Revista Direito em Debate

Revista do Departamento de Ciências Jurídicas e Sociais da Unijuí

Editora Unijuí – Ano XXX – n. 56 – jul./dez. 2021 – ISSN 2176-6622

COVID-19 E BIOPODER: Capitalismo de Vigilância, Estratégias de *E-Government* e Proteção de Dados

http://dx.doi.org/10.21527/2176-6622.2021.56.12053

Recebido em: 16/2/2021
Modificações solicitadas em: 5/4/2021
Aceito em: 19/4/2021

Raissa Arantes Tobbin

Autora correspondente. Universidade Cesumar. Av. Guedner, 1610 – Jardim Aclimação. Maringá/PR, Brasil. CEP 87050-900. http://lattes.cnpq.br/5997745021125050. https://orcid.org/0000-0002-3655-8407. tobbinraissa@hotmail.com

Valéria Silva Galdino Cardin

Universidade Estadual de Maringá; Instituto Cesumar de Ciência, Tecnologia e Inovação (Iceti). Brasil.

RESUMO

O presente trabalho tem por objetivo analisar as estratégias de *e-government* no contexto da pandemia da Covid-19, sob a perspectiva do capitalismo de vigilância de Zuboff e das biopolíticas em Foucault, especificamente em sede da narrativa de vigilância como forma de bem-estar e da necessidade de proteção dos dados pessoais do cidadão, tendo em vista a possibilidade de compartilhamento e utilização indevida pelo Estado e por empresas privadas. Para tanto, o presente artigo utilizou o método hipotético-dedutivo, fundamentado em pesquisa e revisão bibliográfica. Como resultado, verificou-se que a crise da saúde pública impôs aos governos a necessidade de utilização do ambiente virtual para a prestação de serviços e para a concretização de políticas públicas. Tais estratégias, contudo, se baseadas em biopolíticas e no exacerbado capitalismo pós-moderno, podem representar vigilância excessiva, prejudicando os direitos à privacidade e à autodeterminação informativa, essenciais para a proteção dos dados pessoais.

Palavras-chave: Autodeterminação informativa; biopolítica; direitos da personalidade; lei geral de proteção de dados.

COVID-19 AND BIOPOWER: SURVEILLANCE CAPITALISM, E-GOVERNMENT STRATEGIES AND DATA PROTECTION

ABSTRACT

This paper aims to analyze e-government strategies in the context of the Covid-19 pandemic from the perspective of surveillance capitalism of Zuboff and biopolitics of Foucault, specifically in view of the surveillance narrative as a way of well-being and the need for data personal protection on citizens, in view of the possibility of sharing and misuse by the State and private companies. For this, the present work used the hypothetical-deductive method, based on research and bibliographic review. As a result, it was found that the public health crisis imposed on governments around the world the need to use the virtual environment to provide services and implement public policies. However, such strategies, if based on biopolitics and exacerbated postmodern capitalism, may represent excessive vigilance for citizens, damaging their right to privacy and informational self-determination, essential for the protection of personal data.

Keywords: Informative self-determination; biopolitics; personality rights; general data protection law.

1 INTRODUÇÃO

Com a crise de saúde pública provocada pela pandemia da Covid-19, que teve início no final de 2019 e se alastrou ao longo do ano 2020, houve a adoção de medidas globais que determinaram o isolamento social, considerando a inexistência de cobertura de imunização contra o novo coronavírus. Assim, o sistema educacional, o mercado financeiro, o setor corporativo e o comércio foram obrigados a se adequar às perspectivas digitais, na tentativa de prevenir prejuízos e dar continuidade às atividades durante o período de crise.

Dessa forma, o objetivo do presente trabalho é analisar as estratégias de *e-government* adotadas por alguns governos, entre eles o Brasil, por ocasião da pandemia da Covid-19, com base na perspectiva das biopolíticas e do capitalismo de vigilância, que muito têm a lucrar com a coleta, a utilização e o compartilhamento de dados pessoais dos cidadãos no contexto atual. Para tanto, a presente pesquisa utilizou o método hipotético-dedutivo, fundamentado em pesquisa e revisão bibliográfica de obras, artigos de periódicos, notícias, legislação, doutrina e jurisprudência aplicáveis ao tema.

No primeiro tópico do desenvolvimento serão examinadas as medidas de *e-government* utilizadas ao redor do globo na tentativa de conter a disseminação do vírus e prever possíveis surtos da doença. No segundo, tais estratégias serão observadas com base no cenário do biopoder e das biopolíticas em Foucault (1987) e no capitalismo de vigilância (ZUBOFF, 2019), termo atualmente utilizado para designar ações do mercado econômico e tecnológico fundamentadas na monetização de dados pessoais.

No terceiro item abordar-se-á a problemática dessa vigilância excessiva e a necessidade de proteção de dados e, no quarto, o direito à privacidade na era do *Big Data* e o direito à autodeterminação informativa do usuário do ambiente digital, nos termos da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e do consentimento prévio para a utilização dos dados pessoais.

2 A PANDEMIA DA COVID-19 E A AMPLIAÇÃO DE ESTRATÉGIAS DE *E-GOVERNMET*

A pandemia da Covid-19 acelerou de forma exponencial o crescimento de estratégias de *e-government* e de medidas que tentassem conter a disseminação do vírus por meio de atividades realizadas na modalidade de virtual. Conforme apontam Almeida *et al*. (2020, p. 2.488), um esforço mundial vem sendo desenvolvido "para que as lacunas do conhecimento sobre a pandemia sejam respondidas rapidamente pela ciência e pela organização e prática nos serviços de saúde", a fim de que medidas "ágeis, oportunas e eficientes possam ser adotadas pelas autoridades sanitárias de cada país relacionadas à capacidade de diagnóstico, manejo clínico e reabilitação dos casos de Covid-19 e estratégias de prevenção".

Neste cenário, as inovações tecnológicas e suas funcionalidades foram amplamente utilizadas para realizar previsões e controlar possíveis surtos. Segundo Taddeo (2020), cerca de 60 países estão utilizando alguma forma de monitoramento ou sistema de rastreamento e esse número tende a aumentar à proporção que novas medidas para controlar o isolamento sejam desenvolvidas. A China, primeiro país a enfrentar o vírus, adotou rapidamente medidas para conter a disseminação, quais sejam: o "controle de trânsito; o uso de câmeras de medição de temperatura corporal; a utilização pela polícia de capacete de reconhecimento termal; o mapeamento epidemiológico; o monitoramento via *drones*"; a utilização de "*softwares* para reconhecimento facial e medida de temperatura; a checagem de dados telefônicos para verificar contato com infectados" (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 11).

As agências governamentais chinesas desenvolveram um sistema que atribui aos cidadãos um Código QR de mobilidade, que passa a funcionar quando o indivíduo se cadastra em uma plataforma e inclui seus dados pessoais, bem como a localização atual, locais que frequentou e possíveis sintomas da Covid-19 percebidos. Para alcançar a difusão global do código, o governo chinês fez parceria com as plataformas *Alipay* e *Wechat* e, diante da enorme quantidade de dados coletados, passou-se a questionar se estes diriam respeito apenas à saúde e à localização ou se incluiriam o tráfego virtual e o rastreio de compras (CARRASCO; RAMÍREZ, 2020, p. 209).

A Coreia do Sul investiu em testagem rápida e massiva da população, assim como em entrevistas, *tracking*, geolocalização, uso de algoritmos, imagens de câmeras de segurança e dados de compra com cartão de crédito para determinar locais de possíveis surtos (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 14). O aplicativo

Corona100m9 utiliza a localização GPS e informa ao usuário os locais que foram frequentados por pessoas infectadas, dentro do período de contágio. Também informa se o indivíduo viajou para locais onde casos da Covid-19 foram confirmados. A responsabilidade pelo aplicativo é de uma empresa de tecnologia que vem construindo um banco de informações públicas sobre a pandemia (CARRASCO; RAMÍREZ, 2020).

O governo de Cingapura desenvolveu o aplicativo TraceTogheter, que armazena quando e com quem cada usuário do aplicativo esteve a menos de um metro. Logo, se alguém apresenta sintomas, seus contatos recebem a notificação e a orientação para que fiquem em isolamento. Trata-se de uma detecção individualizada e as autoridades podem obter informações criptografadas em caso de risco; aplicativo semelhante também foi desenvolvido no Japão (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 14; CARRASCO; RAMÍREZ, 2020).

Israel alterou sua política de vigilância para que o Ministério de Saúde tivesse acesso a informações presente nos *smartphones* dos cidadãos durante a crise, prevendo políticas de geolocalização e *tracking*. A França e a Itália também utilizaram a inteligência artificial para combater o vírus e verificar o cumprimento do isolamento por meio do uso de dados pessoais constantes nos celulares de seus cidadãos (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 19).

O Ministério da Saúde da Espanha aprovou a Ordem SND 29/2020, que inclui uma série de estratégias de gestão ao Secretariado do Estado da Digitalização e Inteligência Artificial para o desenvolvimento, entre outros, do aplicativo DataCOVID19, para monitorar a população, a fim de conter o vírus (CARRASCO; RAMÍREZ, 2020, p. 208). No âmbito da União Europeia foi desenvolvido um aplicativo de geolocalização (o Pan-European Privacy-Preserving Proximity Tracing) para verificar o cumprimento do isolamento e, ao mesmo tempo, preservar os direitos e garantias individuais da população (CARRASCO; RAMÍREZ, 2020, p. 209).

As empresas de tecnologia também propuseram medidas e o desenvolvimento de sistemas com o intuito de conter a disseminação do vírus. As empresas *Google* e *Apple* formaram uma parceria para combater o vírus e desenvolveram uma iniciativa que começou no final do mês de maio de 2020 com telefones com sistemas *Android* e *iOS* e que armazena dados para informar possíveis focos e pessoas infectadas. De igual modo, ao redor do mundo foram desenvolvidos *chatbots* que simulam conversas para monitorar remotamente pacientes que tenham contraído a doença, de forma que as autoridades sejam avisadas se o indivíduo apresentar sintomas ou quadro de risco (CARRASCO; RAMÍREZ, 2020, p. 210-211).

Já a empresa de cibersegurança israelense NSO vem sendo acusada de manipulação e espionagem, por meio do uso de dados do aplicativo WhatsApp e de fortalecer regimes antidemocráticos, tendo em vista que ofereceu a alguns países um *software* para monitorar celulares e conter a disseminação do vírus (CELLAN-JONES, 2020; FREITAS; CAPIBERIBE; MONTENEGRO, 2020).

No Brasil, em 2020 a cidade de Recife utilizou sistemas de localização de celulares para coordenar e verificar o cumprimento do isolamento social, informando aos cidadãos que o tratamento dos dados é realizado de forma coletiva, com verificação por bairro, que permite a execução de medidas como "o envio de carros de som para a área, o envio de notificações por celular, além de outras ações de comunicação" (MODESTO; EHRHARDT JUNIOR, 2020, p. 153; G1 PE, 2020). Em abril de 2020 o governo federal editou a Medida Provisória (MP) 954, que previa o compartilhamento de dados de empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE), com o intuito de dar continuidade à Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad Contínua) durante a pandemia (FINKELSTEIN; FEDERIGHI; CHOW, 2020).

Em que pese a MP contemplasse o descarte dos dados pelo IBGE com o fim do estado de emergência e proibisse o compartilhamento com empresas privadas e demais órgãos públicos, em sede de julgamento da Ação Direta de Inconstitucionalidade (ADI) 6.387, o Supremo Tribunal Federal (STF) declarou inconstitucional a medida, posto que haveria "uma falta de explicação sobre a finalidade de compartilhamento de dados de clientes entre empresas de telecomunicações e o IBGE durante o período da pandemia", de modo que esta não teria definido de forma clara "como" e "para quê" seriam utilizados tais dados (FINKELSTEIN; FEDERIGHI; CHOW, 2020). Para estes autores (2020, p. 22), a decisão apontou para os riscos do surgimento de eventuais Estados de vigilância.

No âmbito interno também é possível destacar a utilização pelo governo de aplicativos e dispositivos de inteligência artificial para conter a pandemia e conceder benefícios aos brasileiros. É o caso do Auxílio Emergencial, o qual para ser recebido o indivíduo deveria baixar aplicativos (*Caixa Tem* e *Caixa – Auxílio Emergen-*

cial), realizar um cadastro *on-line* com seus dados pessoais e acompanhar a solicitação e o recebimento do auxílio pela via eletrônica (MAGALHÃES, 2021).

Neste contexto, conforme Medeiros *et al*. (2020, p. 2.490):

> Ao considerar que dados podem ser utilizados e compartilhados por diferentes pessoas e organizações simultaneamente, as questões principais a serem harmonizadas giram em torno da governança responsável dos dados baseada na transparência e empoderamento dos cidadãos para que haja confiança e estabelecimento de relacionamentos equilibrados e justos entre indivíduos e organizações.

Diante da necessidade de continuação de serviços essenciais e da concretização de políticas públicas, especialmente voltadas à área da saúde durante a crise, de acordo com Medeiros *et al*. recai sobre o "aparato governamental a responsabilidade de aprofundar medidas de *e-government* e adaptar suas comunicações e práticas para o ambiente virtual, em respeito às diferenças socioeconômicas vigentes". Tal inserção no ciberespaço, todavia, "é passível de exploração por uma miríade de atores capazes de operacionalizar as lógicas e peculiaridades do universo digital segundo agendas particulares" (MEDEIROS *et al*., 2020, p. 652).

Os processos de *e-government* capitalizam as peculiaridades do ciberespaço para a adoção de medidas pela administração pública com vistas a alcançar parcelas sociais conectadas, de modo a agilizar procedimentos administrativos, sendo facilitadores das relações entre o Estado e a sociedade (RUEDIGER, 2003), disponibilizando informações úteis à população e estimulando o exercício da cidadania por meio do princípio da publicidade (artigo 37, CF/88) (RAMPELOTTO; LÖBLER; VISENTINI, 2015).

Como observa Sampaio (2016), apesar da inovação e da gama de possibilidades de operacionalização da administração pública por meio de dispositivos de inteligência artificial, o *e-government* tende a ser excludente, uma vez que é necessário entender que grande parcela da população ainda não tem acesso aos meios tecnológicos ou desenvolveu habilidades de letramento digital. Desta forma, os governos procuram manter métodos e processos mistos, *on-line* e presenciais, com a finalidade de amenizar a exclusão do cidadão na esfera digital.

Tal contexto deve ser analisado principalmente em países subdesenvolvidos ou em desenvolvimento, como o Brasil, com altos níveis de desigualdade econômica, social, educacional, racial, de sexo, etc., de forma que apenas parte de sua população possui acesso às *benesses* da Internet e há também a questão da qualidade de rede, que afeta mesmo os que dispõem de conexão já estabelecida e ininterrupta.

Ao mesmo tempo que o isolamento social impulsiona a virtualização e a digitalização da vida social, também enseja o discurso político de enfrentamento à Covid-19. A necessidade de utilização do ciberespaço pela administração pública dá origem a desafios e vulnerabilidades cibernéticas, que podem afetar inclusive o combate ao vírus (MEDEIROS *et al*., 2020, p. 651; JUNG *et al*., 2020). Como pontuam Tobbin e Cardin (2020a), malgrado a potencialidade da expansão da virtualização das atividades cotidianas, é essencial investigar as ações que têm por objetivo o monitoramento remoto, o acesso à localização e aos rastros dos indivíduos no ambiente virtual, especialmente porque a pandemia acentuou os delineamentos do mercado lucrativo de monetização de dados pessoais (TOBBIN; CARDIN, 2020a).

É fundamental analisar tais ações diante da necessidade de proteção dos direitos da personalidade, entre eles o direito à privacidade e à autodeterminação informativa, tendo em vista a possibilidade de vigilância excessiva e da utilização e do compartilhamento indevido de dados que possam prejudicar os direitos do cidadão, que cada vez mais necessita utilizar dispositivos e aplicativos de inteligência artificial para ter acesso à Internet e a informações sobre cuidados com a saúde, atuar no mercado de trabalho e financeiro, continuar seus estudos e receber benefícios e serviços por parte do Estado, de forma que a própria cidadania passa a ser, gradativamente, exercida pela via digital.

3 CAPITALISMO DE VIGILÂNCIA E BIOPOLÍTICAS: DA VIGILÂNCIA EXCESSIVA E DA NECESSIDADE DE PROTEÇÃO DE DADOS

Diante do crescimento do *e-government* em razão da pandemia, aos governos foi possibilitada a atuação de forma mais presente no ambiente digital por meio da concessão de benefícios, serviços e aplicativos com o escopo de conter a propagação do coronavírus e de manutenção da vida social. As estratégias de mo-

nitoramento remoto reduziram o número de pessoas em hospitais por meio da avaliação tecnológica assistida de sinais vitais, frequência de pulso e respiratória, pressão arterial e temperatura corporal (GERKE *et al*., 2020), revelando-se fundamental analisar tais medidas com base nos conceitos de biopoder e do capitalismo hodierno de vigilância.

Para Foucault (2013), o crescimento do capitalismo deu origem à modalidade específica "do poder disciplinar, cujas fórmulas gerais, cujos processos de submissão das forças e dos corpos, cuja 'anatomia política', podem ser aplicados através de regimes políticos, de aparelhos ou de instituições muito diversas". Desta forma, segundo Fachini e Ferrer (2019, p. 230), a biopolítica objetiva "gerir e garantir um bem-estar social, controlar a segurança do território e da população, enquanto o biopoder cuida e garante a permanência da espécie". Por meio de mecanismos de vigilância ou monitoramento é possível controlar "as taxas de natalidade e de mortalidade em um determinado Estado, para assegurar a manutenção da vida" (FACHINI; FERRER, 2019, p. 230). Este cenário, para Foucault, envolveria uma "série de vigilância, controle, olhares diversos que permitem descobrir, antes mesmo de o ladrão roubar e se ele vai roubar" (FOUCAULT, 2015, p. 7).

Na maioria das vezes as estratégias de vigilância estatal têm por intuito o controle social. A biopolítica manipula a vida cotidiana e o mundo econômico, por meio de instituições públicas ou empresas privadas cujo foco é o desempenho do indivíduo, com objetivo de gerar lucro (FACHINI; FERRER, 2019). Basta verificar que as tecnologias vestíveis, também chamadas de *wearables*, que podem ser relógios, pulseiras, roupas e tecidos inteligentes, objetivam exatamente monitorar o desempenho corporal e diário do indivíduo com base na sua saúde, produtividade e rentabilidade. Segundo Foucault (2013, p. 116), é dócil "o corpo que pode ser submetido, que pode ser utilizado, que pode ser transformado e aperfeiçoado". Ainda, para o autor,

> em qualquer sociedade, o corpo é alvo de poderes muito estritos, que lhe impõem condicionalismos, interdições ou obrigações. No entanto, há várias coisas novas nessas tecnologias. Em primeiro lugar, a escala do controlo: não se trata de cuidar do corpo, em massa, por atacado, como se fosse uma unidade indissociável, mas de o trabalhar em pormenor; trata-se de exercer sobre ele uma coerção subtil, de assegurar controlo ao próprio nível da mecânica – movimentos, gestos, atitudes, rapidez: poder infinitesimal sobre o corpo ativo. Segundo, o objeto do controlo: já não os elementos significantes do comportamento ou a linguagem do corpo, mas a economia, a eficácia dos movimentos, a sua organização interna; a coerção incide mais nas forças do que nos signos; a única cerimónia que importa realmente é a do exercício. Por último, a modalidade: implica uma coerção ininterrupta, constante, que vela mais pelos processos de atividade do que pelo seu resultado, e exerce-se segundo uma codificação que controla o mais apertadamente possível o tempo, o espaço e os movimentos. Estes métodos que permitem o controlo minucioso das operações do corpo, que asseguram a sujeição constante das suas forças e que lhes impõem uma relação de docilidade, podem ser designados por "disciplinas" (FOUCAULT, 2013, p. 117).

A vigilância, discretamente, faz com que as pessoas que estão sendo vigiadas sequer saibam que são manipuladas (FACHINI; FERRER, 2019), o que pode se dar, no mundo atual, por meio da coleta, mediante a utilização, o compartilhamento de dados e o monitoramento remoto, sob a alegação de maior segurança e tentativa de conter epidemias e crises sanitárias. Os estudos sobre biopoder e biopolíticas ganharam novos delineamentos diante da crise sanitária provocada pela Covid-19 e a pandemia, segundo Freitas, Capiberibe e Montenegro

> encontrou um nicho interessante, despertando o desejo – não necessariamente consciente – de maior controle sobre os nossos corpos, seja por quem for, já que esse controle vem sendo alardeado como forma de salvação, como a maneira existente de nos protegermos do maior medo de todos: o medo da morte. O uso do medo por campanhas políticas, especialmente utilizando as mídias sociais, já é conhecido (2020, p. 195).

Para que os dados possam ser utilizados, conforme Freitas, Capiberibe e Montenegro (2020, p. 196), "cria-se um imaginário com representações que apontam para a ideia de que os dados são elementos neutros, descontextualizados temporal, política e historicamente". A narrativa forjada é a de que "toda e qualquer apropriação e uso desses dados pessoais – seja por governos ou por outros atores – não poderão trazer malefícios, mas, ao contrário, serão fundamentais à manutenção da ordem e do bem-estar público" (FREITAS; CAPIBERIBE; MONTENEGRO, 2020, p. 196).

Em sua faceta tecnológica, o biopoder "seduz e conquista o indivíduo por meio de mecanismos discretos que agem diretamente na vida em sociedade", garantindo "o bem-estar social, com uma vigilância tecnológica que torna o indivíduo submisso à tecnologia" (FACHINI; FERRER, 2019, p. 227). As informações coletadas por estes dispositivos de inteligência artificial objetivam compor bancos de dados e perfis comportamentais, que buscam "antecipar preferências, tendências, escolhas e traços psíquicos de indivíduos ou grupos" (FACHINI; FERRER, 2019, p. 227-228) para fins de consumo e controle social (BRUNO, 2006). É o que se convencionou denominar de publicidade comportamental, que é a publicidade direcionada com base na experiência virtual do usuário, que em troca do acesso aos serviços e funcionalidades da rede acaba cedendo seus dados pessoais, o principal ativo do mercado tecnológico atual (TOBBIN; CARDIN, 2020b).

O capitalismo de vigilância, expressão que se tornou popular atualmente por meio dos estudos da norte-americana Shoshana Zuboff (2019) e que explica o fenômeno da monetização dos dados pessoais pelo mercado tecnológico e financeiro, fundamenta-se, para Freitas, Capiberibe e Montenegro (2020, p. 195), "na extração e apropriação de dados pessoais. Empresas de tecnologia, as mais beneficiadas por esse contexto, criam parcerias com governos", que passam a utilizar e depender do fluxo de dados gerenciado pelas empresas de tecnologia (CARDIN; PAULICHI, 2020, p. 235).

Em 2015, a empresa Uber ofereceu à cidade de Boston o acesso ao histórico de dados sobre as viagens realizadas pelo aplicativo na localidade para fins de planejamento urbano e melhoria do tráfego. Já Toronto, no Canadá, forneceu dados de seus cidadãos para a empresa *Sidewalk Labs*, ligada à *Google*, que tem por objetivo criar uma *smart city*, com a utilização de fibra ótica (MOROZOV, 2018; FREITAS; CAPIBERIBE; MONTENEGRO, 2020, p. 196).

Conforme Sousa e Silva (2020, p. 5), os dados são atualmente o principal insumo da economia global baseada na tecnologia, posto que cada vez mais são "processados e economicamente valorados" e, ao se converterem em informação, permitem "facilitar o intercâmbio e maximizar a qualidade nas empresas", uma vez que, diariamente, "os indivíduos vivenciam um processo de produção de dados e de informações que podem ser interpretados e comunicados".

Conforme analisa Monteiro (2018, p. 142),

> existem modelos de negócios de alguns provedores de serviços que dependem da monetização de dados de seus usuários. Pois, a receita dessas empresas provém da publicidade que ofertam pelas suas plataformas, propagandas ligadas a analisar o comportamento do usuário, então, a coleta de dados é a sobrevivência dessas empresas. Existem também as empresas que lucram com a publicidade *on-line* e com os chamados "serviços de dados" ou "data brokers", que coletam, analisam e compartilham as informações. Muitas nem têm relação direta com os consumidores cujos dados são coletados, somente fornecem serviços a outras empresas, incluindo a comercialização desses dados.

A tendência é que cada vez mais governos e Estados dependam de empresas de tecnologia para a atuação da administração pública e para a efetivação de políticas públicas. Tal cenário é muito benéfico para o desenvolvimento e o progresso social, contudo pode atingir certos direitos da personalidade do cidadão e evidencia a imprescindibilidade de proteção de dados pessoais contra intromissões arbitrárias e moralmente desmotivadas.

Dessa forma, surge a necessidade de controlar a circulação destes dados e que as instituições "estabeleçam seus modelos de governança para o tratamento" de dados, buscando "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (SOUSA; SILVA, 2020, p. 2). Explicam Modesto e Ehrhardt Junior (2020, p. 145) que os dados pessoais se relacionam com a pessoa identificada ou identificável, quais sejam: "o nome, o CPF, o endereço, os dados genéticos, o histórico médico, o Internet Protocol (IP) e os dados de localização", que são "vinculados, direta ou indiretamente, a determinado indivíduo, os quais revelam algo sobre ele". Logo, todos os dados coletados passam a ser importantes para esse cenário de monetização, por mais que tais práticas possam parecer inofensivas, especialmente para o cidadão comum, que aparentemente não tem motivos para pensar que estaria sendo vigiado pelo Estado ou que obtivesse informações privilegiadas e passíveis de interesse estatal ou empresarial.

Conforme Estrada (2016, p. 43), a Internet das Coisas possibilita a coleta de informações acerca do local onde o indivíduo andou na rua, estacionou o seu carro e fez compras por meio dos dados de seu cartão de crédito. À medida que são recolhidos tais elementos, afloram questões e preocupações quanto à discriminação, exclusão, criação de perfis, vigilância e controle, criando inquietude entre inovação tecnológica e direito à privacidade.

Nos últimos anos casos internacionais como o do vazamento de informações e esquema de vigilância populacional global perpetrado pela NSA norte-americana no caso Eduard Snowden e da compra de dados pessoais dos usuários da rede social *Facebook*, atingindo cerca de 87 milhões de usuários, que não consentiram com esse compartilhamento, pela empresa de consultoria *Cambridge Analytica*, contratada pelo grupo que promoveu o Brexit e, posteriormente, a campanha presidencial de Donald Trump nas eleições americanas de 2016, demonstraram que a coleta, o tratamento e a amplitude da utilização de dados pessoais ainda é muito distante da compreensão do cidadão comum que utiliza redes sociais, *smartphones*, dispositivos de inteligência e aplicativos fundamentados em algoritmos e no *learning machine* (FORNASIER; BECK, 2020; XAVIER *et al*., 2020; TOBBIN; CARDIN, 2020b).

De acordo com Fornasier e Beck, por mais que estes dados possam tecer uma narrativa comportamental de quem é cada indivíduo, esta não pode ser encarada como verossímil, uma vez que "indivíduos serão sempre mais do que apenas métricas; conjuntos de indicadores transformados em estatística e logo permitindo que algumas conclusões sejam inferidas" (FORNASIER; BECK, 2020, p. 189). Tal fala evidencia a problemática da discriminação algorítmica e de sistemas de inteligência artificial fundamentados em vieses preconceituosos e discriminatórios.

No entender de Queiroz, Teixeira Junior e Knoerr,

> é certo que a imensa maioria desses serviços de controle e vigilância, seja através dos programas de governo ou não, são exercidos por empresas privadas que prestam serviços aos órgãos públicos. Poucos são os atos praticados diretamente pelos servidores públicos. Isso é representativo, pois quando se terceirizam serviços que possuem princípios como o da privacidade envolvidos se tem grande risco (2014, p. 429).

Como compreende Morozov (2018, p. 146), as parcerias promovidas entre governos e as grandes empresas de tecnologia revelam a tendência de estabelecimento de um "estado do bem-estar privatizado, paralelo e praticamente invisível, no qual muitas das atividades diárias são fortemente subsidiadas por grandes empresas de tecnologia" interessadas em monetizar dados. O que muito se questiona, conforme Requião (2020), é o que será feito com as informações e os dados pessoais dos cidadãos coletados durante a pandemia quando a situação de crise mundial acabar. Isto é, o risco de que estes sejam utilizados para além do contexto de controle e prevenção do vírus pelo mercado de monetização de dados, que foi ampliado justamente com a virtualização das atividades cotidianas no cenário pandêmico.

Logo, verifica-se que é fundamental munir o usuário de maior controle acerca de seus dados no ambiente virtual, de forma a consentir ou não com a utilização e o tratamento destes, uma vez que a utilização e o compartilhamento indevido podem lesar os direitos da personalidade do usuário, especialmente a sua privacidade e o direito à autodeterminação informativa.

4 DIREITOS À PRIVACIDADE E À AUTODETERMINAÇÃO INFORMATIVA

A Constituição Federal de 1988 proclama como um dos fundamentos da República Federativa do Brasil, em seu artigo 1º, inciso III, a dignidade da pessoa humana e, o seu artigo 5º prescreve que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização em caso de dano material ou moral (BRASIL, 1988). O Código Civil de 2002 também prevê ser inviolável a vida privada da pessoa natural, em seu artigo 21 (BRASIL, 2002).

Conforme Modesto e Erhardt Junior, atualmente o direito à privacidade "tem sua compreensão ampliada em razão de a evolução das formas de divulgação e apreensão de dados pessoais ter expandido as possibilidades de violação da esfera privada, máxime pelo acesso não autorizado de terceiros a esses dados" (MODESTO; EHRHARDT JUNIOR, 2020, p. 148).

Para Rodotà (2008, p. 50), o conceito atual de privacidade englobaria o controle do indivíduo sobre as próprias informações e para determinar a construção da sua esfera particular. Além disso, a "própria defesa da privacidade requer, portanto, um alargamento da perspectiva institucional, superando a lógica puramente proprietária e integrando os controles individuais com aqueles coletivos". Segundo Doneda,

> hoje a exposição indesejada de uma pessoa aos olhos alheios se dá com maior frequência através da divulgação de seus dados pessoais do que pela intrusão em sua habitação, pela divulgação de notícias a seu respeito na imprensa, pela violação de sua correspondência – enfim, por meios "clássicos" de violação da privacidade (2006, p. 14).

Para o referido autor, os dados são a expressão direta da personalidade do usuário, sendo a sua proteção essencial à dignidade humana (DONEDA, 2011), uma vez que representam preferências, gostos, interesses e desejos dos usuários, potenciais consumidores e destinatários da publicidade comportamental, que se fundamenta na busca, pesquisa e engajamento de conteúdos pelo usuário no ambiente virtual.

Doneda (2006) pontua que é possível a violação dos direitos da personalidade do usuário por meio da utilização inadequada de dados sensíveis, que dizem respeito a questões que envolvem origem genética, sexo, gênero, orientação sexual, bem como escolhas e convicções religiosas e políticas. Como expõem Freitas, Capiberibe e Montenegro (2020, p. 198), o direito e o respeito à privacidade e à proteção dos dados pessoais "são princípios que orientam diretrizes no campo da governança da Internet e dos direitos humanos, mas têm poucas implicações em outros campos". O fato de os instrumentos "de ação pública serem hoje, em sua maioria, desenvolvidos e implementados com a mediação da Internet" – e, na maioria das vezes, utilizando dados – "revela a necessidade de se considerar direitos associados a esse uso como sendo de interesse da governança no setor público de forma transversal e multissetorial".

Nos termos do artigo 2º da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a disciplina da proteção de dados pessoais no Brasil tem como fundamentos: "I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais" (BRASIL, 2018).

Entre os fundamentos citados destaca-se o respeito à autodeterminação informativa, que é "um aspecto fundamental a ser levado em consideração para o uso de dados pessoais, conjuntamente com as garantias de transparência, segurança e minimização no uso de dados" (ALMEIDA *et al*., 2020, p. 2.489). A autodeterminação informativa tem por objetivo assegurar

> um direito constitucional de personalidade que tem por objeto o poder do indivíduo sobre três aspectos: de decidir sobre a divulgação e o uso dos seus dados pessoais; de decidir sobre quando e dentro de quais limites esses dados podem ser revelados; e, por fim, de ter conhecimento sobre quem sabe e o que sabe sobre ele, além de quando e em que ocasião (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 24).

A expressão "autodeterminação informativa" foi utilizada em 1983 pelo Tribunal Constitucional Alemão, no exame da Lei do Censo, que previa que o "Estado pudesse realizar o cruzamento de informações sobre os cidadãos para mensuração estatística da distribuição espacial e geográfica da população" (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 23). A Corte considerou que, tendo em vista o cenário moderno de processamento de dados, a tutela do indivíduo contra a coleta, o armazenamento e a divulgação ilimitada de seus dados pessoais "é abrangida pelos direitos gerais das pessoas garantidos na Constituição alemã" (SOUSA; SILVA, 2020, p. 9).

A Lei Geral de Proteção de Dados Pessoais (LGPD) também visa a garantir o consentimento do usuário para a coleta, o tratamento, a utilização e o compartilhamento de dados pessoais. Nos termos do seu artigo 5º, inciso XII, o consentimento é a "manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018). Conforme Sousa e Silva (2020, p. 17), o termo de consentimento, como "forma de exteriorização prática, coloca-se como instrumento de forma de controle sobre circulação dos referidos dados e informações", uma vez que este permite que o usuário saiba e tenha maior controle acerca de onde, como, por que e para que seus dados poderão ser utilizados no futuro, uma vez que

> no caso de compartilhamento dos dados pessoais com outros controladores exige-se a obtenção do consentimento específico do titular para esse fim. Nesse sentido, o controle por meio do consentimento do titular torna-se instrumento de garantia dos direitos de liberdade, intimidade e privacidade, pois o consentimento possibilita a mudança de eixo da estrutura da privacidade constituída pelo cidadão, informação e segredo, para o eixo da tríade cidadão, informação e controle (SOUSA; SILVA, 2020, p. 8).

Para Sousa e Silva, o consentimento seria a "exteriorização do fundamento da autodeterminação informativa, no seu contexto prático, não constituindo, assim, elemento de construção de seu sentido, mas instrumento de efetivação" (2020, p. 10).

Já Lugati e Almeida (2020) compreendem que é necessário desvincular a ideia de autodeterminação informativa baseada apenas no consentimento, uma vez que este, na realidade, representaria um instrumento utópico e ilusório, visto que facilmente perde seus efeitos (MALHEIRO, 2017), em razão da relação assimétrica da rede e da vulnerabilidade do titular de dados (BIONI, 2020).

Como pontuam Moura e Andrade (2019, p. 123), o direito à autodeterminação informativa também

> não é suficiente para evitar o fornecimento compulsório de dados para a prática dos atos mais corriqueiros de qualquer pessoa física: adquirir um telefone móvel, contratar serviços públicos essenciais, extrair documentos em órgãos públicos, prestar concursos, possuir conta bancária, etc. Logo, a "fé" no consentimento prévio como redoma protetora da privacidade do titular é puramente teórica, e baseada na extrema confiança de que os controladores e operadores de dados irão respeitar todos os ditames da LGPD. Esse ceticismo quanto à proteção do titular pelo simples fato do tratamento de dados depender de seu consentimento pode ser verificado tanto na doutrina pátria quanto na alienígena, que reconhecem a vulnerabilidade do titular e a fragilidade da proteção legal.

Para Lugati e Almeida (2020, p. 29) só seria possível falar em autodeterminação se as tecnologias empoderassem o titular de dados, de forma que este tivesse uma real participação quanto ao processo de tratamento de dados. Neste âmbito, surge a proposta do consentimento granular, de modo que, segundo Bioni (2020), o titular poderia decidir: "(i) quais serão seus dados coletados; (ii) por quais modalidades de tratamentos eles serão submetidos; (iii) por qual período de tempo e frequência; e (iv) a possibilidade de compartilhamento com terceiros". Assim, "o consentimento granular permitiria que o titular dos dados tivesse uma entrada gradual em meio ao fluxo de dados, com a fragmentação de suas autorizações" (LUGATI; ALMEIDA, 2020, p. 26-27).

O artigo 6º da Lei Geral de Proteção de Dados prevê que o tratamento destes deve observar a boa-fé e os seguintes princípios, definidos e explicados no texto da mencionada Lei: *finalidade* (que envolve propósitos legítimos, específicos, explícitos e informados); *adequação* (compatibilidade do tratamento com a finalidade informada); *necessidade* (limitação ao mínimo necessário e à finalidade, com apenas os dados pertinentes, de forma proporcional e não excessiva); *livre acesso* (garante a consulta gratuita e facilitada pelos usuários acerca do tratamento, bem como da integralidade dos dados); *qualidade* (assegura a exatidão, atualização, clareza e relevância dos dados, de acordo com a necessidade de cumprimento da finalidade) (artigo 6º, incs. I ao V da LGPD) (BRASIL, 2018).

Igualmente devem ser observados os princípios: da *transparência* (assegura aos titulares informações claras, precisas e acessíveis acerca do tratamento de dados, observado o segredo comercial e industrial); da *segurança* (medidas técnicas que protejam os dados da utilização indevida, de acidentes ou atividade ilícita de destruição, alteração, perda, comunicação ou difusão); da *prevenção* (adota medidas para prevenir dados em virtude do tratamento dos dados); da *não discriminação* (impossibilidade de tratamento com base em vieses discriminatórios, abusivos ou ilícitos) e da *responsabilização e prestação de contas* (demonstração acerca da adoção de medidas de proteção e da eficácia destas) (artigo 6º, incs. VI ao X da LGPD) (BRASIL, 2018).

Tais princípios demonstram que a coleta e o tratamento devem ser específicos, possuir uma finalidade, serem consentidos e adequados, bem como observarem o direito à igualdade e os direitos da personalidade, tais como o direito à privacidade e à autodeterminação informativa, e que o vazamento e o compartilhamento ilícitos devem ser punidos, tendo em vista a necessidade de transparência, segurança e prevenção de ofensas

ao usuário. Conforme Doneda (2011), o tratamento de dados, especialmente os automatizados, é uma atividade de risco, que se concretiza

> na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental (DONEDA, 2011, p. 92).

Diante da pandemia, na visão de Modesto e Ehrhardt Junior, "encontrar o ponto de equilíbrio no tratamento dos dados pessoais em prol do interesse coletivo é o grande desafio que se impõe cada vez que surge uma nova emergência", pois, "situações de grande preocupação social, como a atual pandemia, costumam propiciar que as pessoas tolerem intrusões cada vez maiores em suas liberdades individuais em nome do bem maior" (MODESTO; EHRHARDT JUNIOR, 2020, p. 154). Isso porque dificilmente medidas planejadas que visem a garantir o bem-estar dissociadas do direito à privacidade alcançarão seus objetivos (FREITAS; CAPIBERIBE; MONTENEGRO, 2020, p. 198).

Na concepção de Linares (2020, p. 146), não se pode perder a oportunidade de salvar vidas e de acelerar as investigações acerca do vírus sob a alegação de privacidade de dados, uma vez que as próprias legislações protetivas (cita-se o Regulamento Geral de Proteção de Dados, da União Europeia, e a Lei Geral de Proteção de Dados, no Brasil, que preveem exceções em que se poderia tratar dados em tempos de crise).

Como compreendem Finkelstein, Federighi e Chow (2020, p. 27) diante da crise de saúde pública e do atual aparato tecnológico, "não há que se questionar se usar ou não os dados pessoais no combate à Covid-19, mas sim como utilizá-los". Logo, é preciso visualizar que o direito à privacidade e a necessidade de proteção de dados, por si sós não inviabilizam "o uso de dados pessoais e a possibilidade de seu uso para responder à pandemia", considerando que a atual emergência de saúde pública "aponta para a premente necessidade de novas formas de governança de dados pessoais que incluam a sociedade civil para a promoção de benefícios equânimes para toda a sociedade" (ALMEIDA *et al*., 2020, p. 2.491).

Observam Modesto e Ehhardt Junior (2020, p. 150) que isolada e receosa em relação à propagação do vírus, a população inicialmente pouco pôde se preocupar com o tratamento e eventuais abusos do direito à privacidade, no entanto a "experiência em outros países demonstra que a perspectiva muda radicalmente quando, uma vez infectada, a pessoa passa a vivenciar as restrições provocadas pela exposição", muitas vezes "não consentida e nem sequer comunicada, de dados pessoais, incluindo dados sensíveis", principalmente pelo fato de que "situações de discriminação e exclusão social nesses casos não têm uma duração que corresponda ao período da doença, podendo persistir por períodos muito mais longos".

Tal posicionamento demonstra que é necessário cautela para a escolha pelo tratamento de dados em detrimento da privacidade e da autodeterminação informativa mesmo diante de um cenário pandêmico e cercado de incertezas, posto que tal opção, no futuro, pode motivar ainda mais a dependência do indivíduo da tecnologia a serviço de interesses particulares, desvinculados do público.

Diante de tal problemática, Almeida *et al*. (2020, p. 2.489) citam a anonimização de dados, que "consiste na aplicação de medidas técnicas para impossibilitar a associação direta ou indireta dos dados ao indivíduo"; já a pseudoanonimização "remove identificadores e os substitui por um código-chave único, sendo estratégias de proteção de dados previstas em algumas leis". Como observam os autores, os dados anonimizados "não são considerados dados pessoais ou o são com algumas ressalvas, enquanto dados pseudoanonimizados são tidos como dados pessoais pelo potencial de reidentificação dos indivíduos", por meio da utilização de um código-chave, mesmo que disponham de um nível de segurança mais elevado.

Embora os dados anonimizados não sejam considerados dados pessoais por leis protetivas, "mesmo sem fazer referência a qualquer indivíduo, podem prejudicar grupos em virtude de informações sobre locais, etnicidade, situações de saúde e condições socioeconômicas", por exemplo, "requerendo escrutinamento ético sobre os potenciais benefícios gerados por tais evidências" (ALMEIDA *et al*., 2020, p. 2.490). É igualmente

essencial evitar, segundo Carrasco e Ramírez (2020, p. 218) políticas intrusivas, mesmo que temporariamente, porquanto é improvável que sejam consideradas necessárias restrições à privacidade que não se mostrem fundamentais para salvar vidas ou contribuir para a continuação das atividades essenciais e econômicas.

Para Finkelstein, Federighi e Chow (2020, p. 27) a pandemia é um teste para as democracias liberais, de modo que este momento "não pode implicar em retrocessos nas liberdades individuais", principalmente considerando a influência do ambiente virtual para a criação de bolhas sociais, ambientes reacionários, antidemocráticos, disseminadores de *fake news* e de manipulação político-ideológica. Assim, os autores defendem como fundamental um debate público acerca da maneira como os dados pessoais estão sendo coletados e tratados pelas autoridades sanitárias, "com vistas a evitar a vigilância intrusiva que vem ocorrendo em diversos países do mundo". De forma que também seria preciso

> (i) realizar uma avaliação a respeito da necessidade de políticas de saúde centradas em dados, assim como quais são suas necessidades e objetivos, amparando-se na ciência; (ii) definir proporcionalidade do tratamento de dados, para fim de restringir a intervenção na esfera privada; (iii) definir rigidamente o ciclo de vida dos dados e a forma de descarte; (iv) garantir ampla transparência a todos os processos; (v) estabelecer salvaguardas específicas e concretas a todos os processos (FINKELSTEIN; FEDERIGHI; CHOW, 2020, p. 26).

Almeida *et al*. (2020, p. 2.490) acrescentam que uma governança responsável de dados inclui a "descrição das metodologias de processamento e análise dos dados, pois dados têm valor de prova, de evidência, na tomada de decisão tanto para políticas públicas quanto para ciência". Isso porque, como lecionam os autores, "todo algoritmo baseado em aprendizagem de máquina expressa a visão do padrão ou regularidade do que deve ser considerado para mensurar". Além disso, o método científico tem "papel preponderante para validar, aumentar a confiabilidade e a utilidade dos resultados. Inclusive no questionamento de suposições, valores e vieses que distinguem opiniões de evidências" (ALMEIDA *et al*., 2020, p. 2.490).

De modo que é necessário questionar: "Por quem e como os dados serão acessados, processados e utilizados? Serão armazenados, reutilizados, descartados após o alcance da finalidade?" Como serão protegidos? "Em caso de abuso ou negligência, quem será responsabilizado?" (ALMEIDA *et al*., 2020, p. 2.490).

Isto é, as políticas de tratamento de dados precisam ser claras e precisas, específicas e moralmente motivadas pelos interesses público ou privado do cidadão, de modo que não há espaço para programas que somente tenham por escopo a coleta indiscriminada, pouco explicada e concedam irrisórios benefícios ao cidadão apenas com o intuito de alimentar o cenário de monetização de dados ou criar Estados de vigilância.

Assim, visualiza-se como fundamental que os dados compartilhados e utilizados em razão da crise de saúde pública por empresas privadas, principalmente em parceria com o Estado, precisam demonstrar em seus termos de uso informações claras e transparentes acerca dos propósitos do acesso, uso, compartilhamento e de quem será a responsabilidade em caso de utilização indevida ou vazamento.

5 CONCLUSÃO

Com a pandemia da Covid-19 houve um *boom* de exploração pelos Estados de estratégias de *e-government* com o intuito de manter o isolamento social, dar continuidade aos serviços essenciais, sobretudo relacionados à saúde e à contenção do vírus e conceder benefícios e serviços aos cidadãos. Desta forma, ao redor do planeta cresceu a utilização de dispositivos e aplicativos de inteligência artificial por meio de monitoramento remoto, reconhecimento facial, *tracking*, geolocalização, etc., com base na coleta, tratamento, utilização e compartilhamento de dados pessoais que possibilitem realizar previsões e elaborar perfis informacionais e comportamentais.

Por certo que a situação de crise sanitária é suficiente para motivar medidas que tentem proteger o cidadão mediante o monitoramento remoto de sintomas, localização e a tentativa de prever possíveis locais de disseminação do vírus e novos surtos, de modo a restringir questões ligadas à privacidade e à autodeterminação informativa do usuário, que cada vez mais pauta sua vida no ambiente virtual e acaba por conceder seus dados e consentir com termos de uso para ter acesso aos benefícios trazidos pela tecnologia. É crucial, contudo, que tais políticas considerem que os dados pessoais são reflexo da personalidade, uma vez que evidenciam gostos, preferências e interesses, merecendo, para tanto, tutela compatível e adequada.

Visualiza-se diante dos desdobramentos do cenário atual pandêmico e da tentativa de manutenção do capitalismo pós-moderno a real possibilidade de criação de Estados de vigilância, alimentados pela coleta de dados pessoais dos cidadãos de forma arbitrária, desmotivada e sem finalidade, propiciados pelo contexto de monetização de dados das grandes empresas do mercado tecnológico, apontado por Zuboff, a serviço do consumo e da manutenção da retórica da vigilância como forma de bem-estar e controle social, já evidenciada por Foucault.

Para que isso não aconteça, é essencial que tais estratégias de *e-government* prevejam de forma clara e precisa como, quando e onde estes dados serão utilizados, uma vez que a utilização destes e o seu compartilhamento para fins de monetização e consumo sem o consentimento do titular ofende a privacidade e a autodeterminação informativa do cidadão, justificativa que motivou a declaração de inconstitucionalidade pelo Supremo Tribunal Federal (STF) da Medida Provisória nº 954 em 2020.

O que se conclui, portanto, é que dificilmente o cidadão comum, que necessita preencher cadastros *on-line*, baixar aplicativos e concordar com termos de uso no ambiente virtual, tem a real noção de como os seus dados podem ser utilizados pelo Estado e por empresas privadas, posto que, aparentemente, aos olhos leigos, não representam grandes informações a seu respeito, tais como nome, endereço, CPF, número de telefone, etc., mas representam informações importantes para inferências do mercado tecnológico, de consumo e para o Estado.

Apesar a existência no Brasil de disposições constitucionais e infraconstitucionais que garantam o direito à privacidade, bem como a proteção de dados e a autodeterminação informativa (Lei Geral de Proteção de Dados) verifica-se que os termos do consentimento atual para a coleta, o tratamento e o compartilhamento de dados ainda são muito questionáveis, dado que este facilmente perde seus efeitos ante a relação assimétrica entre os usuários e o mercado tecnológico em parceria com o Estado, como ocorre nas estratégias de *e-government*, de forma que o fomento da discussão, bem como a maior responsabilização do Estado e, principalmente, das empresas privadas que atuam nesse âmbito em caso de violação e ofensa aos direitos à privacidade, à proteção de dados e à autodeterminação informativa são essenciais para a tutela dos direitos da personalidade contra os efeitos nocivos do capitalismo de vigilância em tempos de crise.

REFERÊNCIAS

ALMEIDA, Bethania de Araujo *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, v. 25, n. 1, p. 2487-2492, jun. 2020. Disponível em: https://scielosp.org/pdf/csc/2020.v25suppl1/2487-2492/pt. Acesso em: 10 out. 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. *Lei nº 10.406,* de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 5 out. 2020.

BRASIL. *Lei nº 13.709*, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 set. 2020.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm. Acesso em: 10 set. 2020.

BRUNO, Fernanda. Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas. *Revista Fronteiras – Estudos Midiáticos,* São Leopoldo, v. 8, n. 2, p. 152-159, maio/ago. 2006. Disponível em: http://revistas.unisinos.br/index.php/fronteiras/ article/view/6129. Acesso em: 16 jul. 2019.

CARDIN, Valéria Silva Galdino; PAULICHI, Jaqueline Silva. Das formas de inteligência artificial e os impactos nos padrões de consumo e a proteção dos direitos da personalidade. *Meritum*, v. 15, n. 4, 2020. Disponível em: http://revista.fumec.br/index.php/meritum/article/view/7954. Acesso em: 10 abr. 2021.

CARRASCO, Carmen Márquez; RAMÍREZ, Juan Ortega. La Covid-19 y los desafíos de la vigilancia digital para los derechos humanos: a propósito de la app DataCOVID prevista en la Orden Ministerial SND/29/2020, de 27 de marzo. *Revista Bioetica y Derecho*, v. 50, p. 205-220, 2020. Disponível em: https://revistes.ub.edu/index.php/RBD/article/view/31377/32112. Acesso em: 20 nov. 2020.

CELLAN-JONES, Rory. Coronavirus: Israeli spyware firm pitches to be Covid-19 saviour. *BBC News,* 2 abr. 2020. Disponível em: https://www.bbc.com/news/health-52134452. Acesso em: 10 abr. 2021.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 10 out. 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

ESTRADA, Manuel Martín Pino. O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade. *Revista de Direito do Trabalho,* v. 42, n. 172, p. 35-54, nov./dez. 2016. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/100576. Acesso em: 10 abr. 2021.

FACHINI, Elaine Cristina Sotelo; FERRER, Walkiria Martinez Heinrich. Biopolítica e biopoder como forma de intervenção na ordem econômica e de controle social: a Lei Geral de Proteção de Dados como inibitória da manipulação social. *Revista Direito UFMS*, Campo Grande, v. 5, n. 2, p. 226-246, jul./dez. 2019. Disponível em: https://periodicos.ufms.br/index.php/revdir/article/view/9153. Acesso em: 4 nov. 2020.

FINKELSTEIN, Carlos; FEDERIGHI, André Catta Petra; CHOW, Beatriz Graziano. O uso de dados pessoais no combate à Covid-19: lições a partir da experiência internacional. *Revista Brasileira de Inteligência Artificial – RBIAD*, v. 1, n. 1, 2020. Disponível em: https://rbiad.com.br/index.php/rbiad/article/view/7. Acesso em: 10 out. 2020.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. *Revista Direito em Debate*, a. XXIX, v. 29, n. 53, p. 182-195, jan./jun. 2020. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033. Acesso em: 10 out. 2020.

FOUCAULT, Michel. *Microfísica do poder*. Tradução Roberto Machado. 2. ed. Rio de Janeiro: Paz e Terra, 2015.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. Tradução Raquel Ramalhete. Petrópolis: Vozes, 1987.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. Lisboa: Edições 70, 2013.

FREITAS, Christiana Soares de; CAPIBERIBE, Camila Luciana Góes; MONTENEGRO, Luísa Martins Barroso. Governança tecnopolítica: biopoder e democracia em tempos de pandemia. *Revista NAU Social*, v. 11, n. 20, p. 191-201, maio/out. 2020. Disponível em: https://portalseer.ufba.br/index.php/nausocial/article/view/36637/21028. Acesso em: 10 out. 2020.

G1 PE. Recife rastreia 700 mil celulares para monitorar isolamento social e direcionar ações contra coronavírus. *G1 PE,* 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: 10 abr. 2021.

GERKE, Sara *et al*. Regulatory, safety, and privacy concerns of home monitoring technologies during Covid-19. *Nature Medicine*, v. 26, p. 1176-1182, 2020. Disponível em: https://www.nature.com/articles/s41591-020-0994-1. Acesso em: 10 out. 2020.

JUNG, Gyuwon *et al*. Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People With Covid-19 in South Korea. *Front Public Health*, v. 8, p. 305, 2020. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7314957/. Acesso em: 8 nov. 2020.

LINARES, Mikel Recuero. La compartición internacional de datos personales relativos a la salud en tiempos de la Covid-19: aspectos éticos y legales para el impulso de la necesaria cooperación. *Revista Bioetica y Derecho*, v. 50, p. 133-148, 2020. Disponível em: https://revistes.ub.edu/index.php/RBD/article/view/31711/32107. Acesso em: 20 nov. 2020.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. *Revista de Direito*, Viçosa, v. 12, n. 2, p. 1-33, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 20 nov. 2020.

MAGALHÃES, André Lourenti. Auxílio Emergencial 2021: como consultar o benefício pelo celular. *CanalTech*, 2 abr. 2021. Disponível em: https://canaltech.com.br/governo/auxilio-emergencial-2021-como-consultar-beneficio-celular/. Acesso em: 10 abr. 2021.

MAGRANI, Eduardo. *Entre dados e robôs*: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MALHEIRO, Luíza Fernandes. *O consentimento na proteção de dados pessoais na Internet:* uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016. 2017. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade de Brasília, Brasília, 2017. Disponível em: bdm.unb.br/handle/10483/18883. Acesso em: 20 mar. 2020.

MEDEIROS, Breno Pauli *et al*. The use of cyberspace by the public administration in the Covid-19 pandemic: diagnosis and vulnerabilities. *Revista de Administração Pública*, Rio de Janeiro, v. 54, n. 4, p. 650-662, jul./ago. 2020.

MODESTO, Jéssica Andrade; EHRHARDT JUNIOR, Marcos. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a Covid-19. *Redes – Revista Eletrônica Direito e Sociedade*, v. 8. n. 2, p. 143-161, 2020. Disponível em: https://revistas.unilasalle.edu.br/index.php/redes/article/view/6770. Acesso em: 10 out. 2020.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? *Instituto Igarapé*, Rio de Janeiro, Artigo Estratégico n. 39, p. 1-17, dez. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-umdireito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 10 nov. 2020.

MOROZOV, Evgeny. *Big tech*: a ascensão dos dados e a morte da política. São Paulo: Ubu, 2018.

MOURA, Plínio Rebouças; ANDRADE, Diego Calasans Melo. O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço. *Revista de Direito, Governança e Novas Tecnologias,* v. 5, n.1, p. 110-133, jan./jun. 2019. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/5568. Acesso em: 20 nov. 2020.

QUEIROZ, Roberlei Aldo; TEIXEIRA JUNIOR, Juarez Ribas; KNOERR, Fernando Gustavo. Controle e vigilância do cidadão através do poder público: um diálogo com Michel Foucault e Hans Jonas sobre programas de governo. *Revista Jurídica Unicuritiba*, v. 4, n. 37, p. 413-442, 2014. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/1057. Acesso em: 10 out. 2020.

RAMPELOTTO, Alexandre; LÖBLER, Mauri Leodir; VISENTINI, Monize Sâmara. Avaliação do sítio da Receita Federal do Brasil como medida da efetividade do governo eletrônico para o cidadão. *Revista de Administração Pública*, v. 49, n. 4, p. 959-984, 2015. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rap/article/view/51614. Acesso em: 10 abr. 2021.

REQUIÃO, Maurício. Covid-19 e proteção de dados pessoais: o antes, o agora e o depois. *Consultor Jurídico*, 5 abr. 2020. Disponível em: https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protecao-dados-pessoais-antes-agora-depois. Acesso em: 10 abr. 2021.

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

RUEDIGER, Marco Aurélio. Governança democrática na era da informação. *Revista de Administração Pública*, v. 37, n. 6, p. 1257-1280, 2003. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rap/article/view/6522. Acesso em: 10 abr. 2021.

SAMPAIO, Rafael Cardoso. e-Orçamentos Participativos como iniciativas de e-solicitação: uma prospecção dos principais casos e reflexões sobre a e-Participação. *Revista de Administração Pública*, v. 50, n. 6, p. 937-958, 2016. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rap/article/view/64709. Acesso em: 10 abr. 2021.

SOUSA, Rosilene Paiva Marinho de; SILVA, Paulo Henrique Tavares da. Proteção de dados pessoais e os contornos da autodeterminação informativa. *Informação & Sociedade: Estudos,* João Pessoa, v. 30, n. 2, p. 1-19, abr./jun. 2020. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/52483. Acesso em: 10 out. 2020.

TADDEO, Mariarosaria. The Ethical Governance of the Digital During and After the COVID-19 Pandemic. *Minds and Machines*, v. 30, p. 171-176, 2020. Disponível em: https://link.springer.com/article/10.1007/s11023-020-09528-5. Acesso em: 4 nov. 2020.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino Cardin. Democracia e vigilância digital em tempos de Covid-19: uma análise do direito à autodeterminação informativa. *In*: SEMINÁRIO INTERNACIONAL DE DIREITOS HUMANOS E DEMOCRACIA, 8., 2020, Santa Cruz do Sul. *Anais* [...]. Santa Cruz do Sul: Essere nel Mondo, 2020a. v. 2. p. 360-369. Disponível em: https://www.unijui.edu.br/eventos/viii-seminrio-internacional-de-direitos-humanos-e-democracia-514. Acesso em: 10 abr. 2021.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Perfis informacionais e publicidade comportamental: direito à autodeterminação informativa e a proteção de dados pessoais no ambiente virtual. CONGRESSO BRASILEIRO DE PROCESSO COLETIVO E CIDADANIA, 8., 2020. *Anais* [...]. 2020b. p. 1.260-1.276. Disponível em: https://revistas.unaerp.br/cbpcc/article/view/2193. Acesso em: 10 abr. 2021.

XAVIER, Fernando *et al*. Análise de redes sociais como estratégia de apoio à vigilância em saúde durante a Covid-19. *Estudos Avançados*, São Paulo, v. 34, n. 99, maio/ago. 2020. Disponível em: https://www.scielo.br/pdf/ea/v34n99/1806-9592-ea-34-99-261.pdf. Acesso em: 10 out. 2020.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism*: the fight for a human future at the new frontier of power. Londres: Profile Books, 2019.