Dados, vigilância e o setor privado no desenvolvimento de ferramentas de rastreamento de contatos durante a pandemia de covid-19

Data, surveillance and the private sector's role in the development of contact tracing tools during the covid-19 pandemic

Murilo Motta [1]

RESUMO: A migração de diversos direitos e serviços para plataformas digitais, devido à pandemia de COVID-19, ensejou discussões quanto à privacidade dos dados dos usuários. Neste contexto, o objetivo deste artigo é analisar o papel do setor privado no desenho de tecnologias utilizadas por governos nacionais em suas políticas públicas de combate à disseminação da COVID-19. A análise realizada explora a economia política dos dados digitais no mundo contemporâneo, bem como a legislação de proteção de dados pessoais existente no Brasil. Em seguida, é estudado o caso da cooperação entre Apple e Google no desenvolvimento de uma interface de programação de aplicativos (API), disponibilizada gratuitamente para o desenvolvimento de aplicativos de rastreamento de contatos. Em suma, o artigo aponta para a importância do debate público sobre o papel de grandes empresas transnacionais no desenho das ferramentas tecnológicas utilizadas na execução de políticas públicas baseadas na coleta de dados pessoais.

Palavras-Chave: capitalismo de vigilância; dados digitais; atores privados; políticas públicas.

Abstract: The migration of several rights and services to digital platforms, due to the COVID-19 pandemic, gave rise to discussions regarding the privacy of user data. Given this context, this article analyzes the private sector's role in the design of technologies used by national governments in their public policies to limit the spread of COVID-19. The analysis carried out explores the political economy of digital data in the contemporary world, as well as the existing legislation for the protection of personal data in Brazil. Then, the case of the cooperation between Apple and Google in the development of an application programming interface (API), which was made available for free for the development of contact tracing applications, is studied. In short, the article points to the importance of public debate on the role of large transnational companies in the design of technological tools used in the execution of public policies based on the collection of personal data.

Keywords: surveillance capitalism; digital data; private actors; public policies.

[1] Mestrando pelo Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas (Unesp, Unicamp, PUCSP). Bolsista CAPES (PROCAD-DEFESA) e membro da Rede de Pesquisa em Autonomia Estratégica, Tecnologia e Defesa (PAET&D). E-mail de contato: murilo.motta@unesp.br https://orcid.org/0000-0002-0604-2020

https://doi.org/10.36311/1982-8004.2021.v14.n2.p91-104

Introdução

A investigação na área de políticas públicas busca compreender as atribuições do Estado em suas diferentes formas de intervenção na sociedade, mas deve também se preocupar com os processos pelos quais atores originalmente não participantes do jogo político passam a deter poderes sobre a gestão da coisa pública (MADEIRA et al, 2020). As grandes empresas transnacionais de tecnologia digital, como Google, Apple, Facebook, Amazon e Microsoft (GAFAM), exercem um papel cada vez maior na modulação das relações em suas plataformas, sejam elas comerciais ou sociais, de trabalho ou de lazer (ZUBOFF, 2019). Desta forma, a dependência dos conhecimentos e das tecnologias de algumas poucas empresas confere a elas poder sobre os representantes eleitos de diversos Estados nacionais ao redor do globo.

As discussões em torno do papel do Estado na regulação das plataformas digitais assumiram importância inédita em 2020, já que a pandemia de COVID-19 gerou uma migração massiva de diversos direitos e serviços para a Internet, levantando preocupações quanto à privacidade dos dados dos usuários. Embora as tecnologias digitais tenham ajudado no combate à disseminação do vírus, elas também aumentaram o acesso de empresas e governos a dados pessoais. Conforme o escândalo da Cambridge Analytica[2] deixou claro, os dados coletados por essas empresas podem ser usados para influenciar decisivamente processos democráticos. De fato, "a possibilidade de extensa e intensa exploração das informações relativas ao usuário colocou em questão o impacto das novas tecnologias sobre a cidadania e a democracia, na medida em que ficaram abalados o direito à privacidade e a liberdade de informação" (GARCIA DOS SANTOS, 2003, p. 145).

Neste contexto, este artigo objetiva compreender qual o papel do setor privado no desenho das ferramentas digitais utilizadas pelas políticas públicas destinadas a conter a pandemia de COVID-19. A pergunta investigada é: qual o interesse de empresas especializadas em tecnologias digitais no desenho de ferramentas de rastreamento de contatos utilizadas em políticas públicas de combate à pandemia? Para responder a esta pergunta, em primeiro lugar, é explorada a economia política dos dados digitais e são apresentadas as formas de proteção de dados pessoais no Brasil. Em seguida, é analisado o caso da cooperação entre Apple e Google no desenvolvimento de uma interface de programação de aplicativos (API), disponibilizada gratuitamente para o desenvolvimento de aplicativos de rastreamento de contatos, como uma estratégia de

[2] A Cambridge Analytica é uma empresa de consultoria política que coletou indevidamente dados pessoais de usuários do Facebook e os utilizou para direcionar propagandas políticas durante as eleições presidenciais estadunidenses de 2016, que elegeram Donald Trump, assim como no referendo britânico, do mesmo ano, que adotou o *BrExit*, a saída do Reino Unido da União Europeia. Estes dados específicos permitiram à empresa o direcionamento de propagandas baseados nos perfis psicológicos de segmentos de usuários da rede social (CADWALLADR; GRAHAM-HARRISON, 2018).

transgressão da esfera de legitimidade de atuação destas empresas, que visa o acúmulo de dados.

A economia política dos dados digitais

Os dados são um componente fundamental da economia política do século XXI. Sua acumulação e circulação é, crescentemente, elemento central do capitalismo contemporâneo. O imperativo de capturar todos os tipos de dados, de todos os tipos de fontes, através de qualquer meio possível, influencia decisivamente o modelo de negócios de empresas, a governança política e as opções de desenvolvimento tecnológico. Contudo, estes dados não são um subproduto "natural" de nossa utilização das novas tecnologias da informação; na verdade, as plataformas e os serviços digitais são deliberadamente desenhados com o intuito de que o usuário gere dados (SADOWSKI, 2019).

A digitalização do mundo, isto é, sua tradução na forma de *dados*, parte da concepção de informação proposta pela cibernética, um campo de estudos interdisciplinar que surgiu na década de 1940, nos EUA, cujo principal objetivo era integrar conhecimentos especializados na dimensão comum do campo da comunicação, uma vez que diversas ciências trabalham com os conceitos de informação, realimentação (*feedback*), controle e aprendizagem (WIENER, 1968, p. 17-18). Segundo Floridi (2010), "nas últimas décadas, tem se tornado comum a adoção de uma Definição Geral da Informação (GDI) em termos de dados + significado", de modo que os dados podem ser definidos como a informação desprovida de seu significado.

A "virada cibernética" é uma expressão cunhada por Garcia dos Santos (2003) para se referir à aliança entre as novas tecnologias de informação e o capital globalizado, a partir da década de 1970. Estas novas tecnologias permitiram o domínio definitivo dos humanos sobre a natureza, de modo que a "natureza humana desponta como último território a ser conquistado" (GARCIA DOS SANTOS, 2003, p. 82). Deste modo, "controlar os consumidores e, principalmente, monitorar as potencialidades de cada uma das dimensões de suas vidas", através da "coleta e o tratamento de informações", tornam-se os principais objetivos das empresas capitalistas (*Ibidem*, p. 144).

De fato, o mercado de grandes quantidades de dados (*Big Data*) é hoje um dos mais lucrativos do globo, embora siga concentrado entre algumas poucas empresas que mantêm estruturas oligopolísticas de competição. Zuboff (2019) vê o uso de *Big Data* como componente fundamental de uma nova forma de capitalismo de informação, que ela chama de "capitalismo de vigilância", em que grandes empresas de tecnologia, como as GAFAM, oferecem serviços e plataformas digitais gratuitos desenhados para extrair o máximo possível de dados de seus usuários; então, estes dados são tratados e vendidos

para terceiros, como modelos preditivos do comportamento humano, que também permitem sua modificação por antecipação.

Para Couldry e Mejias (2019, p. xx), as relações entre os usuários e estas grandes empresas configuram uma nova forma de colonialismo, porque normalizam a extração de dados produzidos por seres humanos enquanto degradam a vida humana, "em primeiro lugar ao expô-la continuamente ao monitoramento e vigilância (por meio dos quais os dados são extraídos) e, em segundo lugar, ao tornar a vida humana um insumo direto para a produção capitalista", de forma análoga ao modo como o colonialismo histórico se apropriou de recursos naturais de territórios estrangeiros.

Desta forma, há uma expropriação do valor agregado pelos usuários às redes digitais por estas empresas, o que aprofunda as relações de subordinação econômica e cultural entre os centros de desenvolvimento de novas tecnologias e as periferias do sistema-mundo capitalista. Com efeito, especialmente no Sul Global, a expropriação destes dados implica uma deficiência nas informações necessárias à gestão do Estado e à implementação de políticas públicas, além de dificultar o desenvolvimento de empresas nacionais de tecnologias digitais e análise de dados.

Para regulamentar as práticas invasivas e desenfreadas de acúmulo de dados, Sadowski (2019) propõe controlar quais tipos de dados as empresas podem coletar, como podem coletá-los e para onde podem enviá-los e armazená-los, bem como limitar a quantidade de dados que uma empresa pode possuir sobre seus usuários. O autor também sugere a criação de novos modelos de propriedade e de governança de dados, por exemplo, quebrando as práticas monopolistas de empresas como as GAFAM e gerenciando alguns setores da economia de dados como parte da infraestrutura pública.

Proteção de dados no Brasil

Em 2018, foi aprovada a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira, que entrou em vigor em setembro de 2020. O objeto da lei são *todos* os tipos de dados pessoais, inclusive os dados digitais. Especificamente, ela estabelece como devem ser coletados, armazenados, processados e deletados os dados que possam identificar algum indivíduo, com o objetivo de proteger a liberdade, a privacidade e o livre desenvolvimento da pessoa natural (BRASIL, 2018).

Conforme o artigo 5º da LGPD, dado pessoal é toda "informação relacionada a pessoa natural identificada ou identificável". A lei também destaca a necessidade de maior cuidado com os dados pessoais sensíveis, que são aqueles "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político" além de todo tipo de "dado referente à saúde ou

à vida sexual, dado genético ou biométrico", quando vinculados a uma pessoa natural (BRASIL, 2018).

Conforme os artigos 17 e 18 da mesma lei, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais à liberdade, à intimidade e à privacidade. O titular dos dados pessoais tem direito à confirmação da existência de tratamento de seus dados; ao acesso a eles; à correção dos incompletos, inexatos ou desatualizados; à anonimização, bloqueio ou eliminação daqueles desnecessários, excessivos ou tratados em desconformidade com o disposto pela LGPD; à portabilidade dos dados a outro fornecedor de serviço ou produto; à eliminação dos dados pessoais tratados; e à revogação do consentimento dado para a coleta ou tratamento deles (BRASIL, 2018).

De acordo com relatório da Data Privacy Brasil (2020), a Lei Federal 13.979/2020, conhecida como "Lei da Quarentena", determinou critérios para atuação do Ministério da Saúde no combate à disseminação da COVID-19, que incluíram a realização compulsória de testes e a mobilização de forças policiais para cumprimento de medidas de isolamento social e quarentena. A legislação prevê que tais medidas, que implicam limitação de direitos constitucionais básicos, como o de locomoção e liberdade econômica, "poderão ser determinadas com base em evidências científicas e em análises sobre as informações estratégicas em saúde e deverão ser limitadas no tempo e no espaço ao mínimo indispensável à promoção e à preservação da saúde pública". A legislação reconhece o respeito à dignidade, aos direitos humanos e às liberdades fundamentais das pessoas, conforme preconiza o artigo 3º do Regulamento Sanitário Internacional, produzido pela Organização Mundial da Saúde (OMS) e adotado pelo Brasil, por meio do Decreto 10.212/2020.

Esta incorporação de princípios da proteção de dados é crucial para dar concretude ao Regulamento Sanitário Internacional, que menciona expressamente a necessidade e o respeito às leis nacionais de proteção de dados. Nesse sentido, devem ser garantidas salvaguardas como limitação temporal, exclusão após uso, medidas técnicas robustas de anonimização e proibição de monetização de dados sensíveis, especialmente seu uso para quaisquer outras finalidades além das necessárias para o combate à pandemia (DATA, 2020).

O artigo 45 desse Regulamento dispõe que as informações de saúde devem ser mantidas em sigilo e processadas anonimamente, mediante balizas de leis nacionais. Seu Parágrafo 1º prevê que os Estados podem tratar dados pessoais "quando isso for essencial para os fins de avaliação e manejo de um risco para a saúde pública", garantindo que os dados pessoais sejam: processados de modo justo e legal, sem outros processamentos desnecessários e incompatíveis com tal propósito; adequados, relevantes

e não excessivos em relação a esse propósito; acurados e, quando necessário, mantidos atualizados, garantindo-se que todas as medidas razoáveis serão tomadas para garantir que dados imprecisos ou incompletos sejam apagados ou retificados; e conservados apenas pelo tempo necessário (BRASIL, 2020).

O QUE É RASTREAMENTO DE CONTATOS?

O rastreamento de contatos (*contact tracing*) é uma ferramenta utilizada por profissionais da saúde, especialmente da epidemiologia, para a detecção de indivíduos que tiveram contatos com uma pessoa infectada com uma determinada doença. O objetivo do rastreamento de contatos é conter o espalhamento de doenças infecciosas, como é a COVID-19, colocando em quarentena não só os casos identificados, mas também os indivíduos com maiores chances de serem vetores da doença. Esta abordagem foi amplamente utilizada no controle das epidemias de HIV/AIDS e Ebola, por exemplo, bem como no combate à disseminação de sífilis e sarampo (SHARON, 2020).

O rastreamento de contatos tradicional envolve uma equipe que, ao identificar um indivíduo infectado, obtém uma lista de locais e pessoas com as quais este indivíduo teve contato recentemente, para que estas pessoas sejam procuradas e testadas. O rastreamento digital de contatos é uma variação desta abordagem tradicional, viabilizado devido ao amplo acesso a smartphones pela população dos grandes centros urbanos (LUCIVERO et al, 2020). Ainda assim, diversos estudos indicam que grupos marginalizados produzem menos dados, porque têm acesso desigual e menor capacidade de se envolver *online*, de forma que as políticas públicas baseadas em dados acabam reproduzindo os padrões de discriminação e exclusão socioeconômica, como afirma Magalhães (2021).

Além disso, o que constitui um "contato" para um *smartphone* nem sempre tem valor epidemiológico, como destaca Sharon (2020). Os profissionais de saúde pública, que tradicionalmente realizam o rastreamento de contatos "analógico", são treinados para realizar um trabalho de detetive epidemiológico, de modo a estabelecer quais contatos são importantes para o contágio de doenças, baseados em critérios como o ambiente que foi compartilhado com outra pessoa, o tipo de atividade realizada no momento e o tempo de duração do contato. A substituição deste tipo de consulta pela troca de sinais via Bluetooth está se mostrando problemática porque alguns telefones podem detectar sinais Bluetooth de até 30 metros de distância, sem serem capazes de determinar a distância exata; ademais, o Bluetooth não identifica a existência de obstáculos à circulação do vírus, como paredes, porque o sinal é transmitido através delas.

Como ressaltam Lucivero e coautoras (2020), cabe aos desenvolvedores dos aplicativos *decidir* se eles coletarão dados de geolocalização por GPS, ou se eles se comunicarão por sinais de Wi-Fi ou Bluetooth; se os dados serão armazenados localmente nos dispositivos dos usuários ou exportados para bancos de dados centralizados; se esses dados também poderão ser usados para fins de pesquisa científica; se os usuários terão algum controle sobre quem pode acessar seus dados; e se os dados serão excluídos automaticamente ao final da pandemia. Estas *decisões* de quem desenha estas tecnologias traduzem questões éticas e legais, incluindo consentimento, limitação de finalidade, minimização de dados e proteção de dados.

Há diferenças significativas entre aplicativos que coletam dados de geolocalização (GPS) e aqueles que rastreiam contatos através do sistema de Bluetooth. Vários dos primeiros sistemas de rastreamento de contatos digitais, por exemplo os usados na China, Coréia do Sul, Índia, Israel e Islândia, usavam dados GPS de localização dos telefones, mas este tipo de dados carece de precisão e é tipicamente não consensual, isto é, os usuários não sabem que o uso de algum aplicativo ou serviço exige o monitoramento da geolocalização do aparelho. Em contrapartida, os aplicativos baseados em Bluetooth evitam rastrear a localização dos usuários e são percebidos como menos intrusivos (SHARON, 2020).

Há também diferenças entre os aplicativos que armazenam os dados dos usuários através de um sistema centralizado e aqueles que utilizam um sistema descentralizado. Aplicativos baseados em sistemas centralizados, como os utilizados inicialmente em Singapura e Austrália, enviam dados coletados pelo telefone de um usuário para um banco de dados central, controlado por uma agência governamental ou autoridade nacional de saúde, que decide para quem enviar um alerta entre os contatos que o telefone de uma pessoa infectada registrou. Essa concentração de dados tem sido um ponto de crítica para os defensores da privacidade, que apoiam amplamente sistemas descentralizados, em que os dados coletados pelos telefones não são enviados a um servidor central, mas são armazenados localmente, nos próprios telefones, que também enviam automaticamente as mensagens de possível contágio para toda a lista de aparelhos que estiveram em sua proximidade recentemente, sem que nenhuma autoridade central seja envolvida (SHARON, 2020).

Assim, apesar de ter um objetivo específico, o processo pelo qual os aplicativos de rastreamento de contatos funcionam pode variar. Ainda que estes aplicativos objetivem atender a uma crise sanitária, deve-se reconhecer o conflito inerente entre a busca por maximizar a efetividade das políticas de controle do deslocamento das pessoas e os limites estabelecidos por direitos e valores fundamentais, como a privacidade e a proteção de dados pessoais.

A cooperação entre Apple e Google

A adoção de tecnologias de rastreamento de contatos, para mitigar a pandemia de COVID-19, por diversas instâncias governamentais ao redor do globo, foi acompanhada de preocupações quanto à privacidade dos usuários. Desde os vazamentos de Chelsea Manning (2010) e Edward Snowden (2013) para o *WikiLeaks*, não há dúvidas quanto às relações íntimas entre o governo dos EUA, suas agências de inteligência e as grandes empresas de tecnologias digitais do país (GREENWALD; MACASKILL, 2013).

De acordo com os documentos disponibilizados por Snowden para jornalistas do *The Guardian*, a *National Security Agency* (NSA) do governo dos EUA, através do programa PRISM, teve acesso aos servidores de armazenamento de dados dos usuários das principais empresas de tecnologias da informação do país, como a Google, a partir de 2009, e a Apple, em 2012.

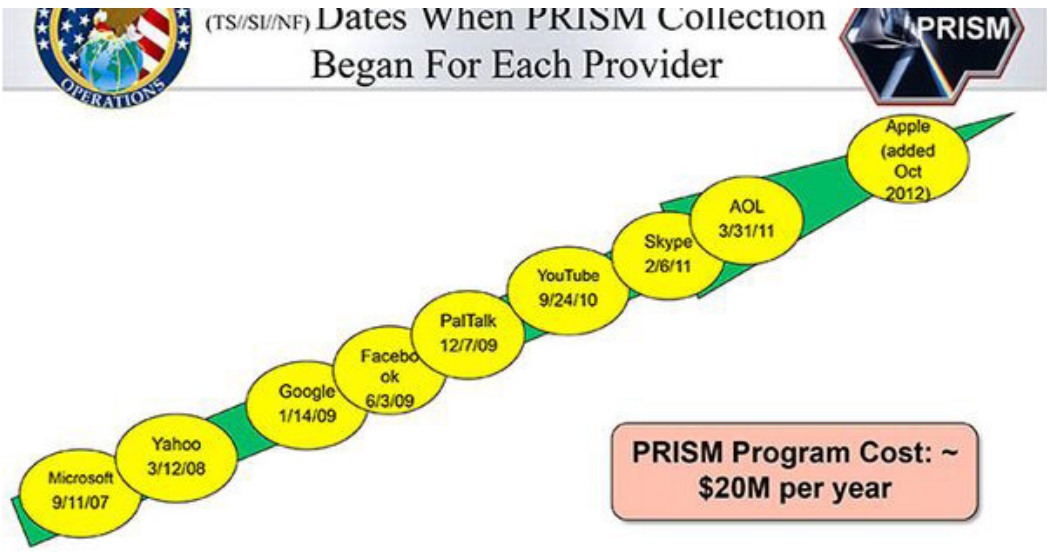

Figura 1: Datas de quando o PRISM começou a coletar dados, por provedor. Reprodução de *The Guardian*, 2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data Acesso em 30/05/2021

Ainda assim, o anúncio de uma parceria entre Apple e Google para o desenvolvimento de uma Interface de Programação de Aplicativos (API) para o rastreamento de contatos de COVID-19, foi bem recebido em todo o globo, após comprovada a eficácia da API na proteção à privacidade dos usuários. A partir desta interface, organismos locais (como o Estado ou a autoridade sanitária competente) puderam desenvolver aplicativos de rastreamento de contatos integrados aos sistemas de saúde nacionais. A API Apple-Google inclui o uso de Bluetooth, de modo que não é necessário acessar os dados de localização dos aparelhos; uma interface que opera

com a geração de códigos de identificação aleatórios, que mudam a cada 20 minutos, de modo que não há necessidade de trocar informações que possam identificar algum aparelho; e a exigência do consentimento expresso do usuário para o compartilhamento de informações. Ademais, os dados são armazenados nos próprios dispositivos e não em servidores centrais (APPLE, 2020).

Lançada em abril de 2020, a interface foi adotada por cerca de 40 países (RAHMAN, 2021). No Brasil, o Ministério da Saúde usou a API Apple-Google para desenvolver o aplicativo de rastreamento de contatos "Coronavirus – SUS":

País	Nome do aplicativo
África do Sul	COVIDConnect
Alemanha	Corona-Warn-App
Arábia Saudita	Tabaud
Áustria	Stopp Corona
Bélgica	Coronalert
Brasil	Coronavirus – SUS
Canadá	COVID Alert
Cazaquistão	Saqbol
Chipre	CovTracer-EN
Croácia	Stop COVID-19
Dinamarca	Smittestop
Equador	ASI
Escócia	Protect Scotland
Eslovênia	OstaniZdrav
Espanha	Radar COVID
Estônia	Hoia
Finlândia	Koronavilkku
Gibraltar	Beat Covid Gibraltar
Grécia	Exo
Irlanda	Covid Tracker
Irlanda do Norte	StopCOVID NI
Itália	Immuni
Japão	COCOA
Letônia	Apturi Covid Latvia
Lituânia	Korona Stop LT
Malta	COVID Alert Malta
Noruega	Smittestopp
Nova Zelândia	NZ COVID Tracer

Países Baixos	CoronaMelder
Panamá	Protégete Panamá
Polônia	ProteGO Safe
Portugal	STAYAWAY COVID
Reino Unido	NHS COVID-19
República Checa	eRouška
Rússia	Госуслуги.COVID трекер
Suíça	SwissCovid
Uruguai	Coronavirus UY
26 estados dos Estados Unidos	Diversos

Tabela 1: Lista de países com aplicativos de rastreamento de contato de COVID-19 baseados na API Apple-Google.
Adaptado de Mishaal Rahman, 2021. Disponível em: https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/ Acesso em 30/05/2021

Segundo o Ministério da Saúde, o "Coronavirus – SUS" reconhece contatos próximos a uma distância de 1,5 a 2 metros e por um tempo mínimo de cinco minutos. Ele funciona entre *smartphones* que tenham o aplicativo instalado, através do envio criptografado das informações de contágio, por meio do uso do Bluetooth de baixa energia. O Ministério também destacou que "além de segura, a nova funcionalidade conserva a privacidade, tanto do paciente infectado como da pessoa que recebe a notificação da possível exposição com o caso confirmado para a COVID-19", já que o aplicativo funciona sem rastrear os movimentos da pessoa testada positiva e sem conhecer sua identidade ou a identidade com quem ela entrou em contato. Além disso, "todos os dados são criptografados e salvos localmente no *smartphone*" e "os dados só ficam disponíveis na ferramenta durante o período de 14 dias" (APLICATIVO, 2020).

Embora o conhecimento e a capacidade de inovação de Apple e Google estejam ajudando a mitigar os efeitos da pandemia, é necessário criticar a invasão da esfera pública por atores privados, uma vez que ela pode implicar a perda de autonomia por parte dos Estados e das sociedades na definição dos usos destas tecnologias. Com efeito, a dependência de atores privados para o desenvolvimento de novas tecnologias contribui não só para a subordinação técnica, mas também para a subordinação cultural, econômica, social e política a algumas poucas empresas sediadas principalmente nos EUA.

Neste sentido, o desenvolvimento desta API faz parte de um fenômeno mais amplo em que as grandes empresas de tecnologia penetram em todas as esferas da vida social. O risco inerente a essa transgressão de esferas da vida social é a concentração de vantagens e poder em alguns poucos atores, como afirma Sharon (2020). No caso da API Apple-Google, as empresas aproveitaram suas vantagens

legítimas na esfera da produção de bens digitais para acessar, de modo ilegítimo, as esferas da saúde e da política. Esta invasão na esfera da saúde pode levar à reorganização da medicina de acordo com os valores e interesses de empresas privadas, enquanto a invasão na esfera da política consolida a dependência do Estado de empresas privadas para a entrega de bens públicos essenciais, levando à formulação de políticas públicas por atores não eleitos.

Ademais, Sánchez-Monedero (2021) ressalta que estas duas empresas estadunidenses podem se permitir o desenvolvimento de uma tecnologia deste tipo, centrada na privacidade dos usuários, justamente porque *já possuem* o acesso à maior parte dos dados dos usuários de seus produtos e serviços. O modelo de negócios destas plataformas, como afirma Srnicek (2017), visa cobrir todas as áreas da vida humana em que elas possam intermediar relações entre oferta e procura, porque isso garante a extração de uma maior variedade de dados de seus usuários, o que lhes garante maior poder de mercado. Portanto, a transgressão de esferas da vida social é uma estratégia destas empresas para concentrar uma variedade cada vez maior de dados, que são utilizados na modulação do comportamento humano como meio de produzir receitas e controle de mercado.

Essa estratégia também consolida a crença de que, dado o melhor algoritmo, a tecnologia pode solucionar todos os problemas humanos e, em consequência, naturaliza a adoção de diversos sistemas de monitoramento e de automação de decisões. Como consequência desta crença, muitos governos nacionais têm tratado a pandemia de COVID-19 como um problema logístico ou de gestão das pessoas, que pode ser solucionado com o rastreamento dos contatos e o controle de deslocamentos, em detrimento de uma estratégia que encare a pandemia como uma crise sanitária, que exige investimentos para aumentar a capacidade de resposta de agentes, instituições e autoridades de saúde (SALVO, 2021).

Conclusão

O rastreamento de contatos é uma ferramenta utilizada para limitar a disseminação de doenças infecciosas. O uso de tecnologias digitais para este fim pode servir de apoio para as políticas públicas de controle da pandemia, mas não pode substituir os investimentos do Estado e da sociedade em pessoal capacitado, em recursos para testes diagnósticos ou no oferecimento de leitos em hospitais.

Em um contexto em que cada vez mais setores da sociedade estão passando por processos de digitalização, a *expertise* técnica que confere às grandes empresas de tecnologia uma vantagem legítima na esfera dos bens digitais, está atualmente sendo convertida em vantagens ilegítimas em outras esferas, como a esfera da saúde e a esfera da

política. Com efeito, como conclui Sharon (2020), Apple e Google não só contribuíram com seus conhecimentos técnicos na formulação de uma resposta à pandemia de COVID-19, mas também determinaram qual caminho poderia ser seguido, uma vez que definiram as condições de existência de aplicativos de rastreamento de contatos e como eles podem ser usados por governos nacionais.

Os países do Sul Global possuem menor capacidade de geração e gestão de dados sobre seus cidadãos, de modo que as empresas privadas passam a preencher a lacuna técnica deixada pelo Estado. Mas, a atuação de empresas privadas é sempre condicionada pela busca de lucros, e a monetização de dados pessoais é o modelo de geração de receita de cada vez mais empresas ligadas à economia digital. Portanto, devemos estar atentos para os usos que são feitos de nossos dados.

Referências

APLICATIVO Coronavírus-SUS vai alertar contatos próximos de pacientes com COVID-19. **Ministério da Saúde: DATASUS**, 2020 [Publicado em 31/07/2020; atualizado em 04/08/2020] Disponível em: https://datasus.saude.gov.br/aplicativo-coronavirus-sus-vai-alertar-contatos-proximos-de-pacientes-com-covid-19/ Acesso em 30/05/2021

APPLE and Google partner on COVID-19 contact tracing technology. **Apple Newsroom,** 2020 [Publicado em 10/04/2020] Disponível em: https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ Acesso em 30/05/2021

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União** de 15/08/2018. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=13709&ano=2018&ato=293QzZ61UeZpWT79e Acesso em 30/05/2021

BRASIL. Decreto Nº 10.212, de 30 de janeiro de 2020. Promulga o texto revisado do Regulamento Sanitário Internacional, acordado na 58ª Assembleia Geral da Organização Mundial de Saúde, em 23 de maio de 2005. **Diário Oficial da União** de 30/01/2020. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.212-de-30-de-janeiro-de-2020-240647604 Acesso em 30/05/2021

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**, Março de 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em 14/03/2021

COULDRY, Nick; MEJIAS, Ulises Ali. **The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism**. Stanford: Stanford University Press, 2019

DATA PRIVACY BRASIL. **Relatório Privacidade e Pandemia: Recomendações Para o Uso Legítimo de Dados no Combate à Covid-19**, 2020 [publicado em 13/04/2020] Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2020/04/relatorio_privacidade_e_pandemia_final.pdf Acesso em 20/05/2021

FLORIDI, Luciano. **Information: A Very Short Introduction**. New York: Oxford University Press. Livro eletrônico não paginado. 2010

GARCIA DOS SANTOS, Laymert. **Politizar as novas tecnologias: o impacto sociotécnico da informação digital e genética**. São Paulo: Editora 34, 2003

GREENWALD, Glenn; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**, 2013 [Publicado em 7/06/2013]. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data Acesso em 20/05/2021

LUCIVERO, Federica; HALLOWELL, Nina; JOHNSON, Stephanie; PRAINSACK, Barbara; SAMUEL, Gabrielle; SHARON, Tamar. Covid-19 and Contact Tracing Apps: Ethical challenges for a social experiment on a global scale. **Journal of bioethical inquiry**, v. 17, n. 4, p. 835-839, 2020

MADEIRA, Ligia; PAPI, Luciana; GELISKI, Leonardo; ROSA, Taciana. Os estudos de políticas públicas em tempos de pandemia, **Blog DADOS**, 2020 [Publicado em 17/04/2020]. Disponível em: http://dados.iesp.uerj.br/os-estudos-de-politicas-publicas-em-tempos-depandemia/ Acesso em 20/05/2021

MAGALHÃES, Larissa G. de. A Pandemia e a Nova Ordem Sociodigital no Sul Global: O Caso de São Paulo. In: MILAN, Stefania; TRERÉ, Emiliano; MASIERO, Silvia (eds.). **COVID-19 from the margins: Pandemic invisibilities, policies and resistance in the datafied society**. Institute of Network Cultures, Amsterdam, 2021

RAHMAN, Mishaal. Here are the countries using Google and Apple's COVID-19 Contact Tracing API. **XDA Developers**, 2021 [Publicado em 25/02/2021] Disponível em: https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/ Acesso em 30/05/2021

SALVO, Philip di. Solutionism, Surveillance, Borders And Infrastructures In The "Datafied Pandemic". In: MILAN, Stefania; TRERÉ, Emiliano; MASIERO, Silvia (eds.). **COVID-19 from the margins: Pandemic invisibilities, policies and resistance in the datafied society**. Institute of Network Cultures, Amsterdam, 2021

SÁNCHEZ-MONEDERO, Javier. Riesgos e Incertidumbres en las Aplicaciones para el Rastreo de Contagios. In: MILAN, Stefania; TRERÉ, Emiliano; MASIERO, Silvia (eds.). **COVID-19 from the margins: Pandemic invisibilities, policies and resistance in the datafied society**. Institute of Network Cultures, Amsterdam, 2021

SHARON, Tamar. Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. **Ethics and Information Technology**, https://doi.org/10.1007/s10676-020-09547-x, julho de 2020

SRNICEK, Nick. **Platform capitalism**. John Wiley & Sons, 2017.

WIENER, Norbert. **Cibernética e Sociedade: o uso humano de seres humanos.** São Paulo: Editora Cultrix, 1968

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Nova York: Public Affairs, 2019

Submetido em: 2021-06-03.
Aprovado em: 2021-06-08.