

Dados pessoais, tecnologias emergentes e a pandemia de COVID-19: renovados desafios à privacidade

Bethânia de Araújo Almeida,¹ Danilo Doneda,² Maria Yury Ichihara,³ Gustavo Corrêa Matta,⁴ Manoel Barral-Netto,⁵ Elaine Rabello,⁶ Fabio C. Gouveia,⁷ Mauricio Lima Barreto⁸

-
- ¹ Socióloga, mestre em ciências sociais e doutora em saúde pública. Servidora da Fundação Oswaldo Cruz (Fiocruz), atua no Centro de Integração de Dados e Conhecimentos para Saúde (Cidacs). Dentre as suas áreas de interesse, estão a governança de dados para pesquisa na área da saúde pública e a sociologia da ciência intensiva no uso de dados.
 - ² Doutor em Direito Civil pela Universidade Estadual do Rio de Janeiro (UERJ), professor no Instituto Brasileiro de Direito Público (IDP) e advogado. Diretor do Centro de Direito, Internet e Sociedade (Cedis) do IDP. Conselheiro indicado pela Câmara dos Deputados para o Conselho Nacional de Proteção de Dados e da Privacidade.
 - ³ Médica, doutora em Saúde Pública, professora colaboradora no Instituto de Saúde Coletiva (ISC), vice-coordenadora do Centro para Integração de Dados e Conhecimentos para Saúde (Cidacs). Atua em avaliação de determinantes e de políticas sociais usando grande volume de dados.
 - ⁴ Pesquisador titular em Saúde Pública da Escola Nacional de Saúde Pública Sergio Arouca (ENSP) da Fundação Oswaldo Cruz (Fiocruz). Coordenador da Rede Zika Ciências Sociais e do Eixo Impactos Sociais do Observatório Covid da Fiocruz. Atualmente, tem se dedicado ao estudo sobre as dimensões sociais, políticas e científicas das emergências em saúde pública no Brasil e no chamado "Sul Global".
 - ⁵ Médico e doutor em Patologia, professor titular aposentado da Faculdade de Medicina da Universidade Federal da Bahia (UFBA) e pesquisador titular da Fundação Oswaldo Cruz (Fiocruz) da Bahia, onde é chefe do Laboratório de Inflamação e Biomarcadores. Atua na área de imunologia das doenças infecto-parasitárias.
 - ⁶ Psicóloga, mestre e doutora em saúde pública. Pesquisadora convidada da Fundação Oswaldo Cruz (Fiocruz) e conselheira na área de saúde global do KIT Royal Tropical Institute, Holanda. Envolvida em educação e pesquisa sobre fortalecimento de sistemas de saúde em países em desenvolvimento.
 - ⁷ Doutor em Química Biológica (Educação, Gestão e Difusão em Biociências) pela Universidade Federal do Rio de Janeiro (UFRJ) e Tecnologista em Saúde Pública da Fundação Oswaldo Cruz (Fiocruz).
 - ⁸ Médico, mestre em Saúde Comunitária e doutor em Epidemiologia. Professor Emérito da Universidade Federal da Bahia (UFBA). Desde 2014, é Pesquisador Especialista da Fundação Oswaldo Cruz (Fiocruz) da Bahia, onde fundou e coordena o Centro de Integração de Dados e Conhecimentos para Saúde (Cidacs).
-

ALMEIDA, B. de A.; DONEDA, D.; ICHIHARA, M. Y.; MATTa, G. C.; BARRAL-NETTO, M.; RABELLO, E.; GOUVEIA, F. C. BARRETO, M. L. Dados pessoais, tecnologias emergentes e a pandemia de covid-19: renovados desafios à privacidade. In: BARRETO, M. L.; PINTO JUNIOR, E. P.; ARAGÃO, E.; BARRAL-NETTO, M. (org.). *Construção de conhecimento no curso da pandemia de COVID-19: aspectos biomédicos, clínico-assistenciais, epidemiológicos e sociais*. Salvador: Edufba, 2020. v. 2.

DOI: <https://doi.org/10.9771/9786556300757.033>

Introdução

Qualquer informação ou acontecimento no mundo natural ou social pode ser registrado e esses registros (dados) podem ser utilizados para diferentes propósitos. Com o estabelecimento de infraestruturas digitalizadas, ferramentas e modelos computacionais a partir da década de 1970, o acúmulo e processamento de grandes volumes de dados tornaram-se possíveis, em escala até então inimaginável. Na atualidade, tecnologias emergentes se entrelaçam com regimes de propriedade e comércio de novos tipos de dados disponibilizados por bilhões de pessoas ao redor do mundo à medida que a utilização de sistemas, aplicativos, plataformas de compras, mídia e redes sociais se tornaram cada vez mais presentes em nossas vidas. Dados se tornaram ativos cujo valor e importância dependem de negociações, interesses sociais, políticos e econômicos. (LEONELLI, 2019)

Dados são igualmente a base para a compreensão científica do mundo, pois subsidiam os achados e as interpretações das pesquisas sendo, portanto, as fontes fundamentais das evidências geradas pela investigação científica. A pesquisa científica tanto pode ser geradora de novos dados, como pode utilizar dados existentes e coletados com outros propósitos. Devido ao aumento

da disponibilidade de dados, o reuso de dados coletados de distintas fontes para pesquisa tem sido crescente na prática científica.

A pandemia de COVID-19 tem chamado a atenção pelos muitos desafios que apresenta nesse campo. Devido às incertezas quanto à convivência com o novo vírus, SARS-CoV-2, agente da pandemia de COVID-19, e as dificuldades em registrar com precisão, em especial o diagnóstico da infecção na população em geral, dados ganharam ainda mais relevância, principalmente os dados pessoais e sensíveis relacionados a comportamentos e a condições de saúde. Tecnologias digitais de rastreamento de sintomas, testagem, contatos e isolamento passaram a ser apresentadas como parte das estratégias de diferentes governos para entender, monitorar e conter a transmissão do vírus e reduzir a carga de doença. Além dos dados rotineiramente coletados pelo sistema de saúde, a coleta e processamento de dados através de aplicativos e dispositivos digitais passaram a ter um papel de destaque na averiguação do cumprimento de quarentena, de verificação probabilística de contágio, do gerenciamento de permissões para sair em público, entre outros aspectos da vida individual e coletiva. (ALMEIDA et al., 2020)

A despeito da importância das tecnologias digitais para o enfrentamento da pandemia de COVID-19, nem sempre tem havido transparência e prestação de contas à sociedade quanto aos tipos de dados coletados, proporcionalidade das operações de tratamento em relação à finalidade de uso, com quem as informações são compartilhadas, se esses dados serão armazenados após a emergência sanitária e sob quais condições, caso necessário. Tais práticas suscitam questionamentos éticos, legais e sociais acerca dos usos dessas ferramentas, pois podem ameaçar a privacidade e podem ter consequências, ainda que não intencionais, sobre direitos civis e políticos pelos potenciais riscos de abusos.

Os novos direitos dos cidadãos sobre seus dados têm sido amparados por leis gerais de proteção de dados, como o *General Data Protection Regulation* (GDPR) na Europa, ou a Lei Geral de Proteção de Dados (LGPD) brasileira. As leis gerais de proteção de dados são marcos importantes, e representam um elemento do processo de regulamentação de tecnologias orientadas por dados (*data-driven technologies*) que precisa avançar para assegurar direitos individuais e coletivos.

Dados pessoais para pesquisa científica em saúde pública de acordo com a Lei Geral de Proteção de Dados

No Brasil, a LGPD, Lei nº 13.709/2018 foi aprovada e sancionada em 2018, e entrou em vigor em setembro de 2020. A LGPD é um marco na regulamentação de dados pessoais no país, tendo sido criada com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A lei prevê que dados pessoais devam ser tratados de forma legal, justa e transparente em relação aos titulares dos dados, em decorrência dos potenciais riscos em relação aos seus direitos e liberdades. Para tal, a lei estabelece uma série de requisitos para que os dados pessoais possam ser legitimamente tratados e limites que devem ser observados no seu tratamento. A conformidade com a lei, portanto, exige que os responsáveis pelo tratamento dos dados pessoais organizem e mantenham registros acerca de qualquer atividade relacionada ao processamento desses dados sob sua responsabilidade, pois os titulares devem ter acesso facilitado às informações sobre qualquer tratamento pelos quais seus dados sejam submetidos. (BRASIL, 2018)

A autodeterminação informativa, com base na autonomia e vontade do titular, 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 dos dados. Existem situações em casos de emergência e de interesse público, como a saúde pública, em que o uso de dados pessoais é legítimo, não sendo necessário o consentimento do titular ou outra condição de legitimidade, desde que haja salvaguardas, proporcionalidade no uso dos dados para alcance das finalidades e especificidades relacionadas às credenciais dos órgãos autorizados a processar esses dados. Assim, a LGPD possui elementos capazes de facilitar a utilização de dados pessoais em políticas e sistemas idealizados para enfrentar a COVID-19. (DONEDA, 2020)

No seu artigo 4º, a lei brasileira estabelece seu escopo e define que não se aplica ao tratamento de dados pessoais realizado para fins exclusivamente jornalístico, artístico e também acadêmico. Para fim acadêmico, remete para os artigos 7º e 11º.

No artigo 7º, define as condições para uso dos dados pessoais, entre as quais, no seu inciso IV, “para a realização de estudos por órgão de pesquisa”, com a ressalva de que deve ser “garantida, sempre que possível, a anonimização”. O artigo 11 veda o uso de dados sensíveis, conforme definido na lei, são “dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural”, sendo possível apenas com o consentimento específico do titular. No entanto, também estabelece algumas exceções, entre as quais para a “realização de estudos por órgão de pesquisa, sendo garantida, sempre que possível, a anonimização”.

A LGPD aborda o tratamento de dados pessoais para pesquisa em âmbito institucional, pois se refere exclusivamente a órgãos de pesquisa definidos como

[...] órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. (BRASIL, 2018, art. 5.º, XVIII)

Além de ambiente controlado e seguro, a anonimização e a pseudoanonimização dos dados são definidas como as principais estratégias, entre outras, que deverão ser adotadas no tratamento dos dados para proteção da privacidade dos indivíduos.

A lei define anonimização como a “[...] utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”. (BRASIL, 2018, art. 5.º, XI) A lei não se aplica aos dados anonimizados. Caso a anonimização seja revertida, os dados passam a ser considerados dados pessoais e as disposições da lei são aplicadas.

Enquanto o conceito de pseudoanonimização é definido na lei como “[...] o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro”. (BRASIL, 2018, art. 13, § 4.º) Na lei, dados pseudoanonimizados são considerados dados pessoais pela possibilidade de rastrear os dados de volta ao indivíduo por meio do código-chave.

As atividades de pesquisa são consideradas enquanto um contexto específico de processamento de dados pessoais pela LGPD,

que deve equilibrar os direitos individuais e a busca pelo interesse público a partir da aplicação de medidas técnicas e organizacionais suficientes e adequadas para garantir a proteção dos dados e o mínimo possível de processamento, possibilitando que sejam alcançados os objetivos das pesquisas, reduzindo os riscos relacionados à sua utilização. A despeito de prever a proibição geral do processamento de dados pessoais sensíveis, existem exceções para prática de cuidados de saúde, saúde pública e alguns setores de pesquisa em que o tratamento é autorizado sob condições específicas. (DONEDA; ALMEIDA; BARRETO, 2019)

A LGPD tem um artigo específico que dispõe sobre estudos em saúde pública, o artigo 13, o qual estabelece que:

[...] os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudoanonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. (BRASIL, 2018)

A pesquisa em saúde possui longa tradição no uso de dados contendo informações pessoais para abordar questões científicas a partir de características da população, de dados laboratoriais, hospitalares, entre outros, orientada pelo embasamento ético e legal. Inclusive, a criação do Departamento de Informática do SUS (Datasus) em 1991, vinculado ao Ministério da Saúde, viabilizou o processamento, armazenamento e disponibilização de bancos de dados nacionais como hospitalizações, notificação de doenças infecciosas e mortes por parte de formuladores de política e

pesquisadores. Estímulo importante, no país, para pesquisas em saúde pública intensiva no uso de grandes bases de dados.

Lembramos ainda que pesquisas científicas que envolvem seres humanos, principalmente nas áreas da Saúde, Ciências Sociais e Humanas, recorrem aos marcos éticos para orientar o uso de dados pessoais e sensíveis. No Brasil, toda pesquisa envolvendo seres humanos requer aprovação do Sistema do Conselho de Ética em Pesquisa (CEP) e Conselho Nacional de Ética em Pesquisa (Conep), criado em 1996 com o objetivo de proteger o participante da pesquisa e assegurar que o estudo seja realizado de acordo com princípios éticos a partir de resoluções e normativas deliberadas pelo Conselho Nacional de Saúde (CNS). A avaliação ética de uma pesquisa baseia-se em um conjunto de fundamentos, entre os quais estão a relevância social da pesquisa e o compromisso com o máximo de benefícios e o mínimo de danos e riscos.

O Sistema CEP/Conep reconhece o Termo de Consentimento Livre e Esclarecido (TCLE) do participante ou de seu responsável legal como o principal instrumento visando demonstrar a autonomia e a liberdade de participação a partir de esclarecimentos sobre a natureza da pesquisa, seus objetivos, métodos, benefícios previstos, potenciais riscos e incômodos que a participação no estudo poderão acarretar, facultando a participação voluntária, a requisição de informações adicionais e a retirada do consentimento a qualquer tempo sem prejuízo algum ao participante.

A crescente produção e uso de dados em um mundo cada vez mais digitalizado fez emergir novas formas de produção de conhecimento, que usam informações que não foram originalmente coletadas para fins de pesquisa, mas que podem ser preparadas e integradas para responder perguntas científicas. Nesses casos, em virtude da impossibilidade de obtenção de termo de consentimento, a dispensa poderá ser solicitada pelo pesquisador ao Sistema CEP/Conep, desde que seja justificada. O pedido de dispensa deve ser

fundamentado e avaliado quanto às responsabilidades assumidas pelos pesquisadores para mitigar riscos e assegurar os direitos dos participantes, incluindo procedimentos voltados à confidencialidade e à privacidade dos titulares dos dados, à proteção da imagem e a não estigmatização de indivíduos ou grupos.

Na LGPD, o respeito a padrões éticos é parte da legalidade do processamento de dados pessoais e sensíveis em pesquisa, que deverá ser consistente com a normatização específica do setor, que no caso será de responsabilidade do Sistema CEP/Conep e da Autoridade Nacional de Proteção de Dados em diálogo com a comunidade científica para definir o que necessitará ser regulado e normatizado como desdobramento da lei. (DONEDA; ALMEIDA; BARRETO, 2019)

A conformidade com as leis gerais de proteção de dados para pesquisa científica e, em particular, a pesquisa em saúde pública, portanto, requer tecnologias, infraestrutura e pessoal especializado para que os dados possam ser tratados de forma lícita, justa e responsável em relação aos titulares dos dados, além de prever o princípio da responsabilização através de acompanhamento das atividades de processamento de dados pelas autoridades designadas, que poderão aplicar sanções quando houver descumprimento da lei.

Aspectos relacionados à privacidade, segurança da informação e finalidade do uso de dados contendo informações pessoais para pesquisa científica e de saúde pública estão presentes na LGPD e nas regulamentações éticas do Sistema CEP/CONEP. A LGPD é uma lei geral voltada ao estabelecimento de princípios e conceitos norteadores para preservar o equilíbrio entre a necessidade de proteger efetivamente os direitos dos titulares dos dados, ao mesmo tempo em que permite o processamento de dados pessoais e sensíveis para determinados fins.

Ao considerar que dados podem ser utilizados e compartilhados por diferentes pessoas e organizações simultaneamente, no caso da utilização de dados pessoais para o enfrentamento da COVID-19, as questões principais a serem harmonizadas giram em torno da governança responsável dos dados baseada na transparência, aplicação de técnicas robustas de anonimização, credenciais dos órgãos autorizados a processar e utilizar esses dados de acordo com a finalidade de uso e responsabilização em caso de negligência ou uso indevido.

Tecnologias orientadas por dados e a pandemia de COVID-19

A produção de conhecimento centrada em dados requer transparência acerca do processo de coleta, tratamento e organização dos dados, pois auxiliam na articulação e multiplicidade de situações para que os dados possam ser organizados e interpretados adequadamente evitando a utilização de dados não representativos ou tendenciosos. Na pesquisa científica, dados são tratados, visualizados, interpretados a partir de modelos e teorias próprios de disciplinas e áreas de conhecimento para servir como confirmação ou refutação empírica da hipótese do estudo. A coerência e validação das observações e experimentos são demonstradas através dos dados que corroboraram os achados e que são avaliados por pares.

Para evitar abusos ou consequências não intencionais em torno do uso dos dados durante a pandemia de COVID-19, existe a defesa de que experiências acumuladas na proteção de dados em crises humanitárias visando o processamento justo de dados de pessoas em situação de vulnerabilidade poderão ser utilizadas. O manual sobre proteção de dados em ações humanitárias

do Comitê Internacional da Cruz Vermelha é mencionado por incluir o uso de aplicativos de localização, biometria e serviços em nuvem. Mencionam, dentre outras coisas, que dados de localização podem ser muito úteis para análise epidemiológica, mas que em contextos de crise política também poderão ser utilizados para localizar indivíduos e grupos, colocando em risco a democracia e os direitos humanos. (ZWITTER; GSTREIN, 2020)

Outros recursos apontam para a centralidade do uso de dados e da experiência acumulada em fazer convergir o seu uso para fins humanitários com a proteção de dados, como na resolução adotada pela Global Privacy Assembly⁹ – que reúne praticamente todas as autoridades nacionais de proteção de dados – ou a documentação arremetida a respeito, bem como é refletido no trabalho do projeto Global Pulse, da Organização das Nações Unidas (ONU).¹⁰

Os usos intensivos de dados apoiados na ciência de dados e aprendizagem de máquina são recursos poderosos na busca de respostas e soluções por parte de governos, cientistas e autoridades sanitárias para ampliar a capacidade de diagnóstico, manejo clínico e reabilitação dos casos como também para subsidiar estratégias de prevenção e alocação de recursos direcionados aos setores e grupos mais vulneráveis, dentre outras possibilidades. Nessa perspectiva, aspectos políticos e regulatórios relacionados à privacidade, segurança da informação e direitos humanos fundamentais precisam ser abordados, harmonizados e implementados em relação ao desenvolvimento e utilização de tecnologias orientadas por dados, principalmente no caso da pandemia de COVID-19 em

⁹ Ver em: <https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-International-Aid-EN.pdf>.

¹⁰ Ver em: <https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/>.

que a coleta e o processamento dos dados acontecem em nome da saúde e do interesse público.

O estabelecimento de novos conceitos jurídicos acerca dessas operações é parte do processo de regulamentação, pois nomear é importante para a compreensão do fenômeno e para orientar as lógicas sociais e econômicas que conformam os usos que damos a essas tecnologias. (ZUBOFF, 2019) Narrativas, discursos e conceitos sobre dados orientam a forma como pensamos sobre eles. Portanto, contribuem para a compreensão social e coletiva acerca de como os dados pessoais são percebidos e utilizados pela sociedade (PATEL, 2020), seja como matéria-prima (*commodities*), produtos privados ou como bens públicos. O estabelecimento de conceitos nos ajuda a entender e a lidar com a complexidade dinâmica dos fenômenos sociais à medida que surgem ou se estabelecem.

Empresas de tecnologia como Google e Facebook possuem considerável parcela dos dados pessoais gerados no mundo, como também os meios para extrair o máximo de valor deles. Poder cada vez maior dado o crescente volume de dados gerados pela migração do uso de computadores para o uso de celulares, que através de aplicativos coletam continuamente dados sobre nossas localizações e comportamentos. Lembra-nos ainda que os dados das pessoas são coletados de forma gratuita, enquanto os métodos de processamento e extração de informações desses dados são patenteados. (ZUBOFF, 2018, 2019) Essas empresas têm se tornado ainda mais poderosas durante a presente pandemia de COVID-19, pelo aumento exponencial das atividades *on-line* e consequente aumento na geração e coleta de dados digitais dos cidadãos do mundo inteiro. (KIND, 2020) Em virtude da falta de regulamentações específicas para o setor de tecnologias orientadas por dados, responsabilidades e obrigações na utilização de tecnologias digitais como estratégia de enfrentamento da pandemia de COVID-19 precisam ser claramente estabelecidas. Por exemplo, no caso de

tecnologias de rastreamento de contato (*Contact Tracing*), que ameaçam a lógica da privacidade pelo constante monitoramento e vigilância, porém permitidas como casos excepcionais para auxiliar na busca de respostas e soluções para a crise sanitária e humanitária que vivemos.

Nesse contexto, duas gigantes do setor, Apple e Google, firmaram parceria, visando garantir a interoperabilidade entre os sistemas iOS e Android, para criação de uma ferramenta de rastreamento para a COVID-19. (NEWSROOM, 2020) Em termos gerais, essas soluções, que entram na classificação de sistemas de *Contact Tracing*, funcionam com a troca de identificadores anônimos entre telefones próximos via *bluetooth*, após a instalação de um aplicativo disponibilizado pela autoridade de saúde nacional ou eventualmente pelo próprio sistema operacional, a depender de como opera a solução. Quando uma pessoa tiver resultado positivo para o coronavírus, deverá fazer esse registro no aplicativo, que o transmitirá para as autoridades de saúde do seu respectivo país. Em seguida, as pessoas com as quais teve contato nos 14 dias anteriores serão alertadas que estiveram em contato com alguém – que não será identificado – que apresentou diagnóstico positivo para o vírus. (PANZZARINO, 2020) Como se trata de tecnologias que ainda estão em fase de desenvolvimento e amadurecimento, há diferenças entre implementações que, com o passar do tempo, podem demonstrar ser muito significativas.

Essas tecnologias emergentes têm sido baseadas em modelos centralizados ou descentralizados. Os modelos descentralizados, como os do *Pan-European Privacy-Preserving Proximity Tracing*¹¹ (PEPP-PT) e *Decentralized Privacy-Preserving Proximity Tracing*¹² (DP-3T) fazem uso de *bluetooth* de baixa energia para troca por

¹¹ Ver em: <https://github.com/pepp-pt/pepp-pt-documentation>.

¹² Ver em: <https://github.com/DP-3T/documents>.

proximidade de chaves criptografadas e visam impedir que os dados sejam utilizados para outros propósitos que não aqueles relacionados ao rastreamento de contatos. Ao remover o aplicativo, os dados armazenados serão excluídos. Já nos sistemas centralizados, os dados são armazenados em um banco de dados central, o que gera maiores incertezas acerca de possíveis usos, para além das finalidades da coleta, sejam durante ou após a pandemia. (CONTACT..., 2020)

Questões e desafios relacionados à confiança nas instituições responsáveis pelo processamento de dados contendo informações pessoais, sejam públicas ou privadas, são colocadas. Surgem também desconfianças e indagações que não visam impedir o uso dos dados para responder à pandemia, mas auxiliar no estabelecimento de salvaguardas para que haja equilíbrio entre interesses diversos e, mesmo, conflitantes. Em sociedades solidamente democráticas, existem instituições que poderão acompanhar e estabelecer limites sobre a atuação do Estado, porém leis e regulações voltadas ao controle das ações de empresas de tecnologias que lidam com tais dados, são ainda incipientes.

Os direitos de indivíduos, comunidades, grupos e populações a quem os dados se referem não estão claramente estabelecidos no desenvolvimento e utilização de tecnologias orientadas por dados. Algoritmos são baseados em modelos criados para levar em consideração algumas características, variáveis em detrimento de outras no conjunto de dados, podendo ter vieses que podem reproduzir desigualdades como etnia, gênero e classe social por exemplo. (WILLIAMS; BROOKS; SHMARGAD, 2018) Adicionalmente, além de aspectos éticos e legais, a integração e uso de dados de distintas fontes perpassam por aspectos metodológicos e sociais com o intuito de evitar interpretações equivocadas, que terão impactos na vida das pessoas.

No que tange às parcerias entre governos e empresas de tecnologia para o desenvolvimento de aplicativos que permitem a coleta de dados pessoais, como localização, contatos e dados de saúde para conter a pandemia de COVID-19, os termos e condições dos contratos precisam ser publicizados, particularmente no que concerne às responsabilidades e processos de tomada de decisão para evitar a comercialização de dados, manipulação de comportamentos e abusos de vigilância, por exemplo. A transparência e prestação de contas à sociedade são essenciais, principalmente em relação às empresas de tecnologia, para que haja transparência e legitimidade no processamento de dados para agir em nome de governos e da população. (NUFFIELD COUNCIL ON BIOETHICS; ADA LOVELACE INSTITUTE, 2020)

Dados coletados, compartilhados e utilizados em nome da saúde pública, especialmente por empresas privadas ou através de parcerias público-privadas, precisam ter termos e condições claros e transparentes sobre os propósitos de acesso, compartilhamento, usos e responsabilizações. Modelos de governança de dados mais justos, responsáveis e sustentáveis, que protejam e defendam princípios éticos e regulatórios, ampliam a confiança dos indivíduos e da sociedade na utilização de seus dados para responder a situações de legítimo interesse público. Aspectos relacionados ao direito à privacidade, direito à proteção de dados pessoais e direitos de grupos não inviabilizam o uso de dados pessoais e a possibilidade de seu uso para responder à pandemia. (ALMEIDA et al., 2020)

Considerações finais

Coleta, processamento e análise de dados, incluindo dados pessoais, são centrais e universais nas ações de saúde pública e,

muito claramente, nas ações de controle de uma pandemia com a que atualmente nos assola. Entretanto, o estabelecimento de um sistema de governança de dados, de forma ética, transparente, responsável e equitativa, é também uma demanda global que não pode ser enfrentada por um único país, jurisdição ou disciplina. O uso de tecnologias digitais para responder aos desafios colocados pela pandemia de COVID-19 pode ser uma oportunidade, não apenas para conter a pandemia, mas também para discutirmos e superarmos os atuais dilemas éticos e sociais de um mundo que passou a ser orientado por dados, com imensas assimetrias de poder e conhecimento em favor de grandes empresas de tecnologia que dominam o setor.

Tecnologias que utilizam dados pessoais como estratégias de enfrentamento da pandemia demonstram que os dilemas não são circunscritos à emergência sanitária, mas que se tornaram mais evidentes com ela. Dilemas que demandam uma ação coletiva e uma abordagem interdisciplinar.

Concebemos que a definição de conceitos e de valores norteadores são centrais para o estabelecimento de políticas, regulamentações e recomendações práticas na defesa da privacidade dos indivíduos, da autonomia da coletividade e dos direitos e deveres entre aqueles que desenvolvem, utilizam e que são impactados por essas tecnologias. Estruturas de governança adequadas precisam coordenar e equilibrar distintos interesses e motivações, possuir mecanismos de proteção contra abusos e de responsabilização caso estes ocorram. A tecnologia é uma ferramenta, e seus usos, aplicações e efeitos assumem formas distintas, a depender das lógicas sociais, políticas e econômicas e dos valores que as orienta. Existindo, portanto, a necessidade de criação de enquadramentos para reflexão e ação acerca da governança de tecnologias emergentes que utilizam dados pessoais em um mundo cada vez mais digitalizado, pois são recursos poderosos na busca

de respostas para a atual crise humanitária e sanitária provocada pela COVID-19 e também para outros desafios sanitários e sociais, sejam eles atuais ou futuros.

Referências

ALMEIDA, B. A. *et al.* Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 25, supl. 1, p. 2487-2492, 2020. Disponível em: <https://www.scielo.br/pdf/csc/v25s1/1413-8123-csc-25-s1-2487.pdf>. Acesso em: 6 jun. 2020.

BRASIL. Lei nº 13.079, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 4 out. 2020.

CONTACT Tracing: to centralise or not centralise, that is the question. London, May 2020. Disponível em: <https://www.adalovelaceinstitute.org/contact-tracing-to-centralise-or-not-to-centralise-that-is-the-question/>. Acesso em: 1 jun. 2020.

DONEDA, D. A proteção de dados em tempos de coronavírus. *Opinião e Análise*, São Paulo, 20 mar. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020>. Acesso em: 16 abr. 2020.

DONEDA, D.; ALMEIDA, B. de A.; BARRETO, M. L. Uso e proteção de dados pessoais na pesquisa científica. *Revista Direito Público*, Brasília, DF, v. 16, n. 90, p. 179-194, 2019.

KIND, C. *What will the first pandemic of the algorithmic age mean for data governance*. London, 2 Apr. 2020. Disponível em: <https://www.adalovelaceinstitute.org/what-will-the-first-pandemic-of-the-algorithmic-age-mean-for-data-governance/>. Acesso em: 16 abr. 2020.

LEONELLI, S. Data – from objects to assets. *Nature*, [s. l.], v. 574, p. 317-320, 2019. Disponível em: <https://www.nature.com/articles/d41586-019-03062-w>. Acesso em: 6 jan. 2020

NEWSROOM. *Apple e Google formam parceria para tecnologia de rastreamento de contato com COVID-19*. São Paulo, 10 abr. 2020. Disponível em: <https://www.apple.com/br/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>. Acesso em: 14 maio 2020.

NUFFIELD COUNCIL ON BIOETHICS AND ADA LOVELACE INSTITUTE. *Webinar - Beyond the exit strategy: ethical uses of data-driven technology in the fight against COVID-19*. London, 20 Apr. 2020. Disponível em: <https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-/strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19>. Acesso em: 24 abr. 2020.

PANZZARINO, M. Apple and Google are launching a joint COVID-19 tracing tool for iOS and Android. *Extra Crunch*, [s. l.], 10 Apr. 2020. Disponível em: <https://techcrunch.com/2020/04/10/apple-and-google-are-launching-a-joint-covid-19-tracing-tool/>. Acesso em: 24 abr. 2020.

PATEL, R. *Changing the Data Governance Ecosystem – through narratives, practices and regulations*. London, 23 Jan. 2020. Disponível em: <https://www.adalovelaceinstitute.org/changing-the-data-governance-ecosystem-through-narratives-practices-and-regulations/>. Acesso em: 27 fev. 2020.

ZUBOFF, S. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs, 2018.

ZUBOFF, S. 'The goal is automate us': welcome to the age of surveillance capitalism. [Entrevista cedida a] John Naughton. *The Guardian*, [s. l.], 20 Jan. 2019. Disponível em: <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook>. Acesso em: 24 abr. 2020

ZWITTER, A.; GSTREIN, O. J. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action*, London, v. 5, n. 1, 2020. Disponível em: <https://doi.org/10.1186/s41018-020-00072-6>. Disponível em: Acesso em: 24 maio 2020.

WILLIAMS, B. A.; BROOKS, C. F.; SHMARGAD, Y. How algorithms discriminate based on data they lack: Challenges, solutions, and policy implications. *Journal of Information Policy*, New York, v. 8, n. 78, p. 78-115, 2018. Disponível em: <https://doi.org/10.5325/jinfopoli.8.2018.0078>. Acesso em: 22 jan. 2019.