LIÇÕES E DESAFIOS DA PANDEMIA DE COVID-19 PARA A PROTEÇÃO DE DADOS PESSOAIS

Carlos Affonso Pereira de Souza[1]
Janaina Costa[2]
João Víctor Vieira Carneiro[3]

RESUMO

A pandemia ocasionada pelo vírus da COVID-19 trouxe consigo relevantes problemas para a proteção de dados pessoais. Por um lado, a necessidade de distanciamento social acelerou a já crescente virtualização das relações sociais e de trabalho e intensificou a coleta e tratamento de dados. A excepcional gravidade da crise sanitária motivou a adoção de soluções tecnológicas para a tutela da saúde coletiva, sobretudo como forma de monitoramento do isolamento social. No caso brasileiro, tem-se como particularidade o estado embrionário da cultura de proteção de dados, posto que a primeira lei nacional sobre a matéria entrou em vigor após o advento da pandemia. Neste cenário, tecem-se aqui comentários sobre três pontos pertinentes ao debate. Primeiramente, aponta-se que o uso de dados é de grande relevância na formulação de políticas públicas eficazes, inclusive no âmbito da saúde. Em seguida, argumenta-se como a disciplina jurídica da proteção de dados pessoais serve como freio a abusos e excessos no tratamento de dados de saúde. Por fim, indicam-se alguns exemplos nacionais e internacionais do uso de tecnologias no combate à pandemia, de modo a ilustrar como o contexto traz novos riscos à privacidade e à tutela dos dados pessoais. O caminho percorrido revela que a proteção de dados adentra um novo paradigma, trazendo ao direito brasileiro, em um contexto peculiarmente problemático, o desafio da consolidação de uma cultura e de seu correspondente anteparo jurídico.

PALAVRAS-CHAVE: Privacidade; Proteção de Dados; Coronavírus; Contact tracing; Vigilância epidemiológica.

1 INTRODUÇÃO

O advento da pandemia de Covid-19 contribuiu para acelerar mudanças profundas nas dinâmicas sociais. Um dos principais impactos da crise sanitária foi a virtualização de grande parte das relações, trocando a comunicação presencial pelo acesso ao espaço digital proporcionado por diversas ferramentas. A sala de aula, de reuniões, e até mesmo a sala de estar

[1] Professor da Universidade do Estado do Rio de Janeiro (UERJ). Diretor do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Professor visitante da Universidade de Ottawa. Pesquisador afiliado ao Information Society Project, da Yale Law School. Advogado.
[2] Advogada. Pós-graduanda em Direito Digital (UERJ); Mestre em Desenvolvimento Econômico e Social pelo IEDES - Paris 1 Panthéon-Sorbonne; Bacharel em Direito (UFMG). Pesquisadora sênior da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).
[3] Graduando em Direito pela Universidade Federal do Paraná (UFPR). Pesquisador do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio) e do Grupo de Estudos de Direito Autoral e Industrial (GEDAI-UFPR).

se converterem em espaços virtuais. O distanciamento social, portanto, converteu grande parte de nossas interações cotidianas em um incessante tráfego de dados pela Internet.

Esse cenário é apenas um dos motivos que torna necessário refletir sobre o legado que a pandemia deixou para a proteção da privacidade e dos dados pessoais. Outro relevante aspecto diz respeito às medidas adotadas no controle da pandemia. O legítimo objetivo de proteger vidas fez com que governos ao redor do mundo fechassem suas fronteiras, restringissem a circulação de pessoas e repensassem suas prioridades orçamentárias. Por outro lado, abriram-se brechas para a proliferação de políticas de vigilância.

Dados e estatísticas são imprescindíveis para a formulação de boas políticas públicas de saúde. Por outro lado, a excepcionalidade da atual crise sanitária revelou a urgência de controlar também o uso de certas informações. A gênese da proteção de dados pessoais enquanto tema regulatório se deu, várias décadas atrás, justamente com a finalidade de refrear a interferência estatal na privacidade dos cidadãos.

No caso brasileiro, entretanto, a primeira legislação compreensiva sobre o tema está ainda em sua primeira infância. Sancionada em 2018, a Lei Geral de Proteção de Dados (LGPD) só entrou em vigor em sua integralidade em agosto de 2021, mais de um ano após o início da pandemia. Assim, a cultura de proteção de dados começou a se instalar no país em um momento de excepcional gravidade.

Conforme visto adiante, as medidas de combate à pandemia levantaram questionamentos sobre a privacidade e a proteção de dados em vários países. No peculiar contexto em que se encontra a proteção de dados no Brasil, é preciso assegurar direitos para que a exceção não se torne regra.

2 A IMPORTÂNCIA DOS DADOS PESSOAIS NAS POLÍTICAS PÚBLICAS DE SAÚDE

Uma das principais potencialidades do uso de dados pela Administração Pública é subsidiar a elaboração de políticas públicas e de soluções que atendam às necessidades dos cidadãos de maneira eficaz. É a partir de análises, baseadas em evidências que é possível melhor compreender os problemas e anseios da população e buscar a melhor solução e alocação de recursos adequados. Como sintetiza Miriam Wimmer (2019, p. 127), “conhecer seus cidadãos é, para o Estado, pré-requisito para o desempenho de suas finalidades públicas”.

De fato, a capacidade dos administradores de saúde, pesquisadores e tomadores de decisão de planejar e desenvolver melhores tratamentos, responder a crises de saúde pública e distribuir recursos de forma eficiente depende de seu acesso a uma ampla variedade de dados confiáveis. Isso inclui informações clínicas no nível do paciente, bem como estatísticas sobre a prestação de serviços de saúde, desempenho de provedores de serviços de saúde, resultados do paciente, taxas e causas de mortalidade, surtos de doenças e tendências de saúde pública que possam ser analisadas ao longo do tempo.

No âmbito epidemiológico, por exemplo, informações atualizadas podem significar a diferença entre um surto local que é facilmente contido e uma epidemia (DYE et al. 2016). O tratamento e a pesquisa relacionados a doenças comuns, como câncer, também dependem de históricos de pacientes derivados de uma variedade de fontes (por exemplo, hospitais, laboratórios de patologia, radioterapia, registros de óbito, etc.).

O acesso a dados é crucial para a ação em saúde pública, e o seu rápido compartilhamento é crítico durante uma emergência de saúde pública como uma pandemia (DYE *et al*, 2016). A questão do acesso aos dados para controlar epidemias não surgiu com a emergência atual, mas já era destaque como elemento chave durante as epidemias de Ebola em 2013 na África Ocidental e de SARS em 2003 (WHITTY *et al*, 2015).

Os dados agregados e identificados de forma única teriam, portanto, o condão de otimizar uma ampla gama de questões de saúde pública e o monitoramento mais eficiente dos tratamentos dos pacientes, do progresso da doença e dos resultados das políticas públicas implementadas (WORLD BANK, 2018).

2.1 PROGRAMAS DE IMUNIZAÇÃO

A América Latina possui alguns dos registros computadorizados de vacinação mais antigos do mundo. Esses registros além de avaliar metas anuais consideradas isoladamente, otimizam a análise e o monitoramento detalhados de pessoas ou grupos não vacinados, facilitando, assim, estratégias de vacinação e gestão de recursos disponíveis mais adequados. Neste contexto, os dados pessoais são imprescindíveis para informar políticas públicas garantidoras do acesso equitativo e da distribuição eficiente das vacinas ─ assim, pode-se aferir a vulnerabilidade de determinadas populações com base em estatísticas geográficas ou de faixas etárias, por exemplo.

O uso de tecnologias de informação e comunicação (TICs) no apoio aos serviços de saúde têm aumentado exponencialmente nas últimas décadas em todo o mundo. A Organização Mundial da Saúde reconheceu esta tendência através da resolução WHA58.28 (OMS, 2005), que aponta como a ampliação de informações coletadas possibilita análises e pesquisas outrora impensáveis.

2.2 MEDIDAS DE MONITORAMENTO EPIDEMIOLÓGICO

Na elaboração de políticas públicas de saúde, o monitoramento epidemiológico é imprescindível. O combate a doenças como a dengue, por exemplo, exige grandes esforços por parte do Estado brasileiro. Conforme explicam Sarlet, Fernandes e Ruaro (2020, n.p.), as pesquisas de natureza epidemiológica buscam

> identificar determinantes de saúde e doença; descrever estados de saúde em populações; investigar surtos de doenças; comparar grupos; usar, com graus crescentes de complexidade, os conceitos de viés, de confusão e de interação e se familiarizar com as abordagens epidemiológicas para a inferência causal.

Deste modo, a coleta de informações populacionais se mostra essencial ao controle epidemiológico. Neste cenário, o controle da dengue no país suscitou extensa discussão jurídica em relação a seus impactos sobre a privacidade de cidadãos ─ afinal, as visitas de agentes de saúde configurariam desrespeito à inviolabilidade do domicílio? Após anos de controvérsia, a Lei nº 13.301/2016 passou a possibilitar o ingresso forçado dos agentes, demonstrando que o direito à privacidade do lar não se sobrepõe ao direito coletivo à saúde (ABREU, 2021).

Para além da privacidade do domicílio, o tratamento de dados pessoais, sobretudo com a crescente informatização do Sistema Único de Saúde,[4] também é um subsídio para o monitoramento epidemiológico. Com o advento da Lei Geral de Proteção de Dados (Lei 13.709/2018 ou LGPD), o uso de dados pessoais por órgãos de pesquisa para fins de estudos em saúde pública, inclusive epidemiológicos, recebeu novos contornos legais. Entre eles, merece destaque a vedação à revelação de dados pessoais no momento da divulgação dos resultados da pesquisa (Art. 13, §1º). Os dados de saúde recebem uma abordagem diferenciada também em outros contextos, conforme verifica-se a seguir.

[4] Cf. Aragão e Schiocchet (2020, p. 699) para uma lista extensa de sistemas de informação já desenvolvidos pelo SUS.

3 DADOS DE SAÚDE E A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Conforme apontado acima, os dados pessoais são essenciais para a formulação de políticas de saúde pública. Na terminologia adotada pela LGPD, os dados referentes à saúde são enquadrados no conceito de dados sensíveis. Para melhor compreensão da matéria, cumpre tecer alguns comentários preliminares sobre a proteção de dados pessoais no ordenamento jurídico brasileiro.

3.1 CONCEITOS GERAIS DE PROTEÇÃO DE DADOS PESSOAIS

A privacidade tornou-se objeto de tutela jurídica a partir do século XIX,[5] ainda que fosse socialmente valorizada antes de seu tratamento pelo direito. No entanto, com o avanço das tecnologias de informação e comunicação no século XX e a crescente digitalização de informações particulares, a proteção de dados pessoais surgiu como uma espécie de herdeira do direito à privacidade (DONEDA, 2011). O paradigma atual para a proteção de dados nos países da tradição de *civil law* pode ser associado ao Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, que guarda similaridades com a nossa LGPD.

A proteção de dados incide sobre os tratamentos realizados por controladores e operadores sobre os dados pessoais ─ isto é, quaisquer operações em meio físico ou digital que destes fazem uso. A estes agentes de tratamento é atribuída uma série de obrigações legais, à medida em que são garantidos aos titulares dos dados pessoais direitos sobre como terceiros utilizam dados que lhes digam respeito.

Ao contrário de correntes doutrinárias que situam os dados pessoais na categoria de bens jurídicos, a legislação europeia e brasileira adotam a teoria personalista, que os concebe como elementos da personalidade (ROCHFELD, 2018). Neste sentido, dados pessoais são definidos legalmente como informações relacionadas a pessoas naturais identificadas ou identificáveis (titulares) ─ nota-se, portanto, inequívoco vínculo entre o dado pessoal e a figura do titular deste dado. No contexto da saúde pública, todavia, uma categoria de dados pessoais revela ter grande importância: os dados sensíveis.

[5] Trata-se da proposição do conceito de *right to privacy* no direito estadunidense, já extensamente debatida na doutrina especializada, feita em 1890 por Samuel Warren e Louis Brandeis.

3.2 DADOS DE SAÚDE ENQUANTO DADOS PESSOAIS SENSÍVEIS

A confidencialidade dos dados referentes à saúde têm sido objeto de diversas regulações ao longo das últimas décadas. No direito estadunidense, por exemplo, adotou-se em 1996 o *Health Insurance Portability and Accountability Act* (HIPPA) para fixar padrões para o tratamento e o compartilhamento de dados no setor de saúde.[6] No âmbito da União Europeia, a *Recomendação R(97)5 de 1997 sobre a proteção de dados médicos* demonstrou, outrossim, a necessidade de instituir salvaguardas para o uso de dados pessoais em diversos setores da saúde, desde políticas públicas até pesquisas científicas na área médica.

No Brasil, a privacidade e a segurança dos registros médicos de pacientes também foi objeto da Resolução 1.821/2007 do Conselho Federal de Medicina (SARLET; FERNANDES; RUARO, 2021). No que tange aos dados mantidos pelo Sistema Único de Saúde (SUS), a Portaria de Consolidação nº 1/2017 do Ministério da Saúde, em seu artigo 231, II, também se atenta à necessidade de assegurar sua privacidade e segurança (BONAFÉ, 2019). Desta maneira, percebe-se que a tutela desta espécie de informação antecede a edição da LGPD.

Esta preocupação regulatória não surgiu sem motivos. Em certos contextos, os dados pessoais recebem maior proteção jurídica por serem mais suscetíveis a usos que levam à discriminação, estigmatização, exclusão ou segregação ─ aqui se insere o conceito de dados pessoais sensíveis (KONDER, 2020). Destarte, conforme sustenta Danilo Doneda (2019), o tratamento diferenciado conferido pelo GDPR e pela LGPD aos dados sensíveis decorre da tutela da igualdade material da pessoa humana, e não somente da tutela da privacidade.

Uma das situações em que um dado pessoal é considerado sensível é justamente quando se refere à saúde do seu titular. Nos termos da LGPD, dado sensível é aquele que diz respeito à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;" (Art. 5º, II).

Ao mencionar expressamente os *dados referentes à saúde* na definição acima, a LGPD confere a eles a tutela diferenciada que recebem os dados sensíveis. Por consequência, as hipóteses que possibilitam seu tratamento são mais estritas ─ e as obrigações imputadas aos agentes de tratamento, por sua vez, mais rigorosas.

[6] Sobre o HIPPA e seus limites, confira-se as ponderações de Robichau e Sanders (2014, p. 21-29).

Percebe-se que na lei brasileira os dados de saúde não são conceituados, sendo somente mencionados como espécie do gênero dados sensíveis. O GDPR, por outro lado, delimita em seu Art. 4(15) o significado de dados relativos à saúde ─ segundo o regulamento, tratam-se dos "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde".

De todo modo, a LGPD impõe que os dados sensíveis relativos à saúde do titular se sujeitam a regras específicas, contidas nos parágrafos do Artigo 11. Veda-se seu uso compartilhado para fins de vantagem econômica, exceto se fundado nas hipóteses relativas à prestação de serviços de saúde, assistência farmacêutica e assistência de saúde. Ademais, proíbe-se que operadoras de planos privados de saúde tratem tais dados para a seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

3.3 DADOS NÃO SENSÍVEIS E POSSÍVEIS INFERÊNCIAS SOBRE A SAÚDE DO TITULAR

Apesar do enquadramento distinto conferido aos dados de saúde, é possível que dados de outra natureza também revelem informações sobre a saúde do titular. Como aponta Bruno Bioni (2020), um dado "trivial" pode se transformar em um dado sensível, especialmente mediante o uso de tecnologias que possibilitam a correlação de uma grande quantidade de dados (por exemplo, mineração de dados ou *Big Data*).

Um notável exemplo ocorrido em 2012 ilustra o problema. A rede estadunidense de supermercados *Target* analisou padrões de consumo de suas clientes de modo a detectar quais delas podem estar grávidas. O aumento no consumo de produtos como loções hidratantes e certos tipos de suplementos vitamínicos, notou a empresa, se relacionava a certas etapas da gestação. A descoberta possibilitou o *marketing* direcionado para gestantes, como o envio de cupons para produtos para bebês. Em um caso específico, o envio de tais cupons por correio levou o pai de uma adolescente a descobrir sua gestação antes que ela tivesse a oportunidade de informá-lo do fato (HILL, 2012).

Deste modo percebe-se que, com as tecnologias adequadas, um conjunto de dados sobre certa pessoa pode gerar informações sobre sua saúde, o que pode ser feito por meio de processos de inferência, ao invés de mera observação direta (SKOPEK, 2018). Desta forma,

ocorrem *tratamentos sensíveis de dados*, capazes de "transformar dados inofensivos em informações potencialmente discriminatórias", como aponta Laura Schertel Mendes (2014, p. 76).

A LGPD aborda brevemente este problema em seu Art. 11, §1º, ao dispor que o tratamento de dados pessoais que possa revelar dados sensíveis, com risco de dano ao titular, também é sujeito às hipóteses de tratamento específicas para dados sensíveis. Dito de outra forma, mesmo os dados que não sejam *a priori* sensíveis poderiam assim ser considerados para os fins da Lei, quando levarem concretamente a informações de caráter sensível sobre os titulares (VIOLA; TEFFÉ, 2021).

Nessa direção, já existe doutrina no sentido de que o rol contido na definição de dados sensíveis pelo Art. 5º, II da LGPD não é taxativo, e sim exemplificativo (MULHOLLAND, 2019). Esse entendimento se baseia na percepção de que a *sensibilidade* de um dado pessoal é definida pelos efeitos potencialmente lesivos de seu tratamento (KONDER, 2020).

3.4 O VAZAMENTO DE DADOS DO SUS E A SEGURANÇA DE DADOS NA SAÚDE PÚBLICA

Se os dados sobre a saúde de determinada população possibilitam políticas públicas mais eficazes, seu mau uso traz grande potencial de danos a titulares. Disto decorre a necessidade de garantir um grau elevado de cautela em seu armazenamento e tratamento. Neste sentido, um dos princípios que norteiam a Lei Geral de Proteção de Dados é o princípio da *segurança*, definido pelo Art. 6º, VII como a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".[7]

Tão importante é a segurança para a proteção de dados pessoais que a lei destina um capítulo inteiro ao tema (Arts. 46-49). Segundo a norma, governos, empresas e outras entidades devem adotar medidas de segurança ─ tanto técnicas quanto administrativas ─ para

[7] Também merece menção o princípio da prevenção (Art. 6º, VIII), definido como a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

preservar suas informações em face de acessos não autorizados e outras situações ilícitas, sejam elas acidentais ou não (SOUZA, 2020).

No âmbito da saúde, um caso aponta os riscos inerentes ao tratamento de dados. Conforme apurado pelo Estado de S. Paulo, uma falha de segurança no sistema de notificações do Sistema Único de Saúde (SUS) em 2020 deixou expostos, por mais de seis meses, os dados de mais de 200 milhões de brasileiros (CAMBRICOLI, 2020).

Conquanto os dados pessoais expostos não fossem dados sensíveis ─ conforme a matéria, tratavam-se de dados como CPF, endereço e telefone ─ o incidente revela a necessidade da adoção de medidas de segurança mais robustas na saúde pública. A ausência de uma política nacional única de segurança de dados de saúde e a crescente limitação no orçamento do SUS apontam para um possível agravamento do problema (ARAGÃO; SCHIOCCHET, 2020). Deste modo, outra preocupação pertinente para a proteção de dados de saúde se refere justamente às medidas de segurança adotadas pelos agentes que realizam seu tratamento.

4 O TRATAMENTO DE DADOS NO CONTEXTO DA PANDEMIA DE COVID-19

Se o tratamento de dados pessoais se mostra imprescindível à formulação de políticas públicas eficazes na área sanitária, é necessário considerar que a pandemia de Covid-19 trouxe novas preocupações à área de proteção de dados. A crise global acarretada pelo coronavírus trouxe consigo a necessidade de controle sanitário em níveis nunca antes vistos. Disto decorre um aumento nas práticas de vigilância (*surveillance*), sobretudo governamentais, em face das dinâmicas sociais de (in)segurança, vulnerabilidade e risco ─ neste contexto, corpos e patógenos passam a ser medidos, monitorados e regulados (FRENCH; MONAHAN, 2020).

A (compreensível) urgência na contenção da propagação do vírus levou ao desenvolvimento e implementação de soluções tecnológicas para o gerenciamento da crise. Em certos países ─ conforme elabora-se a seguir ─ tecnologias de monitoramento permitiram considerável sucesso na limitação do número de casos de Covid-19 e óbitos decorrentes da virose. Entretanto, à medida em que se fiscalizam os cidadãos, sua privacidade é atingida. Disto advém um complexo problema: como estabelecer os limites entre a garantia do direito à privacidade e a execução de políticas públicas de saúde eficazes?

4.1 SAÚDE PÚBLICA VERSUS PROTEÇÃO DE DADOS NO BRASIL E NO MUNDO

O uso de dados pessoais em tecnologias empregadas no combate à Covid-19 instou autoridades e organizações a se manifestar sobre seus impactos sobre a privacidade. Como afirmou a Organização Mundial da Saúde (2020), a vigilância tecnológica na saúde pública é uma importante aliada de governos, mas também ameaça direitos e liberdades fundamentais ─ a vigilância se situa, portanto, em uma linha tênue entre o controle epidemiológico e o controle populacional em sentido amplo.

Outro ponto de especial pertinência diz respeito ao possível saldo pós-pandêmico para a proteção de dados. Consoante aponta Doneda (2020), diversos tratamentos de dados se justificam somente na atual emergência sanitária, de modo pontual e contextual. Corre-se o risco, portanto, de criar-se um legado de vigilância e hipertrofia do uso desses dados para finalidades diferentes após o fim dessa emergência.

Nesse sentido, as principais organizações internacionais de direitos humanos emitiram uma declaração conjunta enfatizando que o uso de ferramentas de tecnologia de vigilância deve receber limitações legais (KAYE, 2020). Especialistas da Organização das Nações Unidas (2020) alertaram que as medidas de emergência podem ser distorcidas por governos e instituições de segurança. Deste modo, afirmam que, para prevenir que tais abusos perdurem, torna-se fundamental que as medidas adotadas sejam restritas aos meios menos intrusivos possíveis para a proteção da saúde pública.

Nessa mesma toada, a Comissão Interamericana de Direitos Humanos (2020) ressaltou que mesmo as medidas excepcionais que envolvam a restrição de direitos devem ser pautadas pelos princípios internacionais de legalidade, necessidade, proporcionalidade e temporalidade, visando a "*impedir que medidas como o estado de exceção ou emergência sejam utilizadas de forma ilegal, abusiva e desproporcional, causando violações dos direitos humanos ou afetando o sistema democrático de governo*". Merece destaque, ademais, a orientação para a tutela da privacidade e da proteção dos dados da população afetada.

As regras estabelecidas por regulamentos como o GDPR e a LGPD já estabelecem parâmetros mínimos aplicáveis também ao contexto pandêmico. Neste sentido, o Comitê Europeu para a Proteção de Dados (2020a) reiterou a importância dos princípios do GDPR, destacando que o uso de dados pessoais no combate à pandemia deve ocorrer de modo a limitar

a quantidade de dados utilizados, bem como o período de seu tratamento e a adequação dele às finalidades informadas aos titulares.

O uso de dados de saúde já é viabilizado nas normas europeias e brasileiras, a depender da finalidade do tratamento. O Art. 9(2)i do GDPR possibilita o tratamento de dados de saúde se este "for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde". Em sentido semelhante, a LGPD possibilita o tratamento de dados sensíveis para a "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (Art. 11, II, f).

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2020) ressalta o papel das autoridades de proteção de dados para suprir incertezas normativas que impedem o uso de dados pessoais no enfrentamento à doença e suas decorrências. Mais de trinta autoridades europeias já se manifestaram publicamente neste sentido.[8]

Conquanto controle o uso de dados pessoais, a disciplina jurídica da proteção de dados não deve ser percebida como um obstáculo para a contenção da pandemia e seus efeitos. Como observado pela organização Global Privacy Assembly (2020), os princípios gerais da proteção de dados *possibilitam*, na verdade, o uso de dados pessoais em prol do interesse público, garantindo ao mesmo tempo salvaguardas aos direitos dos titulares.

4.2 SISTEMAS DE CONTACT TRACING E A EXPERIÊNCIA INTERNACIONAL

Sendo o SARS-CoV-2 um vírus transmissível por meio do ar, a proximidade física (breve ou prolongada) entre uma pessoa infectada e outra não-infectada sugere que esta última muito provavelmente tenha contraído o vírus. A partir desta lógica, tecnologias de *contact tracing* foram uma das soluções adotadas por governos para o controle da crise sanitária em seus territórios.

O *contact tracing* ─ expressão anglófona que pode ser traduzida como "rastreamento de contatos" – é uma técnica que busca identificar indivíduos que mantiveram contato próximo com uma ou mais pessoas infectadas. A realização do rastreamento de contatos prescinde de uma aplicação tecnológica ─ o *contact tracing* pode ser feito manualmente através

[8] Conforme levantamento realizado pelo Research Group on Law, Science, Technology & Society (2021).

da listagem e notificação de contatos por vias não automatizadas (LI, 2020). Todavia, a aplicação de métodos manuais de rastreamento de contatos é ineficiente e trabalhosa em cenários como o da pandemia de Covid-19, pois requer que cada pessoa recorde com quem esteve em contato recentemente (BARRAT *et al*, 2020). Soluções tecnológicas são, portanto, uma perspectiva mais eficaz.

À vista disso, nota-se que a implementação tecnológica do *contact tracing* pode ser feita de diversos modos. Com base no modo como são coletadas e armazenadas as informações, Ahmed *et al* (2020) identificaram abordagens centralizadas, descentralizadas e híbridas nas aplicações de *contact tracing* utilizadas durante a pandemia de coronavírus. Como apontam os autores, certas aplicações são desenvolvidas de modo a anonimizar os dados pessoais, o que garante um grau mais elevado de privacidade, ainda que nenhuma abordagem seja completamente imune a ataques maliciosos ou usos abusivos de dados pessoais.[9]

De qualquer forma, o método mais empregado na pandemia consistiu no uso da tecnologia *Bluetooth*, presente em todos os *smartphones* modernos, para detectar a proximidade física entre uma pessoa e outros usuários de celulares, registrando, por meio de *tokens* digitais armazenados em seu aparelho, uma lista de cada um destes usuários. Desta maneira, após confirmada a infecção de determinada pessoa, os indivíduos com quem teve contato recente recebem uma notificação alertando sobre a ocorrência de tal contato, bem como a consequente possibilidade de contágio (MARTINEZ-MARTIN *et al*, 2020). Entretanto, a efetividade dessa solução depende da identificação de pessoas infectadas; em outros termos, a medida requer uma testagem em massa para ser eficiente, o que não ocorreu em todos os países.

4.2.1 Aplicativos de *contact tracing* ao redor do mundo

Após a OMS reconhecer a Covid-19 como uma pandemia em março de 2020, diversas medidas foram prontamente adotadas por governos, como o fechamento de fronteiras e a restrição de aglomerações.[10] No mesmo mês, o aplicativo *TraceTogether*, lançado em Singapura, chamou a atenção internacional como uma das primeiras implementações digitais de *contact tracing* contra a nova doença. Após instalado em um celular, o aplicativo usou a tecnologia *Bluetooth* para registrar a proximidade entre pessoas mediante o uso de *tokens*

[9] A orientação do Comitê Europeu para a Proteção de Dados (2020b) é dar preferência ao uso de dados anônimos em aplicações de *contact tracing*.
[10] Cf. Hale *et al* (2021) para uma análise compreensiva das políticas de resposta à pandemia.

armazenados tanto no dispositivo quanto em um servidor do governo (DUBOV; SHOPTAWB, 2020).

Outra forma de implementação utilizou também dados de localização dos dispositivos, como se verificou nos aplicativos de países como Israel e Coreia do Sul. Esta abordagem foi alvo de críticas a partir do princípio da minimização ─ o argumento aponta a desnecessidade de saber *onde* alguém esteve para provar seu contato com uma pessoa infectada (ABELER *et al*, 2020).

Uma forma mais invasiva de *contact tracing* foi empregada pelo governo chinês. O sistema Health Code, implementado pelo WeChat e Alipay, utilizou dados de GPS e de operadoras telefônicas para acompanhamento da localização de seus usuários. O risco de contágio foi então calculado; com base nele, cada usuário recebia em seu aplicativo um *QR-code* de cor verde, amarela ou vermelha. O código deveria ser escaneado para o acesso a um grande número de locais e serviços públicos ─ assim, foram impostas restrições aos usuários cujo *QR-code* era amarelo ou vermelho (risco moderado ou alto de contágio). O modo como tais dados foram armazenados e compartilhados levantaram suspeitas sobre possíveis desvios de finalidade no seu tratamento (LIANG, 2020).

Dezenas de outros sistemas foram desenvolvidos e adotados desde o início da pandemia. As principais diferenças entre eles residiu na tecnologia de rastreamento escolhida (como *Bluetooth*, GPS ou antenas de telefonia móvel) e o grau de centralização no armazenamento e processamento dos dados (GLASMEYER, 2020). De todo modo, um aspecto crucial para a eficácia desses sistemas foi o grau de sua adoção pela população. Com uma adesão baixa, não houve como garantir que o risco de contágio calculado por um aplicativo fosse confiável. Além disso, a testagem em massa foi outro critério imprescindível, como mencionado anteriormente.

4.3 A EXPERIÊNCIA BRASILEIRA

No Brasil, algumas discussões atinentes à proteção de dados surgiram durante a crise sanitária.

A primeira delas foi acarretada pela publicação da Medida Provisória nº 954, de 17 de abril de 2020. A norma impunha às empresas de telecomunicações a obrigação de compartilhar dados pessoais de seus clientes com o IBGE, objetivando a realização de pesquisas

por telefone durante a pandemia. Ao menos cinco ações foram propostas no STF contra esta disposição, considerada abusiva pelos autores. O julgamento resultou na suspensão da eficácia da MP, apontando a excessividade do compartilhamento de dados e a ausência de medidas de segurança (ABREU, 2021).

Outra polêmica se deu em torno da criação do Sistema de Monitoramento Inteligente (SIMI) pelo governo do estado de São Paulo. Instituído em maio de 2020, o SIMI consiste em um ambiente computacional que possibilita ao governo estadual consultar dados de operadoras de telefonia móvel. As informações agregadas e anonimizadas são usadas para calcular o índice de isolamento social da população paulista, a partir da localização de aparelhos celulares (GLASMEYER, 2020). As objeções judiciais ao SIMI não resultaram em sua suspensão, entendendo os magistrados que a anonimização assegura o sigilo dos dados pessoais, inexistindo portanto violação ao direito à privacidade (ABREU, 2020).

Ao contrário do que ocorreu em outros países, a adoção do *contact tracing* não se deu com vigor no Brasil. O aplicativo CORONAVÍRUS SUS, publicado pelo Ministério da Saúde em junho de 2020, foi a principal iniciativa do governo federal para o rastreamento de contatos, utilizando a tecnologia *Bluetooth* para registrá-los de modo anonimizado. A confirmação da infecção era feita voluntariamente pelo usuário, devendo ser previamente validada em outro sistema integrado às bases de dados do SUS (GLASMEYER, 2020).

De todo modo, a eficácia do aplicativo foi contestada, visto que foi implementado tardiamente, com pouca publicidade e estímulo ao seu uso (FRAGOSO, 2021). Além disso, outro fator foi a variedade de aplicativos de menor porte disponíveis ao público brasileiro, incluindo os de uso regional empregados no Rio Grande do Norte (“Tô de Olho”) e no Recife (em parceria entre a prefeitura e a *startup* In Loco).

5. CONCLUSÃO

Mesmo com o gradual arrefecimento da pandemia, seus efeitos sobre a privacidade e a proteção de dados serão indeléveis. A necessidade de isolamento acelerou a tendência de virtualização das relações humanas. Trabalho, lazer, convívio social ─ estas e outras esferas da vida em sociedade passaram a se dar, mais do que nunca, por meio de telas e dispositivos.

Em meio a uma das mais graves crises sanitárias da história recente, surgiram novos dilemas para a tutela jurídica da privacidade e dos dados pessoais. O cenário brasileiro,

sobretudo, evidenciou um grande desafio, pois a primeira legislação nacional sobre proteção de dados entrou em vigor em meio ao caos pandêmico. A incipiente cultura de proteção de dados no país deu seus primeiros passos, portanto, já em uma situação excepcional.

O dilema do conflito entre privacidade e saúde pública é um dos mais notórios sintomas dessa excepcionalidade. Como aponta Yuval Harari (2020), a pandemia foi portanto um grande teste de cidadania.

A disciplina jurídica da proteção de dados, como visto anteriormente, não deve ser encarada como um obstáculo na luta contra a pandemia e seus efeitos. Na realidade, ela proporciona legitimidade e segurança jurídica no uso de dados pessoais, estabelecendo balizas para que o tratamento de dados não extrapole suas finalidades. Assim, interferências sobre a privacidade dos cidadãos devem ser limitadas ao mínimo necessário para atingir os objetivos que a justificam.

O paradigma pós-pandêmico em que adentra a privacidade será, certamente, um dos grandes desafios jurídicos desta geração.

REFERÊNCIAS

ABELER, Johannes et al. COVID-19 contact tracing and data protection can go together. **JMIR mHealth and uHealth**, v. 8, n. 4, 2020.

ABREU, Jacqueline de Souza. Privacidade, proteção de dados pessoais e crises epidemiológicas: racionalidades e lições da pandemia. **Internet & Sociedade**, v. 1, n. 3, p. 5-26, jun. 2021.

AHMED, Nadeem et al. A survey of COVID-19 contact tracing apps. **IEEE Access**, v. 8, p. 134577-134601, 2020.

ARAGÃO, Suéllyn Mattos; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, v. 14, n. 3, 2020, p. 692-708.

BARRAT, Alain et al. Effect of manual and digital contact tracing on COVID-19 outbreaks: a study on empirical contact data. **Journal of the Royal Society Interface**, v. 18, n. 178, 2020.

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

BONAFÉ, Lucas Alves da Silva. LGPD e o tratamento de dados na saúde. In: GUTIERREZ, T. S. D.; NUNES, M. **LGPD na saúde**. [s.l.]: Machado Nunes, 2019. Livro eletrônico. p. 44-63. Disponível em: https://lgpdesaude.com.br/wp-content/uploads/2019/08/LGPD_digital_v3-atualizado.pdf. Acesso em: 28 nov. 2021.

CAMBRICOLI, Fabiana. Nova falha no Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros. **Estado de S. Paulo**, 02 dez. 2020. Disponível em: https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340. Acesso em: 29 nov. 2021.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Resolução 1/2020: Pandemia e Direitos Humanos nas Américas**. Washington: Comissão Interamericana de Direitos Humanos, 2020. Disponível em: https://www.oas.org/pt/cidh/decisiones/pdf/Resolucao-1-20-pt.pdf. Acesso em: 23 nov. 2021.

COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS. **Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the Covid-10 outbreak**. Bruxelas: União Europeia, 2020a. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf. Acesso em: 23 nov. 2021.

COMITÊ EUROPEU PARA A PROTEÇÃO DE DADOS. **Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak**. Bruxelas: União Europeia, 2020b. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en. Acesso em: 24 nov. 2021.

DONEDA, Danilo. A proteção de dados em tempos de coronavírus. **Jota**, 25 mar. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020. Acesso em: 25 nov. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** 2. ed. São Paulo: Thomson Reuters, 2019.

DUBOV, Alex; SHOPTAWB, Steven. The value and ethics of using technology to contain the COVID-19 epidemic. **The American Journal of Bioethics**, v. 20, n. 7, p. W7-W11, 2020.

FRAGOSO, N. et al. **Privacy and Data Protection in the Pandemic: report on the Use of Apps and Alternative Measures in Brazil**. São Paulo, InternetLab, 2021. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2021/04/Privacy-and-Data-Protection-in-the-Pandemic_05.pdf. Acesso em: 28 nov. 2021.

FRENCH, Martin; MONAHAN, Torin. Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19? **Surveillance & Society**, v. 18, n. 1, mar. 2020, p. 1-11.

GLASMEYER, R. A implementação do Contact Tracing e a montagem de vigilâncias na pandemia da Covid-19. **Internet & Sociedade**, v. 1, n. 2, pp. 200-220, 2020.

GLOBAL PRIVACY ASSEMBLY. **Statement by the GPA Executive Committee on the Coronavirus (Covid-19) pandemic**. 17 mar. 2020. Disponível em: https://globalprivacyassembly.org/gpaexco-covid19/. Acesso em: 26 nov. 2021.

HALE, Thomas et al. A global panel database of pandemic policies (Oxford COVID-19 Government Response Tracker). **Nature Human Behaviour**, v. 5, n. 4, p. 529-538, 2021.

HARARI, Yuval Noah. The world after coronavirus. **Financial Times**, 20 mar. 2020. Disponível em: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. Acesso em: 24 nov. 2021.

HILL, Kashmir. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. **Forbes**, 16 fev. 2012. Disponível em: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/. Acesso em: 30 nov. 2021.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. **Lei geral de proteção de dados pessoais: e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Thomson Reuters, 2020, p. 441-458.

LI, Tiffany C. Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis. **Loyola University Chicago Law Journal**, v. 52, n. 3, p. 767-865, 2020.

LIANG, Fan. COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. **Social Media + Society**, v. 6, n. 3, p. 1-4, 2020.

MARTINEZ-MARTIN, Nicole et al. Digital contact tracing, privacy, and public health. **Hastings Center Report**, v. 50, n. 3, p. 43-46, 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do advogado**, n. 144, nov. 2019, p. 47-53.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos. **COVID-19: States should not abuse emergency measures to suppress human rights – UN experts**. Genebra: Organização das Nações Unidas, 2020. Disponível em: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722. Acesso em: 16 nov. 2021.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. **Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: interim guidance**. 28 May 2020. Genebra: World Health Organization, 2020. Disponível em: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1. Acesso em: 27 nov. 2021.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. Assembleia Mundial da Saúde. **Resolution WHA58.28 on eHealth**. Genebra: Organização Mundial da Saúde, 2005. Disponível em: https://www.who.int/healthacademy/media/WHA58-28-en.pdf. Acesso em: 23 nov. 2021.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Ensuring data privacy as we battle COVID-19**. Paris: OCDE, 2020. Disponível em: https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/. Acesso em: 27 nov. 2021.

RESEARCH GROUP ON LAW, SCIENCE, TECHNOLOGY & SOCIETY. **European data protection authorities and other national resources on Covid-19**. 2021. Disponível em:

https://lsts.research.vub.be/en/european-data-protection-authorities-and-other-national-resources-on-covid-19. Acesso em: 28 nov. 2021.

ROBICHAU, Bernard Peter; SANDERS, Michael Clore. **Healthcare Information Privacy and Security: Regulatory Compliance and Data Security in the Age of Electronic Health Records**. New York: Apress, 2014.

ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 10, n. 1, p. 61-84, maio 2018.

SARLET, Gabrielle Bezerra Sales; FERNANDES, Márcia Santana; RUARO, Regina Linden. A proteção de dados no setor de saúde em face do sistema normativo brasileiro atual. In: DONEDA, Danilo et al. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 490-510.

SKOPEK, Jeffrey M. Big Data's Epistemology and Its Implications for Precision Medicine and Privacy. In: COHEN, I. G. et al. **Big Data, health law, and bioethics**. Cambridge: Cambridge University Press, 2018, p. 30-41.

SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à luz da Lei 13.709/2018. In: TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. **Lei geral de proteção de dados pessoais: e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Thomson Reuters, 2020, p. 413-437.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. In: DONEDA, Danilo et al. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 117-148.

WHITTY, Christopher J. M. et al. Providing incentives to share data early in health emergencies: the role of journal editors. **The Lancet**, v. 386, n. 10006, p. 1797-1798, 2015.

WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. **Revista do advogado**, n. 144, nov. 2019, p. 126-133.

WORLD BANK. **The Role of Digital Identification for Healthcare: the Emerging Use Cases**. Washington: World Bank, 2018. Disponível em: https://openknowledge.worldbank.org/bitstream/handle/10986/31826/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf. Acesso em: 26 nov. 2021.

.