar de não existir, em regra, hierarquização entre as bases legais da LGPD.

A institucionalização dessas técnicas de controle pode, ainda — e o ideal é que seja —, ser objeto de uma autorregulação superveniente e compartilhada entre trabalhadores e empresas, através de regular processo de negociação coletiva de trabalho, que observe regras de *compliance*(57) e os direitos fundamentais ligados à privacidade e a saúde, a fim de contemplar e harmonizar todos os interesses, direitos e obrigações que estão em aparente tensão, dentro do contexto do princípio da prevalência ampla do negociado sobre o legislado. Nesse cenário, é recomendável também a realização de relatórios de impacto, conforme previsto no art. 38 da LGPD, além de auditorias prévias e constantes.

Comprometer a sociedade civil organizada, *in casu*, as entidades sindicais, com a busca de soluções possíveis para criação de um sistema eficaz e adequado de proteção desses direitos fundamentais constitui medida democrática e que pode ser um fator decisivo para que essa matéria ingresse efetivamente nas pautas de preocupação coletiva dos protagonistas sociais e econômicos.

No contexto excepcional de saúde do trabalhador (o que envolve a própria noção de saúde pública), existem situações em que os dados pessoais, ainda que sensíveis, sejam tratados mesmo sem o consentimento do titular, desde que observados requisitos específicos como: (i) a proteção da vida ou da incolumidade física do trabalhador ou de terceiros (como é o caso da comunidade empresarial);(58) (ii) a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde das empresas e/ou dos sindicatos, serviços de saúde ou autoridade sanitária;(59) (iii) no caso da administração pública, é possível o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos", além de convênios e outros instrumentos;(60) e (iv) no âmbito da administração privada, o empregador também deve manipular esses dados com o escopo de instituir, acompanhar, redirecionar ou calibrar sua política interna (corporativa) de prevenção de

*Proteção de Dados Pessoais em Direito Fundamental*. Câmara dos Deputados: Ciência, Tecnologia e Comunicações, 9 ago. 2019. Disponível em: <https://www.camara.leg.br/noticias/565439-PEC-TRANSFORMA-PROTECAO-DE-DADOS-PESSOAIS-EM-DIREITO-FUNDAMENTAL>. Acesso em: 10 jul. 2020.

(55) ABRUSIO, Juliana; CAMPOS, Ricardo; MARANHÃO, Juliano. A Proteção de Dados Pessoais no STF e o Papel do IBGE. *Consultor Jurídico,* maio 2020. Disponível em: <https://www.conjur.com.br/2020-mai-29/maranhao-campos-abrusio-protecao-dados-stf-ibge>. Acesso em: 8 jul. 2020.

(56) BRASIL. LGPD, arts. 5º, XII e 7º, I.

(57) O *Compliance* está ligado diretamente ao princípio da boa-fé que pode ser definido como: "É o dever ético de comportamento reto, leal para com os interesses do outro contratante, tendo por fundamento a confiança recíproca que um deposita no outro no senso de que devem agir sempre de acordo com as intenções manifestadas e vertebralizadas nas cláusulas do ajuste. O elemento confiança, assim, atua de maneira a diminuir a complexidade das relações contratuais, reduzindo, para o sujeito, a insegurança quanto ao futuro. Com ela, a parte tem condições de projetar sua ação conforme um conjunto relativamente pequeno de possibilidades, excluindo do seu planejamento aquilo em que confia — mais do que espera — que não acontecerá. (...) Assim, o artigo 422 (do Código Civil) tem perfeita adaptação na seara laboral, consolidando em definitivo a noção de que o contrato de trabalho rende ensejo a uma duplicidade de espécies de deveres: os de prestação e os genéricos de conduta. A boa-fé, portanto, configura um elemento intrínseco ao contrato de emprego, na medida em que, limitando a autonomia da vontade das partes, resgata o conteúdo ético da relação capital-trabalho". (SILVA, Paulo Renato Fernandes da. As repercussões do Código Civil de 2002 sobre o contrato de trabalho e o neoconstitucionalismo. *Revista do Tribunal Regional do Trabalho da 10ª Região* (Brasília), v. 19, n. 20, 2015).

(58) BRASIL. LGPD. arts. 7º, VII e 11, II, "e".

(59) *Ibidem,* arts. 7º, VIII e 11, II, "f".

(60) *Ibidem,* art. 7º, III.

acidentes de trabalho e de promoção da saúde do trabalhador.[61]

Mesmo nos casos de coleta e tratamento de dados de saúde sem o consentimento do titular (o empregado), a natureza dos dados se mantém sensível, o que exige cautelas especiais, principalmente contra incidentes de vazamento, o que deve constar de um Relatório detalhado de Impacto de Dados Pessoais,[62] além de observação estrita aos princípios legais da proteção de dados. Dentre eles, merecem destaque os princípios da finalidade[63] e adequação,[64] que criam a obrigação para o controlador de cumprimento da finalidade específica para qual os dados do titular foram coletados (saúde do trabalhador que, em última instância, reverbera diretamente na saúde pública), sob pena de graves violações aos regramentos de proteção de dados que orientam o Brasil.[65]

Ainda, entende-se que o tratamento de dados em conformidade com a LGPD deve se reger pelo princípio da necessidade[66] que, a partir da ideia de minimização, impõe o dever de coletar apenas os dados estritamente necessários para as finalidades definidas pelo controlador. Além disso, a fim de resguardar a privacidade dos titulares, os dados pessoais devem ser, sempre que possível, anonimizados ou pseudonimizados,[67] inclusive no contexto de estudos, análises e pesquisas relativas às políticas empresariais de proteção à saúde do trabalhador e do meio ambiente de trabalho e, claro, de saúde pública também.[68] Apesar de semelhantes, os processos de pseudonimização e anonimização são distintos. Enquanto no primeiro a informação permanece identificável, a partir de informações suplementares, no segundo a reidentificação é, em tese, impossível. Daí resulta que sobre o tratamento dos dados anônimos não incidem as regras da LGPD, pois não dizem respeito a uma pessoa física singular identificada ou identificável.[69]

No mesmo sentido, caso os dados de localização e proximidade sejam divulgados pelas empresas de telecomunicações, a lei exige que a empresa envolvida apenas divulgue a terceiros (no caso ao empregador) informações agregadas sobre o uso de seus serviços por usuários quando não for possível sua identificação, direta ou indireta, ou a violação de sua intimidade.[70] Em outras palavras, no caso de divulgação dos dados por essas empresas, eles não podem ser dados pessoais que identifiquem ou levem à identificação dos indivíduos, de forma a afastar a aplicação da LGPD.

Nesse ponto, devemos remarcar que, dentro do poder diretivo do empregador, reside também o poder de controle sobre os empregados, motivo pelo qual esse tipo de monitoramento vinculado ao contrato de emprego e no exercício dos poderes e deveres inerentes a este, faz parte integrante das atribuições deferidas à empresa.

O controle judicial também deve ser rígido. De maneira geral, o controle exercido pelo Judiciário brasileiro é sólido e consistente no que diz respeito à proteção dos dados pessoais. Ilustrado pela jurisprudência do Supremo Tribunal Federal, o entendimento preponderante é o de estabelecer garantias robustas para a manutenção da privacidade e outros direitos igualmente fundamentais do trabalhador.[71][72] No contexto da atual pandemia, o Supremo Tribunal Federal deferiu medida cautelar impedindo a disponibilização de dados de clientes pelas operadoras

(61) CF/88: "Art. 194. A seguridade social compreende um conjunto integrado de ações de iniciativa dos Poderes Públicos e da sociedade, destinadas a assegurar os direitos relativos à saúde, à previdência e à assistência social."
(62) BRASIL. LGPD. art. 38.
(63) *Ibidem*, art. 6º, I.
(64) *Ibidem*, art. 6º, II.
(65) CLEMENTE, Rachel Ellmann; JUNI, Amanda. *Contact Tracing* e Privacidade em Tempos de Pandemia. *Migalhas*, 31 mar. 2020. Disponível em: <https://www.migalhas.com.br/depeso/323077/contact-tracing-e-privacidade-em-tempos-de-pandemia>. Acesso em: 1º jul. 2020.
(66) BRASIL. LGPD, art. 6º.
(67) Nos termos da LGPD, art. 13, § 4º, a pseudonimização é o processo pelo qual os dados perdem a "possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro". Por sua vez, de acordo com o art. 5º, XI, da Lei, a anonimização refere-se ao processo de desidentificação de dados pela utilização de "meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".
(68) BRASIL. LGPD, arts. 7º, IV, 11, II, "c"; e 13.
(69) *Ibidem*, art. 12.
(70) BRASIL. Lei n. 9.472, de 16 de julho de 1997 (Lei Geral das Telecomunicações), art. 72, § 2º.
(71) BRASIL. Supremo Tribunal Federal. HC 86094, Rel. Min. Marco Aurélio, Primeira Turma. Julgado em 20.09.2005.
(72) *Id*. RE 389808, Rel. Min. Marco Aurélio, Tribunal Pleno. Julgado em 15.12.2010.

de telefonia ao Instituto Brasileiro de Geografia e Estatística — IBGE por força de medida provisória alegadamente inconstitucional.

A medida provisória em questão dispõe que as operadoras de telefonia fixa e móvel devem disponibilizar ao IBGE "a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas" para produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.(73)A Corte Suprema deferiu o pedido de medida cautelar para suspensão de tal obrigação por considerar, dentre outros fatores, que a ausência de garantias de tratamento adequado e seguro dos dados compartilhados, aliada ao fato de que, à época, ainda não se encontrava em vigor a LGPD, que define os critérios de responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais, violaria o direito fundamental à privacidade e da inviolabilidade do sigilo dos dados pessoais previstos no artigo 5º, X e XII, da Constituição brasileira.

### *5. Conclusão*

O debate acerca do aparente conflito entre o direito à privacidade/proteção de dados pessoais e o direito à saúde pública e corporativa, principalmente no contexto das políticas de saúde do trabalhador, vem sendo travado há muito tempo. No entanto, tal batalha não se baseia em um tudo ou nada: não é necessário violar um direito para que se tenha acesso ao outro.

O mesmo pressuposto se aplica à saúde do trabalhador e de todos que com ele compartilham o ambiente empresarial. Existem mecanismos que, ainda que não sejam completamente infalíveis, permitem o tratamento de dados pessoais (inclusive os dados de localização), de maneira a minimizar possíveis violações da privacidade dos empregados, impedindo um cenário de vigilância e arbitrariedade.

Nessa seara, o Brasil conta com um robusto quadro regulatório e fiscalizador. Nesse contexto de pandemia, caberá à sociedade organizada, especialmente aos entes de representação profissional e empresarial, e às cortes brasileiras, em conjunto com os órgãos de fiscalização, encontrar o equilíbrio entre o direito à proteção dos dados de localização e a saúde do trabalhador. Além disso, seria igualmente alvissareiro elaborar novos regulamentos que se adequem às tecnologias, cada vez mais avançadas, bem como se adaptem às demandas e necessidades de setores econômicos ou de empresas específicas, tanto para utilização e tratamento de dados de localização quanto para minimizar o risco de eventuais violações.

Assim, ainda que a proteção da privacidade do trabalhador no contexto das novas tecnologias (em especial da multiplicação dos sistemas baseados em localização) ainda se mostre um desafio, tanto do ponto de vista regulatório e judicial quanto do tecnológico, a privacidade não deve ser, em regra, um obstáculo às políticas públicas e corporativas de saúde, especialmente aquelas voltadas para o combate da pandemia, desde que em consonância com boas práticas técnicas e mandamentos regulatórios. O que deve ser levado em consideração pelas autoridades é o caminho a ser seguido numa realidade pós-pandêmica, para que a vigilância exacerbada dos trabalhadores (e dos cidadãos) continue sendo a exceção e não a regra geral.

### *6. Referências*

ABRUSIO, Juliana; CAMPOS, Ricardo; MARANHÃO, Juliano. A Proteção de Dados Pessoais no STF e o Papel do IBGE. *Consultor Jurídico*, maio 2020. Disponível em: <https://www.conjur.com.br/2020-mai-29/maranhao-campos-abrusio-protecao-dados-stf-ibge>. Acesso em: 8 jul. 2020.

AGÊNCIA CÂMARA DE NOTÍCIAS. *PEC Transforma Proteção de Dados Pessoais em Direito Fundamental*. Câmara dos Deputados: Ciência, Tecnologia e Comunicações, 9 ago. 2019. Disponível em: <https://www.camara.leg.br/noticias/565439-PEC-TRANSFORMA-PROTECAO-DE-DADOS-PESSOAIS-EM-DIREITO-FUNDAMENTAL>. Acesso em: 10 jul. 2020.

AMARAL, Bruno do. Prefeitura do Recife Coleta Localização dos Celulares para Mapear Isolamento Social. *Teletime*, 25 mar. 2020. Disponível em: <https://teletime.com.br/25/03/2020/prefeitura-do-recife-coleta-localizacao-dos-celulares-para-mapear-isolamento-social/>. Acesso em: 9 jul. 2020.

ATAEI, Mehrnaz; KRAY, Christian. Ephemerality is the New Black: A Novel Perspective on Location Data Management and Location Privacy in LBS. *In:*

(73) BRASIL. Medida Provisória n. 954, de 17 de abril de 2020.

GERTNER, Georg; HUANG, Haosheng (ed.). *Progress in Location-Based Services 2016*. Switzerland, spring 2017.

BACA, Murtha (ed.). *Introduction to Metadata*. 3. ed. Los Angeles: Getty Research Institute, 2016.

BRASIL. Lei n. 9.472, de 16 de julho de 1997.

_____ . Lei n. 13.709, de 14 de agosto de 2018.

_____ . Medida Provisória n. 954, de 17 de abril de 2020.

_____ . Supremo Tribunal Federal. HC 86094, Rel. Min. Marco Aurélio, Primeira Turma. Julgado em 20.9.2005.

_____ . Supremo Tribunal Federal. RE 389808, Rel. Min. Marco Aurélio, Tribunal Pleno. Julgado em 15.12.2010.

CARTA dos Direitos Fundamentais da União Europeia, 2000. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. Acesso em: 10 jul. 2020.

CLEMENTE, Rachel Ellmann; JUNI, Amanda. Contact Tracing e Privacidade em Tempos de Pandemia. *Migalhas*, 31 mar. 2020. Disponível em: <https://www.migalhas.com.br/depeso/323077/contact-tracing-e-privacidade-em-tempos-de-pandemia>. Acesso em: 8 jul. 2020.

CLEMENTE, Rachel Ellmann; JUNI, Amanda. Contact Tracing e Privacidade em Tempos de Pandemia. *Migalhas*, 31 mar. 2020. Disponível em: <https://www.migalhas.com.br/depeso/323077/contact-tracing-e-privacidade-em-tempos-de-pandemia>. Acesso em: 1º jul. 2020.

CONVENÇÃO Europeia dos Direitos Humanos, 1953. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 10 jul. 2020.

CREMONINI, Marco *et al.* Privacy on the Internet. *In:* VACCA, John R. (ed.). *Computer and Information Security Handbook*. 2. ed. Waltham: Morgan Kaufmann, 2013.

DECLARAÇÃO Universal dos Direitos Humanos, 1948. Disponível em: <https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf>. Acesso em: 10 jul. 2020.

ELECTRONIC FRONTIER FOUNDATION (EFF). *COVID-19 and Digital Rights*. Disponível em: <https://www.eff.org/issues/covid-19>. Acesso em: 11 jun. 2020.

FREUDIGER, Julien; SHOKRI, Reza; HUBAUX, Jean-Pierre. On the optimal placement of Mix Zones. *In:* GOLDBERG, Ian; ATALLAH, Mikhail J. (eds.). *Privacy Enhancing Technologies*. Berlim, springer, 2009.

G1. *Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra Coronavírus*. 24 mar. 2020. Disponível em: <https://g1.globo.com/pe/pernambuco/noticia/2020/03/24/recife-rastreia-700-mil-celulares-para-monitorar-isolamento-social-e-direcionar-acoes-contra-coronavirus.ghtml>. Acesso em: 9 jul. 2020.

HOEPMAN, Jaap-Henk. Privacy design strategies. *In:* CUPPENS-BOULAHIA, Nora *et al.* (ed.). *ICT Systems and Privacy Protection*. Nova Iorque, springer 2014.

HOH, Baik; GRUTESER, M. Protecting Location Privacy Through Path Confusion. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks* (SECURECOMM'05), Atenas, 2005.

IENCA, Marcello *et al.* Digital tools against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid. *The Lancet Digital Health* 2020, 29 jun. 2020. p. 1. Disponível em: <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30137-0/fulltext>. Acesso em: 12 jun. 2020.

KHOSHGOZARAN, Ali; SHAHABI, Cyrus; SHIRANI-MEHR, Houtan. Location privacy: Going beyond K-anonymity, cloaking and anonymizers. *Knowledge and Information Systems*, v. 26, p. 435-465, mar. 2011.

KRUMM, John. A survey of computational location privacy. *Pers Ubiquit Comput* 13, p. 391-399, 2009.

LANA, Alice de Perdigão; MECABÔ, Alex; SANTOS, Sanalí de Lima. *As tecnologias de geolocalização e crise epidemiológica:* reflexões para uma solução conciliatória. Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná, revisão por Roberto Nelson Brasil Pompeo Filho, jun. 2020. Disponível em: <https://www.gedai.com.br/as-tecnologias-de-geolocalização-e-crise-epidemiologica-reflexoes-para-uma-solucao-conciliatoria/>. Acesso em: 7 jun. 2020.

MAGRANI, Eduardo. *Entre Dados e Robôs:* Ética e Privacidade na Era da Hiperconectividade. Porto Alegre: Arquipélago Editorial, 2019.

MAH, Luís. O Modelo Sul-coreano na Luta Contra a COVID-19: Estado, Transparência e Direitos Individuais. *Público Portugal*, 15 maio 2020. Disponível

em: <https://www.publico.pt/2020/05/15/opiniao/modelo-sulcoreano-luta-covid19-estado-transparencia-direitos-individuais-1916540/amp>. Acesso em: 8 jul. 2020.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). *WHO Director-General's opening remarks at the media briefing on COVID-19*, mar. 2020. Disponível em: <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020>. Acesso em: 5 jun. 2020.

PACTO Internacional sobre os Direitos Civis e Políticos, 1966.

POMERANTZ, Jeffrey. *Metadata*. Cambridge: The MIT, 2015.

QU, Youyang *et al.* Privacy Preservation in Smart Cities. *In:* RAWAT, Danda B.; GHAFOOR, Kayhan Zrar (eds.). *Smart Cities Cybersecurity and Privacy*. Amsterdã: Elsevier, 2019.

RODOTÁ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SERVICK, Kelly. Cellphone Tracking Could Help Stem the Spread of Coronavirus. Is privacy the Price? *Science Magazine*, mar. 2020. Disponível em: <https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-of-coronavirus-privacy-price>. Acesso em: 8 jul. 2020.

SILVA, Paulo Renato Fernandes da. As repercussões do Código Civil de 2002 sobre o contrato de trabalho e o neoconstitucionalismo. *Revista do Tribunal Regional do Trabalho da 10ª Região*, Brasília, v. 19, n. 20, 2015. Disponível em: <https://revista.trt10.jus.br/index.php/revista10/issue/view/3>.

SOLOVE, Daniel J. *Nothing to Hide:* The False Tradeoff between Privacy and Security. New Haven: Yale University Press, 2011.

TAN, Rong; SI, Wen; WANG, Jian. A privacy protection model for location-based social networking services. *In:* SHAO, Fun; SHU, Wise; TIAN, Tracy (eds.). *Engineering Technology and Applications*. Londres: CRC Press, 2014.

UNIÃO EUROPEIA. Agência dos Direitos Fundamentais da União Europeia (FRA). *Tech answers to COVID-19 should also safeguard fundamental rights*. Viena: FRA Press Release, 28 maio 2020. Disponível em: <https://fra.europa.eu/sites/default/files/fra_uploads/pr-2020-covid-rights-impact-apps_en.pdf>. Acesso em: 6 jun. 2020.

UNIÃO EUROPEIA. Conselho. *Contact Tracing Apps* (Council of Europe Portal). Disponível em: <https://www.coe.int/en/web/data-protection/contact-tracing-apps>. Acesso em: 5 jun. 2020.

XIN, Kang G. *et al.* Privacy protection for users of location-based services. *IEEE Wireless Communications*, v. 19, n. 1, fev. 2012.