

A VIGILÂNCIA POR DADOS NO CONTEXTO DA COVID-19: IMPLICAÇÕES E DESAFIOS PARA AS RELAÇÕES DE TRABALHO

Samuel Rodrigues de
Oliveira,
Pontifícia Universidade
Católica do Rio de Janeiro
(PUC-Rio), <https://orcid.org/0000-0002-7059-580X>

Marcos Aragão
Couto Oliveira,
Pontifícia Universidade
Católica do Rio de Janeiro
(PUC-Rio), <https://orcid.org/0000-0001-5180-0524>

Dorival Fagundes
Cotrim Junior,
Pontifícia Universidade
Católica do Rio de Janeiro
(PUC-Rio), <https://orcid.org/0000-0002-7389-7635>

Data de submissão:
01/03/2021
Data de aceite:
17/12/2021

Data surveillance in the context of covid-19: implications and challenges

RESUMO

Trata-se de um artigo construído sob a metodologia exploratória para discutir o tema da vigilância do trabalhador no ambiente de trabalho, especificamente no sentido de controle, operada através do tratamento de dados pessoais no contexto da pandemia de COVID-19. Inicialmente contextualiza-se a pandemia do novo coronavírus e em seguida apresenta-se a discussão acerca das implicações das novas tecnologias no ambiente de trabalho, sobretudo a vigilância operada a partir do tratamento de dados pessoais. Alguns exemplos internacionais são trazidos a título ilustrativo. Conclui-se no sentido de que essa forma de monitoramento deve ser utilizada em caráter excepcional e, quando utilizada, deve obedecer ao regime jurídico da proteção de dados, atendendo aos fins propostos, adequados e claramente informados, sob pena de violação dos direitos e garantias fundamentais.

Palavras-chave: Privacidade. Proteção de dados. Tecnologias de monitoramento. Trabalho. Vigilância.

Abstract

This article is built under an exploratory methodology to discuss the theme of surveillance of the worker in the workplace, specifically in the sense of control, operated through the processing of personal data in the context of the COVID-19 pandemic. Initially, the pandemic of the new coronavirus is contextualized and then the discussion about the implications of new technologies in the workplace is presented, focusing on the surveillance operated through the processing of personal data. Some international examples are brought as an illustration. We conclude in the sense that this form of monitoring must be used on an exceptional



basis and, when used, must obey the legal regime of data protection, attending to the proposed, adequate and clearly informed purposes, under penalty of violation of the fundamental rights and guarantees.

Keywords: Data protection. Labour. Monitoring technologies. Privacy. Surveillance.

1. INTRODUÇÃO E APONTAMENTOS METODOLÓGICOS

A essa altura, a crise sanitária (mas também financeira e política) provocada pela pandemia do “novo” coronavírus não é novidade^{1 2}. O que talvez seja novidade, contudo, são os reflexos do combate à COVID-19 no que diz respeito ao recrudescimento e surgimento de práticas de vigilância.

Manifestando justificada preocupação com o fortalecimento de práticas de monitoramento, sobretudo o tecnológico, no contexto da pandemia de COVID-19, mais de 130 grupos de direitos humanos, incluindo a Anistia Internacional e a *Human Rights Watch*, assinaram conjuntamente uma carta alertando contra os perigos da consolidação da vigilância. No documento, temos a seguinte consideração:

A tecnologia pode e deve desempenhar um papel importante durante este esforço para salvar vidas, tal como difundir mensagens de saúde pública e aumentar o acesso aos cuidados de saúde. Entretanto, um aumento nos poderes de vigilância digital do Estado, como a obtenção de acesso a dados de localização de telefones celulares, ameaça a privacidade, a liberdade de expressão e a liberdade de associação, de maneiras que poderiam violar direitos e degradar a confiança nas autoridades públicas - minando a eficácia de qualquer resposta de saúde pública. Tais medidas também constituem riscos de discriminação e podem prejudicar de forma desproporcional comunidades já marginalizadas.³⁴

¹ HUANG et al, 2020.

² BONG et al, 2020.

³ JOINT CIVIL SOCIETY STATEMENT, 2020.

⁴ JOINT CIVIL SOCIETY STATEMENT, 2020. Tradução nossa. No original: “Technology can and should play an important role during this effort to save lives, such as to spread public health messages and increase access to health care. However, an increase in state digital surveillance powers, such as obtaining access to mobile phone location data, threatens privacy, freedom of expression and freedom of association, in ways that could violate rights and degrade trust in public authorities – undermining the effectiveness of any public health response. Such measures also pose a risk of discrimination and may disproportionately harm already marginalized communities”.

Em razão da natureza do tema abordado no presente trabalho, é possível classificá-lo, no que se refere a seus objetivos, como uma pesquisa exploratória. Segundo Gil (2002), esse tipo de pesquisa objetiva proporcionar maior familiaridade com o problema, a fim de torná-lo mais explícito ou de construir hipóteses.

Nesse sentido, o presente artigo objetiva discutir o controle e a vigilância operados a partir do tratamento de dados pessoais (*dataveillance*) no contexto da pandemia do novo coronavírus, com foco nas relações de trabalho e, especialmente, em conjunturas de trabalho remoto. Apresentam-se algumas situações concretas de uso abusivo dessas tecnologias, bem como algumas implicações de ordem ética e desafios a serem superados.

Em razão da natureza do tema abordado no presente trabalho, é possível classificá-lo, no que se refere a seus objetivos, como uma pesquisa exploratória. Segundo Gil (2002), esse tipo de pesquisa objetiva proporcionar maior familiaridade com o problema, a fim de torná-lo mais explícito ou de construir hipóteses. Expõe o autor que

[...] estas pesquisas têm como objetivo principal o aprimoramento de idéias ou a descoberta de intuições. Seu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado. Na maioria dos casos, essas pesquisas envolvem: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que “estimulem a compreensão”.⁵

Diante da relativa novidade do assunto, a pesquisa bibliográfica revela-se de grande importância para a concretização dos objetivos pretendidos. Como aponta Fonseca, a pesquisa científica pode basear-se fundamentalmente na pesquisa bibliográfica, “procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta”⁶.

Assim, em um primeiro momento, contextualiza-se a questão da vigilância durante a pandemia do novo coronavírus, para apresentar em seguida algumas das implicações identificadas e finaliza-se argumentando que tecnologias de monitoramento devem ser utilizadas excepcionalmente e, quando empregadas, deverão pautar-se conforme a regulação jurídica vigente, com vistas a proteção dos dados e seguindo rigorosamente os fins propostos, adequados e informados, a fim de que sejam garantidos os direitos fundamentais da pessoa humana.

⁵ GIL, 2002, p. 41.

⁶ FONSECA, 2002, p. 32.

1. COVID-19 E O (NEM TÃO) “NOVO NORMAL”: PRÁTICAS DE VIGILÂNCIA NO CONTEXTO DA PANDEMIA

Em se tratando de uma emergência de saúde global, esforços extraordinários tiveram de ser, e têm sido realizados para o enfrentamento à COVID-19. Felizmente, hoje contamos com um desenvolvimento e aparatos tecnológicos inimagináveis⁷ há até poucas décadas, cuja importância para o enfrentamento da doença e de sua propagação é indiscutível. A questão é que, mais frequentemente que não, o uso de novas tecnologias vem ocorrendo de maneira desproporcional – em termos jurídicos, sem observância de princípios como finalidade, adequação, necessidade e precaução^{8 9}.

Ao redor do globo, não faltam exemplos do emprego de tecnologias de vigilância para enfrentamento da doença. Na Moldávia, por exemplo, a polícia tem utilizado sistemas de reconhecimento facial para identificar cidadãos que não estejam cumprindo as orientações de isolamento social¹⁰, tal como na Rússia, onde, além de tecnologias de reconhecimento facial^{11 12}, códigos QR foram adotados como “passes digitais” a fim de controlar o fluxo de pessoas em Moscou^{13 14}. Na China, epicentro inicial da doença, há uma combinação de diferentes técnicas de monitoramento: controle de aglomerações mediante análise de dados de geolocalização de aparelhos celulares; rastreamento de contato (*contact tracing*)^{15 16}; reconhecimento facial para monitorar o deslocamento de infectados¹⁷; *Scanners* de temperatura corporal e sistemas programados para reconhecer se as pessoas estavam ou não utilizando máscaras foram umas das primeiras inovações adotadas na capital chinesa, Pequim¹⁸.

Curiosamente, enquanto em diversos países se discutem as eventuais violações a direitos e garantias fundamentais decorrentes

⁷ NEWLANDS et al., 2020.

⁸ NGUYEN, 2020.

⁹ OLIVEIRA, 2021.

¹⁰ TRANSNITRA NEWS, 2020.

¹¹ BBC, 2020.

¹² DO CARMO BARRIGA et al, 2020.

¹³ RFE/RL, 2020.

¹⁴ MUSIANI et al, 2020.

¹⁵ FERRETI et al, 2020.

¹⁶ WORLD HEALTH ORGANIZATION, 2020a.

¹⁷ GIELOW, 2020.

¹⁸ BORAK, 2020a.

das medidas de vigilância adotadas ou fortalecidas recentemente, principalmente aquelas sobre as quais os cidadãos não possuem a capacidade de consentir, como reconhecimento facial, o Departamento de Segurança Interna dos Estados Unidos demonstrou uma preocupação no sentido contrário¹⁹. Uma nota do serviço de inteligência do departamento, de maio de 2020, manifesta expressamente o receio de que o uso de máscaras pela população impossibilite o emprego de tecnologias de reconhecimento facial pelas forças policiais do país²⁰. Todavia, para a felicidade do *Homeland Security*, e lamento dos cidadãos estadunidenses (não só estadunidenses, diga-se de passagem), *softwares* de reconhecimento facial têm sido aperfeiçoados, de modo que já atingem níveis de acurácia considerados satisfatórios mesmo se a pessoa a ser identificada ou reconhecida estiver usando uma máscara²¹.

Além de discussões sobre práticas de vigilância operadas por autoridades governamentais em espaços públicos, outras questões igualmente relevantes têm sido levantadas^{22 23}. Por exemplo, como é sabido, a pandemia de coronavírus implicou alterações estruturais no âmbito da educação, fazendo com que determinadas atividades, como aulas e exames, passassem a ser realizadas remotamente^{24 25}. Com isso, ferramentas foram desenvolvidas a fim de monitorar os alunos, sobretudo durante a realização de provas, de modo a coibir possíveis atos fraudulentos. É o caso do *Proctorio*, software adotado por algumas universidades dos EUA e que, a partir da *webcam* dos computadores, analisa os movimentos da cabeça e dos olhos dos estudantes²⁶. O programa também registra a presença de ruídos no cômodo onde o computador se encontra, além de registrar os movimentos do mouse e o uso do teclado, indicando, para o examinador, a existência de quaisquer aspectos tidos como suspeitos²⁷.

¹⁹ Para ver uma atuação anterior à pandemia de COVID-19 do referido Departamento, conferir: MCCLELLAN, 2020.

²⁰ HVESTENDAHL & BIDDLE, 2020.

²¹ BORAK, 2020b.

²² GASSER et al, 2020.

²³ WORLD HEALTH ORGANIZATION, 2020b.

²⁴ SANTOS JUNIOR & MONTEIRO, 2020.

²⁵ SENHORAS, 2020.

²⁶ SWAUGER, 2020.

²⁷ FEATHERS, ROSE, 2020.

Independentemente de terminologias, o ponto é que, na forma atual do capitalismo, mais importante (e mais lucrativo) do que atender às demandas das pessoas humanas é “vender previsões de seus comportamentos”, dentro e fora dos ambientes de trabalho.

A utilização desse tipo de *software* de monitoramento, por si só, já é abusiva^{28 29}. Além disso, há uma outra questão que torna a prática ainda mais absurda: a existência de vieses racistas nos algoritmos empregados^{30 31}. O programa *ExamSoft*, que será utilizado para fiscalizar candidatos prestando o *bar exam* (espécie de “exame da ordem dos advogados” dos Estados Unidos), não é capaz de analisar, adequadamente, a biometria facial de pessoas de pele negra³². Questionada por alunos preocupados com eventuais prejuízos decorrentes do enviesamento do programa, a resposta dada pela *ExamSoft* é de que eles deveriam manter uma fonte de luz clara em seus rostos, durante os dois dias de realização do exame³³. Como veremos com mais detalhe a seguir, novas tecnologias tornam possíveis práticas de vigilância mais diversificadas também no ambiente de trabalho, presencial ou remoto, o que, por sua vez, possibilita um monitoramento cada vez mais invasivo dos trabalhadores^{34 35 36}. Segundo Alexandra Mateescu e Aiha Nguyen³⁷, o monitoramento dos empregados tem se tornado paulatinamente interligado à coleta de dados pessoais, na medida em que ferramentas de monitoramento e vigilância têm coletado novos tipos de dados sobre trabalhadores, permitindo certo controle sobre atividades e até mesmo qualidades pessoais que há pouco tempo não era possível.

Isso está diretamente ligado ao fenômeno intitulado “capitalismo de vigilância”³⁸, “capitalismo digital”³⁹, ou “colonialismo de dados”⁴⁰. Independentemente de terminologias, o ponto é que, na forma atual do capitalismo, mais importante (e mais lucrativo) do que atender às demandas das pessoas humanas é “vender previsões de seus comportamentos”⁴¹, dentro e fora dos ambientes de trabalho.

²⁸ ANDREJEVIC & SELWYN, 2020.

²⁹ HARTZOG & SELINGER, 2018.

³⁰ NOBLE, 2018.

³¹ CARREIRA & CARVALHO, 2020.

³² SMUHA, 2020.

³³ JOHNSON, 2020.

³⁴ UCHOA-DE-OLIVEIRA, 2020.

³⁵ ABÍLIO, 2020.

³⁶ ZUBOFF, 2018.

³⁷ MATEESCU, NGUYEN, 2020.

³⁸ ZUBOFF, 2018.

³⁹ SADOWSKI, 2020.

⁴⁰ COULDRY; MEJIAS, 2019.

⁴¹ ZUBOFF, 2019.

A professora Shoshana Zuboff, em artigo de 2019, pontuou:

Agora, os atuais detentores do capital de vigilância criaram uma quarta mercadoria fictícia, fruto da expropriação das experiências humanas reais, cujos corpos, pensamentos e sentimentos são tão intactos e inocentes quanto os campos e florestas que abundavam na natureza antes de sua absorção pelo mercado. De acordo com essa lógica, a experiência humana é mercantilizada pelo capitalismo de vigilância, para renascer como “comportamento”. Traduzidos em dados, estes assumem seu lugar na fila interminável que alimenta as máquinas concebidas para fazer previsões que se compram e se vendem.

Essa nova economia, produtora de dados e que destes se alimenta inescrupulosamente, impacta de maneira significativa o mundo do trabalho, uma vez que as relações laborais passam a serem formadas dentro deste espectro de dados, o qual passa a ilustrar mais uma face da hipossuficiência do trabalhador em relação ao seu patrão, marcada pelas engrenagens de vigilância, programadas também para garantir o assujeitamento daqueles mais vulneráveis. Isso significa dizer que, nesta nova conjuntura de mercado, a proteção do trabalhador (também um princípio-mor da justiça trabalhista brasileira), deve necessariamente englobar a proteção contra estes mecanismos de vigilância, a partir, por exemplo, da criação de normas reguladoras nítidas de proteção de dados pessoais dos trabalhadores vulneráveis.

2. VIGILÂNCIA E MONITORAMENTO NO AMBIENTE DE TRABALHO: A *DATAVEILLANCE* DO TRABALHO PRESENCIAL AO TRABALHO REMOTO

Ainda no contexto da pandemia, dada a necessidade do isolamento social para fins sanitários, as relações trabalhistas passaram a ser mediadas por aplicativos e softwares de todas as estirpes. Diversas atividades próprias do mundo do trabalho, como reuniões, conversas informais com parceiros de trabalho, confecção de aulas e seminários, atendimentos médico-sanitários, atividades de entregadores de bicicletas e outros meios de transporte, votações dos parlamentares nos congressos, foram afetadas pela pandemia de COVID-19, e estão sendo convertidas em dados. Aqui encontra-se uma alteração paradigmática, própria da Revolução 4.0: todo movimento, todo fluxo nos mais diversos e plurais ambientes de

Um ponto problemático é que as práticas de monitoramento das pessoas que trabalham acabam por revelar algumas camadas e formas distintas de discriminação, operando nas formas de disciplina, aumento das formas de exploração do trabalho e na redistribuição dos riscos e custos gerados pela crise sanitária.

trabalho, agora é convertido em dados. É justamente isso que caracteriza esta nova economia (a dos dados): a conversão de todos os fluxos da vida humana em dados, isto é, em informações capazes de serem capturadas, processadas, lidas e aplicadas para os mais diversos fins, sobretudo como forma contemporânea de vigilância dos comportamentos dos trabalhadores.

Um ponto problemático é que as práticas de monitoramento das pessoas que trabalham acabam por revelar algumas camadas e formas distintas de discriminação, operando nas formas de disciplina, aumento das formas de exploração do trabalho e na redistribuição dos riscos e custos gerados pela crise sanitária. Aiha Nguyen utiliza os termos do guia industrial de prevenção de infecções e práticas higiênicas do CDC estadunidense para contextualizar em quais áreas o uso das tecnologias de monitoramento se encontram⁴². Essas divisões são apresentadas em ordem decrescente de eficácia e importância: eliminação (remoção física do risco); substituição (substituição do risco); controles de engenharia (isolar as pessoas do risco); controles administrativos (mudanças de comportamento); equipamentos de proteção pessoal (EPIs).

Os dois primeiros níveis de prevenção normalmente são aplicados a práticas ou equipamentos da indústria que apresentem riscos desnecessários ou que podem ser substituídos por alternativas menos insalubres. No caso da presente crise sanitária, tais camadas de prevenção ainda são inviáveis no curto prazo. A única forma de remover completamente o risco de infecção no trabalho é a completa interrupção da atividade econômica⁴³, solução de pouca duração e cada vez mais inviável nas esferas econômica e política.

Dessa forma, ao menos em nível do funcionamento de empresas, restam as alternativas menos eficazes das últimas três camadas. Controles de engenharia são usos de tecnologia e estrutura para a redução dos riscos, entre eles: afastamento das áreas de trabalho, melhor filtração de ar, barreiras físicas entre pessoas que trabalham e fontes de infecção⁴⁴. São os mais efetivos, pois não exigem necessariamente mudanças de comportamento de quem trabalha, mas podem apresentar maior investimento imediato, pois exigem a

⁴² NGUYEN, 2020, p. 7.

⁴³ DECHSUPA et al, 202.

⁴⁴ US DEPARTMENT OF LABOR, 2020.

compra de equipamentos e reorganização da estrutura física e condições de trabalho⁴⁵. Também podemos notar que esses controles de engenharia exigem pouco ou quase nenhuma forma de vigilância ou monitoramento por parte do empregador.

O mesmo não pode ser dito das formas de controle administrativo. Mais abrangentes, podem se materializar na forma da alteração do tempo da jornada de trabalho, da possibilidade do trabalho remoto (“*home office*”, em termo brasileiro) por tempo indeterminado ou daqueles que apresentam sintomas, da criação de normas de distanciamento físico entre as pessoas que trabalham, instauração de normas de higiene (como lavar as mãos após contato e/ou proibir tocar em determinadas superfícies) e o treinamento no uso dos EPIs⁴⁶.

Os equipamentos de proteção individual apresentam a última e menos efetiva camada de proteção, ao utilizar máscaras, luvas e outros para tentar separar a pessoa dos riscos presentes no local de trabalho. Ambas últimas camadas de segurança apresentadas não somente se demonstram menos eficazes, mas também transferem o risco e a responsabilidade do uso diretamente para a pessoa que trabalha. A proteção oferecida pelos EPIs exige então o constante autocuidado daqueles que os usam, mais vulneráveis ao erro humano, às reais condições do uso responsável desses EPIs, do desgaste físico e mental que podem ocasionar em um descuido⁴⁷. Essas inerentes limitações da eficácia das EPIs fazem mais do que transferir o risco e responsabilidade para aqueles que trabalham: parecem justificar a intensificação de monitoramento eletrônico exercida pelo empregador.

Outra preocupação é o uso da vigilância em conjunto com as normas de controle administrativo e o uso do EPIs. Ao criar normas de distanciamento, higiene no trabalho e uso de EPIs, o empregador transfere toda a responsabilidade para os hábitos individuais de seus trabalhadores. Com isso, não somente aumenta a carga mental e física necessária para desempenhar suas funções, mas também abre espaço para o uso do poder disciplinar do empregador, caso aquele que trabalhe seja descoberto descumprindo as normas de

⁴⁵ NGYUEN, 2020, p. 8.

⁴⁶ NGYUEN, 2020, p. 8.

⁴⁷ HEISLER; MISHORI, 2020.

segurança. Ou seja, além de eximir o empregador da responsabilidade, a transferência dos riscos opera de forma dupla para o trabalhador: cabe à ele se proteger da doença e aumentam as chances de ser suspenso ou demitido. Essas consequências ficam mais visíveis quanto mais precário é o trabalho, demonstrando como esse poder disciplinar opera de forma interseccional⁴⁸.

Práticas de monitoramento podem se apresentar de algumas formas, como já comentadas: o uso de rastreamento de contato em larga escala por ferramentas digitais, verificações da saúde das pessoas que trabalham de forma constante, possivelmente invasivas e eventualmente feitas sem um consentimento, ou o uso de monitoramento do distanciamento físico utilizando câmeras ou o uso de um aplicativo da empresa nos celulares pessoais dos empregados. A crise sanitária e o combate ao COVID-19 são justificativas para o crescimento dessas formas de vigilância, mas seus usos e consequências parecem ultrapassar esse objetivo, fornecendo a possibilidade do empregador monitorar interações entre empregados, em especial entre grupos minoritários, como pessoas de Cor, imigrantes e trabalhadores precarizados em geral⁴⁹.

A transição generalizada para o trabalho remoto em virtude da pandemia de COVID-19 também aumentou a incidência de práticas de vigilância digital nos lares dos trabalhadores, de modo que muitos profissionais que atualmente estão trabalhando em suas casas estão agora sujeitos a uma vigilância maior do que a anteriormente experimentada⁵⁰. As vendas de ferramentas de vigilância do “local de trabalho” (neste caso, remoto) aumentaram desde o início da pandemia, levantando discussões sobre como os empregadores monitoram o desempenho dos funcionários e as implicações desse monitoramento em sua privacidade (NEWLANDS et al., 2020).

Fato é que os empregadores sempre buscaram maneiras de monitorar seus funcionários. Com o aumento do número de trabalhadores em *home office*, novas tecnologias de vigilância digital surgiram ou foram adaptadas, a fim de possibilitar aos empregadores maior controle sobre as atividades exercidas remotamente⁵¹. Hoje é possível

⁴⁸ COLLINS, BILGE, 2016, p. 9

⁴⁹ NGYUEN, 2020, p. 16

⁵⁰ NEWLANDS et al., 2020

⁵¹ AISTON; BARNET, 2020

No âmbito da proteção dos dados pessoais aplicados à realidade do trabalho, é importante ter em mente que os trabalhadores são, ao fim e ao cabo, os titulares dos dados pessoais, enquanto os patrões são os operadores ou controladores, os tratadores e tomadores de decisão a respeito dos dados.

que os empregadores tenham acesso a imagens obtidas através de *webcams*, rastreiem os movimentos de *mouse* e teclado e até mesmo reconheçam as emoções dos empregados. São as funções de *softwares* tais como *StaffCop*, *Teramind*, *Hubstaff*, *CleverControl* e *Time Doctor*, que realizam o rastreamento de atividades em tempo real, tirando capturas de tela dos computadores dos trabalhadores em intervalos regulares e, em alguns casos, podem ser instaladas sem o conhecimento dos funcionários⁵².

Um caso que merece destaque é o da PwC, uma das maiores empresas de finanças e contabilidade do mundo, que, em junho de 2020, passou a utilizar um *software* de monitoramento baseado no reconhecimento facial de seus empregados. A função do programa é, mediante uso constante de *webcam*, registrar todos os momentos em que o empregado se ausentar da frente do computador e solicitar explicações por escrito para cada ausência registrada⁵³. Infelizmente, esse não é um caso isolado: além do programa da PwC, outros *softwares* com funções semelhantes encontram-se à venda no mercado, como *Sneek* e *InterGuard*⁵⁴. Além da clara invasão à privacidade dos trabalhadores, o uso desse tipo de sistema tem levantado discussões sobre a sua própria remuneração, já que determinados empregadores têm descontado intervalos de ausência ou distração da frente do computador por considerar que, na prática, são horas “não trabalhadas”⁵⁵.

No âmbito da proteção dos dados pessoais aplicados à realidade do trabalho, é importante ter em mente que os trabalhadores são, ao fim e ao cabo, os titulares dos dados pessoais⁵⁶, enquanto os patrões são os operadores ou controladores, os tratadores e tomadores de decisão a respeito dos dados⁵⁷. Ou seja, na qualidade de agentes de tratamento⁵⁸, as empresas captadoras e processadoras de dados dos trabalhadores devem respeitar as disposições normativas trazidas pela Lei Geral de Proteção de Dados brasileira.

⁵² FINNEGAN, 2020

⁵³ WEBBER, 2020

⁵⁴ LAKER et al., 2020

⁵⁵ MATEESCU; NGUYEN, 2020

⁵⁶ Art. 5º, V, LGPD.

⁵⁷ Art. 5º, V e VII, LGPD.

⁵⁸ Art. 5º, IX, LGPD.

De forma exemplificativa, as empresas de entregas por aplicativos devem ser transparentes quanto aos dados coletados dos seus trabalhadores-entregadores, quanto ao uso dos dados de geolocalização, quanto às providências tomadas para o descarte seguro destes dados. Devem, ainda, comprovar a instituição de medidas cibernético-securitárias para a proteção das informações sobre os seus empregados, tanto referentes à rendimento, produtividade, escalas e estados de saúde.

A LGPD é um instrumento normativo nacional importante para a garantia destes direitos fundamentais, especialmente quando a regulação trabalhista não consegue lidar de maneira satisfatória com estas relações de vigilância, próprias desta nova economia. Ainda considerando a pandemia da COVID-19, não somente os empregadores, como também as plataformas de videoconferência, de planejamento de rotinas e atividades, dentre muitas outras estão recolhendo dados privados, sensíveis ou não⁵⁹, dos trabalhadores e usuários. Portanto, percebe-se que os desafios são imensos no que tange à vigilância, monitoramento, tratamento e processamento dos dados, o que exige ações mais assertivas de regulação forte e bem definida.

Em tempos de configurações capitalistas de vigilância objetivando o controle e a docilização dos corpos, a modulação de comportamento, a padronização de condutas, o espelhamento de atividades, a mimetização de hábitos, é fundamental definir normativas para restringir tratamentos violadores de direitos (que vão desde tratamento discriminatórios à comercialização dos dados pessoais) por parte dos empregadores e das empresas cujo objeto é nada mais que fornecer aparatos de vigilância baseados em dados⁶⁰.

Faz-se urgente e primordial uma regulação pública, e não privada, da exploração econômica dos dados pessoais, especificamente dos trabalhadores, o que também implica tratar a proteção de dados pessoais como um direito público de ordem coletiva e não meramente individual⁶¹ (ainda que o aspecto individual seja importante), uma vez que o enfrentamento dos poderes concentrados,

⁵⁹ Art. 5º, I e II, LGPD.

⁶⁰ NOCCHI, 2020

⁶¹ NOCCHI, 2020

Tratar do tema do controle e vigilância dos dados pessoais, com ênfase nas relações de trabalho remoto, é fundamental, seja pela necessidade de controlar essas informações sensíveis, seja pela necessidade de publicizar este tema para que os trabalhadores tenham ciência dos seus direitos, ou, ainda, pela pouca produção existente neste campo aqui no Brasil.

oligopolistas do capital sobre os diversos grupos vulnerabilizados, exige formações socioeconômicas de ordem coletiva, plural, radicalmente democrática e profundamente pública.

CONSIDERAÇÕES FINAIS

Tratar do tema do controle e vigilância dos dados pessoais, com ênfase nas relações de trabalho remoto, é fundamental, seja pela necessidade de controlar essas informações sensíveis, seja pela necessidade de publicizar este tema para que os trabalhadores tenham ciência dos seus direitos, ou, ainda, pela pouca produção existente neste campo aqui no Brasil.

Inúmeros exemplos abordados explicitaram as práticas de vigilância no contexto da pandemia de COVID-19, quando se abordou os inúmeros usos desproporcionais das novas tecnologias por empresas e pelos Estados. Sintomáticos são os casos de vigilância por geolocalização, *contact tracing*, monitoramento do fluxo de pessoas nas ruas etc. Ainda mais impressionante é o caso do Departamento de Segurança Jurídica dos Estados Unidos, preocupados com a perda de eficácia dos sistemas de vigilância em virtude do uso de máscaras, o que já foi superado.

Ao abordar o tema, ainda foram trazidas discussões a respeito dos impactos das novas tecnologias no campo educacional, dos novos dados que passaram a ser coletados com a emergência global dos trabalhos remotos, e dos algoritmos racistas. Com relação à vigilância do trabalho remoto em tempos pandêmicos, especificamente, identificamos as múltiplas camadas de discriminação sofridas pelos trabalhadores, os modos de engenharia para redução dos riscos, o uso dos controles administrativos, incluindo alterações na duração da jornada de trabalho e o recrudescimento do home office. Ademais, problematizamos o uso de EPIs em relação aos demais tipos de vigilância, uma vez que estes permitem aos empregadores transferirem a responsabilidade do cuidado para os trabalhadores.

Exemplos de práticas de vigilância do trabalho também foram apontados, o que inclui desde um rastreamento em larga escala, inclusive com o uso de câmeras, nem sempre utilizadas apenas para fins

legais, como o monitoramento da interação entre os empregados; o rastreamento de movimentos dos mouses e das emoções, mesmo sem o consentimento dos funcionários; e os softwares que permitem identificar quando os trabalhadores se levantam da cadeira, o que tem levado certas corporações a descontarem dos salários esses momentos de não trabalho durante a jornada. Percebe-se, portanto, que a privacidade é violada de múltiplas formas e pouco tem se abordado este problema..

Por fim, realizadas essas breves considerações sobre o uso de novas tecnologias de vigilância para o combate à COVID-19, é preciso, uma vez mais, reconhecer criticamente a sua importância. Vivemos em uma situação excepcional que, por sua vez, demanda e seguirá demandando certas medidas excepcionais. Mas mesmo estas devem sempre ser restritas à sua finalidade, adequadas, necessárias, transparentes e seguras; devem ser, ainda, temporárias, de modo a mitigar a possibilidade de uso secundário de dados para fins que não o enfrentamento ao coronavírus. Somente com a observância desses critérios é que poderemos lidar com e superar essa crise de maneira adequada, preservando-se ainda nossos direitos e garantias fundamentais. Não obstante, o que temos identificado, infelizmente, são apenas as múltiplas formas de violação das subjetividades dos trabalhadores. Até quando será assim?

REFERÊNCIAS

ABILIO, Ludmila Costhek. Uberização: a era do trabalhador just-in-time?. *Estud. av.*, São Paulo, v. 34, n. 98, p. 111-126, 2020. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142020000100111&lng=en&nrm=iso. Acesso em: 26 fev. 2021.

AISTON, Joe; BARNETT, Alexander. Remote work and the risks of employee surveillance. *Workplace Insight*. Disponível em: <https://workplaceinsight.net/remote-work-and-the-risks-of-employee-surveillance/>. Acesso em: 28 fev. 2021.

ANDREJEVIC, Mark; SELWYN, Neil. Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, v. 45, n. 2, p. 115-128, 2020.. BBC. "Coronavirus: Russia uses facial recognition to tackle Covid-19". Disponível em: <https://www.bbc.com/news/av/world-europe-52157131/coronavirus-russia-uses-facial-recognition-to-tackle-covid-19>. Acesso em: 20 set. 2020.

BONG, C.L. et al. *The COVID-19 Pandemic: Effects on Low and Middle-Income Countries*. *Anesth Analg*. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/32243287/>. Acesso em: 26 fev. 2021.

BORAK, Masha. "Beijing considers using facial recognition to fight a new Covid-19 outbreak", 2020a. Disponível em: <https://www.scmp.com/abacus/tech/article/3089378/beijing-considers-using-facial-recognition-fight-new-covid-19-outbreak>. Acesso em: 20 set. 2020.

BORAK, Masha. "Wearing a mask won't stop facial recognition anymore." 24 de fevereiro de 2020b. Disponível em: <https://www.scmp.com/abacus/tech/article/3052014/wearing-mask-wont-stop-facial-recognition-anymore>. Acesso em: 20 set. 2020.

CARRERA, Fernanda; CARVALHO, Denise. Algoritmos racistas: a hiper-ritualização da solidão da mulher negra em bancos de imagens digitais. *Galáxia* (São Paulo), n. 43, p. 99-114, 2020.

COLLINS, Patricia Hill; BILGE, Sirma. *Intersectionality*. Cambridge: Polity Press, 2016.

COULDRY, Nick.; MEJIAS, Ulisses. A. *The costs of connection: how data is colonizing human life and appropriating it for capitalism*. Stanford, California: Stanford University Press, 2019.

DECHSUPA, Sinsuda et al. "Positive impact of lockdown on COVID-19 outbreak in Thailand." *Travel medicine and infectious disease*, vol. 36, 2020. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/32569811/>. Acesso em: 26 fev. 2021.

DO CARMO BARRIGA, Antónia et al. The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance?. *Social Sciences & Humanities Open*, v. 2, n. 1, 2020.

FEATHERS, Todd; ROSE, Janus. “Students Are Rebelling Against Eye-Tracking Exam Surveillance Tools”. 24 de setembro de 2020. Disponível em: <https://www.vice.com/en/article/n7wxvd/students-are-rebelling-against-eye-tracking-exam-surveillance-tools>. Acesso em: 20 set. 2020.

FERRETTI, L. et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, v. 368, n. , p.8, 8 maio 2020.

FINNEGAN, Matthew. The New Normal: When work-from-home means the boss is watching. Computerworld. Disponível em: <https://www.computerworld.com/article/3586616/the-new-normal-when-work-from-home-means-the-boss-is-watching.html>. Acesso em: 28 fev. 2021.

FONSECA, J. J. S. *Metodologia da pesquisa científica*. Fortaleza: UEC, 2002. Apostila.

GIELOW, Igor. Tecnologia usada no combate à pandemia de coronavírus ameaça privacidade”. Folha de São Paulo. Disponível em: <https://folha.com/oguv5840>. Acesso em: 20 set. 2020.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2002.

HARTZOG, W., & SELINGER, E. (2018). Facial recognition is the perfect tool for oppression. *Medium*.

HEISLER, Michele and MISHORI, Ranit. 2020. “Governors Must Protect the Health Workers Who Protect Us.” Bloomberg Quint, June 26. Retrieved from <https://www.bloombergquint.com/gadfly/states-must-protect-health-workers-amid-the-coronavirus-crisis>.

HUANG, C. et al. *Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China*. *Lancet*, v. 395, 2020. DOI:10.1016/S0140-6736(20)30183-5.

HVISTENDAHL, Mara; BIDDLE, Sam. Homeland Security Worries Covid-19 Masks Are Breaking Facial Recognition, Leaked Document Shows. 16 de julho de 2020. Disponível em: <https://theintercept.com/2020/07/16/face-masks-facial-recognition-dhs-blueleaks/>. Acesso em: 20 set. 2020.

JOHNSON, Khari. “ExamSoft’s remote bar exam sparks privacy and facial recognition concerns”. 29 de setembro de 2020. Disponível em: <https://venturebeat.com/2020/09/29/examssofts-remote-bar-exam-sparks-privacy-and-facial-recognition-concerns/>. Acesso em: 30 set. 2020.

JOINT CIVIL SOCIETY STATEMENT. “Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights.” 2 de abril de 2020. Disponível em: <https://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf>. Acesso em: 20 set. 2020.

LAKER, Ben et al. How to Monitor Remote Workers — Ethically. *MIT Sloan Management Review*. Disponível em: <https://sloanreview.mit.edu/article/how-to-monitor-remote-workers-ethically/>. Acesso em: 28 fev. 2021.

LAU, Hien et al. The positive impact of lockdown in Wuhan on containing the COVID-19 outbreak in China. *Journal of travel medicine*, v. 27, n. 3, 2020.

LIMA, Jacob Carlos; OLIVEIRA, Daniela Ribeiro de. Trabalhadores digitais: as novas ocupações no trabalho informacional. *Soc. estado.*, Brasília, v. 32, n. 1, p. 115-143, Apr. 2017. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-69922017000100115&lng=en&nrm=iso. Acesso em: 26 fev. 2021. <https://doi.org/10.1590/s0102-69922017.3201006>.

MATEESCU, Alexandra; NGUYEN, Aiha. Explainer: Workplace Monitoring & Surveillance. Data & Society, 2020. Disponível em: <https://datasociety.net/library/explainer-workplace-monitoring-surveillance/>. Acesso em: 26 fev. 2021.

MCCLELLAN, Elizabeth. Facial Recognition Technology: Balancing the Benefits and Concerns. *Journal of Business & Technology Law*, v. 15, n. 2, p. 363, 2020

MUSIANI, Francesca, et al.. The Russian ‘Sovereign Internet’ Facing Covid-19. Institute of Network Cultures. *Stefania Milan, Emiliano Treré & Silvia Masiero (eds.) COVID-19 from the Margins. Pandemic Invisibilities, Policies and Resistance in the Datafied Society*, pp. 174-178, 2021, Theory on Demand #40, 978-94-92302-72-4. (hal-03128294).

NEWLANDS, Gemma; LUTZ, Christoph; TAMÒ-LARRIEUX, Aurelia; et al. Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, v. 7, n. 2, p. 2053951720976680, 2020.

NGUYEN, Aiha. New Digital Infrastructures of Workplace Health and Safety. Centre for Media, Technology and Democracy, 2020. Disponível em: <https://www.mediatechdemocracy.com/work/new-digital-infrastructures-of-workplace-health-and-safety>. Acesso em: 26 fev. 2021.

NICOLA, M. et al. The socio-economic implications of the coronavirus pandemic (COVID-19): A review. *Int J Surg*,

v. 78, 2020. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/32305533/>. Acesso em: 25 fev. 2021.

NOBLE, S. U. *Algorithms of Oppression: how search engines reinforce racism*. NYU Press, 2018.

NOCCHI, Paula. O Direito Coletivo Do Trabalho No Capitalismo De Vigilância. *Justificando*, [s.l.], 14 maio 2021. Disponível em: <https://www.justificando.com/author/paula-nocchi/>. Acesso em: 24 nov. 2021.

OLIVEIRA, S. R. *Sorria, você está sendo filmado! Repensando Direitos na Era do Reconhecimento Facial*. São Paulo: Thomson Reuters Brasil, 2021.

QIU, Y.; CHEN, X.; SHI, W. Impacts of social and economic factors on the transmission of coronavirus disease 2019 (COVID-19) in China. *BMJ*, medRxiv 2020.03.13.20035238. DOI:10.1101/2020.03.13.20035238

RFE/RL. “COVID-19: Moscow Introduces ‘Digital Passes’ As Officials Warn Of Infection Spike; WHO Warns Belarus Must Do More”. Disponível em: <https://www.rferl.org/a/covid-19--rusia-belarus--iran-digital-permits-who-businesses-reopen/30547557.html>. Acesso em: 20 set. 2020.

SANTOS JUNIOR, Verissimo Barros dos; MONTEIRO, Jean Carlos da Silva. Educação e covid-19: as tecnologias digitais mediando a aprendizagem em tempos de pandemia. *Revista Encantar-Educação, Cultura e Sociedade*, v. 2, p. 01-15, 2020.

SADOWSKI, Jonathan. *Too smart: how digital capitalism is extracting data, controlling our lives, and taking over the world*. Cambridge, Massachusetts: MIT Press, 2020.

SENHORAS, Eloi Martins. Coronavírus e educação: análise dos impactos assimétricos. *Boletim de Conjuntura (BOCA)*, v. 2, n. 5, p. 128-136, 2020.

SMUHA, Nathalie A., *Trustworthy Artificial Intelligence in Education: Pitfalls and Pathways*, 2020. Disponível em: <https://ssrn.com/abstract=3742421>. Acesso em: 25 fev. 2021.

SWAUGER, Shea. Our bodies encoded: Algorithmic test proctoring in higher education. *Critical Digital Pedagogy*, 2020.

TRANSNITRA NEWS. “Moldova: Transnistria uses facial recognition to identify quarantine violators.” Disponível em: <https://privacyinternational.org/examples/3629/moldova-transnistria-uses-facial-recognition-identify-quarantine-violators>. Acesso em: 20 set. 2020.

UCHOA-DE-OLIVEIRA, Flávia Manuella. Saúde do trabalhador e o aprofundamento da uberização do trabalho em tempos

de pandemia. *Rev. bras. saúde ocup.*, São Paulo, v. 45, n. 22, 2020. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0303-76572020000101501&lng=en&nrm=iso. Acesso em: 25 fev. 2021.

US Department of Labor and US Department of Health & Human Services. 2020. Guidance on Preparing Workplaces for COVID-19. Disponível em: <https://www.osha.gov/sites/default/files/publications/OSHA3990.pdf>. Acesso em: 25 fev. 2021.

WEBBER, Ashleigh. PwC facial recognition tool criticised for home working privacy invasion. Disponível em: <https://www.personneltoday.com/hr/pwc-facial-recognition-tool-criticised-for-home-working-privacy-invasion/>. Acesso em: 28 fev. 2021.

WORLD HEALTH ORGANIZATION. Contact tracing in the context of COVID-19: interim guidance. World Health Organization; 2020. Disponível em: <https://apps.who.int/iris/handle/10665/332049>. Acesso em: 21 fev. 2021.

ZUBOFF, Shoshana. *Big other: capitalismo de vigilância e perspectivas para uma civilização de informação*. In: BRUNO, F. et al. (Org.) *Tecnopolíticas da vigilância: Perspectivas da margem*. São Paulo: Boitempo, 2018.

ZUBOFF, Shoshana. Um capitalismo de vigilância. *Le Monde Diplomatique*, [s.l.], 3 jan. 2019. Disponível em: <https://diplomatique.org.br/um-capitalismo-de-vigilancia/>. Acesso em: 26 fev. 2021.

QUALIFICAÇÃO

Samuel Rodrigues de Oliveira é doutorando em Teoria do Estado e Direito Constitucional pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Mestre em Direito e Inovação e graduado em Direito pela Universidade Federal de Juiz de Fora (UFJF). Especialista em Relações Internacionais.

Marcos Aragão Couto Oliveira é doutorando em Direito Constitucional e Teoria do Estado. Mestrado em Direito Constitucional e Teoria do Estado. Especialista em Direito e Processo do Trabalho. Membro do grupo de estudos Gênero, Democracia e Direito do NDH PUC-Rio. Membro do grupo de estudos Trabalho no Século XXI - Trab21 - FND.

Dorival Fagundes Cotrim Junior é doutorando em Direito e em Saúde Coletiva. Mestre em Direito Constitucional e Teoria do Estado. Graduado em Ciências Jurídicas e Sociais.