DATA PRIVACY BRASIL
PUBLICAÇÕES

Bruno R. Bioni
Rafael A. F. Zanatta
Mariana Rielli
Gabriela Vergili
Iasmine Favaro
& Organizadores

Os dados e o vírus

Pandemia, proteção de dados e democracia

Ana Paula Assis Buosi
Silvio Gonçalves Xavier Júnior
João Araújo Monteiro Neto
Luís Fernando Costa Oliveira
Henrique Junqueira Arruda de Souza
Marina Sayuri Kitayama
Viviane Ceolin Dallasta Del Grossi
Thaís Coelho da Silva
Lucas Bulhões
Daniel Pereira Campos
Elora Raad Fernandes
Cindyneia Cantanhede
Walter Britto Gaspar
Afonso Carvalho de Oliva
Fabricio Barili
Raphael Marques de Barros
Marco Aurélio Fernandes Garcia
Fernando Bottega Pertile
Maurício Requião
Laiane Maris Caetano Fantini
Marco Aurélio Rodrigues da Cunha e Cruz
Luís Henrique Kohl Camargo

DataPrivacyBR

Data Privacy Brasil

OS DADOS E O VÍRUS: PANDEMIA, PROTEÇÃO DE DADOS E DEMOCRACIA

São Paulo

07 de julho de 2020

DATA PRIVACY BR - OS DADOS E O VÍRUS: PANDEMIA, PROTEÇÃO DE DADOS E DEMOCRACIA ARTIFICIAL - SÃO PAULO/SP 1ª EDIÇÃO – JULHO 2020

EQUIPE INSTITUCIONAL

DIRETORES
Bruno Ricardo Bioni
Rafael Zanatta

LÍDER DE PROJETOS
Mariana Marques Rielli

PESQUISADORAS
Gabriela Machado Vergili
Iasmine Favaro Lima

MARKETING & DESIGN
Victor Scarlato
Júlio A.O. Araújo

EQUIPE DE PROJETO

ORGANIZAÇÃO
Bruno Ricardo Bioni
Rafael Zanatta
Mariana Marques Rielli
Gabriela Machado Vergili
Iasmine Favaro

ARTE DA CAPA
Vitor César

DIAGRAMAÇÃO
Júlio A.O. Araújo

Dados Internacionais de Catalogação na Publicação (CIP)
Câmara Brasileira do Livro, SP, Brasil

615 BIONI, Bruno Ricardo | **27 ZANATTA,** Rafael Augusto | **555 RIELLI,** Mariana Marques | **497 VERGILI,** Gabriela Machado I **732 LIMA,** Iasmine Favaro

OS DADOS E O VÍRUS: PANDEMIA, PROTEÇÃO DE DADOS E DEMOCRACIA [LIVRO ELETRÔNICO] / Bruno R. Bioni... [et al.] – São Paulo: Reticências Creative Design Studio, 2020.
xxp; 21x29,7cm | 1 Mb ; PDF

ISBN 987-65-87614-02-1

1. Coronavírus (COVID-19) – Prevenção 2. COVID19 – Pandemia 3. Direito de Privacidade 4. Isolamento Social 5. Tecnologia e direito

20-38762 **CDU 342.721**

ÍNDICE PARA CATÁLOGO SISTEMÁTICO:
Privacidade: Proteção de dados pessoais: Direito 442.721

Maria Alice Ferreira - Bibliotecária - CRB-8/7964

A Associação Data Privacy Brasil de Pesquisa ("Data Privacy Brasil") é uma entidade civil sem fins lucrativos sediada em São Paulo. A organização dedica-se à interface entre proteção de dados pessoais, tecnologia e direitos fundamentais, produzindo pesquisas e ações de incidência perante o sistema de Justiça, órgãos legislativos e governo. A partir de uma Política de Financiamento Ético e Transparência, a associação desenvolve projetos estratégicos de pesquisa em proteção de dados pessoais, mobilizando conhecimentos que podem ajudar reguladores, juízes e profissionais do direito a lidar com questões complexas que exigem conhecimento profundo sobre como tecnologias e sistemas sócio-técnicos afetam os direitos fundamentais. A Associação possui financiamento de filantropias internacionais como Ford Foundation, Open Society Foundations e AccessNow. Para mais informações, visite www.dataprivacybr.org.

SUMÁRIO

APRESENTAÇÃO DA OBRA

Bruno R. Bioni, Rafael Zanatta, Mariana Rielli, Gabriela Vergili e *Iasmine Favaro*

A atual pandemia da COVID-19, causada pela disseminação do novo Coronavírus (SARS-COV2), tem causado profundos efeitos sobre todos os aspectos da vida humana e das relações sociais. Uma das questões diretamente mobilizadas nesse contexto, especialmente em razão das medidas de combate à doença, é a privacidade e a proteção de dados.

De um lado, em países como a China e os Estados Unidos, práticas como o emprego de *drones*[1][2] e câmeras de segurança, inclusive dentro da casa das pessoas[3], tornaram-se corriqueiras como forma de avaliar níveis de isolamento social para controle da pandemia, o que atinge frontalmente o direito à privacidade. Por outro, países em todos os pontos do espectro político vêm adotando tecnologias para auxiliar nos seus esforços de combate ao coronavírus, levantando inúmeras questões sobre a proteção de dados pessoais que alimentam essas tecnologias. Trata-se, por exemplo, do tratamento de dados de geolocalização para formação de mapas de calor[4], das diferentes técnicas de rastreamento de contatos[5], da divulgação, total ou parcial, de dados pessoais de saúde, dentre outros. Surgem questionamentos, ancorados na realidade que vem se desenhando, sobre o que restará após a pandemia e se essas tecnologias perdurarão, resultando em maior vigilância e controle sobre os indivíduos.

---

1 NOVAK, Matt. China usa drones de maneiras cada vez mais distópicas para combater o surto de coronavírus. Gizmodo Uol. 16 de fevereiro de 2020. Disponível em: https://gizmodo.uol.com.br/china-drones-coronavirus/

2 ROLFINI, Fabiana. Drone será usado para detectar pessoas com sintomas de covid 19 nos EUA. Olhar Digital. 23 de abril de 2020. Disponível em: https://olhardigital.com.br/coronavirus/noticia/drone-sera-usado-para-detectar-pessoas-com-sintomas-de-covid-19-nos-eua/99824

3 ESCOVAR, João Victor. China coloca câmeras nas casas para vigiar quarentena. O Consumerista. 05 de maio de 2020. Disponível em: https://www.oconsumerista.com.br/2020/05/china-cameras-casas-quarentena/

4 Mapas de calor, apps: especialistas explicam uso de dados contra a covid-19. Tilt Uol. 29 de abril de 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/04/29/mapas-de-calor-apps-especialistas-explicam-uso-de-dados-contra-a-covid-19.htm

5 HIGA, Paulo. Como funciona a tecnologia feita por Apple e Google para monitorar COVID-19. Tecnoblog. 24 de abril de 2020. Disponível em: https://tecnoblog.net/335748/como-funciona-a-tecnologia-feita-por-apple-e-google-para-monitorar-covid-19/

Tal quadro, largamente agravado pelos níveis de conectividade que hoje experimentamos, suscita uma série de questões políticas, jurídicas e filosóficas que merecem aprofundamento. Com isso em mente, a Associação Data Privacy Brasil de Pesquisa, no âmbito do seu projeto *Os Dados e o Vírus*, decidiu abrir um concurso de ensaios sobre a relação entre as medidas sanitárias de combate à COVID-19 e a proteção de dados pessoais, tendo como perguntas norteadoras as seguintes:

a)Quais os limites de interpretação do artigo 6º da Lei 13.979/2020 diante dos parâmetros da autodeterminação informativa e do direito à proteção de dados pessoais?

b) De que modo os princípios da Lei Geral de Proteção de Dados Pessoais podem impactar ações e protocolos de compartilhamento de dados entre empresas e autoridades sanitárias?

c) Quais seriam exemplos de rompimento do princípio da finalidade no compartilhamento de dados entre empresas e governos no contexto da Lei 13.979/2020 e quais seriam os remédios jurídicos disponíveis para interrupção desta violação do direito?

d) Quais os riscos de normalização de um "estado de exceção" com relação ao uso de dados pessoais e constituição de um cenário de vigilância crônica?

e) Quais as lições que podem ser obtidas, da perspectiva do balanceamento entre proteção à saúde pública e respeito aos direitos fundamentais, a partir da experiência de países asiáticos como Singapura e Coréia do Sul?

No edital, estabeleceu-se que os ensaios deveriam ter, no máximo, 05 páginas e que seriam corrigidos e pontuados a partir de determinados critérios: (1) originalidade do ensaio (até 3 pontos), (2) coerência lógica e concatenação de ideias (até 3 pontos), (3) parâmetros de citação (1 ponto), (4) utilização de fatos recentes e exemplos de outros países (2 pontos), (5) precisão de linguagem (1 ponto). Foram recebidos 60 ensaios e, destes, foram selecionados os 5 melhores, que receberam premiações, e mais 13, perfazendo os 18 melhores ensaios, todos com nota superior a 8, de acordo com os critérios mencionados. Um ponto interessante a se destacar é que, dos 18 selecionados, 10, ou seja, cerca de 55%, são de autores de fora de São Paulo, provenientes de universidades em estados como Ceará, Sergipe, Rio de Janeiro, Maranhão, Rio Grande do Sul,

Minas Gerais, Bahia e Santa Catarina. A Associação Data Privacy Brasil de Pesquisa tem como missão sair do eixo Rio-São Paulo e dialogar com pesquisadores e pesquisadoras de todos os cantos do país, de forma que o índice de exogenia verificado é muito positivo.

Após análise do conjunto dos ensaios selecionados para a publicação, foi possível separá-los em quatro temas. No primeiro tópico temático, chamado *A Responsabilidade do Poder Público*, encontram-se ensaios que defendem a necessidade de uma responsabilidade estatal em prestar contas e em estabelecer um sistema de governança de dados que favoreça a transparência, em especial, nas circunstâncias da pandemia. O primeiro texto desse eixo, intitulado *A governança do compartilhamento de dados pessoais em tempos de crise: Desafios e Perspectivas*, de Ana Paula Assis Buosi, Silvio Gonçalves Xavier Junior e João Araújo Monteiro Neto, afirma que os debates sobre compartilhamento de dados pessoais têm ignorado o papel da construção de um bom modelo de governança como forma de produzir um equilíbrio entre uso de dados e proteção dos direitos dos cidadãos. No caso brasileiro, discute a inadequação dos órgãos atuais dentro do Ministério da Saúde e a notória ausência de uma Autoridade Nacional de Proteção de Dados e sugere, como modelo, uma combinação de multissetorialismo com práticas de governança FAT (Fairness, Accountability and Transparency). No segundo ensaio, *A interpretação do art. 6º da Lei n. 13.979/2020 - Ofensa à autodeterminação informativa e ausência de accountability por parte da Administração Pública*, o autor Luiz Fernando Costa Oliveira analisa as consequências práticas do art. 6º da Lei 13.979/2020 sobre o titular de dados, mais especificamente quanto ao seu direito à autodeterminação informativa. Devido a este impacto sobre o cidadão, o autor entende que a Administração Pública deveria prestar contas sobre a sua atuação e a forma como utiliza os dados pessoais. Neste sentido, a transparência e a *accountability* teriam uma função essencial para evitar um uso inadequado e um fluxo desnecessário de dados. O terceiro texto, de Henrique Junqueira Arruda de Souza, intitulado *Crise sanitária e privacidade: um ensaio sobre a confluência entre direitos fundamentais e o interesse público* trata da necessidade de equilíbrio entre a defesa dos direitos fundamentais e as operações para concretizar o interesse público. Portanto, outras tecnologias, mais protetivas, deveriam ser consideradas, como, por exemplo o *blockchain*, que favorece a encriptação de informações, para tornar compartilhamentos obrigatórios de dados mais seguros. Assim, sugere a existência de parâmetros mais bem delineados para auxiliar o Poder Público a lidar

com crises como a da COVID-19. Finalmente, o ensaio *Dados pessoais e coronavírus, do abuso à legitimidade*, de Marina Kitayama, afirma que os dados pessoais são essenciais no combate à propagação do coronavírus, mas é preciso controlar os abusos. O ensaio analisa as falhas e brechas da Lei 13.979/2020, que dificultam uma melhor definição de escopo do tratamento de dados e ampliam a possibilidade estatal de avançar sobre os direitos dos titulares de dados de forma abusiva. Deste modo, a transparência do processo deve ser cobrada da Administração Pública.

O segundo núcleo temático, *A ausência de salvaguardas que fragiliza direitos*, reúne ensaios que demonstram como a ausência de mecanismos mais eficazes de proteção do titular de dados fragiliza seus direitos, como a autodeterminação informativa, o direito à privacidade e o direito à proteção de dados. O foco aqui está mais no indivíduo e menos no Estado. O primeiro ensaio deste grupo, *Transparência, privacidade e proteção de dados em tempos de Coronavírus e além da pandemia*, de Viviane Ceolin Dallasta Del Grossi, lida com a questão da dicotomia criada entre saúde e proteção de dados e como a última vem sendo flexibilizada em favor da primeira. A tese apresentada no ensaio é que um contraponto a esse estado de coisas é o aumento da transparência e do acesso à informação, por meio de instrumentos como a própria Lei de Acesso à Informação brasileira e ferramentas de dados abertos e transparência ativa, ações que deveriam ser priorizadas em prejuízo de ingerências sobre a privacidade e a proteção dos dados dos cidadãos. O segundo ensaio, de Thais Coelho, intitulado *Relação entre medidas emergenciais para o combate ao COVID-19 e a privacidade e proteção de dados pessoais*, a autora defende que o tratamento de dados pessoais, inclusive sensíveis, é permitido ao Poder Público, no entanto, não pode, de forma alguma, ser indiscriminado. O ensaio apoia-se nos casos da Coreia do Sul, Alemanha e Israel, distinguindo as abordagens governamentais em relação à operação implementada no Brasil, de forma a apontar a fragilização do princípio da autodeterminação informativa e do direito à proteção de dados no país. Já no terceiro texto*, Dados de geolocalização: o limbo entre privacidade e saúde pública em tempos de covid-19*, o autor Lucas Bulhões trata da situação pandêmica e como a ausência de salvaguardas legais coloca em risco direitos dos cidadãos. É destacada a importância de se tomar medidas para o combate à COVID-19, como a geolocalização para mapeamento da transmissão do vírus, exemplo mais explorado pelo autor. Entretanto, a lacuna normativa específica sobre a questão, tendo em vista

que a Autoridade Nacional de Proteção de Dados ainda não foi criada e a LGPD não está em pleno vigor, desfavorece o titular de dados.

O terceiro núcleo, *O problema do uso de dados sensíveis*, por sua vez, abrange textos que cuidam da necessidade de uma maior proteção a dados sensíveis e outros dados que estão ainda mais vulneráveis frente às alterações causadas pelo combate ao coronavírus, como os dados de crianças e adolescentes e os dados de saúde. No primeiro ensaio, intitulado *Pandemia e futuro da saúde: questões sobre telemedicina e privacidade*, o autor Daniel Pereira Campos, aborda como diferentes países vêm adotando um relaxamento nas permissões relativas à prática da telemedicina, inclusive para outras especializações, como psicologia. Por outro lado, aponta que, a despeito de inúmeras regulações sobre o tema, pouco se avançou em termos de privacidade e proteção de dados nesse contexto. Defende a necessidade de colocar os titulares em posição de centralidade, ainda mais quando se trata de dados pessoais sensíveis. Em seguida, as autoras Elora Raad Fernandes e Cindyneia Cantanhede, no ensaio *Proteção de crianças e adolescentes por design: um debate necessário em meio à crise da Covid-19* partem da premissa de que crianças e adolescentes hoje, já extremamente conectados, têm seu contato com os meios digitais e a internet intensificado em razão da pandemia e isso pode ter efeitos sobre sua segurança e direitos, já que as tecnologias da informação e comunicação não são desenhadas tendo em vista o interesse desses indivíduos em formação. Assim, o texto sustenta que menores de idade devem ter suas necessidades e peculiaridades consideradas desde a concepção de produtos e serviços que fazem uso de dados pessoais. Por fim, o último texto deste capítulo é *Proteção de dados, COVID-19 e estigma*, do autor Walter Britto Gaspar, e desloca a discussão da violação de dados pessoais para o campo do estigma, especificamente no que se refere à pandemia do coronavírus e seus efeitos sobre determinadas populações e grupos étnicos/sociais. Trata de exemplos internacionais em que a reversão de processos de anonimização, ou a identificação propriamente dita de pessoas, conduziu a situações discriminatórias e estigmatizantes, revelando uma faceta relativamente pouco discutida da proteção de dados pessoais.

O último eixo da publicação, e o que contém mais ensaios, é *O receio de uma vigilância contínua*. Essa seção reúne textos que discorrem sobre como medidas de vigilância, que se valem de dados pessoais, podem impactar o futuro e resultar em um estado

de monitoramento constante. O primeiro texto, de Afonso Carvalho de Oliva, intitula-se *O auxílio emergencial e a vigilância dos consumidores pós-COVID-19* e trata da problemática da criação de contas poupança digitais para recebimento do auxílio emergencial do governo federal, criado em razão da pandemia da COVID- 19, e como isso desloca milhões de cidadãos, antes fora do radar, para o centro de um sistema de vigilância de crédito. Além disso, o autor aponta que, no caso das contas criadas em razão do auxílio, o dado pessoal resultante já possui uma camada extra de categorização, uma vez que se sabe que o indivíduo correspondente se encaixa no perfil econômico para recebimento do auxílio. Em seguida, o ensaio *Coronavírus: um intensificador do Estado de vigilância,* de Fabrício Barili, tem como objetivo elucidar como um Estado chamado de exceção pode, a partir do pretexto da pandemia da COVID-19, intensificar suas práticas de vigilância sobre os indivíduos e grupos sociais. A tese apresentada no ensaio é que, nesses contextos de exceção, as práticas de vigilância que se instauram tornam-se o novo normal, não havendo possibilidade de retorno ao estado anterior. No Brasil e no mundo, o emprego de tecnologias para o combate ao coronavírus se encaixa, segundo o autor, nessa lógica. O próximo ensaio, intitulado *A Naturalização da Vigilância em Massa em Tempos de Emergência*, de Raphael Marques de Barros, trata dos mecanismos de vigilância adotados e intensificados com a crise da COVID-19 no Brasil e no mundo. A partir de exemplos históricos, como o Patriot Act após o ataque terrorista de 11 de setembro nos Estados Unidos, busca demonstrar como esse tipo de interferência sobre os mais diversos aspectos da vida e dos direitos das pessoas tende a se estabelecer, mesmo após o fim da circunstância que lhe deu origem, no caso a pandemia do coronavírus. O quarto ensaio da coletânea, *Saúde e Proteção de Dados - Fundamentos da Vigilância Epidemiológica Social*, é de Marco Aurélio Fernandes Garcia e questiona a obrigatoriedade do compartilhamento de dados pessoais para a identificação de indivíduos suspeitos de estar infectados ou confirmadamente infectados com a COVID-19, imposto pelo art. 6º da Lei nª 13.979/2020. Para esta análise, o autor trata da relação entre saúde e privacidade, e aborda o mecanismo de notificação compulsória para demonstrar que um dispositivo como este, que torna obrigatório o compartilhamento de dados, pode ser arriscado e favorecer uma maior vigilância. O quinto ensaio, de Fernando Bottega Pertile, intitula-se *Quais os limites da atuação dos governos em tempos de coronavírus e quais os deveres dos cidadãos vigilantes?*. Com o objetivo de esclarecer como os Estados podem reforçar uma vigilância intensa, o autor apresenta diversas as formas de monitoramento

estatal implementadas ao redor do mundo em vista da pandemia causada pelo coronavírus. São apresentados detalhes sobre cada tipo de coleta e uso de dados pessoais para, na sequência, apontar as proteções ou regulamentações oferecidas por legislações de proteção de dados. Na sequência, Covid-19 e as entranhas do capitalismo de vigilância, de Maurício Requião, tem como foco as tecnologias de vigilância implementadas nacional e internacionalmente em função da crise pandêmica. Neste sentido, questiona-se o efetivo custo-benefício da implementação dessas tecnologias para garantia da saúde, havendo uma nítida preocupação com o risco à democracia e à esfera individual de cada cidadão. Laiane Maris Caetano Fantini traz o sétimo ensaio da lista, *Coronavírus - SUS: aspectos relevantes da privacidade e proteção de dados e tecnologia de vigilância*, em que destaca o uso da tecnologia com a finalidade de vigilância, em análise específica do aplicativo associado ao SUS, e busca entender como este tratamento de dados pessoais estaria ou não respaldado pelo ordenamento brasileiro vigente. O último ensaio da coletânea é o *As relações de precedência condicionada como limite à vigilância extrema: o repasse de informações pelas operadoras de telecomunicação*, escrito por Marco Aurélio Rodrigues da Cunha e Cruz e Luís Henrique Kohl Camargo, que analisam o uso de medidas tecnológicas aplicadas no combate à Covid-19, enquanto carecemos de soluções farmacológicas, para entender os seus efeitos de vigilância dentro do Estado Democrático.

A Associação Data Privacy Brasil de Pesquisa espera que essa publicação, que conta com uma rica diversidade temática dentro do escopo maior da privacidade e proteção de dados e as medidas de combate à COVID-19, seja uma leitura informativa e elucidativa e que possa ser mais um material de qualidade em meio às diversas produções que vêm sendo desenvolvidas nesse tema. A coletânea complementa análises feitas no relatório *Privacidade e Pandemia*[6], publicada por nossa equipe de pesquisa em 15 de abril de 2020, ainda no primeiro mês da crise da Covid-19 no Brasil.

6 BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à Covid-19. São Paulo: Data Privacy Brasil, 2020. Disponível em: https://www.dataprivacybr.org/os-dados-e-o-virus/

Em tempos de crise e intensificação do desastre social brasileiro – com milhares de mortos e aumento do temor coletivo em torno da doença –, é momento de união e reflexão coletiva sobre os direitos que não queremos e não podemos abandonar.

PARTE I

A RESPONSABILIDADE DO PODER PÚBLICO

A GOVERNANÇA DO COMPARTILHAMENTO DE DADOS PESSOAIS EM TEMPOS DE CRISE: DESAFIOS E PERSPECTIVA

Ana Paula Assis Buosi[7], Silvio Gonçalves Xavier Júnior[8] e João Araújo Monteiro Neto[9]

INTRODUÇÃO

A proteção da privacidade, apesar do seu estado conceitual de desarranjo causado tanto por debates conceituais como por políticas públicas de vigilância[10][11], ainda é considerada, pela maior parte da literatura legal, um dos pilares da construção de uma sociedade democrática[12]. É também um valor indispensável para que "possamos balizar a construção de nossas relações com outras pessoas[13] permitindo a proteção de esferas autônomas de nossa vida"[14], englobando, historicamente, desde o controle sobre o corpo até a proteção de dados pessoais.

Apesar das inconsistências e ambiguidades de sua construção conceitual[15], a proteção legal à privacidade alcançou um patamar significativo no último século. Por meio de sua incorporação em constituições, leis específicas ou decisões judiciais, o direito à privacidade tem garantido às pessoas a possibilidade de controlar o acesso, uso ou a divulgação de elementos de sua vida privada. Essa última perspectiva representa um dos elementos que levaram Cate[16] a indicar a privacidade como uma "construção anti-social

---

7 Pós-graduanda em Direito Constitucional nas Relações Privadas pela Universidade de Fortaleza e integrante do GETIS (Grupo de Estudos em Tecnologia, Internet e Sociedade).
8 Pós-graduando em Direito Digital e Compliance pelo IBMEC e integrante do GETIS
9 PhD, Professor do Curso de Direito da Universidade de Fortaleza. Coordenador do GETIS e orientador do Legal Tech Lab da UNIFOR.
10 Solove, Daniel J. Understanding Privacy. HUP, 2009.
11 Cannataci, Joseph. The Individual and Privacy: Volume I (The Library of Essays on Law and Privacy, Vol. 1. Routledge, 2015.
12 Gavison, Ruth. Privacy and the limits of law, 89 Yale Law Journal, p. 421 – 455, 1980.
13 Rachels, James. "Why Privacy is Important" in Philosophical Dimensions of Privacy: Na Anthology. Ferdinand Schoeman, Ed., 1984.
14 Rössler, Beate. The Value of Privacy. (2005)
15 Gross, Hyman. Th concepto f Privacy, New York University Law Review, 34, 1967.
16 Cate, Fred H. Privacy in the Information Age, 29, 1997.

que conflita em alguns aspectos com interesses da sociedade como a condução de políticas governamentais mais efetivas".

Nesse sentido, tanto a legislação europeia (GDPR) como a legislação brasileira de proteção de dados pessoais estabelecem mecanismos legais que autorizam a utilização de dados pessoais, inclusive os sensíveis, sem o consentimento de seus titulares. Trata-se dos casos em que a operação de tratamento se mostre necessária para albergar os interesses coletivos como, por exemplo, a proteção da saúde pública.

O presente ensaio realizou uma revisão bibliográfica da literatura sobre privacidade, proteção de dados e estudos sobre regulamentação e governança. Concentrou-se nas ações governamentais relativas ao combate à COVID-19 no Brasil, apresentando os elementos socio-legais na utilização de dados pessoais em casos de grave risco à saúde coletiva. Demonstrou-se mecanismos de governança específicos aplicados em caso de uso de dados pessoais em cenários de crise. Propõem-se, finalmente, alguns elementos a serem observados na governança de dados pessoais em tempos de crise.

ELEMENTOS CONTEXTUAIS SOBRE DADOS PESSOAIS SENSÍVEIS NO CENÁRIO PANDÊMICO

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018[17], define em seu art. 5ª, inciso I, que dados pessoais seriam as informações relativas a uma pessoa natural que seja identificada ou identificável, adotando o conceito expansionista de dado pessoal[18]. Já os dados pessoais sensíveis recebem esse adjetivo porque tratam de caracteres

17 BRASIL. Lei nº 13.709, de 2018. BRASILIA, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 15 abr. 2020.
18 BIONI, Bruno. Dados "anônimos" como antítese de dados pessoais: o filtro da razoabilidade. Disponível em: <http://genjuridico.com.br/2019/10/11/dados-anonimos-antitese-dados-pessoais/>. Acesso em: 15 abr. 2020.

com um forte conteúdo existencial, subjetivo e individualizante. Esse feixe de características, como os dados sobre a saúde, se subvertidas, poderiam ser utilizadas de forma discriminatória e estigmatizante, ofendendo a dignidade de seus titulares.

Por suas peculiaridades, os dados pessoais sensíveis possuem uma abordagem diferenciada. Para tanto, o legislador elegeu o consentimento como a base legal apta ao tratamento dessas informações, conforme disposto pelo art. 11, inciso I, da LGPD. Porém, a Lei também estabelece situações excepcionais em que o tratamento de dados pessoais sensíveis pode ocorrer sem o consentimento do titular. Trata-se do disciplinado pelo art. 11, inciso II, alíneas "b", "e" e "f". Assim, nos casos em que a execução de políticas públicas estiver prevista em leis ou regulamentos pelo agente administrativo, quando houver a necessidade de proteção à vida ou à incolumidade física, ou, ainda, a tutela da saúde seja viabilizada, exclusivamente, em procedimento executado por profissionais da área, autoridades sanitárias nos serviços de saúde, não haverá a necessidade do consentimento do titular dos dados.

A realidade exposta pelo modo como o Coronavírus manifesta os seus sintomas de forma diversificada na população, somada à indisponibilidade de infraestrutura do sistema de saúde brasileiro para o atendimento dessa demanda excepcional, fizeram com que o governo se articulasse na tentativa de melhor gerir a nova crise do setor de saúde. Por esse motivo, foi editada a Lei nº 13.979/2020[19] que versa sobre medidas emergenciais no âmbito da saúde decorrente da disseminação da COVID-19, enquanto subsistir o quadro emergencial de saúde internacional. O art. 6º e os parágrafos do diploma legal dispõem sobre o compartilhamento de dados da saúde entre as entidades

19 BRASIL. Lei nº 13.979, de 2020.BRASILIA, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L13979.htm>. Acesso em: 15 abr. 2020.

da administração pública, em todas as suas esferas, e as pessoas jurídicas de direito privado. Estas, quando requeridas pela autoridade sanitária, também compartilharão informações com o desiderato de identificar contaminados e suspeitos de contaminação pelo Coronavírus.

Tal circunstância culminou com iniciativas brasileiras de mapeamento dos dados de indivíduos nos estados do Rio de Janeiro, de Pernambuco e São Paulo[20], com a finalidade de monitorar o deslocamento da população. Dessa forma, os órgãos públicos poderiam observar se as pessoas estão respeitando a quarentena, traçando estratégias mais assertivas no combate da propagação do vírus.

O momento vivenciado não é peculiar somente no ambiente nacional. Por se tratar de uma crise de saúde global, vários países adotaram medidas no sentido de monitorar a disseminação da infecção entre seus cidadãos. Em Israel[21], as empresas de telecomunicações compartilham os dados de localização dos dispositivos móveis com as autoridades de saúde, monitorando as pessoas infectadas para que elas cumpram a quarentena. Na China[22], as atividades de controle são mais diversificadas e severas: robôs entregam comidas em hospitais, reconhecimento facial quantifica a temperatura das

20 ESTADO, Agência. TIM fecha parceria com Prefeitura do Rio para rastrear movimento e combater vírus. Disponível em: <https://www.infomoney.com.br/economia/tim-fecha-parceria-com-prefeitura-do-rio-para-rastrear-movimento-e-combater-virus/>. Acesso em: 15 abr. 2020. Gabinete de Imprensa. Prefeitura do Recife usa tecnologia como aliada na contenção do novo coronavírus. Disponível em: <http://www2.recife.pe.gov.br/noticias/24/03/2020/prefeitura-do-recife-usa-tecnologia-como-aliada-na-contencao-do-novo-coronavirus>. Acesso em: 15 abr. 2020. Isolamento social em São Paulo é de 47%, aponta Sistema de Monitoramento Inteligente. Disponível em: <https://www.saopaulo.sp.gov.br/noticias-coronavirus/isolamento-social-em-sao-paulo-e-de-47-aponta-sistema-de-monitoramento-inteligente/>. Acesso em: 15 abr. 2020.

21 LOMAS, Natasha. Israel passes emergency law to use mobile data for COVID-19 contact tracing. Disponível em: <https://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing/>. Acesso: 15/04/20.

22 TIDY, Joe. Coronavirus: How China's using surveillance to tackle outbreak. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf. Acesso em: 15 abr. 2020.

pessoas e drones são instrumentos de vigilância da política de *lockdown* e cumprimento de quarentena.

Em linhas gerais, o monitoramento das atividades dos indivíduos, visando o contingenciamento da pandemia, tem-se revelado, em certa medida, um instrumento inidôneo para o tratamento de dados sensíveis. Essa vigilância demonstra-se precária nos mecanismos de transparência e de boas práticas adotadas pelos governos e pelas empresas encarregadas de coletar esses dados. É necessário que as ações relativas à vigilância de dados sensíveis sejam norteadas por boas diretrizes.

O *European Data Protection Board* (EDPB) no seu "*Statement on the processing of personal data in the context of the COVID-19 outbreak*"[23] publicou um documento orientador de condutas para o enfrentamento da situação pandêmica, no contexto limitador de liberdades. Dentre as diretrizes estão presentes o resguardo dos princípios da proporcionalidade, finalidade e confidencialidade, das bases legais de tratamento e dos direitos do titular dos dados. Expõem-se ainda a determinação da adoção de técnicas de tratamento menos invasivas e de menor impacto na privacidade dos titulares. Mesmo possuindo mecanismos protetivos vigentes e uma estrutura mínima de governança, vários países europeus enfrentam questionamentos sobre o escopo, a licitude e fiscalização do uso dos dados pessoais.

No contexto brasileiro a situação é desafiadora. Além de LGPD não se encontrar vigente e de não existir uma estrutura de governança pré-estabelecida, a Lei nº

23 European Data Protection Board (EDPB). Statement on the processing of personal data in the context of the COVID-19 outbreak. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf. Acesso em: 15 abr. 2020>.

13.979/2020 também é omissa no modo como a tomada de decisões sobre as informações pessoais de saúde dos indivíduos desenvolver-se-á. Assim, é necessário que a sociedade civil brasileira conheça os métodos empregados na vigilância de seus dados sensíveis como forma de também se vigiar a atuação estatal.

A GOVERNANÇA DO USO DE DADOS PESSOAIS SENSÍVEIS: UM CAMINHO A SER DESENHADO

Percebe-se que o tratamento de dados pessoais em situações emergências é entendido pelos órgãos públicos como uma ferramenta importante para orientar os processos de planejamento, resposta e avaliação de políticas e intervenções públicas. A utilização dessas informações não é algo inédito, haja vista a edição, pelo Comitê Internacional da Cruz Vermelha, de um guia sobre como proteger dados pessoais em atividades humanitárias[24].

O mesmo se aplica, inclusive, às medidas de monitoramento invasivo e granularizado dos *data subjects* implantadas em outros países e que agora se tenciona operar no Brasil. Apesar da tentativa de construção de uma narrativa de aceitação do uso desses dados, percebe-se a existência de vozes exigindo um diálogo maior sobre esses processos. Entretanto, considerável parte desses debates se furta a observar como a construção de mecanismos de governança pode ser um fator chave para o uso equilibrado dos dados pessoais.

Esse descuido com a dimensão da governança, fortalecido pela questionável omissão legal sob o tópico, potencializa o risco de operações de compartilhamento. Não há

24 International Committee of the Red Cross. Handbook on Data Protection in Humanitarian Action, 2017. Disponível em: <https://shop.icrc.org/e-books/handbook-on-data-protection-in-humanitarian-action.html?_ga=2.236018121.977086259.1586968722-2015191266.1586968722>. Acesso em: 15 abr. 2020.

uma lei de proteção de dados em vigência, tampouco uma estrutura mínima de governança apta a realizar a fiscalização indicando quem seria o responsável pelo exame das trocas de dados e qual seria a forma do compartilhamento das informações, atinente ao formato e às salvaguardas aplicáveis.

Considerando-se que a Autoridade Nacional de Proteção de Dados não se encontra operacionalizada, percebe-se uma lacuna institucional e procedimental quanto a governança das atividades de compartilhamento de dados pessoais. Ressalte-se que a temática não é estranha ao Ministério da Saúde, conforme o desenho da minuta[25], que estabelece uma estrutura mínima de governança e processos que regulam o acesso à informação e à cessão de dados custodiadas pelo SUS.

A partir da normatização instituída pela Comissão Intergestores Tripartide (CIT) do Ministério da Saúde, infere-se que a atribuição de normatizar e fiscalizar as atividades de compartilhamento de dados pessoais ficaria a cargo do Comitê Gestor da Estratégia de Saúde Digital[26]. Este possui a atribuição de acompanhar o desenvolvimento de aplicações informatizadas pelo Ministério da Saúde, coletando informações dos processos de atenção à saúde, e de monitorar e avaliar a implementação de projetos relacionados à utilização de ferramentas e dados digitais.

Dessa estrutura governamental, infere-se a inadequação conceitual e operacional para assumir a governança de um processo que alcança a privacidade da sociedade com o compartilhamento de dados pessoais sensíveis de saúde em larga escala. O comitê não

25 BRASIL. Minuta nº x, de 2018. Dispõe sobre a proteção e tratamento de dados pessoais em saúde e estabelece procedimentos para acesso à informação e cessão de bases de dados contendo informações pessoais custodiadas pelo SUS. Brasília, Disponível em: <https://www.saude.gov.br/images/pdf/2018/fevereiro/21/minuta-res-cit-dados-pessoais.pdf>. Acesso em: 14 abr. 2020.
26 BRASIL. Resolução nº 46, de 29 de agosto de 2019. Brasília, Disponível em: <http://www.in.gov.br/en/web/dou/-/resolucao-n-46-de-29-de-agosto-de-2019-221309239>. Acesso em: 14 abr. 2020.

possui exogenia, sendo composto somente por representantes do governo. Os entendimentos adotados se desenvolvem em espaços não transparentes, sem processo de responsabilização e prestação de contas, *accountability*, cujo critério de decisão dá-se por consenso e não por votação. Ademais, o comitê carece de recursos humanos e operacionais para fiscalizar, com o rigor técnico e legal, operações complexas com volume significativo, quantitativo e qualitativo, de dados pessoais sensíveis. A combinação desses elementos reforça o risco associado às atividades de compartilhamento que ora se pretendem realizar.

Nesse contexto, a adoção de valores e *frames* de governança, como os observados em operação no Comitê Gestor da Internet do Brasil e os aplicados às áreas de inteligência artificial e algoritmos, podem ser um ponto de partida. Associado a isso, a combinação do multissetorialismo[27] com as indicações de práticas de governança FAT (Fairness, Accountability and Transparency), permitem a estruturação de um mecanismo que seja capaz de garantir: a usabilidade dos dados, a adoção de práticas capazes de respeitar os direitos dos titulares dos dados e a operabilidade de medidas de minimização dos riscos da atividade de compartilhamento.

CONSIDERAÇÕES FINAIS

Algumas posturas indicam que um "certo nível de inacessibilidade seja um dos fatores mais importantes para a operação do direito à privacidade"[28]. Sustenta-se que o mais adequado para proteger as esferas informacionais pessoais seria a prática de *governability* e legitimidade regulatória[29]. As práticas, estruturadas em um mecanismo

27 Drake, W., 2011. Multistakeholderism: External Limitations and Internal Limits. MIND: Multistakeholder Internet Dialog, Collaboratory Discussion Paper Series No. 2. Berlin: Internet Policymaking Collaboratory, pp. 68-72.
28 Allen, Anita. Uneasy Access: Privacy for Women in a Free Society. Rowman & Littlefield, 1988.
29 Black, J., 2008. Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. Regulation & Governance. 2 (2), pp. 137-164.

multissetorial de governança FLAT (Fair, Legitimate Accountable and Transparent) possibilitam o desenvolvimento de um *framework* apto a exercer a governança em processos futuros de compartilhamento de dados pessoais em tempos de emergência pública.

A INTERPRETAÇÃO DO ARTIGO 6º DA LEI N. 13.979/2020 – OFENSA À AUTODETERMINAÇÃO INFORMATIVA E AUSÊNCIA DE *ACCOUNTABILITY* POR PARTE DA ADMINISTRAÇÃO PÚBLICA

Luís Fernando Costa Oliveira[30]

INTRODUÇÃO

A pandemia decorrente do covid-19 está deixando o mundo desesperado, seja pela crescente proliferação do "coronavírus" prejudicando a saúde da pessoa, ou mesmo os reflexos econômicos e sociais sequentes do isolamento.

A partir deste acontecimento, várias nações (e de forma conjunta)[31] começaram a utilizar medidas para conter o crescimento do covid-19. No ensaio, nós analisaremos o artigo 6° Lei 13.979/2020[32] que dispõe sobre "as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019".

---

30 Advogado do Escritório Costa e Garcia Advogados Associados. Bacharel em Direito pela Faculdade São Francisco de Piumhi. Especialista em Direito Empresarial pela Escola de Direito da Fundação Getúlio Vargas. Possui experiência na área de Direito, com ênfase em Direito Societário, Direito das Startups, Direito Digital, Investimentos e Direito Tributário. Disponível em: <http://lattes.cnpq.br/2401171428062068>. Acessado em: 15/04/2020.

31 Global Privacy Assembly. Mission and Vision. Disponível em: <https://globalprivacyassembly.org/the-assembly-and-executive-committee/strategic-direction-mission-and-vision>. Acessado em: 14/04/2020.

32 BRASIL. Lei n. 13.979/2020, de 6 de fevereiro de 2020 (Medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L13979.htm>. Acessado em: 13/04/2020.

O artigo em comento determina que qualquer dado poderá ser compartilhado, independente da vontade do titular. Além de ser uma medida imperiosa, pode esta acarretar discriminações no uso de informações. Os dados quando utilizados sobre determinado fato, até podem não conduzir problemas aquele titular, mas se associado a outros dados, levam detalhes da personalidade do indivíduo identificando-o, ou mesmo, trazendo à tona dados sensíveis da pessoa[33].

Para trazer segurança, titularidade, transparência, autonomia e impedir a discriminação pelo uso de dados pessoais e pessoais sensíveis, o artigo 6° da Lei 13.979/2020deverá ser interpretado à luz dos quatro elementos componentes da privacidade (pessoa-informação-circulação-controle[34]) e do princípio da autodeterminação informativa[35]. Na sequência, apontaremos que a ausência de *accountability*[36] por parte da Administração Pública, é capaz de prejudicar o fluxo informacional dos titulares de dados.

33 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Forense, 2020. p. 95.
34 Ibidem. p. 94.
35 "Privacidade como autodeterminação informativa/existencial e reconhecimento da construção dinâmica da identidade pessoal conjugam-se, assim, como novas formas de manifestação da proteção jurídica da pessoa humana contra as ameaças e estigmatização e discriminação oriundas do desenvolvimento tecnológico. Com efeito, a principal preocupação com relação ao armazenamento e circulação de informações relativas à pessoa humana diz respeito à sua utilização para submetê-la a estigmas, viabilizando sua discriminação perante as demais. Entre os diversos dados relativos à pessoa, alguns são especialmente idôneos a facilitar processos sociais de exclusão e segregação, razão pela qual seu controle deve ser ainda mais rigoroso. Essa é a chave de leitura adequada para compreender a qualificação de dados pessoais como sensíveis". KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: TEPEDINO, Gustavo, FRAZÃO, Ana, OLIVA, Milena Donato (coordenação). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 1ed. São Paulo: Thomson Reuters Brasil, 2019. p. 451.
36 Ana Frazão, nos remete os perigos decorrentes da sociedade de vigilância e fluxo de informação sem a devida transparência e accountability. "No contexto de uma sociedade de vigilância, o Big Data tudo vê, sendo capaz de capturar todas as pegadas digitais dos usuários para, a partir daí, utilizar seus "poderes" não apenas para registrar e processar o passado e o presente, como também para antecipar e decidir o futuro das pessoas. E o mais preocupante é que faz tudo isso sem a devida transparência e *accountability*. Já que os algoritmos utilizados por governos e grandes agentes empresariais são normalmente considerados segredos, respectivamente de Estado ou de negócios". FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In:* TEPEDINO, Gustavo, FRAZÃO, Ana, OLIVA, Milena Donato (coordenação). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 1ed. São Paulo: Thomson Reuters Brasil, 2019. |p. 38.

AUTODETERMINAÇÃO INFORMATIVA E ACCOUNTABILITY

O artigo 6° da Lei n.13.979/2020[37], origina quatro problemáticas: a) exclui de forma arbitrária, o direito do titular de controlar a obtenção dos seus próprios dados; b) não filtra quais categorias de dados poderão ser compartilhados; c) não apresenta nenhuma política interna de coleta, tratamento, segurança e eliminação dos dados; d) não traz política interna de transparência e *accountability*[38].

A redação do artigo 6° da Lei n. 13.979/2020 têm como consequência o afastamento do titular do dado do seu status de direito ao "consentimento informado" para o mero "consentimento implícito"[39]. O consentimento informado está diretamente ligado ao direito de privacidade de dados e a autodeterminação informativa[40].

O artigo 6° ao impor a obrigatoriedade de compartilhamento de dados, corrói o direito do titular em decidir quais os dados poderão ser circulados, se aquela informação

37 Transcrição in verbis: Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.
§ 1º A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária.
§ 2º O Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais.

38 A General Data Protection Regulation (GDPR), esclarece que o a accountability é de suma importância para o controlador, que deverá usar de medidas e registros adequados que demonstrem que aquele ente (público ou privado), detém conformidade e responsabilidade com as regras e regulamentações para a proteção de dados. Ela aponta duas chaves principais para esta conformidade: a) responsabilidade no cumprimento da GDPR e b) capacidade de demonstração da conformidade. "There are two key elements to accountability. First, the accountability principle makes it clear that controllers and processors are responsible for complying with the GDPR. Second, controllers and processors must be able to demonstrate compliance" (destaque nosso). Golden Data. What does "accountability" mean under EU Data Protection law? Disponível em: <https://medium.com/golden-data/what-does-accountability-mean-under-eu-data-protection-law-af630e40648b>. Acessado em: 14/04/2020.

39 Gustavo Tepedino e Chiara Spadaccini explicam a diferença dos dois tipos de consentimento: "(...) consentimento implícito (situação em que se entende que uma pessoa consentiu com algo em razão da conduta que assume) para o consentimento informado, o qual orienta inclusive normas relativas a circulação de informações, visto que manifesta de uma série de disposições que prescrevem quais devem ser as informações fornecidas ao interessado para que seu consentimento seja validamente expresso". TEPEDINO, Gustavo, de TEFFE, Chiara Spadaccini. O consentimento e proteção de dados na LGPD. In: TEPEDINO, Gustavo, FRAZÃO, Ana, OLIVA, Milena Donato (coordenação). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.1ed. São Paulo: Thomson Reuters Brasil, 2019.p. 291.

40 Podemos definir a autodeterminação informativa como: "(...) a faculdade de o particular controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos a ele". Ibidem. p. 291.

poderá ser transmitida, e, impedir o direito do titular de acompanhar o tratamento daquela informação.

A Administração Pública, ao compartilhar dados de titularidade da pessoa natural, de forma obrigatória e sem processamento adequado, acarreta reflexos negativos à pessoa natural. Há um *fluxo informacional desnecessário*, sob a justificativa de "evitar a propagação do covid-19", o que pode ocasionar uma discriminação de dados, ofensiva a dignidade da pessoa humana.

Questiona, se seria necessário, para evitar a disseminação da covid-19, dados sobre a opinião política, raça, filiação a organizações de caráter político e religioso, opção sexual. Certamente não; porém, o artigo 6° não veda esta possibilidade. Pelo contrário: ele a permite e reforça.

Desta forma, a importância da autodeterminação informativa é possibilitar que o titular de dados, por meio de sua fiscalização pessoal, consiga impedir qualquer abuso no fluxo informacional, direcionando-o a finalidade a que ela foi empregada, atendendo assim, a sua legítima expectativa, conforme ensina Bruno Bioni[41]:

> *"O principal vetor para alcançar tal objetivo é franquear ao cidadão controle sobre seus dados pessoais. Esta estratégia vai além do consentimento do titular dos dados, pelo qual ele autoriza o seu uso. Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expetativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da personalidade".*

41 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Forense, 2020. p. 104-105.

Mesmo nos casos de possibilidade de uso dos dados sem o consentimento do titular[42], em nenhuma hipótese deve ser impedida a autodeterminação informativa, para que o titular acompanhe este fluxo informacional compartilhado e participe do processo decisório de qual informação será pertinente para atingir o fim almejado.

Outro problema enfrentado em relação ao artigo 6° da Lei n. 13.979/2020 é se a Administração Pública, enquanto controladora, conseguirá processar adequadamente os fluxos de informações, respeitando a transparência e *accountability*. O grande problema ao deixar a enorme quantidade de fluxo informacional nas mãos do Estado, é que este é visivelmente inapto[43] para dar segurança e tratamento à circulação dos dados.

Há uma ausência de transparência e *accountability*, que visam dar nitidez e segurança por meio de processos internos de tratamento de dados, impossibilitando qualquer ofensa a direitos extrapatrimoniais decorrentes da personalidade humana.

Ana Frazão ressalta que para existir um processo confiável, deverá ser elaborado um controle que atenda: a qualidade de dados, que traduz como a forma pertinente e adequada para entender se aquela informação justifica a sua utilização[44]; e a qualidade do processamento de dados, que é a verificação da idoneidade dos programas utilizados, para assegurar um resultado assertivo[45].

O artigo 6° da Lei n. 13.979/2020 não apresenta nenhuma disposição ou nota técnica apresentando quais os dados que serão aplicados para justificar a sua utilização. Ele

---

42 Artigos 7° e 11, II.
43 Ao analisar apenas o site do Ministério da Saúde, fica nítido que este sequer tem uma política de proteção de dados, ou mesmo adequação a Lei 13.709/2018 (Lei Geral de Proteção de Dados), tampouco subsídios técnicos e de infraestrutura para armazenar e tratar os dados das pessoas naturais no Brasil.
44 FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo, FRAZÃO, Ana, OLIVA, Milena Donato (coordenação). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 1ed. São Paulo: Thomson Reuters Brasil, 2019. p. 38.
45 Ibidem. p. 38.

também não direciona a programação idônea no processamento dos dados, deixando um vácuo legislativo-normativo de como seriam os procedimentos para assegurar que o covid-19 não se prolifere no Brasil, sem que isso ocasione discriminação no uso do fluxo informacional.

Assim, o controlador deixa de praticar atos para atender a conformidade, diferente das tentativas feitas por outros países, que tentam criar um parâmetro de flexibilização para fazer o compartilhamento de dados, obedecendo suas leis de proteção de dados e a personalidade humana, sem provocar em uma discriminação informacional. Exemplos internacionais demonstram a preocupação com o regime jurídico de proteção de dados mesmo em tempos de pandemia.

O Centro de Controle e Prevenção de Doenças norte americano, por exemplo, solicitou às companhias aéreas apenas o nome, data de nascimento, endereço (domiciliar e e-mail) e número de telefone dos passageiros referente a determinados voos[46].

Mesmo a China, que não é exemplo de proteção de dados, emitiu orientações reconhecendo a necessidade de limitar a coleta de dados e seu uso durante esta crise de saúde pública[47].

Por fim, na Itália, foi adotado uma normativa que faz o cruzamento entre o Regulamento Europeu de Proteção de Dados e covid-19, com intuito restringir categorias de proteção dados especiais que podem ser suspensas durante o combate da covid-19[48].

Já o Brasil vai na contramão do planeta, não cria quais categorias de proteção,

46The International Association of Privacy Professionals. COVID-19 response and data protection law in the EU and US. Disponível em: <https://iapp.org/news/a/covid-19-response-and-data-protection-law-in-the-eu-and-us>. Acessado em: 14/04/2020.
47 Ibidem.
48 Ibidem.

obriga o compartilhamento de qualquer dado com a Administração Pública, retira o direito do titular de decidir, quais os dados poderão ser circulados, fiscalizar e acompanhar os seus fluxos informacionais inerentes à pessoa humana.

A ausência de fiscalização por parte do titular, e a ainda não vigente, a Lei Geral de Proteção de Dados[49] (que poderá ser prorrogada)[50], encaminha para uma grande insegurança jurídica no manuseio de dados ao combate ao coronavírus, retira direitos fundamentais do titular, e não demonstra como o cruzamento de dados, poderá resolver a disseminação no covid-19 no território brasileiro.

CONSIDERAÇÕES FINAIS

Conforme Hipócrates, extremos remédios são apropriados para extremas doenças[51]. Não obstante, a virtude está no meio (*in medio virtus*). Desta forma, mesmo as doenças mais extremas – como a covid-19 – não devem ser substrato para arbitrariedades da Administração Pública. O presente ensaio mostra os perigos, em particular ao sistema jurídico de proteção dos elementos da privacidade, que podem advir da ânsia de combater a covid-19, tais como crescimento de índices de discriminação, a ausência de transparência no manuseio dos dados e a impossibilidade de controle de dados por parte do titular.

49 BRASIL. Lei n. 13.709, de 15 de agosto de 2018 (Lei Geral de Proteção de Dados). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acessado em: 13/04/2020.
50 SENADO. Projeto de Lei n. 1179, de 30 de março de 2020. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141306>. Acessado em: 14/04/2020.
51 Conforme citação atribuída a Hipócrates, traduzida para o latim como: “ad extrema morbus, extrema remedia”.

CRISE SANITÁRIA E PRIVACIDADE: UM ENSAIO SOBRE A CONFLUÊNCIA ENTRE DIREITOS FUNDAMENTAIS E O INTERESSE PÚBLICO

Henrique Junqueira Arruda de Souza[52]

INTRODUÇÃO

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais brasileira (Lei nº 13.709/18), prevista para o próximo ano, representa um marco normativo inédito na tutela dos milhões de dados e informações pessoais disponibilizadas, coletadas e tratadas diariamente em território nacional. Ainda que a proteção desse bem jurídico, e verdadeiro ativo econômico na posse de empresas e organizações, já estivesse prevista na legislação esparsa – **Código de Defesa do Consumidor**, **Marco Civil da Internet**, **Lei do Sigilo Bancário** -, a nova legislação representa uma verdadeira mudança de paradigma no tocante à proteção de dados pessoais e um avanço desejável e amplamente aguardado no atual cenário caótico decorrente da pandemia causada pelo novo coronavírus.

LEI GERAL DE PROTEÇÃO DE DADOS: CONCEITOS E POSSIBILIDADES

Sem maiores surpresas, a LGPD traz consigo clara inspiração nos princípios e diretrizes da **GDPR (*General Data Protection Regulation*)** europeia, que representa o principal diploma normativo em vigor a respeito do tema, a começar pelos princípios que devem reger as atividades de coleta e tratamento de dados pessoais. Desta forma, a lei brasileira adiciona um décimo princípio ao rol (art. 6º, lei nº 13.709/2018) daqueles já

52 Graduando em Direito pela Universidade Federal de Lavras (UFLA) e membro do Núcleo de Inovação Tecnológica da Universidade Federal de Lavras (NINTEC/UFLA).

contemplados pela GDPR, qual seja, a **vedação à discriminação** (art. 6º, inc. IX), proibindo expressamente o processamento de dados para finalidades ilícitas e/ou práticas discriminatórias abusivas. Assim, o referido princípio, juntamente com aqueles referentes à **transparência**, **precisão**, **qualidade** e **integridade** dos dados, bem como à **limitação do tratamento às finalidades explícitas** e à **responsabilização** dos agentes responsáveis pelo tratamento, compõe, por assim dizer, a estrutura normativa da lei brasileira.

Prosseguindo, a distinção sobremaneira relevante para a proposta deste ensaio, inclusive já dotada de aplicações práticas[53], trata-se daquela entre dados pessoais sensíveis e não sensíveis. Muito embora os bens jurídicos ligados à honra, à privacidade e em última instância à dignidade já sejam tutelados em nosso ordenamento, os dados pessoais representam uma nova, e juridicamente relevante, dimensão (muito além da concepção do ***right of privacy***[54] americano do século XIX) da pessoa humana, justificando a necessidade de diretrizes mais claras em torno do tema. Nesse sentido, reputa-se como **dado pessoal** (art. 5º, inc. I) as informações de qualquer natureza relacionadas à pessoa natural identificada ou identificável. A seu turno, o legislador preocupou-se em delimitar um conjunto de informações que, pelo fato de versarem sobre aspectos existenciais especialmente relevantes para o pleno desenvolvimento da personalidade do ser humano - como saúde, genética, orientação sexual, convicções religiosas, opiniões político-partidárias, a condição social - são dignos de uma tutela ainda mais restritiva. São os chamados **dados pessoais sensíveis** (art. 5º, inc. II). É válido mencionar, ainda, que, no caso da GDPR europeia, há uma louvável preocupação com os casos nos quais

53 Tribunal de Justiça do Rio Grande do Sul - TJRS, Apelação Cível nº 0296615-34.2018.8.21.7000. Relator: Eugênio Facchini Neto. Julgado em: 18 de dezembro de 2018.
54 WARREN, Samuel D.; BRANDEIS, Louis D.; The Right to Privacy. Harvard Law Review, Volume 4, No. 5, pp. 193-220, 1890. Disponível em: <https://links.jstor.org/sici?sici=0017811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C>.

existe desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, sobretudo quando o agente responsável se trata de autoridade pública.

A lei geral brasileira, por sua vez, não faz menção explícita a tais situações, sendo, no entanto, inequívoco que a assimetria entre as partes deve ser considerada para fins de aferir se, de fato, o consentimento foi colhido de maneira livre e expressa. Tal cuidado e atenção são ainda mais imperiosos em hipóteses nas quais, como é o caso das relações de consumo ou de trabalho, a vulnerabilidade de uma das partes é presumida. Especialmente nos casos em que o consentimento é condição *sine qua non* para o acesso a determinados serviços – situação comumente chamada de *take-it-or-leave-it choice*[55] – ou mesmo ao emprego, haverá necessidade de uma análise criteriosa para avaliar se a manifestação de vontade realmente atende aos requisitos legais.

DADOS PESSOAIS NO CONTEXTO DA PANDEMIA

As múltiplas iniciativas no sentido de minimizar os efeitos do *lockdown*, que têm gerado até mesmo parcerias improváveis[56] em cenários de normalidade, estão focadas, primordialmente, no rastreamento baseado nos contatos e interações de um determinado indivíduo, dada a "ubiquidade" dos dispositivos móveis.

Logo, a partir de avanços consideráveis nos campos da criptografia, das redes descentralizadas, da computação em nuvem e, em geral, do poder de processamento dos computadores e smartphones, as tecnologias empregadas por governos e organizações privadas possibilitam o armazenamento e a transferência de uma miríade de dados e

55 BORGESIUS, Frederik Zuiderveen; KRUIKEMEIER, Sanne; BOERMAN, Sophie; HELBERGER, Natali. Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. European Data Protection Law Review, Volume 3, Issue 3, p. 353-368, 2018. Disponível em: <https://ssrn.com/abstract=3141290>.
56 "Apple and Google Team Up to 'Contact Trace' the Coronavirus". Disponível em: <https://www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html>.

informações, que, como mencionado anteriormente, representam verdadeiros ativos dotados de valor econômico. Nesse sentido, é que a utilização da tecnologia visando dar concretude a relações com efeitos jurídicos representa um campo já explorado, ao menos no que se refere às relações de cunho eminentemente patrimonial. Criptomoedas, *smart contracts* e o licenciamento de direitos de propriedade intelectual são alguns dos exemplos mais notáveis.

Especificamente, valendo-se da combinação das redes *peer-to-peer*, de algoritmos criptografados e mecanismos de consenso descentralizados, a *blockchain*[57] permite que diferentes pessoas entrem em acordo a respeito de um determinada circunstância ou acontecimento (vide uma transação de criptomoedas), de modo que o registro dessa situação seja verificável de uma maneira segura e transparente. O fato é que a real potencialidade do *blockchain* permanece, ainda, em grande medida, desconhecida. Entretanto, os potenciais usos e efeitos que versam sobre uma classe de ativo específico nos interessa: os dados pessoais.

Ao passo em que habilita a troca de dados e informações de maneira descentralizada, e, portanto, sem a intermediação de entidades de qualquer gênero, as características inerentes à *blockchain* também traduzem situações pouco "exploradas" pelos seus entusiastas, sobretudo no que tange à proteção de dados pessoais: a exposição, à centenas de milhares de computadores e outros dispositivos, tornando virtualmente impossível a remoção ou exclusão de determinado dado, sensível ou não. O confronto com as características inerentes da *blockchain* se torna mais evidente a partir do art. 7º da LGPD, que apresenta a hipótese de tratamento de dados pessoais tornados públicos,

57 Novo app usará blockchain para monitorar coronavírus sem expor usuários. Disponível em: <https://www.uol.com.br/tilt/noticias/afp/2020/04/15/aplicativo-para-combater-coronavirus-e-criado-na-america-latina.htm>.

sejam eles tornados públicos pelo próprio titular ou disponibilizados por ente público, podendo, tal tratamento ser realizado para finalidades diferentes daquela que motivou sua publicização inicial. É importante reiterar que a LGPD se aplica a todos aqueles que realizam tratamento de dados, incluindo o governo e as entidades destinadas à realização de atividades não lucrativas, como as instituições de pesquisa. Todavia, espera-se impacto significativo sobretudo na economia, seja diante do valor econômico dos dados, seja porque a atividade empresarial depende cada vez mais deles.

Para que não haja dúvida da amplitude da sua aplicação, a LGPD, em seu art. 5º, define como controlador toda "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (inc. VI) e como operador toda "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (inc. VII), agrupando-os conjuntamente na categoria de agentes de tratamento (inc. IX). Como se depreende do excerto, qualquer pessoa, natural ou jurídica, de direito público ou privado, pode ser considerada controladora ou operadora desde que, respectivamente, tenha poder decisório sobre tratamento de dados ou realize o referido tratamento em nome do controlador, independentemente da finalidade para a qual os dados estejam sendo utilizados. Embora a atuação de cada agente tenha peculiaridades para efeitos da definição do regime jurídico, há várias hipóteses de deveres comuns, assim como de responsabilidade solidária entre os dois, além da possibilidade de o próprio operador ser equiparado ao controlador (art. 42).

Portanto, no que se refere especificamente à coleta, tratamento e compartilhamento de dados pessoais de pacientes acometidos pelo COVID-19, e mesmo aqueles com mera suspeita de infecção (art. 6º, lei nº 13.979/2020) a temática reveste-se de singular importância, justamente por lidar com fatores de risco evidentes, a começar

pela vulnerabilidade inerente àqueles que se encontram infectados pelo vírus ou em situação de estrito monitoramento, e não menos relevante, por tratar-se da utilização explícita de dados sensíveis por parte do poder público, ainda que justificável do ponto de vista da preservação da saúde pública.

Ressalta-se que os gestores públicos devem ser cobrados[58] e, eventualmente, responsabilizados por excessos decorrentes de medidas que violem direitos fundamentais, tomadas no contexto da pandemia.

CONSIDERAÇÕES FINAIS

Tomando como exemplo iniciativas[59] já existentes no sentido de construir verdadeiras soluções baseadas na tecnologia disponível, com o intuito de armazenar grandes volumes de dados relativos à saúde, aos antecedentes criminais, à renda e qualquer tipo de informação que reconduza a uma pessoa natural identificada ou identificável no tempo e no espaço, ainda assim, é preciso ter em mente que as reais aplicações das várias inovações surgidas no contexto da *Lex Cryptographia*[60], despidas de qualquer regulação, podem ter efeitos catastróficos, especialmente se utilizadas por indivíduos e/ou empresas mal-intencionadas. Neste sentido, pode-se conceituar a natureza aberta da arquitetura empregada na *blockchain* e demais tecnologias correlatas como uma verdadeira faca de dois gumes.

Uma das possibilidades de resposta, perpassa, justamente, por não atrelar os dados à noção clássica de propriedade individual bem como aos direitos subjacentes nesse

58 MPF cobra explicação do governo de SP sobre uso de dados de celulares. Disponível em: <https://noticias.r7.com/sao-paulo/mpf-cobra-explicacao-do-governo-de-sp-sobre-uso-de-dados-de-celulares-15042020>.
59 "Amsterdã usa algoritmos para detectar violência doméstica e risco de despejo". Disponível em: <https://www1.folha.uol.com.br/mundo/2020/01/amsterda-usa-algoritmos-para-detectar-violencia-domestica-e-risco-de-despejo.shtml>.
60 WRIGHT, Aaron; DE FILLIPPI, Primavera. Decentralized Blockchain Technology and the Rise of Lex Cryptographia, 2015. Disponível em: <https://ssrn.com/abstract=2580664>.

tipo de relação jurídica. Relegar os dados, sobretudo aqueles sensíveis, à proteção característica de outros tipos de propriedade, pode, ao fim e ao cabo, reduzi-los à condição de verdadeiras *commodities*, que, inseridas na lógica da nova economia digital, restam entregues, diariamente, por milhões de pessoas, em troca de benefícios tão ilusórios quanto sua segurança. Assim, o que se deve perseguir é uma espécie de "despatrimonialização" dos dados pessoais[61], em que merece destaque, a ideia do consentimento contextual[62], especialmente no que tange as relações entre operadores de planos de saúde e segurados, tão relevantes na atual conjuntura socioeconômica. A ideia de perseguir um nível de segurança ótimo e ajustável conforme o fluxo da relação contratual, de modo a impedir a concessão de um consentimento inequívoco e definitivo para as novas situações que se amoldam na cadeia de vínculos obrigacionais parece bastante razoável para pautar a relação entre titulares e aqueles responsáveis pela coleta e o compartilhamento de dados pessoais, no âmbito público ou particular.

Nesse sentido é que os próximos esforços, legislativos e tecnológicos, devem buscar uma maior harmonização, de modo a traçar e estabelecer parâmetros que permitam uma maior clareza na ponderação entre os direitos fundamentais em jogo no momento da eclosão de crises que extrapolam fronteiras entre o público e o privado.

61 TEPEDINO, Gustavo. Premissas metodológicas para a constitucionalização do direito civil. Revista da Faculdade de Direito da UERJ, n. 5. Rio de Janeiro, 1997.
62 BIONI, Bruno Ricardo. Proteção de dados pessoais – a função e os limites do consentimento. Rio de Janeiro, Forense, 2019.

DADOS PESSOAIS E CORONAVÍRUS, DO ABUSO À LEGITIMIDADE

Marina Sayuri Kitayama[63]

Promulgada no dia 06 de fevereiro de 2020, a Lei 13.979 surge com o objetivo de regulamentar medidas do governo que visem o enfrentamento da crise de saúde pública ocasionada pela pandemia do coronavírus. Dentre as medidas, o artigo 6º da Lei, que autoriza às autoridades públicas a requisição de dados relativos à identificação de infectados para fins de combate à propagação do vírus[64], recai precisamente sobre a temática da proteção de dados pessoais. Isso nos move, então, à necessária análise acerca da interpretação do artigo à luz do que disciplina a matéria de direito.

As tecnologias informacionais representam, sem dúvida, ferramenta poderosa a guiar e auxiliar a atuação do poder público em diversas situações[65]. Em relação ao combate à Covid-19, alguns países optaram por investir fortemente em políticas de ação contra a pandemia com base em controles realizados a partir da apreensão de dados pessoais de seus cidadãos[66]. Dentre esses, a China é o caso mais paradigmático. O país detém controle informacional quase total sobre a população, precisando quem são infectados, suspeitos ou não, quem integra algum grupo de risco, onde reside cada indivíduo e qual sua geolocalização atual. Para isso, todos recebem um dispositivo que

63 Aluna de graduação da Faculdade de Direito da Universidade de São Paulo.
64 BRASIL. Lei ordinária n. 13.979 de março de 2020. Medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Disponível em: <http://www.in.gov.br/en/web/dou/-/lei-n-13.979-de-6-de-fevereiro-de-2020-242078735>.
65 NISSENBAUM, Helen. Privacy in context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, California, 2010, Introduction.
66 Covid-19: como promover a saúde pública e proteger a privacidade? Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/covid-19-como-promover-a-saude-publica-e-proteger-a-privacidade/?surface=meter_limit_reached&article_url=https%3A%2F%2Fpolitica.estadao.com.br%2Fblogs%2Ffausto-macedo%2Fcovid-19-como-promover-a-saude-publica-e-proteger-a-privacidade%2F>.

rastreia seus passos e que alerta as autoridades chinesas caso o cidadão ultrapasse determinações de movimentação do governo[67].

Não é inesperado que uma realidade como a chinesa nos soe um tanto distópica. Esse estranhamento não se dá somente em razão de uma incapacidade econômica ou tecnológica para que algo parecido seja implementado no Brasil. Em nosso caso, o verdadeiro impeditivo encontra-se nas barreiras inerentes a um estado democrático de direito com uma visão política e cultural particular sobre a privacidade. Essa visão está amarrada na ideia de que, assim como as tecnologias informacionais podem ser ferramentas úteis para que se atinja fins de interesse público, também poderiam ser úteis para o exercício de fins contrários a este. Há um temor não infundado a respeito da possibilidade do Estado, controlando amplamente informações a respeito de seus cidadãos, exercer de forma abusiva o poder advindo desse controle. Tal abuso poderia expressar-se desde na criação de um estado de vigilância constante até a na tomada de decisões discriminatórias justificadas pelos reflexos de preconceitos sociais já existentes.[68] É justamente pelos perigos potenciais que representam, que o direito brasileiro garante a proteção de dados de seus cidadãos.

Portanto, a interpretação correta do artigo 6º da lei 13.979 exige a observância do que o ordenamento entende e disciplina a respeito da proteção de dados pessoais. Para interpretá-lo desse modo, o presente ensaio propõe-se a traçar em que medidas a normativa em questão é legítima, e assim, posteriormente buscar compreender os limites de sua aplicação.

---

67 Disponível em: https://www.bbc.com/portuguese/internacional-52129955
68 RODOTÀ, Stefano. Org. BODIN, Maria Celina. Trad. DONEDA, Danilo e DONEDA, Luciana. A vida na sociedade de vigilância, a privacidade hoje. Rio de Janeiro: Renovar, 2008, Parte I, cap.1.

Diferentemente do que ainda possa se pensar, a proteção de dados não é matéria que se propõem a barrar o fluxo informacional, de maneira quase contrária, seu grande mote é, em realidade, assegurar que esse fluxo se dê apropriadamente[69]. Diante a forma como a sociedade atual é organizada, tentar impedir o compartilhamento de dados seria um ideal impossível e, até, desinteressante. Hoje, os dados são base de nosso modo de produção, da forma como nos relacionamos, sendo ainda condição de acesso a uma infinidade de produtos e serviços. A informação passou a ser fundamental no desenvolvimento de estratégias empresariais e políticas diversas, não sendo à toa o fato de tornar-se uma moeda de troca.

Nesse sentido, é justamente pela sua posição central na organização social e pela capacidade de serem utilizados como insumo para que se alcance o interesse público, que se legitima o uso dos dados pessoais pelas autoridades estatais. Note-se contudo, que esse uso encontra-se condicionado a um fim quisto pela coletividade e está sujeito às normas que visam conter suas potencialidades perigosas. Portanto, o artigo 6º da Lei, para que legítimo, deve ser aplicado em observância ao ordenamento jurídico no que diz respeito à proteção de dados pessoais. Isso requer, principalmente, uma atenção em relação ao princípio da ponderação sobre os atos administrativos de requisição de informações de identificação de cidadãos, bem como atenção à preservação da autodeterminação informativa dos brasileiros.

No contexto de uma sociedade informacional[70], a proteção de dados pessoais tornou-se direito autônomo, relacionado não somente a questões relativas à

69 "What people care most about is not simply restricting the flow of information but ensuring that it flow appropriately, and an account of appropriate flow is given here through the framework of contextual integrity." In: NISSENBAUM, Helen. Privacy in context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, California, 2010, Introduction.
70 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Forense, 2020. Parte I, cap. 1.

privacidade em um sentido individual[71], mas também assumindo um papel perante a coletividade, uma vez que a maneira como as informações são tratadas trazem implicações diretas na vida cotidiana de todos. Porém, mais que isso, os dados como representação do indivíduo perante a sociedade tornam-se extensão de sua própria personalidade, o que leva ao entendimento de que, atualmente, a proteção de dados pessoais trata-se de um direito fundamental.[72] Assim, apesar de ser comum a acepção dos dados como a nova *commodity* da economia global, deve-se ponderar que mesmo dada sua relevância econômica notória, os dados pessoais não estão no campo do direito da propriedade, e sim da personalidade e, por isso, não são matéria prima como o petróleo. Por tal razão, é essencial que a técnica hermenêutica sobre a aplicação do artigo 6º caput e seu § 1º ocorra sob um procedimento de balização a fim de que possíveis violações à proteção de dados sejam limitadas pela relação finalidade e necessidade da ação estatal.

A Lei deixa em aberto uma série de questões que não podem ser interpretadas de forma a prejudicar o lado mais fraco da relação entre cidadão e Estado. A normativa, por exemplo, não deixa claro a quais dados de identificação de infectados ela se refere. Poderiam eles serem relativos à doenças estigmatizantes que colocam o paciente em grupo de risco?[73] Poderiam, por exemplo, fazer referência às pessoas com quem o então infectado teve contato ou com quem reside? Seria legal caso se tratassem de informações instantâneas da atual localização daquele indivíduo? A falta de clareza da Lei não pode ser entendida como uma prerrogativa para a atuação discricionária do Estado, não sendo todos ou quaisqueres os dados pessoais essenciais para a

71 RODOTÀ, Stefano. Org. BODIN, Maria Celina. Trad. DONEDA, Danilo e DONEDA, Luciana. A vida na sociedade de vigilância, a privacidade hoje. Rio de Janeiro: Renovar, 2008, Parte I, cap.1.
72 Idem.
73 COSTA, Vinicius Venancio. 'Lei coronavírus', saúde e reflexos na privacidade Os direitos dos titulares estão em salvaguarda? Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lei-coronavirus-saude-e-reflexos-na-privacidade-14032020>.

implementação de políticas de combate à pandemia. Assim, ter-se claro aquilo que é necessário e aquilo que é excesso torna-se imprescindível para que a coleta de informações pessoais pelo poder público seja de fato legítima perante o direito à proteção de dados e ao ordenamento jurídico como um todo.

Está de acordo com essa visão a postura adotada pelas empresas de telefonia móvel em resposta à requisição dos dados pessoais de localização dos aparelhos celulares da população. Segundo a SindiTelebrasil[74], as empresas irão repassar para o Governo Federal os dados dos quase 220 milhões de celulares de brasileiros de modo aglomerado, estatístico e anonimizado (de modo similar foram firmados também acordos com outros entes da federação e empresas de telefonia[75]). Em entrevista à BBC News Brasil[76] o presidente-executivo do sindicato afirmou que o compartilhamento de informações individualizadas da maneira como requisitado pelo poder público seria ilegal, sendo esse também o entendimento da Advocacia-Geral da União.

Apesar desse cuidado das empresas, tem razão Rodotà[77] ao dizer que *" (...) é fácil objetar que mesmo as coletâneas de dados anônimos podem ser manipuladas de forma gravemente lesiva aos direitos dos indivíduos: tenha-se em mente o uso que pode ser feito dos dados, agregados, que digam respeito a uma minoria racial ou linguística; ou as consequências de uma decisão política ou econômica tomada justamente com base na análise de dados anônimos. (...)".* Diante tal possibilidade, é essencial a existência de

74 Coronavírus: governo brasileiro vai monitorar celulares para conter pandemia, BBC Brasil. Disponível em: <https://www.bbc.com/portuguese/brasil-52154128?fbclid=IwAR3OML6IzSag7s31OzUH6BhUAp0oQbaZCPYlZaHgGol29HAW-mpd_s3CdUDo>.
75 Governo vai usar dados de operadoras para monitorar pandemia, Folha UOL. Disponível em: <https://www1.folha.uol.com.br/mercado/2020/04/governo-vai-usar-dados-de-operadoras-para-monitorar-deslocamentos-na-pandemia.shtml>.
76 Coronavírus: governo brasileiro vai monitorar celulares para conter pandemia, BBC Brasil. Disponível em: <https://www.bbc.com/portuguese/brasil-52154128?fbclid=IwAR3OML6IzSag7s31OzUH6BhUAp0oQbaZCPYlZaHgGol29HAW-mpd_s3CdUDo>
77 RODOTÀ, Stefano. Org. BODIN, Maria Celina. Trad. DONEDA, Danilo e DONEDA, Luciana. A vida na sociedade de vigilância, a privacidade hoje. Rio de Janeiro: Renovar, 2008. P. 32.

uma política de transparência sobre o tratamento desses dados e de intervenção daqueles interessados para que possam controlar a exatidão daquelas informações.

Por isso, mais que garantir que o fluxo de dados atenda aos critérios da relação necessidade e finalidade, é essencial que se assegure a *autodeterminação informativa*[78] dos indivíduos, conceito que diz respeito ao controle do titular sobre seus dados, sendo algo bem mais complexo que apenas a ideia de consentimento formal. Nesse caso, a concretização da autodeterminação está intrinsecamente ligada a dois pontos, o dever de transparência daqueles que controlam e processam os dados pessoais e a existência de instrumentos que permitam ao titular e intereressados questionarem o uso e a qualidade dessas informações.

Um dos instrumentos mais importantes que garantem um mínimo de dever de transparência do poder público é a Lei de Acesso à Informação, a salvaguarda da norma é imprescindível para que o cidadão acompanhe a atuação estatal e portanto essencial quando pensamos em uma política de transparência do controle dos dados da população. Por tal razão, a aprovação da MP 928/2020[79] no dia 24 de março causou enorme preocupação ao suspender os prazos de resposta para os pedidos de informações feitos à administração baseados na LAI. As restrições impostas pela medida foram suspensas dois dias após sua promulgação e, em 30 de abril, o STF, em decisão unânime, as derrubou por violação ao princípio da transparência e da publicidade[80]. A MP, pensando somente nas implicações quanto à proteção de dados, se mantida, traria

78 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Forense, 2020. Parte I, cap. 2.
79 Medida provisória suspende prazosde respostas via lei de acesso à informação, Senado notícias. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/03/24/medida-provisoria-suspende-prazos-de-respostas-via-lei-de-acesso-a-informacao>.
80 STF confirma decisão que impede restrições na Lei de Acesso à Informação. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/04/30/stf-confirma-decisao-que-impede-restricoes-na-lei-de-acesso-a-informacao

um estado de extremo dequilíbrio informacional, reduzindo drasticamente a possibilidade dos indivíduos sequer imaginarem se há algo a ser questionado a respeito do uso de seus dados pessoais pela autoridade estatal.

A sociedade deve atentar-se à instauração de uma caixa preta sobre as atividades realizadas com seus dados. Tratando-se de um contexto de caráter emergencial e de extrema gravidade, é esperado que muitas medidas sejam tomadas de maneira menos cautelosa que o necessário. Sabe-se, por exemplo, que até a primeira dezena do mês de abril, o Governo Federal não havia nem ao menos definido quem estaria à frente da política de governança desses dados, tampouco qual seria o período de armazenamento, a estratégia de segurança e anonimização e nem disponibilizou o instrumento jurídico referente ao acordo de cooperação firmado com as empresas de telefonia que compartilharão dados da população[81]. A falta de transparência é motivo de grande preocupação, pois dificulta, se não impossibilita, o controle dos titulares sobre a utilização daquilo que é extensão de sua própria personalidade.

O que se conclui a partir da conjuntura apontada é que a utilização de dados pessoais dos indivíduos é, ao que indicam outras experiências, ferramenta poderosa no combate à propagação da Covid-19, o que legitima medidas de requisição de informações nos termos do artigo 6.º da Lei 13.979/2020. Contudo, a interpretação do texto normativo está sujeita aos ditames do ordenamento jurídico sobre a matéria de proteção de dados pessoais, de forma a ser fundamental que os dados compartilhados sejam somente aqueles essenciais e apresentados da maneira menos intrusiva possível,

81 Covid-19: como promover a saúde pública e proteger a privacidade? Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/covid-19-como-promover-a-saude-publica-e-proteger-a-privacidade/?surface=meter_limit_reached&article_url=https%3A%2F%2Fpolitica.estadao.com.br%2Fblogs%2Ffausto-macedo%2Fcovid-19-como-promover-a-saude-publica-e-proteger-a-privacidade%2F>.

como dados anônimos, conglomerados ou estatísticos. Mesmo assim, ainda é essencial a existência de políticas de transparência concretas a respeito do tratamento desses dados e das ações tomadas a partir deles, porque é isso que torna possível aos indivíduos se auto-determinarem informativamente nesse contexto. A falta de transparência que tem sido dada à questão não pode deixar de ser cobrada, pois só há uma forma de garantir a efetividade da livre circulação informacional, tornando-a uma via de mão dupla.

PARTE II

A AUSÊNCIA DE SALVAGUARDAS QUE FRAGILIZA DIREITOS

TRANSPARÊNCIA, PRIVACIDADE E PROTEÇÃO DE DADOS EM TEMPOS DE CORONAVÍRUS E ALÉM DA PANDEMIA

Viviane Ceolin Dallasta Del Grossi

> *Sobre se eu tenho a sensação de que a janela de tempo para debater como queremos viver no futuro e qual será nossa atitude em relação a essas tecnologias está pouco a pouco se fechando, sim, a tenho. Não porque as pessoas continuem se comportando da mesma maneira. Hoje em dia as pessoas são mais conscientes do que nunca da vigilância, e estão mais indignadas do que nunca por isso, mas também se sentem impotentes diante dessa transformação.*
>
> Edward Snowden[82]

> *O coronavírus é o novo terrorismo. É o pretexto mais recente para violações de direitos, e temo que persista muito depois que a crise terminar.*
>
> Kenneth Roth[83]

No dia 31 de março de 2020, a organização Access Now lançou um relatório com recomendações de privacidade e proteção de dados para que os governos enfrentem a COVID-19[84] de uma maneira que respeite os direitos humanos. As recomendações do documento sobre privacidade e proteção de dados na luta contra a pandemia se concentraram em três categorias de iniciativas: (a) coleta e uso de dados de saúde; (b) rastreamento e geolocalização; e (c) parcerias público-privadas.

82 Resposta dada por Edward Snowden, em setembro de 2019, em uma entrevista publicada pelos sete jornais europeus que formam parte da LENA - Leading European Newspaper Alliance, uma iniciativa que surgiu em 2016 para fomentar o jornalismo de qualidade. Entrevista disponível em: <https://brasil.elpais.com/brasil/2019/09/13/internacional/1568390496_167835.html>. Acesso em: 30 mar. 2020.

83 Diretor da Human Rights Watch. "Autocratas tentam sobreviver ao inimigo invisível". Disponível em: < https://www.anj.org.br/site/component/k2/97-midia-nacional/27711-autocratas-tentam-sobreviver-ao-inimigo-invisivel.html>, acesso em 15 abr. 2020.

84 RECOMMENDATIONS on privacy and data protection in the fight against COVID-19. Disponível em: <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>, acesso em 10 de abr. 2020.

Na mesma linha da recomendação da Access Now, no dia 06 de abril de 2020, a Autoridade Europeia de Proteção de Dados, Wojciech Wiewiórowski, em comunicado intitulado "EU Digital Solidarity: a call for a pan-European approach against the pandemic"[85], referiu que o Regulamento Geral de Proteção de Dados Europeu (GDPR) afirma que o direito à proteção de dados pessoais não é um direito absoluto, deve ser considerado em relação à sua função na sociedade e equilibrado com outros direitos fundamentais, de acordo com o princípio da proporcionalidade. Observado que a legalidade do tratamento dos dados pessoais - mesmo os chamados dados sensíveis, como dados sobre saúde - pode ser alcançada quando o tratamento for necessário por razões de interesse público substancial, com base na legislação da União ou dos Estados-Membros, que será proporcional ao objetivo perseguido, em caráter temporário (apenas enquanto perdurar a crise), com propósitos e acesso aos dados limitados.

Tais critérios também estão presentes na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) que, em que pese ainda não ter entrado oficialmente em vigor, deve ser utilizada como um norte na implementação das iniciativas de monitoramento no país[86].

85 EU Digital Solidarity: a call for a pan-European approach against the pandemic. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf>, acesso em 10 abr. 2020.
86 É o que recomenda, inclusive, a Electronic Frontier Foundation (EFF), umas das principais organizações de defesa dos direitos digitais. A Analista de políticas para a América Latina da EFF, Veridiana Alimonti, declarou que em que pese não ter entrado ainda em vigor, "medidas para o combate ao vírus vindas do poder público e da iniciativa privada devem ter suas regras como base". Disponível em: <https://tribunademinas.com.br/especiais/tech/13-04-2020/uso-de-dados-pessoais-no-combate-a-covid-19-precisa-ser-transparente.html>. Acesso em 14 abr. 2020. A mesma orientação é expressa na Nota expedida pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (Secretaria de Telecomunicações Departamento de Serviços de Telecomunicações NOTA INFORMATIVA Nº 1192/2020/SEI-MCTIC), em 30 de março de 2020, em resposta à ANATEL – "Por meio do Ofício n. 101/2020/GPR-ANATEL, de 23 de março de 2020 (SEI 5320294), e do Ofício n. 121/2020/GPR-ANATEL, de 29 de março de 2020 (SEI 5346966), a Agência Nacional de Telecomunicações - Anatel dá ciência a este Ministério de iniciavas referentes ao compartilhamento de dados de usuários de serviços de telecomunicações para fins de combate ao COVID-19 e solicita considerações técnicas e jurídicas quanto ao tema".

Nesse contexto, a Autoridade Europeia de Proteção de Dados sugeriu nesse documento que os países membros desenvolvessem um "aplicativo móvel COVID-19 comum". O aplicativo seria idealmente construído em coordenação com a Organização Mundial de Saúde e garantiria a proteção de dados por design desde o início. Assim, Wojciech Wiewiórowski declarou que “a solidariedade digital se recusaria a replicar os modelos de negócios agora manchados e desacreditados de vigilância e direcionamento constantes que prejudicaram a confiança na sociedade digital, mas permitirão que a proteção de dados sirva a humanidade durante este exame extraordinário”.

Ainda não está claro quem iria desenvolver o aplicativo, mas um grupo de pesquisadores de oito países da UE lançou recentemente o código do aplicativo “Rastreamento de proximidade de preservação de privacidade pan-europeu”. Usando sinais *bluetooth* entre telefones celulares, o aplicativo poderá detectar quando os usuários estão próximos o suficiente para infectar um ao outro. Esses dados seriam armazenados apenas no dispositivo da pessoa. Mais tarde, se o indivíduo apresentar um resultado positivo para coronavírus, o aplicativo usaria os dados para alertar aqueles que estiveram em contato com a pessoa infectada. Esse sistema tem várias vantagens em relação à proteção e privacidade dos dados: os dados são anonimizados e a identidade da pessoa que usa o aplicativo não é revelada. Terceiros não têm acesso aos dados coletados, o que garantiria que nem mesmo os governos possam adquirir informações que possam ser potencialmente mal utilizadas no futuro e, mais, o aplicativo seria usado voluntariamente, o que dependeria que uma parcela significativa da população europeia decidisse usá-lo[87].

87 Aqui entram as valiosas ponderações de Yuval Harari em artigo publicado no Financial Times em que refere que “(...) a solução não é impor um regime autoritário. A solução é restaurar a confiança na ciência, na mídia e nas autoridades públicas. Depois de ter essa confiança, você pode confiar nas pessoas para fazer a coisa certa, mesmo sem vigilância constante e medo de punição”. (...) Pedir às pessoas que escolham entre privacidade e saúde é, de fato, a própria raiz do problema. Porque essa é uma escolha falsa. Podemos e devemos desfrutar tanto de privacidade quanto de saúde. Podemos escolher proteger nossa saúde e impedir a epidemia de coronavírus. não instituindo regimes totalitários de vigilância, mas capacitando os cidadãos". (...) Para que isso ocorra, precisamos

Mecanismos de vigilância e acesso a dados de usuário em parceria com telefônicas têm sido estratégias adotadas por inúmeros países recentemente, como forma de combater a propagação do vírus, garantindo que as medidas de isolamento impostas estão sendo respeitadas, inclusive, com diversas iniciativas em curso no Brasil[88]. A China é um exemplo máximo dessa política, já sendo caracterizada como um Estado policial digital[89].

Em que pesem todas as diretrizes já recomendadas mundialmente para utilização dessas tecnologias no combate ao coronavírus – temporariedade, limitação de propósito e de acesso, excepcionalidade das medidas –, a discussão subjacente diz respeito à flexibilização do direito à privacidade em prol do direito à saúde, sem que passemos a viver em um estado de exceção permanente, ou seja, assegurar que essas medidas se-

garantir que a tecnologia seja regulamentada e colete apenas os dados necessários, e que esses dados sejam armazenados adequadamente e por um período definido. Também é absolutamente crucial garantir que os dados coletados com o objetivo de combater a pandemia de coronavírus não sejam utilizados para outros fins, como policiamento, e que tenhamos as salvaguardas necessárias para impedir que isso acarrete danos. Trechos traduzidos livremente. FINANCIAL Times. Yuval Noah Harari: the world after coronavirus disponível em: <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75>, acesso em 05 abr. 2020.

88 No contexto nacional, interessante a leitura da Nota expedida pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (Secretaria de Telecomunicações Departamento de Serviços de Telecomunicações NOTA INFORMATIVA Nº 1192/2020/SEI-MCTIC), em 30 de março de 2020, em resposta à ANATEL – "Por meio do Ofício n. 101/2020/GPR-ANATEL, de 23 de março de 2020 (SEI 5320294), e do Ofício n. 121/2020/GPR-ANATEL, de 29 de março de 2020 (SEI 5346966), a Agência Nacional de Telecomunicações - Anatel dá ciência a este Ministério de iniciavas referentes ao compartilhamento de dados de usuários de serviços de telecomunicações para fins de combate ao COVID-19 e solicita considerações técnicas e jurídicas quanto ao tema", Nº do Processo: 01250.013581/2020-12.

89 Esse tipo de vigilância teria precedentes históricos, disse Maya Wang, pesquisadora da Human Rights Watch na China. A China tem um histórico de uso de grandes eventos, incluindo os Jogos Olímpicos de Pequim de 2008 e a Expo Mundial de 2010 em Xangai, para introduzir novas ferramentas de monitoramento que superam seu objetivo original, disse Wang."O surto de coronavírus está provando ser um desses marcos na história da disseminação da vigilância em massa na China", disse ela. Tradução livre. Disponível em: <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>. Acesso em 10 abr. 2020. Os governos de São Paulo e de Pernambuco são exemplos de utilização das técnicas de monitoramento, em que pese a determinação de suspensão de utilização dessas tecnologias pelo Presidente da República recentemente. Disponível em: <https://blogs.oglobo.globo.com/lauro-jardim/post/bolsonaro-intervem-e-trava-geolocalizacao-celular.html>, acesso em 13 abr. 2020. O governo do estado de São Paulo está sendo questionado judicialmente acerca do monitoramento, ver: < https://www.conjur.com.br/2020-abr-14/doria-questionado-justica-monitoramento-celulares>, acesso em 15 abr. 2020.

jam realmente temporárias e os dados não sejam utilizados posteriormente para finalidades escusas e ilegais, visto que ativistas alertam para a facilidade com que os dados agregados podem ser posteriormente reidentificados[90].

No contexto nacional, no dia 23 de março de 2020, foi publicada a Medida Provisória nº 928, para fins de alterar a Lei nº 13.979, de 6 de fevereiro de 2020, que dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019, e revogar o art. 18 da Medida Provisória nº 927, de 22 de março de 2020.

O direito de acesso à informação está explicitado no art. 6º, da Lei nº 13.979/2020:

> *Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.*
>
> *§ 1º A obrigação a que se refere o caput deste artigo estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária.*
>
> *§ 2º O Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais.*

O §1º acima remete a todas as ponderações efetuadas no presente ensaio até o momento, sendo curioso que um dos principais pontos de interesse e atenção das iniciativas governamentais ultimamente estejam se dando primordialmente na utilização do

90 Ver: <https://www.brasil247.com/ideias/combate-ao-coronavirus-pode-levar-a-destruicao-da-privacidade-na-internet-alertam-ativistas>, acesso em 12 abr. 2020.

disposto neste parágrafo, em que as empresas de telefonia estão sendo instadas a fornecer dados sensíveis de usuários, sem que antes uma abordagem séria esteja se dando de modo a efetivar o disposto no §2º do mesmo artigo.

É precisamente sobre a regra insculpida no §2º acima que as iniciativas governamentais deveriam se debruçar imediatamente, de forma a melhor atender ao interesse público na área da saúde, visto que desde o início da crise ocasionada pela pandemia, foram identificados problemas em relação aos dados publicados pelo Ministério da Saúde, a ausência de divulgação de informações sobre quantidade de testes disponíveis e administrados, e de materiais e equipamentos de proteção para a área da saúde, bem como a falta de transparência sobre as metodologias de coleta de dados.

Diferentemente do que outros países têm feito para lidar com a crise, o Brasil não está divulgando informações mínimas sobre a disponibilidade de insumos básicos para lidar com a situação. Se disponíveis, tais informações permitiriam avaliar a capacidade de poder público dar conta de uma demanda que promete ser crescente, sem prazo de término.

Certamente há intensa procura desses dados também via Lei de Acesso à Informação, mas, nessa situação de emergência, o país não dispõe de tempo para aguardar que o governo disponibilize respostas individualizadas e em até 30 dias a cada cidadão que formule um pedido. É necessário que esses dados estejam disponíveis em formato aberto, no próprio portal de dados abertos do governo federal (dados.gov.br).

Desse modo, a divulgação das informações sobre: quantidade de testes e materiais de enfrentamento da epidemia disponíveis e distribuídos a cada estado, compras públicas de equipamentos (máscaras, testes, ventiladores etc.), incluindo quantidades, destinação e contratos e taxa de ocupação de leitos de UTI, no portal de dados abertos

do governo federal (dados.gov.br), configuraria medida extremamente salutar para a melhor tomada de decisão de gestores sobre alocação e gerenciamento de recursos no combate à epidemia[91].

No que diz respeito à falta de transparência sobre as metodologias de coleta dos dados, o Ministério da Saúde não disponibiliza informações sobre os métodos adotados e tratamento dos dados, tampouco um histórico com as eventuais mudanças de metodologia ao longo do período[92].

Nesse contexto, o que se pretende com o presente ensaio é alertar para a necessidade de utilização da tecnologia, cruzamento e gerenciamento de dados que deve ser efetuada pelo poder público, com fundamento no interesse coletivo, como medida prioritária antes de pretender atuar na restrição de privacidade dos cidadãos. Onde há recursos escassos, como em nosso país, deve-se pautar pela conscientização e reforço da confiança pública, com a divulgação dos dados que interessam a todos no combate e melhor gerenciamento da crise, com o cumprimento do disposto no §2º, do art. 6º, da Lei nº 13.979/2020, em caráter primordial, sem reproduzir acriticamente iniciativas externas, as quais, posteriormente, teremos dificuldade de combater e saber se realmente foram cessadas.

---

91 "Uma dúvida que pode estar ocorrendo aos epidemiologistas engajados em tentar projetar a capacidade do sistema de saúde, por exemplo, é a respeito de recursos físicos: quantos testes já foram administrados e quantos há em estoque? Responder esse tipo de informação com um prazo mais dilatado – ou negá-la sem possibilidade de recurso – significa promover a falta de agilidade na busca de soluções alternativas. (CAMPAGNUCCI, Fernanda; SOARES, Marcelo. "Pandemia não é hora de quebrar termômetros"). Disponível em: <https://brpolitico.com.br/noticias/artigo-pandemia-nao-e-hora-de-quebrar-termometros/>, acesso em 30 mar. 2020.

92 A imprensa já reportou problemas no formulário de notificação compulsória, conforme publicado pelo Estado de S. Paulo em 20/03/20: "Falha em protocolo do ministério abre brecha para subnotificação de casos de coronavírus". Disponível em: <https://saude.estadao.com.br/noticias/geral,falha-em-protocolo-doministerio-abre-brecha-para-subnotificacao-de-casos-de-coronavirus,70003240788>, acesso em 20 mar. 2020.

A depender das movimentações mundiais que estamos vivenciando, se a preocupação aventada por Edward Snowden, em um momento pré-pandemia, já fazia sentido, a emergência em saúde pública global ocasionada pelo Coronavírus acelerou exponencialmente o fechamento dessa janela de tempo para estabelecermos como queremos viver no futuro próximo e como o direito à privacidade será usufruído depois disso.

RELAÇÃO ENTRE MEDIDAS EMERGENCIAIS PARA O COMBATE AO COVID-19 E A PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Thaís Coelho da Silva

O conceito de proteção de dados está em constante mudança, assim como o seu objeto: o tratamento de dados pessoais e a privacidade de seu detentor. Por muitos anos, as informações, especialmente as particulares, permaneceram reguladas por institutos genéricos[93] e, certamente, um dos imbróglios para a mudança desse cenário foi a dificuldade em entender o significado de privacidade.

Por causa disso, propôs Daniel J. Solove[94] que o conceito de privacidade deveria considerar a dinamicidade de seu objeto, e não se ater apenas a parâmetros fixos de aferimento. Isso significa que o contexto que cerca esse direito deve ser ponderado a fim de ampliar sua proteção, pois a privacidade, enquanto um direito da personalidade e, também, por estar diretamente relacionada com à dignidade da pessoa humana (art.

[93] Nas palavras de Pupo: "(...) historicamente, a privacidade estava intimamente ligada ao fato de a pessoa ter uma forma de delimitá-la e protegê-la. Em seus primórdios, a propriedade seria a forma absoluta de exercício desse direito." (Pupo, Alvaro de Carvalho Pinto. *Privacidade, liberdade de expressão e proteção dos dados pessoais: uma perspectiva brasileira com base na jurisprudência do Supremo Tribunal Federal*. 2017. 121 f. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2017, p. 12).

[94] SOLOVE, Daniel J. *Understanding Privacy*. Harvard University Press: Cambridge, Massachusetts, 2010, p. 06-08.

1º, inciso III da CF), assegura ao sujeito o direito à autodeterminação e ao pleno desenvolvimento de sua personalidade[95].

Nessa esteira, a proteção de dados adquire suma relevância pois torna-se o principal instrumento na busca pelo uso dados de forma justa em uma sociedade informatizada, bem como para a proteção da privacidade dos indivíduos, visto que decorre da garantia da inviolabilidade da vida privada (art. 5º, inciso X da CF)[96], direito de natureza fundamental que não admite interpretação restritiva para diminuir o seu campo de incidência.

E é a partir desse pressuposto que se inicia a análise das medidas emergenciais de combate ao COVID-19 e a sua relação com a privacidade e a proteção de dados, especialmente no que tange aos limites de interpretação do art. 6º da Lei 13.979/2020 – informalmente denominada "Lei da Quarentena" – diante dos parâmetros de autodeterminação informativa e do direito à proteção de dados pessoais.

No contexto de proteção de dados, a autodeterminação informativa, prevista pelo art. 2º, inciso II da Lei 13.709/18 ("Lei Geral de Proteção de Dados – LGPD")[97] é um dos princípios norteadores que busca transmitir ao usuário o poder de decisão e proteção sobre seus dados, de modo que este tenha controle sobre as ações as quais suas informações são submetidas[98]. O controle, certamente, não é absoluto, mas suficiente para

---

[95] Supremo Tribunal Federal – STF. Ação direta de inconstitucionalidade: ADI 4815, Relator(a): Min. CÁRMEN LÚCIA, Tribunal Pleno, julgado em 10/06/2015, PROCESSO ELETRÔNICO DJe-018 DIVULG 29-01-2016 PUBLIC 01-02-2016, p. 07. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057>. Acesso em: 03 abr. 2020.

96 ZANON, João Carlos. Direito à proteção dos dados pessoais. 1. Ed. São Paulo: Editora Revista dos Tribunais, 2013, p. 122.

97 Nos termos do art. 65, inciso II da Lei 13.709/18, a mesma passará a viger em 14 de agosto de 2020. (BRASIL, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais, Brasília, DF, ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 03 abr. 2020).

98 MARTINS, Leonardo. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Montevidéu: Fundação Kontad Adenauer, 2005, p. 233-235.

que o indivíduo tenha conhecimento sobre o tratamento de seus dados. Ademais, consigne-se que, embora a Lei 13.709/18 ainda não esteja vigendo, seus preceitos devem nortear a legitimidade de todas as atividades que impliquem no uso de dados pessoais[99].

Com base nisso é que deve ser interpretado o art. 6º da Lei 13.979/2020 que determina como uma das medidas de enfrentamento à pandemia causada pelo COVID-19 o compartilhamento obrigatório de dados de pessoas infectadas ou com suspeita de infecção entre os órgãos e entidades do Poder Público, bem como de entidades privadas com este, se, nesse caso, os dados forem requisitados por autoridade sanitária.

Por óbvio, o consentimento do usuário em relação ao compartilhamento de dados é possível de ser suprido, não somente com fulcro no art. 11, inciso II, alínea f, da Lei 13.709/18, mas também à luz do princípio da supremacia do interesse público[100], pois a pandemia causada pelo COVID-19 mostrou-se extremamente contagiosa representando sério risco para a saúde pública e demais áreas de relevância para o país.

Além disso, o compartilhamento de dados mostrou-se essencial no combate ao aumento exponencial de casos do COVID-19 em países como a Coreia do Sul[101], que através do uso de dados de geolocalização dos celulares de infectados, alertou aqueles que com este tiveram contato para realizarem testes para a doença. Entretanto, se não

---

99 FILHO, Demócrito Reinaldo. A utilização de dados de geolocalização na epidemia do coronavírus. Juristas, 29 mar. 2020. Disponível em: <https://juristas-com-br.cdn.ampproject.org/v/s/juristas.com.br/2020/03/29/a-utilizacao-de-dados-de-geolocalizacao-no-combate-a-epidemia-do-coronavirus/?amp=1&usqp=mq331AQF-KAGwASA%3D&amp_js_v=0.1#aoh=15859158924935&amp_ct=1585916170452&referrer=https%3A%2F%2Fwww.google.com&amp_tf=Fonte%3A%20%251%24s&ampshare=https%3A%2F%2Fjuristas.com.br%2F2020%2F03%2F29%2Fa-utilizacao-de-dados-de-geolocalizacao-no-combate-a-epidemia-do-coronavirus%2F>. Acesso em: 03 abr. 2020.

100 Nas palavras de Bandeira de Mello "O princípio da supremacia do interesse público sobre o interesse privado é princípio geral de Direito inerente a qualquer sociedade. É a própria condição de sua existência." (BANDEIRA DE MELLO, Celso Antônio. Curso de Direito Administrativo. 20. Ed. São Paulo: Malheiros, 1994, p. 20).

101 OJARDIAS, Frédéric. Testes em massa e rastreamento de celulares fazem parte da receita de sucesso do controle do COVID-19 na Coreia do Sul. Rádio França Internacional, sede desconhecida, 30 mar. 2020. Disponível em: <http://www.rfi.fr/br/mundo/20200330-testes-em-massa-e-rastreamento-de-celulares-fazem-parte-da-receita-de-sucesso-do-controle-da-covid-19-na-coreia-do-sul>. Acesso em: 03 abr. 2020.

há que se falar em autodeterminação informativa no tocante à permissão do indivíduo para que o Governo tenha acesso aos seus dados em caso de contágio confirmado, há que cogitá-la no que se refere ao processamento dessas informações.

Isso porque o controle dos dados previsto pelo princípio da autodeterminação informativa vai além da simples permissão ou denegação do acesso aos mesmos, englobando aspectos de: como, quando, onde e para que fins podem ser colhidas as informações pessoais[102]. Além disso, determina o artigo 45 do Regulamento Sanitário Internacional, aprovado pelo Decreto Legislativo nº 395/09, que as medidas sanitárias emergenciais devem respeitar as liberdades públicas, a dignidade da pessoa humana e que o tratamento dos dados neste cenário emergencial deve ser justo e adequado à finalidade que se presta, em consonância com o art. 6º, inciso I da Lei 13.709/18 e com o art. 7, inciso VIII, alíneas "a", "b" e "c" da Lei 12.965/14 ("Marco Civil da Internet").

No caso do art. 6º da Lei 13.979/2020, a problemática reside em diversos fatores, o que impede que o mesmo esteja em total consonância com o princípio da autodeterminação informativa e com o direito à proteção de dados.

O primeiro deles consubstancia-se no fato de que não foi delimitada a extensão das medidas de compartilhamento de dados pessoais, pois da leitura do art. 6º da referida legislação não se consegue precisar: a) forma de coleta dos dados e a sua modalidade de armazenamento: se no banco de dados do Governo ou em outro apartado; b) como será feita a identificação dessas informações: anônimas ou não; c) como será a destruição desses dados após o término da vigência da Lei; d) a existência de mecanismos para contestar a medida administrativamente em caso de abuso de autoridade e

[102] TEPEDINO, Gustavo. *Liberdades, tecnologia e teoria da interpretação.* Revista da Academia Paranaense de Letras Jurídicas, v. 53, 2014, p. 95.

para qual autoridade administrativa recorrer; e) quais as sanções aplicáveis aos agentes no caso de uso indevido dos dados e f) qual a abrangência do termo "autoridade sanitária" e quem seria competente para definir tais critérios para eventual contraditório e responsabilização.

Todas essas omissões vão de encontro às diretrizes dadas por autoridades de proteção de dados de outros países para os Governos que desejam fazer uso de dados pessoais no combate ao COVID-19[103], pois o caráter extremamente genérico do art. 6º da Lei 13.979/2020 não somente dificulta o resguardo do direito à privacidade e à proteção de dados dos indivíduos, mas também a própria atuação do Governo, que verá seu trabalho embaraçado devido à ausência de diretrizes para balizá-lo, sem prejuízo de, ainda, ser interpelado via Poder Judiciário.

Isso acontece porque embora o Poder Público esteja legitimado a acessar os dados sensíveis dos cidadãos na presente situação, o tratamento conferido a essas informações não pode ser indiscriminado nem sujeito ao bel prazer da autoridade pública, sob pena de fomentar um verdadeiro Estado de exceção, no qual, sob a justificativa do provisório e excepcional, legitimam-se medidas antidemocráticas[104] com vistas a perpetuação da vigilância desmedida.

---

103 Nas palavras do Conselho Europeu de Proteção de Dados "1.3 With regard to the processing of telecom data, such as location data, national laws implementing the ePrivacy Directive must also be respected. In principle, location data can only be used by the operator when made anonymous or with the consent of individuals. However, Art. 15 of the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security. Such exceptional legislation is only possible if it constitutes a necessary, appropriate and proportionate measure within a democratic society. These measures must be in accordance with the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Moreover, it is subject to the judicial control of the European Court of Justice and the European Court of Human Rights. In case of an emergency situation, it should also be strictly limited to the duration of the emergency at hand." (European Data Protection Board, The. Statement on the processing of personal data in the context of the COVID-19 outbreak. Publicado em: 19 de mar. 2020. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf> Acessado em: 03 abr. 2020)

104 AGAMBEN, Giorgio. Estado de exceção. Tradução de Iraci D. Poleti. 2. Ed. São Paulo: Boitempo, 2004, p. 13.

Dito isso, outro imbróglio trazido pela dicção do art. 6º da Lei 13.979/2020 diz respeito à inclusão dos suspeitos de contágio pelo COVID-19 no rol de sujeitos cujos dados poderão vir a ser acessados pelo Governo. A referida medida se revela temerária e de alto risco à proteção dos dados sensíveis, pois o compartilhamento de dados de infectados apenas se comprovou frutífero quando aliado à testagem em massa, a exemplo do que ocorreu na Coréia do Sul[105]. Inclusive, a Alemanha[106] apenas cogitou adotar o referido compartilhamento somente após ter efetuado a testagem da maioria dos suspeitos de contágio de COVID-19, o que demonstra a importância da atuação em conjunto dessas medidas, não em apartado.

No entanto, intenciona-se no Brasil o mesmo sucesso, sem que, em contrapartida, o país disponha dos meios necessários para tanto, pois as orientações das autoridades de saúde nacionais são no sentido de que as testagens apenas devem ocorrer nos casos graves, sendo os demais – suspeitos – mantidos em quarentena até o aparecimento de complicações que requeiram o uso do sistema de saúde e, finalmente, a realização do teste para o COVID-19[107]. Ou seja, a política adotada é a da testagem mínima.

Em virtude disso, qualquer pessoa que apresente os sintomas do COVID-19 – os quais frequentemente se confundem com os da gripe ou de alergias – poderá ser considerada como caso suspeito e, consequentemente, estará sujeita à medida de compartilhamento de dados com o Governo, sem que, em compensação, seja-lhe garantido qualquer instrumento para contestar, administrativamente, tal ação, pois, neste caso em

105 Coronavírus: o que está por trás do sucesso da Coreia do Sul para salvar vias em meio à pandemia. BBC News, London, 16 mar. 2020. Disponível em: <https://www.bbc.com/portuguese/internacional-51877262>. Acesso em: 02 abr. 2020.
106 BUSVINE, Douglas. Coronavírus: Alemanha pretende lançar aplicativo que vai ajudar a rastrear possíveis casos de infecção. O Globo, Rio de Janeiro, 30 mar. de 2020. Disponível em:<https://oglobo.globo.com/mundo/coronavirus-alemanha-pretende-lancar-aplicativo-que-vai-ajudar-rastrear-possiveis-casos-de-infeccao-2433941>. Acesso em: 01 abr. 2020.
107 VARGAS, Mateus. Governo quer, por enquanto, reduzir testes do COVID-19 só em cidades com transmissão comunitária. Estadão, São Paulo, 13 mar. de 2020. Disponível em: <https://saude.estadao.com.br/noticias/geral,governo-quer-por-enquanto-reduzir-testes-da-covid-19-so-em-cidades-com-transmissao-comunitaria,70003232569>. Acesso em: 01 abr. 2020.

específico, a não confirmação do contágio não ocorre por recusa do indivíduo, e sim por uma política do Governo.

Em síntese, pessoas que não estão infectadas pelo COVID-19, mas que apresentem sintomas semelhantes terão seu direito à proteção de dados mitigado, devido à impossibilidade do Estado de submetê-las à testagem para o COVID-19.

Tendo em vista esse cenário, afigura-se mais prudente restringir o compartilhamento de dados apenas aos casos confirmados de contágio pelo COVID-19, a exemplo do que decidiu a Suprema Corte de Israel, que proibiu o Governo de usar os dados de geolocalização dos suspeitos de contágio pelo COVID-19, restringindo o acesso a informações pessoais apenas aos casos confirmados de contágio[108].

Isso acontece porque através de dados de geolocalização o Governo consegue fácil acesso a outras informações sensíveis que podem ser deduzidas por uma simples análise dos locais onde o indivíduo frequenta, por exemplo, se uma pessoa visita com habitualidade um tempo religioso, a sua orientação religiosa já estará manifesta; se frequenta certas casas noturnas, a sua orientação sexual também será conhecida e assim sucessivamente acontecerá com outros dados sensíveis.

Além disso, temos o fato de que, no Brasil, o compartilhamento de dados de suspeitos de contágio pelo COVID-19, assim como os casos confirmados, não foi devidamente regulamentado, o que faz concluir que, se a aplicação da medida já é questionável para os casos confirmados de COVID-19 ante a sua imprecisão, é mais ainda quando

108 HENDRIX, Steve. Israel is using cellphone surveillance to warn citizens: You may already be infected. The Washington Post, Washington D.C., 19 mar. de 2020. Disponível em: <https://www.washingtonpost.com/world/middle_east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html>. Acesso em: 01 abr. 2020.

pretende afastar uma garantia de ordem fundamental baseada unicamente na mera suspeita que nem ao menos possui expectativa de ser confirmada ou afastada. Com base nisso, a interpretação do art. 6º da Lei 13.979/2020 à luz do princípio da autodeterminação informativa e do direito à proteção de dados deve ser feita de forma cautelosa, a fim de se evitar que, na tentativa de salvaguardar a saúde pública, fragilizem-se outros direitos importantes cuja proteção também não pode ser esquecida.

DADOS DE GEOLOCALIZAÇÃO: O LIMBO ENTRE PRIVACIDADE E SAÚDE PÚBLICA EM TEMPOS DE COVID-19

Lucas Bulhões

Com a declaração do estado de "pandemia" do novo Coronavírus (COVID-19), pela Organização Mundial da Saúde (OMS)[109], e seus consequentes desafios à saúde pública e à ordem econômica mundial, diversos agentes públicos e privados começaram a empenhar esforços em prol do apaziguamento dessa crise viral. Doações milionárias, distribuição gratuita de álcool gel e máscaras, entrega de comida àqueles que pertencem aos grupos de risco do vírus e desassistidos, são só alguns exemplos das importantes iniciativas que estão sendo tomadas pelas autoridades públicas, empresas e pessoas no combate ao COVID-19.

No entanto, dentre tantas iniciativas, passa-se quase despercebida a atuação do setor tecnológico em meio à pandemia. Muitas empresas de telecomunicação, *big techs* e *startups* estão sendo procuradas por agentes governamentais, os quais buscam acesso

109 Organização Mundial da Saúde declara pandemia do novo Coronavírus. Empresa Brasil de Telecomunicação (EBC). Publicado em 11.03.2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-03/organizacao-mundial-da-saude-declara-pandemia-de-coronavirus>. Acesso em 05.04.2020

aos seus ativos mais valiosos: os dados pessoais de seus usuários, mais especificamente, seus dados de geolocalização.

A importância do acesso a tais informações pessoais e invasivas pode ser resumida pela velha máxima *scientia potentia est* ("conhecimento é poder"), atribuída ao filósofo Francis Bacon. Isto pois, o *conhecimento* acurado da localização de pessoas infectadas ou suspeitas de infecção, concede às autoridades o *poder* de traçar estratégias mais efetivas no combate à disseminação do vírus, seja determinando o distanciamento social do indivíduo infectado, seja mapeando as regiões com maior índice de disseminação, seja proibindo reuniões em determinados espaços púbicos ou, até mesmo, proibindo o funcionamento do comércio nacional.

Na China, foco inicial da disseminação do COVID-19, o poder de *vigilância digital* por parte do Estado não é novidade para ninguém. Logo, não é de se espantar que, segundo reportagem do jornal *South China Morning Post*[110], o governo chinês esteja não apenas coletando, mas disponibilizando publicamente os dados de geolocalização dos indivíduos infectados ou com suspeita de infecção, com o intuito de que os demais cidadãos evitem a proximidade destes locais.

A política tem se mostrado efetiva e replicada por outros Estados asiáticos, a exemplo da Coréia do Sul que, após implementação de política de monitoramento semelhante, demonstrou uma queda abrupta da taxa de disseminação do vírus[111]. Nesse

110 CHEN, Celia; HU, Minghe. Coronavirus accelerates China´s big data collection but privacy concerns remain. South China Moring Post. Publicado em 26.02.2020. Disponível em: <https://www.scmp.com/tech/apps-social/article/3052232/coronavirus-accelerates-chinas-big-data-collection-privacy>. Acesso em 05.04.2020

111 LYONS, Kim. Governments around the world are increasingly using location data to manage the coronavirus. The Verge. Publicado em 23.03.2020. Disponível em: <https://www.theverge.com/2020/3/23/21190700/eu-mobile-carriers-customer-data-coronavirus-south-korea-taiwan-privacy>. Acesso em 05.04.2020

sentido, é acertada a percepção do filósofo Byung-Chul Han que, em reportagem ao jornal El País[112], afirmou ser a Ásia um continente em que *as epidemias não são combatidas somente pelos virologistas e epidemiologistas, e sim principalmente pelos especialistas em informática e macrodados*.

Entretanto, a grande maioria dos Estados regidos pelo regime democrático não dispõem de um controle tão próximo e invasivo de seus cidadãos, motivo pelo qual estão tendo de recorrer às empresas de telecomunicação e entretenimento digital a fim de obterem a localização de seus usuários infectados ou suspeitos de infecção. Afinal, são essas as empresas que possuem poder de rastreio de nossos celulares e, consequentemente, poder de coleta de dados geolocacionais.

A título de exemplo temos os Estados Unidos, epicentro mundial da disseminação do vírus, em que o Presidente Donald Trump se uniu com representantes do Google, Facebook, Apple e Amazon com o intuito de obter acesso à localização dos norte-americanos infectados ou suspeitos de infecção (em, pelo menos, 500 cidades), e, com tais dados, verificar a adesão e respeito à política nacional do *stay-at-home*[113].

Até mesmo a Europa, principal referência e vanguardista na proteção de dados pessoais, esteve em contato com algumas empresas de telecomunicação, em busca da

112 HAN, BYUNG-CHUL. O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han. El País. Publicado em 22.03.2020. Disponível em <https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html>. Acesso em 06.04.2020.
113 TAU, Byron. Government Tracking How People Move Around in Coronavirus Pandemic. The Wall Street Jornal. Publicado em 28.03.2020. Disponível em <https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202>. Acesso em 06.04.2020

localização anonimizada de seus usuários infectados, a fim de poder mapear a disseminação da doença e enviar suprimentos médicos para os territórios mais afetados.[114]

Apesar de parecer distante, estas políticas de geolocalização já pertencem à realidade brasileira. A Prefeitura de Recife, por exemplo, firmou parceria com a *startup* In Loco e afirmou que monitorará mais de 700 mil aparelhos celulares anonimamente, a fim de medir o "índice de isolamento" e traçar políticas de conscientização mais efetivas para ampliar o isolamento social[115]. O estado de São Paulo, seguindo os passos da capital nordestina, também garantiu que se utilizará da infraestrutura das principais operadoras de telefonia nacionais objetivando localizar os paulistas e desenvolver um Sistema de Monitoramento Inteligente (SIMI-SP) – o qual será compartilhado com prefeitos de municípios com mais de 30 mil habitantes, para que estes possam traçar políticas públicas mais precisas e direcionadas[116].

Portanto, posta esta realidade e sendo certa a efetividade de tais políticas de monitoramento, observa-se um certo desconforto por parte de juristas, que começam a se deparar com o surgimento de um dilema jurídico com duas facetas: uma faceta teórica, que questiona a potencial ameaça ao direito à privacidade; e uma faceta pragmática, que diz respeito à omissão legislativa no tocante à regulamentação para o tratamento de dados de geolocalização.

---

114 HIGA, Paulo. Operadoras na Europa vão rastrear localização de celulares para combater Covid-19. Tecnoblog. Publicado em 26.03.2020. Disponível em: <https://tecnoblog.net/331251/operadoras-na-europa-vao-rastrear-localizacao-de-celulares-para-combater-covid-19/>. Acesso em 06.04.2020

115 ARIMETHEA, Bruna; CAPELAS, Bruno. InLoco e Prefeitura de Recife vão monitorar 700 mil celulares em prol de isolamento social. O Estado de S. Paulo. Publicado em 25.03.2020. Disponível em: <https://link.estadao.com.br/noticias/inovacao,inloco-e-prefeitura-de-recife-vao-monitorar-700-mil-celulares-em-prol-de-isolamento-social,70003248010>. Acesso em 06.04.2020

116 São Paulo faz parceria com operadoras de telefonia para monitorar quarentena. CNN Brasil. Publicado em 09.04.2020. Disponível em: <https://www.cnnbrasil.com.br/nacional/2020/04/09/sao-paulo-faz-parceria-com-operadoras-de-telefonia-para-monitorar-quarentena>. Acesso em 12.04.2020

O direito à privacidade é constitucionalizado no art. 5º, inc. X, da nossa Carta Magna[117] e consiste, grosso modo, no *direito a viver sem ser molestado pelo Estado ou por terceiros no que toca aos aspectos da vida pessoal e familiar*[118]. Trata-se de um dos direitos mais queridos pelo nosso ordenamento devido à sua estreita relação com a proteção da dignidade e personalidade. Afinal, não é desejável viver sob a vigilância de um Estado autoritário igual ao idealizado por George Orwell, em sua obra 1984.

No entanto, há de se notar que, diferentemente do romance distópico de Orwell, em que o monitoramento social por parte do *Big Brother* visava uma manutenção de poder político, o monitoramento atual da geolocalização dos infectados ou suspeitos de infecção intenciona tão somente a promoção urgente da saúde pública, em um contexto emergencial.

De todo modo, encontramo-nos diante da colisão entre dois direitos fundamentais – *saúde pública v. privacidade* – em que os constitucionalistas certamente proporiam a aplicação do famigerado *princípio da proporcionalidade*. Tal princípio, proposto pelo jurista alemão Robert Alexy, propõe um sopesamento entre direitos fundamentais conflitantes para verificar qual direito deve *prevalecer no caso concreto sem, contudo, aniquilar o outro direito*.

Sendo assim, considerando este mandamento principiológico, é imperativo que, em um declarado "estado de emergência"[119], haja a sobreposição dos direitos coletivos em detrimento dos direitos individuais. Até porque, *in casu*, considerando o potencial

117 Art. 5º, inc. X, CF: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.
118 MARINONI, Luiz Guilherme; MITIDIERO, Guilherme; SARLET, Ingo Wolfgang. Curso de Direito Constitucional, 8ª edição, Saraiva Educação, São Paulo, 2019.
119 VALENTE, Jonas. OMS declara estado de emergência global em razão do coronavírus. Empresa Brasil de Telecomunicação. Publicado em 30.01.2020. Disponível: <https://agenciabrasil.ebc.com.br/saude/noticia/2020-01/oms-declara-estado-de-emergencia-global-em-razao-do-coronavirus>. Acesso em 12.04.2020

de disseminação do COVID-19, a saúde de um indivíduo implica na saúde de toda a sociedade.

No entanto, importante esclarecer que a promoção da saúde pública por meio do monitoramento geolocacional não pressupõe uma negligência à privacidade. Pelo contrário. A exemplo da Europa (como já mencionado), observa-se que existem ferramentas técnico-jurídicas para tratar os dados de forma menos invasiva, tais como a anonimização dos dados coletados, a notificação dos titulares dos dados, o compromisso com o descarte de tais dados após o fim da pandemia, a fiscalização por parte de uma Autoridade Nacional, a edição de normas, dentre outras estratégias que assegurem o sigilo dos dados.

Vale observar que este entendimento é endossado, inclusive, pela Organização Mundial da Saúde (OMS), que afirmou ser a tecnologia bem-vinda no combate ao COVID-19, desde que delineados os limites dos direitos humanos e privacidade[120].

Abordada a questão do direito à privacidade, chega-se, enfim, à faceta pragmática do dilema, qual seja, a viabilidade legal do tratamento de dados geolocacionais no Brasil. Afinal, qual o seria o fundamento constitucional ou legal para o tratamento de dados geolocacionais? As bases legais previstas na nossa Lei Geral de Proteção de Dados (LGPD) abarcam tal tratamento? A declaração presidencial de "estado de emergência" teria o condão de flexibilizar os direitos fundamentais à privacidade e à proteção de dados pessoais? O que será feito com os dados após o fim da pandemia?

120 NEBEHAY, Stephanie; REVILL, John. Technical help offered to fight virus must safeguard privacy, right: WHO. Thomson Reuters. Publicado em 25.03.2020. Disponível em: <https://www.reuters.com/article/us-health-coronavirus-who-technology/technical-help-offered-to-fight-virus-must-safeguard-privacy-rights-who-idUSKBN21C37N>. Acesso em 06.04.2020.

São muitos questionamentos para poucas respostas. Afinal, como bem preleciona o jurista alemão Friedrich Müller [121], o Direito surge posteriormente à realidade, para adequar-se a ela. Logo, o fato de não haver precedente histórico para a realidade na qual vivemos resulta, naturalmente, em um desamparo legal. É exatamente o que acontece com o tema de dados geolocacionais: não há previsão legal expressa. Logo, tal situação nos obriga a ampliar a extensão da interpretação das normas vigentes ou, então, a editar novas leis.

A Lei Geral de Proteção de Dados mostra-se omissa no tocante aos dados de geolocalização. No entanto, ela define expressamente, em seu art. 6º, quais princípios devem nortear e legitimar o tratamento de dados pessoais no Brasil – dentre os quais, encontramos: *finalidade*, *necessidade*, *transparência* e *não discriminação*. Ora, o tratamento de dados geolocacionais de forma anonimizada, notificada e com propósito específico de promoção da saúde pública coaduna com os princípios supracitados e permite depreender a sua legalidade.

Outra possível base legal diz respeito à Lei 13.979/20, elaborada especificamente para o enfrentamento do vírus. Esta Lei traz, também em seu art. 6º, a obrigatoriedade do compartilhamento de dados pessoais, entre órgãos e entidades da administração pública, das pessoas infectadas ou com suspeita de infeção pelo coronavírus[122]. A teleologia do mandamento está no próprio dispositivo, qual seja, *o combate à propagação do vírus*. Não obstante, o mandamento é bastante genérico e promove um certo receio

121 CANOTILHO, JJ. Gomes. Direito Constitucional e Teoria da Constituição. Coimbra: Almedina. 7ª edição. pag. 1213
122 Art. 6º, caput, Lei 13.797/20: É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.

quanto à inclusão dos dados geolocacionais, já que é notório o potencial invasivo desta espécie de dados pessoais.

Neste contexto, não se pode deixar de notar que a existência de uma Autoridade Nacional de Proteção de Dados (ANPD), prevista no art. 55-A da LGPD, seria extremamente relevante, haja vista a competência desta autoridade para regulamentar e estabelecer diretrizes aos agentes públicos e privados quanto às formas e limites para o tratamento de dados geolocacionais – especialmente, num momento frágil e que exige uma flexibilização de interpretação legal em prol do direito fundamental à saúde pública.

Portanto, considerando a ausência da ANPD e o surgimento de políticas públicas municipais e estaduais envolvendo o monitoramento de dados geolocacionais, faz-se necessária a edição pressurosa de lei ou medida provisória que estabeleça as diretrizes específicas para o tratamento destes dados. Uma lei que imponha limites temporais e espaciais para este tratamento e, concomitantemente, imponha mecanismos técnicos e jurídicos para a preservação da privacidade, tais como a anonimização dos dados coletados e/ou notificação de seus titulares.

Em síntese, neste contexto de pandemia, tecnologia e monitoramento geolocacional são ferramentas aliadas à saúde pública e, portanto, valendo-se das lições de Müller, resta ao Direito adequar-se para atender a este anseio social. Afinal, em tempos de COVID-19, a saúde de um é a saúde de todos.

PARTE III

O PROBLEMA DO USO DE DADOS SENSÍVEIS

PANDEMIA E FUTURO DA SAÚDE: QUESTÕES SOBRE TELEMEDICINA E PRIVACIDADE

Daniel Pereira Campos

Em meio à tragédia desencadeada pela pandemia de COVID-19, já se tornou comum certa previsão de que um "novo mundo" surgirá dos escombros da atual ordem social. O novo coronavírus teria, assim, acelerado transformações, para usar o adjetivo da moda, "disruptivas", especialmente nos campos da tecnologia, da saúde e da informação. Não me proponho neste ensaio, naturalmente, a empreender esforços para testar prognósticos tão ousados, mas, sim, a investigar alguns dos desdobramentos concretos e já observáveis advindos da pandemia e das medidas políticas adotadas como respostas. Mais especificamente, busco analisar questões sobre seu impacto na promoção de soluções remotas de assistência à saúde e suas consequências para privacidade dos usuários destas ferramentas – ou seja, a relação entre telemedicina e a proteção de dados pessoais.

Antes de qualquer coisa, uma nota conceitual: ainda que admitindo sua pluralidade semântica, a Organização Mundial de Saúde define, de modo amplo, a telemedicina como oferta de serviços de saúde mediante a utilização de tecnologias de informação e comunicação, sendo a distância um fator crucial[123]. Assim, apesar do nome, o conceito aqui tratado inclui bem mais que somente a prestação de serviço associado ao

123 WORLD HEALTH ORGANIZATION. A health telematics policy in support of WHO's Health-for-all strategy for global health development: report of the WHO Group Consultation on Health Telematics, 11-16. Genebra, 1997. Disponível em:<https://apps.who.int/iris/bitstream/handle/10665/63857/WHO_DGO_98.1.pdf?sequence=1&isAllowed=y>. Acesso em: 14 abr. 2020.

profissional médico, podendo, a depender do caso, referir-se a serviços de enfermagem ou psicologia, por exemplo.

Dito isso, mesmo que voltada para o cenário atual, espera-se que a análise das tensões entre as medidas de promoção à telemedicina e a legislação de proteção à privacidade de dados permita, a partir de uma comparação entre Brasil e países que mais têm dedicado esforços no combate à pandemia, a identificação de contornos para navegar esse alardeado "novo mundo". Afinal, debater os usos e potencialidades destes serviços, ora tidos como soluções mágicas livres de amarras e ora vistos como um pesadelo à privacidade dos pacientes, oferece oportunidade única para entrever possíveis consequências da pandemia no campo de proteção de dados.

Mas antes do novo, retornemos ao presente: no atual combate à pandemia, como dito, a adoção de soluções de telemedicina constituiu um dos pilares da política de enfrentamento. Em suas diretrizes para Europa, a Organização Mundial de Saúde mencionou a telemedicina entre os serviços essenciais para "fortalecer a resposta dos sistemas de saúde à COVID-19"[124]. De acordo com esta nova política, tendo em vista a otimização da prestação de serviços de saúde durante o confinamento, a telemedicina deve ser um dos modelos alternativos para serviços de assistência e suporte a decisões clínicas. Nesse contexto, países dentro e fora da Europa, permitiram ou ampliaram hipóteses de uso de telemedicina, com variados graus de flexibilidade[125].

124 WORLD HEALTH ORGANIZATION. Strengthening the Health Systems Response to COVID-19 - Technical guidance #1 (1 April 2020). Disponível em: <http://www.euro.who.int/__data/assets/pdf_file/0007/436354/strengthening-health-systems-response-COVID-19-technical-guidance-1.pdf?ua=1>. Acesso em: 14 abr. 2020.
125 Ibidem.

No Brasil, em 20 de março, o Ministério da Saúde publicou a Portaria nº 467/2020, regulamentando a telemedicina como uma medida de combate ao novo coronavírus[126]. Além disso, o Conselho Federal de Medicina, órgão tradicionalmente refratário à prática, posicionou-se favoravelmente à ampliação do oferecimento de cuidados em saúde à distância por meio de ofício ao Ministro da Saúde[127]. Ademais, em 15 de abril de 2020, foi sancionada a Lei nº 13.989/2020, liberando o uso de telemedicina enquanto durar a crise ocasionada pelo coronavírus[128]. Contudo, a preocupação com a garantia aos direitos de privacidade de dados passou ao largo das medidas adotadas. Salvo menção na Portaria indicada acima de que o atendimento deve ser realizado por meio que garanta a "integridade, segurança e o sigilo das informações", a regulação emergencial sobre telemedicina foi omissa sobre o tema[129]. Em outros países, entretanto, houve soluções e medidas, tanto no campo da telemedicina quanto no campo da proteção de dados, que buscaram outros caminhos para os dilemas trazidos pela pandemia.

Nos EUA, o país com maior número de casos confirmados até a data da publicação, as medidas de ampliação do uso de telemedicina foram expressivas. Pelo menos temporariamente, como parte do pacote trilionário de combate ao novo coronavírus, o Medicare, programa governamental de assistência à saúde dos idosos, cobrirá integral ou

126 BRASIL. Ministério da Saúde. Portaria nº 467, de 20 de março de 2020. Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19. Brasília. Disponível em: <http://www.in.gov.br/en/web/dou/-/portaria-n-467-de-20-de-marco-de-2020-249312996>. Acesso em: 15 abr. 2020.

127 CONSELHO FEDERAL DE MEDICINA. Ofício CFM nº 1756/2020. Brasília. Disponível em: <http://portal.cfm.org.br/images/PDF/2020_oficio_telemedicina.pdf>. Acesso em: 13 abr. 2020.

128 BRASIL. Lei nº 13.989, de 15 de abril de 2020. Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2).. Brasília. Disponível em: <http://www.in.gov.br/en/web/dou/-/lei-n-13.989-de-15-de-abril-de-2020-252726328 >. Acesso em: 06 mai. 2020.

129 BRASIL. Ministério da Saúde. Portaria nº 467, de 20 de março de 2020. Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19. Brasília. Disponível em: <http://www.in.gov.br/en/web/dou/-/portaria-n-467-de-20-de-marco-de-2020-249312996>. Acesso em: 15 abr. 2020.

parcialmente todos os serviços de telemedicina, revogando política anterior que impedia reembolsos fora de áreas rurais e para novos pacientes[130].

Além disso, no campo de privacidade, as medidas de ampliação foram acompanhadas por flexibilização nos padrões de segurança da informação e de dados das plataformas utilizadas para telemedicina. Nesse sentido, durante o estado de emergência, os prestadores de saúde sujeitos aos regulamentos sanitários do Health Insurance Portability and Accountability Act (HIPAA) poderão fornecer serviços de telemedicina por meio de tecnologias de comunicação remota, sem que haja imposição de penalidades para eventual uso de ferramentas fora da regulamentação. Cumpre mencionar que, em todo caso, o fornecimento de telemedicina em desconformidade com os parâmetros deve ser sempre realizado de boa-fé e não significa um abandono às diretrizes de segurança[131]. Ademais, os prestadores são incentivados a informar os pacientes de que esses aplicativos de terceiros apresentam riscos à privacidade e devem também ativar todos os mecanismos de criptografia e privacidade disponíveis ao usá-los. Há, ainda, uma lista de recomendações que exclui determinadas aplicações e softwares por eventual risco à privacidade dos usuários, tais como Facebook Live, Twitch, ou TikTok[132].

Já na Europa, a experiência francesa, além de relacionada a um sistema de proteção de dados notoriamente próximo ao brasileiro, também permite analisar um ordenamento com restrições à telemedicina bastante similares ao nosso sistema anterior à

130 AMERICAN MEDICAL ASSOCIATION. CARES Act: AMA COVID-19 pandemic telehealth fact sheet. Disponível em: <https://www.ama-assn.org/delivering-care/public-health/cares-act-ama-covid-19-pandemic-telehealth-fact-sheet>. Acesso em: 15 abr. 2020.
131 ESTADOS UNIDOS DA AMÉRICA. Department of Health and Human Services. Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency. Disponível em: <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>. Acesso em : 14 abr. 2020.
132 Ibidem.

pandemia. Para ajudar os médicos a se ambientarem com a prática, o Ministério de Saúde francês analisou e avaliou várias soluções, indicando, para cada uma delas, as funcionalidades disponíveis e o nível garantido de segurança. O Ministro da Saúde também editou diretrizes para facilitar o acesso às teleconsultas, de modo a limitar os riscos de transmissão e de saturação dos estabelecimentos de saúde[133].Quanto à proteção de dados pessoais, os profissionais são obrigados a usar ferramentas, independentemente de serem ou não avaliadas pelo Ministério, em conformidade com o Regulamento Geral sobre a Proteção de Dados da União Europeia e a política geral sistema de segurança de sistemas de informação. No entanto, se isso for "impossível" e "exclusivamente como parte da resposta à epidemia do COVID-19", os profissionais de saúde poderão, excepcionalmente, utilizar outras ferramentas que não atendam aos requisitos, em linha com a regulamentação[134].

Por outro lado, na Espanha, um país que culturalmente já possui menos restrições à telemedicina[135] e no qual também se reportou aumento em seu uso[136], não houve medida legal que expressamente contemplasse o serviço como parte central da estratégia de combate à pandemia. O Real Decreto-Lei nº 8/2020, de 17 de março, que dispôs sobre as medidas extraordinárias para impedir o impacto econômico e social do COVID-19, não incluiu um plano sobre o assunto[137]. De fato, tanto no caso espanhol quanto no

133 FRANÇA. Ministère des Solidarités et de la Santé. Téléconsultation et COVID-19 : qui peut pratiquer à distance et comment? Disponível em: <https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/professionnels-de-sante/article/teleconsultation-et-covid-19-qui-peut-pratiquer-a-distance-et-comment>.Acesso em: 12 abr. 2020.
134 FRANÇA. Le Service Public de La Diffusion du Droit. Arrêté du 23 mars 2020 (Dernière modification: 16 juin 2020), de 23 de março de 2020. Disponível em: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000041748109&dateTexte=20200625>. Acesso em: 24 jun. 2020.
135 MOMENTUM. Telemedicine in Spain. Disponível em: <http://www.telemedicine-momentum.eu/spain/>. Acesso em: 13 abr. 2020.
136 20 MINUTOS. Telemedicina: ¿es posible ir al medico sin passar por la consulta? Disponível em: <https://www.20minutos.es/noticia/4208093/0/telemedicina-es-posible-ir-al-medico-sin-pasar-por-la-consulta/>. Acesso em: 13 abr. 2020.
137 ESPANHA. Boletín Oficial del Estado. Real Decreto-ley nº 8/2020, de 17 de março de 2020. Disponível em: <https://www.boe.es/buscar/act.php?id=BOE-A-2020-3824>. Acesso em: 15 abr. 2020.

caso francês, o Regulamento Geral sobre a Proteção de Dados da União Europeia e Diretiva nº 2011/24/NA (conforme alterada), relativa aos direitos em matéria de cuidados de saúde transfronteiriços, oferecem parâmetros normativos para a prática, sem, contudo, especificar qualquer medida para situações excepcionais de pandemia, deixando espaço para legislação interna dos países-membros.

Logo, a partir da análise acima, nota-se tendência na ampliação do uso e liberação da telemedicina em países que antes restringiam essa prática. Por outro lado, mesmo em países que já a permitiam de maneira mais ampla, as soluções quanto às questões de privacidade são diversas. Feito esse panorama comparativo, qual seriam as reflexões que as abordagens distintas sobre o tema nos permitem ter, sob uma perspectiva de privacidade de dados?

Primeiramente, chama à atenção, tanto na Espanha quanto no Brasil, que se ignore o aumento exponencial do uso de telemedicina durante a pandemia e se presuma que essa utilização emergencial ocorra inteiramente em conformidade com os padrões de segurança e proteção de dados. Afinal, sob risco de soar óbvio, ainda que não se possa perder de vista a proteção e a segurança – o contrário seria arriscar tornar a solução um outro problema -, é preciso considerar que momentos de graves crises sanitárias impõe flexibilidade e razoabilidade. Existe, certamente, complexidade na discussão sobre Estado de Direito e suspensão temporária de direitos, mas há caminhos que antecedem esse debate. Afinal, independentemente de qualquer restrição, a prática de proativamente garantir e orientar e, na medida do possível, disponibilizar ferramentas recomendadas diminui riscos e coloca os titulares em posição cada vez mais central, especialmente se tratando de dados de natureza sensível. Assim, coloca-se ainda mais em evidência o papel fundamental que autoridades, sejam dedicadas à privacidade ou não, têm ao regulamentar e oferecer diretrizes ao público em momentos de crise. Para futuro

da proteção de dados pessoais no Brasil e para a tão esperada Autoridade Nacional de Proteção de Dados, fica a lição da importância de se pensar em privacidade como uma prática constante, não apenas como uma moldura textual estática.

PROTEÇÃO DE CRIANÇAS E ADOLESCENTES POR DESIGN: UM DEBATE NECESSÁRIO EM MEIO À PANDEMIA DE COVID-19

Elora Raad Fernandes[138] *e Cindyneia Ramos Cantanhede*[139]

O USO DE TECNOLOGIAS NO COMBATE À COVID-19

A sociedade vive, hoje, sob uma crise global, causada pela Covid-19. Além do distanciamento social de mais de 3,9 bilhões de pessoas,[140] governos e sociedades empresárias de todo o mundo têm utilizado diversas tecnologias para conter a pandemia, como câmeras de reconhecimento facial, monitoramento da geolocalização do usuário, pulseiras eletrônicas etc.[141] A partir dessas ferramentas é possível, por exemplo, identificar aqueles que entraram em contato próximo com pessoas infectadas, acompanhar sintomas e monitorar os que se encontram em quarentena, isolamento ou distanciamento social.[142]

---

138 Doutoranda em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ) e bolsista DS/CAPES. Mestra em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF) e bacharela em Direito pela mesma instituição. E-mail: elorafernandes@live.com.
139 Graduanda em Direito pela Universidade Federal do Maranhão (UFMA). E-mail: cindyneiacantanhede@gmail.com.
140 AHEY, Ryan. Half the world in lockdown: 3.9 billion people are currently called on to stay in their homes due to coronavirus. Daily Mail. [s.l.]. 2 abr. 2020. Disponível em: <http://dailym.ai/2RznOfR>. Acesso em: 10 abr. 2020.
141GIELOW, Igor. Tecnologia usada no combate à pandemia de coronavírus ameaça privacidade. Folha de São Paulo. São Paulo. 5 abr. 2020. Disponível em: https://bit.ly/2K3eCMu. Acesso em: 13 abr. 2020. Graduanda em Direito pela Universidade Federal do Maranhão (UFMA) e bolsista do Grupo PET Conexões em Direitos Humanos. E-mail: cindyneiacantanhede@gmail.com."
142 VOSLOO, Steven; PENAGOS, Melanie; RAFTREE, Linda. COVID-19 and children's digital privacy. Unicef. [s.l.]. 7 abr. 2020. Disponível em: <https://uni.cf/3enf99T>. Acesso em: 11 abr. 2020.

No Brasil, especificamente, diversas parcerias têm sido firmadas para o controle da pandemia devido à autorização legal dada pela Lei 13.979/2020[143]. O estado de São Paulo assinou contrato com a Telefônica para que ela ceda dados de localização de seus clientes; na cidade do Rio de Janeiro, foi realizado um acordo entre a prefeitura e a Tim, para identificar aglomerações e movimentação de pessoas; a prefeitura de Recife assinou contrato com a sociedade empresária In Loco, que vende "dados de localização, o monitoramento de 800 mil pessoas com direito a enviar SMS caso a quarentena esteja sendo descumprida".[144] Em nível federal, as operadoras também têm se movimentado e já anunciaram que vão disponibilizar ao Ministério da Ciência, Tecnologia, Inovações e Comunicações "uma solução única de dados para monitorar mobilidade populacional, deslocamentos e pontos de concentração".[145]

Quando utilizadas de forma ética, na tutela da saúde, as Tecnologias de Informação e Comunicação (TIC) podem ajudar a salvar vidas e ser um fator essencial para a superação de pandemias. Todavia, da forma como têm sido utilizadas, sem a devida transparência e *accountability*, têm gerado diversos questionamentos acerca da privacidade e da proteção de dados dos cidadãos. Seu uso para esse fim não é algo novo e, da mesma forma, foi bastante aplaudido e criticado na última crise causada pela Ebola.[146] Como seria possível, portanto, utilizar o potencial das tecnologias sem que o

143 Destaca-se que, além da Lei 13.979/2020, o Regulamento Sanitário Internacional também traz regras acerca da proteção de dados aplicáveis ao contexto da pandemia (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. Brasília.)

144 DIAS, Tatiana. Vigiar e lucrar: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela vivo. The Intercept Brasil. [s.l.]. 13 abr. 2020. Disponível em: <https://bit.ly/3chayEz>. Acesso em: 13 abr. 2020.

145 Ibid.

146 WALL, By Matthew. Ebola: can big data analytics help contain its spread? BBC. [s.l.]. 15 out. 2014. Disponível em: <https://bbc.in/2ygFWo1>. Acesso em: 14 abr. 2020.

mundo pós-pandemia, a ser herdado pelas crianças e pelos adolescentes, esteja sob vigilância constante?

PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES

Em um mundo hiperconectado, as TIC trazem diversas oportunidades para crianças e adolescentes, possibilitando novas maneiras de concretizar os direitos humanos consagrados em nosso ordenamento, como o direito à educação, à informação e ao lazer. Esses mesmos recursos podem, porém, gerar riscos, sobretudo levando-se em consideração a condição especial de pessoa vulnerável e em desenvolvimento dos menores.

Em relação aos riscos ligados à privacidade e à proteção de dados, os chamados "nativos digitais" estão experimentando algo nunca visto por outra geração. Seus dados são tratados desde a concepção, através de exames de ultrassom digitais, de babás eletrônicas e do monitoramento nas escolas, de modo que, quando chegarem à idade adulta, terão muito mais dados coletados que a geração de seus pais.

Diferentemente do equilíbrio esperado na utilização das tecnologias, o que se verifica, hoje, é um mundo cada vez mais conectado, no qual crianças e adolescentes convivem normalmente com a Inteligência Artificial, naturalmente dão ordens aos assistentes virtuais e têm seu brinquedo inteligente como melhor amigo. Os grandes dossiês digitais, produtos dessa interação constante, geram, contudo, vários efeitos adversos[147]

[147] Pode-se citar como efeitos adversos, primeiramente, o fato de esse grande arsenal de informações ser extremamente valioso para o modelo de negócios baseado em publicidade direcionada, de forma que, quanto mais tempo a geração Z permanece *online*, maior o retorno financeiro. Em segundo lugar, a bolha dos filtros, advinda da extrema personalização do conteúdo por meio de algoritmos, pode engessar o desenvolvimento social, discriminar comportamentos destoantes e gerar falhas de cognição e de relacionamento social em crianças e adolescentes. Por fim, a quantidade de informação sobre um mesmo indivíduo ou grupos de indivíduos, juntamente com a falta de transparência sobre o tratamento dos dados, gera situações de disparidade de poder, nas quais a vigilância passa a ser uma constante.

e as aplicações de Internet não costumam contemplar em seu *design* as necessidades especiais dessas pessoas.

No atual contexto social, todavia, a relação dos menores com a tecnologia é cada vez mais levada aos extremos. Impossibilitados de frequentar as escolas, crianças e adolescentes passam a relacionar-se com o meio social principalmente através de plataformas *online*. As instituições de ensino passam a disponibilizar aulas à distância (aquelas, claro, com suporte para tanto, situação que pode gerar, inclusive, o aprofundamento das desigualdades sociais),[148] sua relação com os avós e outros membros da família passa a ser exclusivamente por meio da Internet e todo o lazer pode acabar se resumindo aos jogos *online* e às redes sociais.

Ademais, crianças e adolescentes, assim como os adultos, estão submetidos a uma maior vigilância nesse período atípico. Além dos dados utilizados para o monitoramento do distanciamento social, dados de saúde, considerados sensíveis, estão sendo tratados, sem que todas as salvaguardas presentes na Lei Geral de Proteção de Dados (LGPD) estejam em vigor. Assim, duas questões chamam a atenção neste contexto, no tocante aos menores: a) eles são titulares de dados mais vulneráveis e, até agora, as tecnologias utilizadas para o combate à pandemia não têm levado em consideração suas peculiaridades; e b) eles serão os adultos de um mundo pós-pandemia, que tem o potencial de se caracterizar por uma vigilância cada vez mais intensa.

COVID-19 E A PROTEÇÃO DE CRIANÇAS E ADOLESCENTES POR *DESIGN*

Desde o início da crise da Covid-19, como já explicitado, as TIC têm sido amplamente utilizadas no combate à pandemia, o que gera inúmeras preocupações em torno

148 BANDEIRA, Olívia; PASTI, André. Como o ensino a distância pode agravar as desigualdades agora. Nexo Jornal. [s.l.]. 3 abr. 2020. Disponível em: <https://bit.ly/3ey3w0a>. Acesso em: 12 abr. 2020.

da privacidade dos indivíduos e da proteção de seus dados. Isso costuma ser amenizado com a alegação de que não haveria uso de dados pessoais quando as informações são agregadas e anonimizadas. No Brasil, as operadoras de celular que têm realizado parcerias com os governos defendem que utilizam dados estatísticos e que, portanto, não haveria qualquer violação a esses direitos.[149]

Contudo, o que tem preocupado os especialistas é a falta de transparência relativamente ao tratamento de dados, bem como a inexistência de parâmetros para esse tratamento, como os trazidos pela LGPD.[150] Primeiramente, pois não houve qualquer tipo de debate público em relação à escolha das tecnologias a serem utilizadas. Assim, não se sabe se elas são seguras, nem se não seria possível adotar tecnologias menos invasivas para atingir a mesma finalidade de tutela à saúde. Em segundo lugar, pois o ideal seria a assunção de um compromisso de que os dados tratados para o fim específico do combate à epidemia tivessem apenas essa finalidade e fossem imediatamente descartados com o seu fim[151]. Por fim, porque a anonimização dos dados depende sempre das tecnologias disponíveis na ocasião de tratamento e da granularidade dos dados coletados. Assim, em combinação com outros dados, saber onde alguém se encontra às 3h da madrugada facilita sua identificação, por exemplo.[152]

149 GROSSMAN, Luís Osvaldo. Privacidade divide Anatel e MCTIC em uso de dados móveis no combate à Covid-19. Convergência Digital. [s.l.]. 3 abr. 2020. Disponível em: <http://abre.ai/aZV7>. Acesso em: 13 abr. 2020.
150 BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19. Conciliando o combate à COVID-19 com o uso legítimo de dados pessoais e o respeito aos direitos fundamentais. São Paulo: Data Privacy Brasil, 2020.
151 Visto que a LGPD não está ainda em vigor, a Lei 13.979 de 2020 estabeleceu base legal, em seu art. 6º, para o tratamento de dados pessoais com a finalidade exclusiva de evitar a propagação do vírus (BRASIL. Lei nº 13.979, de 6 de fevereiro de 2020. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Brasília). Apesar disso, o sistema de proteção bastante abrangente criado pela LGPD seria fundamental para apaziguar controvérsias e proteger melhor os dados dos cidadãos.
152 DONEDA apud GROSSMAN, Luís Osvaldo. Privacidade divide Anatel e MCTIC em uso de dados móveis no combate à Covid-19. Convergência Digital. [s.l.]. 3 abr. 2020. Disponível em: http://abre.ai/aZV7. Acesso em: 13 abr. 2020.

Nos relatos disponíveis *online* sobre os pacientes de Singapura, essa falsa anonimização fica clara. A partir das informações relacionadas ao 96º caso de infecção por Covid-19 confirmado neste país, por exemplo, sabe-se que se trata de um menino de 12 anos e é possível identificar onde ele se encontra internado, qual o seu bairro de residência e a escola que frequenta.[153] Não seria possível, a partir desses dados, a fácil identificação dessa criança por seus colegas? Outra situação a se destacar ocorreu em Hong Kong, onde uma garota de 13 anos foi identificada em um restaurante utilizando um bracelete, que tinha como objetivo monitorar aqueles em quarentena. Ela, então, foi seguida, filmada e humilhada na Internet.[154]

No Brasil, o *site* The Intercept conseguiu identificar, recentemente, dois usuários da Vivo, a partir de bases de dados vendidas como anônimas à Secretaria de Turismo do Espírito Santo. A planilha, disponível no *site* da secretaria, tem informações de "milhares de pessoas não identificadas. Mas, se combinadas e cruzadas com outras bases, esse monte de informações permite que se chegue a perfis bem específicos. E, assim, a pessoas específicas também".[155] Diante desse cenário, portanto, não há como garantir que as parcerias realizadas no país para o combate à pandemia lidariam apenas com dados, de fato, anonimizados e agregados.

Nesse sentido, destaca-se o Termo de Recomendação Nº 07/2020, emitido pelo Ministério Público do Distrito Federal e Territórios, no qual recomenda ao Secretário de Estado do Distrito Federal que expeça portaria

153 UPCODE ACADEMY. Case 96: 12 year-old male Singapore Citizen. 2020. Disponível em: <http://abre.ai/aZV9>. Acesso em: 13 abr. 2020.
154 RICH, Motoko. Why Asia's New Wave of Virus Cases Should Worry the World. The New York Times. [s.l.]. 31 mar. 2020. Disponível em: http://abre.ai/aZWa. Acesso em: 13 abr. 2020.
155 DIAS, Tatiana. Vigiar e lucrar: nós identificamos dois clientes dos dados de localização 'anônimos' vendidos pela vivo. The Intercept Brasil. [s.l.]. 13 abr. 2020. Disponível em: https://bit.ly/3chayEz. Acesso em: 13 abr. 2020.

> proibindo o repasse à imprensa jornalística dos dados pessoais de pacientes que venham a óbito em decorrência de complicações do COVID19, tais como nome, filiação, endereço, profissão ou quaisquer outros que permitam a identificação de seus titulares, limitando-se a informar dados objetivos, como a causa mortis, gênero, idade e a preexistência de comorbidades.[156]

Ainda não se sabe, exatamente, quais as consequências que esse monitoramento, precipuamente a partir de dados sensíveis, pode exercer em crianças e adolescentes. Sabe-se, porém, que, historicamente, as aplicações da Internet não são desenhadas tendo em vista os interesses particulares dos menores. Assim, considerando que aqueles atualmente envolvidos no tratamento de dados para o combate à pandemia são os mesmos atores que desenvolvem as aplicações utilizadas pela maioria das pessoas,[157] pode-se esperar pouca informação sobre os efeitos desse uso no que se refere a esse público específico.

Isso é extremamente preocupante, principalmente considerando que os adultos de amanhã são as crianças de hoje. Decisões estão sendo tomadas para o enfrentamento da pandemia sem que se leve em consideração as consequências do uso massivo de tecnologias de vigilância para o futuro – em especial daquelas que passam a estar "sob a pele"[158] –, que pode se caracterizar pela naturalização da perda das liberdades e da exacerbação das desigualdades.

---

156 DISTRITO FEDERAL. MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. Termo de Recomendação nº 07/2020. Brasília, 2020. Disponível em: <https://bit.ly/3bj87RW>. Acesso em: 14 abr. 2020, p. 3.

157 Pode-se citar, por exemplo, além das operadoras de celular, o Facebook (HOLMES, Aaron. Facebook built a tool last year to map the spread of diseases. Now it's being used to combat coronavirus. Here's how it works. Business Insider. [s.l.]. 18 mar. 2020. Disponível em: https://bit.ly/2KjhvJr. Acesso em: 12 abr. 2020.), o Google e a Apple (GREENBERG, Andy. How Apple and Google Are Enabling Covid-19 Contact-Tracing. Wired. [s.l.]. 10 abr. 2020. Disponível em: <https://bit.ly/2yUD3JF>. Acesso em: 12 abr. 2020).

158 HARARI, Yuval Noah. Yuval Noah Harari: the world after coronavirus: the world after coronavirus. Financial Times. [s.l.]. 20 mar. 2020. Disponível em: <https://on.ft.com/3acr4UW>. Acesso em: 10 abr. 2020, tradução nossa.

É importante que a falsa dicotomia entre a tutela da saúde e dos dados pessoais seja eliminada.[159] Quando a população se sente empoderada, através de informações e autoridades confiáveis, um monitoramento severo não se faz necessário. As tecnologias a serem utilizadas devem permitir que cada um tome decisões pessoais mais informadas e também responsabilize o Estado por suas decisões.[160]

E, para aqueles que ainda não podem tomar algumas decisões sozinhos, deve-se recordar que o princípio do melhor interesse presente no *caput* do art. 14, da LGPD,[161] apenas reflete um princípio há muito existente em nosso ordenamento, pela ratificação da Convenção sobre os Direitos da Criança, mas frequentemente esquecido no desenvolvimento de leis e políticas públicas. Além desse princípio, que deve ser considerado cogente,[162] a Constituição Federal, em seu art. 227, traz a necessidade de prioridade absoluta em relação aos direitos de crianças e adolescentes.[163]

Sendo assim, faz-se necessário, cada vez mais, que esses direitos sejam incorporados pelas tecnologias e que crianças e adolescentes integrem seu processo de desenvolvimento, desde o início. Os menores são parte do ecossistema de vigilância digital e não devem ser considerados um adendo tardio na criação de soluções para produtos ou serviços, bem como na formulação de leis e políticas públicas. "Os dados relacionados à saúde coletados de todos os usuários, incluindo crianças, podem ser benéficos para as sociedades, mas somente se forem feitos com segurança e sem a perda de confiança da geração mais jovem de usuários da Internet".[164] Com efeito, além de cuidar daqueles que cuidam das crianças e dos adolescentes, a partir da proteção de dados de todos os

159 ZANATTA, Rafael; BIONI, Bruno. Proteção de dados faz parte da vacina contra Covid-19. Jota. [s.l.]. 4 maio 2020. Disponível em: <https://bit.ly/2L4dd99>. Acesso em: 06 maio 2020.
160 HARARI, Yuval Noah. Yuval Noah Harari: the world after coronavirus: the world after coronavirus. Financial Times. [s.l.]. 20 mar. 2020. Disponível em: https://on.ft.com/3acr4UW. Acesso em: 10 abr. 2020.
161 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília.
162 PEREIRA, Tânia da Silva. O "melhor interesse da criança". In: PEREIRA, Tânia da Silva. O melhor interesse da criança: um debate interdisciplinar. Rio de Janeiro: Renovar, 2000. p. 1-101.
163 BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República.
164 VOSLOO, Steven; PENAGOS, Melanie; RAFTREE, Linda. COVID-19 and children's digital privacy. Unicef. [s.l.]. 7 abr. 2020. Disponível em: <https://uni.cf/3enf99T>. Acesso em: 11 abr. 2020, tradução nossa.

brasileiros, é imperativo desenvolver políticas específicas, que considerem as peculiaridades dessas pessoas.

PROTEÇÃO DE DADOS, COVID-19 E ESTIGMA

Walter Britto Gaspar

Buscando no Twitter pela hashtag #eunaosouumvirus, vemos que a rede está repleta de mensagens em apoio à campanha, que responde a casos frequentes e notórios de xenofobia contra asiáticos após a emergência global do COVID-19. Entre os relatos e notícias, vemos casos de pessoas agredidas verbal e fisicamente por sua aparente herança genética. Em um dos que alcançou maior circulação, uma senhora agride verbalmente no Metrô do Rio de Janeiro uma passageira, acusando-a de espalhar a doença[165].

O problema vai além dos humores inflamados da população. Tornou-se notório o embate travado entre o filho do Presidente Jair Bolsonaro, Eduardo, e a Embaixada da China[166]. Não apenas Eduardo: o Ministro da Educação, Abraham Weintraub, também se envolveu na controvérsia e a Procuradoria-Geral da República chegou a requerer ao Supremo Tribunal Federal instauração de inquérito contra o Ministro para investigar crime de racismo[167]. A retórica de ambos se baseava na culpabilização dos chineses pelo COVID-19.

165 SAYURI, Juliana. #EuNãoSouUmVírus: epidemia do covid-19 dispara racismo contra asiáticos. TAB UOL, 12 de fev. de 2020, disponível em: <https://tab.uol.com.br/noticias/redacao/2020/02/12/eunaosouumvirus-ameaca-de-pandemia-dispara-racismo-contra-amarelos.htm>, acesso em 15 de abr. de 2020.

166 CORRÊA, Ricardo. Eduardo Bolsonaro ataca a China, que reage, e força Maia a pedir desculpas. O Tempo, 19 de mar. de 2020, disponível em: <https://www.otempo.com.br/politica/eduardo-bolsonaro-ataca-a-china-que-reage-e-forca-maia-a-pedir-desculpas-1.2313145>, acessado em 15 de abr. de 2020.

167 MENDONÇA, Ana. PGR pede ao STF abertura de inquérito contra Weintraub por racismo contra China. Estado de Minas, 14/04/2020, disponível em: <https://www.em.com.br/app/noticia/politica/2020/04/14/interna_politica,1138534/pgr-pede-ao-stf-abertura-de-inquerito-contra-weintraub-por-racismo-con.shtml>, acesso em 14 de abr. de 2020.

Esse não é um fenômeno novo. Em 1918, teve início uma pandemia do vírus influenza que infectaria cerca de 500 milhões de pessoas e vitimaria cerca de 50 milhões. Sua origem geográfica não é conhecida, mas sabe-se que em novembro de 1918 essa gripe chegou à Espanha vinda da França. Os jornais espanhóis da época não estavam sob regime de censura de guerra e, portanto, tinham liberdade para noticiar o efeito da nova gripe sobre o país. Isto criou a falsa percepção de que ela o impactava mais gravemente do que a outras nações europeias. Em virtude disto, esta gripe seria comumente conhecida como "gripe espanhola"[168].

Não apenas a origem geográfica ou a marca genotípica podem ser o fundamento de agressões físicas, verbais ou simbólicas. Durante a epidemia do vírus da imunodeficiência humana (HIV) nos Estados Unidos nos anos 1980, a doença era conhecida como "câncer gay" e profundamente ligada ao preconceito já existente em relação a homossexuais e usuários de drogas injetáveis[169]. A opinião pública chegava a propor e apoiar iniciativas de testagem e isolamento em massa desses grupos, tratando-os como o ponto focal da doença e culpabilizando-os pela infecção em função de comportamentos taxados como "de risco".

Em torno disto, e com base nos escritos de Erving Goffman[170], uma extensa literatura na área de saúde coletiva formou-se a respeito do estigma relacionado à AIDS. Em artigo publicado em 1988, Gregory Helek e Eric Glunt escreviam[171]:

---

168 Spanish flu. Wikipedia. Disponível em: <https://en.wikipedia.org/wiki/Spanish_flu>. Acesso em 15 de abr. de 2020.
169 LIMA, I. F. D. DE; ALMEIDA, F. D. DE; RISI, M. TEREZA. AIDS homossexualidade e estigma social nos anos 1980: as vozes da mídia nos jornais brasileiros da Coleção ABIA. XXVIII Congresso Brasileiro de Biblioteconomia e Documentação. Anais...Vitória, ES: 2019.
170 Para Goffman, o estigma é um atributo que provoca profundo descrédito da sociedade em geral (os "normais") em relação ao estigmatizado, tornando-o um "estrangeiro" (*outsider*), arruinando sua identidade social e atribuindo-lhe comportamentos desviantes. Ver GOFFMAN, E. Stigma: Notes on the management of spoiled identity. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1963.
171 HEREK, G. M.; GLUNT, E. K. An Epidemic of Stigma: Public Reactions to AIDS. **American Psychologist**, v. 43, n. 11, 1988, p. 888.

> *"É uma nova doença que é uniformemente fatal; é causada por um agente infeccioso invisível que pode estar latente no corpo por um período desconhecido; a epidemia é percebida tanto como fora de controle quanto como potencialmente catastrófica. Por causa dessas características, julgamentos individuais associados à AIDS são frequentemente realizados sob condições de ansiedade e são, portanto, provavelmente defeituosos."*

Fora a característica de ser "uniformemente fatal" e o período desconhecido de latência do agente infeccioso, são contornos semelhantes aos da atual pandemia. Naturalmente, a AIDS tem elementos próprios muito particulares que não permitem uma comparação direta. No entanto, pensar sobre como sociedades encararam a epidemia de HIV/AIDS pode prover paralelos quando miramos o COVID-19.

Helek e Glunt avaliam que o estigma em relação à doença acontece porque ela põe os "normais" em contato imediato com a mortalidade, algo que rompe com a atitude natural da vida cotidiana e provoca uma ansiedade fundamental. Como uma resposta a esse sentimento, grupos de "normais" tendem a identificar a doença a um "outro" grupo – os outsiders -, de modo a se distanciar da morte[172].

Recorramos a um exemplo mais próximo da atual crise de saúde. Durante os surtos de SARS (Síndrome Respiratória Aguda Grave) em 2003, também causados por um

172 Idem, p. 887.

coronavírus, viu-se emergir uma epidemia – de medo, desinformação e estigma – dentro da epidemia[173]. Person et al. destacam que o

> *"Medo da SARS emergiu de uma ansiedade subjacente a uma doença com causa desconhecida e possivelmente fatal. A estigmatização de pacientes potenciais da SARS surgiu logo cedo na epidemia, à medida que a mídia global reportava histórias dramáticas vindas da Ásia"*[174].

O efeito desse estigma sobre o enfrentamento das respectivas epidemias e pandemias é palpável. Entre o reforço de processos pré-existentes de discriminação e a relutância em procurar testagem, tratamento ou prevenção devido ao medo de ser estigmatizado[175], o fenômeno tem implicações reais sobre como governos enfrentam crises de saúde.

Aqui, no entanto, gostaríamos de focar a atenção em um aspecto específico do estigma, que é a criação de um "outro", e sua interseção com o problema da proteção de dados pessoais. Ao comentar o trato que os "normais" dispensam ao estigmatizado, Goffman nota que "Por definição, é claro, acreditamos que a pessoa com um estigma não é inteiramente humana. Com base nisto, exercemos várias discriminações, pelas quais, ainda que de forma impensada, reduzimos suas oportunidades de vida"[176].

---

173 PERSON, B. et al. Fear and Stigma: The Epidemic within the SARS Outbreak. Emerging Infectious Diseases, v. 10, n. 2, p. 358–363, fev. 2004.
174 Tradução nossa. PERSON, B. et al. Fear and Stigma: The Epidemic within the SARS Outbreak. Emerging Infectious Diseases, v. 10, n. 2, fev. 2004, p. 358.
175 MAHAJAN, A. P. et al. Stigma in the HIV/AIDS epidemic: a review of the literature and recommendations for the way forward. AIDS, v. 22, n. Suppl 2, p. S57–S65, ago. 2008.
176 GOFFMAN, E. Stigma: Notes on the management of spoiled identity. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1963, p. 5.

Lembremos que a proteção de dados pessoais nasce de um longo caminho de desenvolvimento do direito à privacidade. Neste trajeto, passa por quatro "gerações" normativas que incorporam, cada vez mais intensamente, a informação e os meios técnicos e tecnológicos de seu tratamento. Chega-se, assim, à proteção de dados pessoais, que é o meio pelo qual se implementa na prática a autodeterminação informativa – a capacidade do sujeito de controlar a sua representação informacional[177].

Essa representação é indistinguível da própria identidade física e moral do titular dos dados. As esferas do real e do virtual – ou, melhor, do informacional – já são, em nossa sociedade da informação, muito profundamente conectadas. Sob essa perspectiva, compreendemos com mais precisão o motivo pelo qual o legislador optou por incluir entre o rol de fundamentos da nossa Lei Geral de Proteção de Dados (LGPD) o livre desenvolvimento da personalidade (art. 2º, VII) e a autodeterminação informativa (art. 2º, II). São consequência de uma compreensão da proteção de dados ancorada na privacidade, como uma representação da personalidade – em última análise, como condição para a plena realização da dignidade da pessoa humana[178].

Retornando agora ao ponto focal deste ensaio. Percebamos a incongruência fundamental entre um regime jurídico fundado na proteção da personalidade e uma dinâmica social operacionalizada pela construção de um "outro" menos humano que nós, "normais". Esse outro, por ser menos humano, tem menos personalidade, identidade –

177 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2ª edição. São Paulo: Thomson Reuters Brasil, 2019.
178 CRFB/88, art. 1º, III. Aqui, recordamos as palavras de Luiz Edson Fachin sobre a continuidade lógica entre dignidade humana e direitos da personalidade: "Essa perspectiva principiológica da dignidade humana informa e conforma todo o ordenamento jurídico, servindo de substrato normativo e axiológico para todos os demais direitos não patrimoniais, como os direitos da personalidade". FACHIN, Luiz Edson. Análise crítica, construtiva e de índole constitucional da disciplina dos direitos da personalidade no Código Civil brasileiro: fundamentos, limites e transmissibilidade. Revista jurídica, 363, 2007, pp. 43-60.

uma identidade "arruinada" – e merece, portanto, menos direitos. Assim nasceram, durante a epidemia de HIV/AIDS, declarações como esta, publicada em 1986 em artigo de opinião no New York Times[179]:

> *"Everyone detected with AIDS should be tattooed in the upper forearm, to protect common-needle users, and on the buttocks, to prevent the victimization of other homosexuals."*

No enfrentamento da atual pandemia do COVID-19, governos do mundo inteiro têm reafirmado os benefícios do tratamento massivo de dados pessoais. De fato, o controle da difusão da doença em alguns países corrobora a vantagem do uso de ferramentas conectadas de monitoramento. No entanto, é preciso estar muito atento às ameaças aos direitos fundamentais em um contexto de crise de saúde.

Se em uma situação corriqueira a tomada de decisão já é nebulosa devido à imprevisibilidade de novas tecnologias, adotar uma postura responsável em relação à privacidade pode ser ainda mais desafiador diante da pandemia. Populações inteiras, inclusive gestores públicos e legisladores, estão sujeitos aos efeitos do estigma apontados anteriormente. Isto significa que podem caminhar na direção de padrões heurísticos[180], isto é, não lógico-racionais, em virtude do medo da fatalidade da doença – o "*germ panic*"[181]. Isto conduz não apenas ao cenário de xenofobia que vemos atualmente, mas

179 Buckley, W. F. Jr.. Crucial steps in combating the AIDS epidemic: Identify all the carriers. New York Times, 18 de mar. de 1986, p. A27; apud HEREK, G. M.; GLUNT, E. K. An Epidemic of Stigma: Public Reactions to AIDS. American Psychologist, v. 43, n. 11, 1988, p. 886.
180 HEREK, G. M.; GLUNT, E. K. An Epidemic of Stigma: Public Reactions to AIDS. American Psychologist, v. 43, n. 11, p. 886–891, 1988.
181 PAPPAS, G. et al. Psychosocial consequences of infectious diseases. Clinical Microbiology and Infection, v. 15, n. 8, p. 743–747, ago. 2009.

também a escolhas erradas sobre a estruturação de programas de monitoramento cujas falhas levam a violações de direitos.

Isto fica muito claro quando analisamos alguns casos recentes do uso de tecnologias de monitoramento de movimentação contra o COVID-19. Na Coreia do Sul, onde aplicativos oferecem essa funcionalidade, houve casos notórios de "desanonimização" dos dados supostamente anonimizados[182]. De fato, dado um banco de dados variado ou vultoso o bastante, toda pretensão de anonimização é falsa[183].

Diante disto, é fundamental que programas governamentais busquem mitigar os riscos de identificação das pessoas infectadas ou mesmo testadas. É importante considerar, ainda, que ao lidar com o medo e a ansiedade das populações, não se pode esperar racionalidade dos grupos envolvidos, devido aos processos de estigmatização e o *germ panic*. Finalmente, é essencial que esses programas se desenrolem de forma transparente e que seus fundamentos e especificações técnicas sejam levados ao escrutínio público, de modo que falhas na anonimização – que podem levar a um recrudescimento das dinâmicas de desumanização típicas do estigma em relação à saúde – sejam identificadas e corrigidas.

182 Sobre essas falhas e as suas consequências estigmatizantes, cf.: ACCESS NOW. Recommendations on privacy and data protection in the fight against COVID-19. [s.l: s.n.]. Disponível em: <https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>. Acesso em: 15 de abr. de 2020; e "MORE scary than coronavirus": South Korea's health alerts expose private lives. The Guardian. Disponível em: <https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives>. Acesso em: 15 de abr. de 2020.

183 Tratamos em maiores detalhes da ilusão da anonimização em GASPAR, W. B. Proteção de dados à deriva: O difícil equilíbrio entre controle e privacidade. Disponível em: <https://medium.com/centro-de-tecnologia-e-sociedade/proteção-de-dados-à-deriva-o-difícil-equilíbrio-entre-controle-e-privacidade-7ef40094ccc7>. Acesso em: 15 de abr. de 2020. Cf. também MAGRO, Américo Ribeiro. A (in)eficácia do direito à anonimização de dados pessoais em face da análise de big data dos metadados produzidos no âmbito da internet das coisas. In: TEIXEIRA, Tarcisio; MAGRO, Américo Ribeiro (coord.). Proteção de dados: Fundamentos jurídicos. Salvador: Editora JusPodivm, 2020; e MAGRANI, E. A internet das coisas. Rio de Janeiro: FGV Direito Rio, 2018. Disponível em: <http://eduardomagrani.com/trilogiaculturadigital/>. Acesso em 15 de abr. de 2020.

PARTE IV

O RECEIO DE UMA VIGILÂNCIA CONTÍNUA

O AUXÍLIO EMERGENCIAL E A VIGILÂNCIA DOS CONSUMIDORES PÓS-COVID-19

Afonso Carvalho De Oliva[184]

INTRODUÇÃO

Neste breve ensaio, busca-se analisar os riscos envolvidos no mecanismo eleito pelo Governo Federal para a concessão do Auxílio Emergencial de Renda prevista na lei nº. 13.982, qual seja, a abertura de contas digitais para aqueles que não possuíam contas bancárias no momento do cadastramento no programa social, atingindo, com isso, a camada da população que, outrora, encontrava-se longe dos olhos fiscalizatórios do Estado em questões econômicas.

Trata-se da inclusão de cerca de 30 milhões de novos consumidores nas bases de dados que alimentam, também, os recentemente regulamentados cadastros positivos de crédito, com o detalhe especial de que o preenchimento de certos requisitos legais garante uma maior categorização desses consumidores, com impacto direto na dedução mais acertada do perfil de consumo de cada cidadão e, consequentemente, na concessão de crédito no país.

No estudo que segue, tenta-se demonstrar como a criação dessas contas digitais – manobra utilizada como solução, no "estado de exceção" decorrente da pandemia do COVID-19, para a distribuição do auxílio emergencial de renda – trará implicações para a futura análise de crédito daqueles que se encontravam à margem dos sistemas automatizados regulados pelo Cadastro Positivos de Crédito, repercutindo como mais uma

[184] Advogado. Doutorando em Ciências Jurídicas Privatísticas na Universidade do Minho (Portugal). Mestre em Direito pela Universidade Tiradentes (Sergipe - Brasil). Coordenador do Núcleo de Prática Jurídica da Faculdade de Direito 8 de Julho (Sergipe – Brasil). contato@afonsooliva.com

ferramenta capaz de reforçar a vigilância crônica sobre o mercado de consumo brasileiro.

O AUXÍLIO EMERGENCIAL DE RENDA

A pandemia desencadeada pela síndrome respiratória COVID-19, oriunda da variante SARS-CoV-2 da família Coronavírus, não representou apenas um severo golpe nos sistemas de saúde de todo o mundo, mas, também, desencadeou um severo processo de crise econômica global.

No Brasil, a crise econômica já vem sendo alvo dos mais diversos estudos em busca de uma saída[185]. Todavia, por características inerentes à conformação da base econômica brasileira, o impacto da crise econômica reveste-se de características peculiares, as quais acabam por dificultar a solução, uma vez que 41,1% da força de trabalho brasileira são compostos por pessoas em atividades informais[186] – aquelas que não possuem registro em carteira de trabalho, empregadores e trabalhadores autônomos sem CNPJ e pessoas que auxiliam familiares em atividades domésticas ou empresariais sem o devido registro.

Em termos numéricos, esse percentual significa um grupo de 38,4 milhões de pessoas, o qual representa parcela da população que, no momento em que os estados iniciaram a publicação de decretos determinando o isolamento social compulsório, com o encerramento de atividade comerciais formais e informais em todo o país, viu-se privada de qualquer tipo de rendimento financeiro, uma vez que não mais podia desempenhar

185 PESSÔA, Samuel, Opinião - Samuel Pessôa: A macroeconomia da pandemia, Folha de S.Paulo, disponível em: <https://www1.folha.uol.com.br/colunas/samuelpessoa/2020/04/a-macroeconomia-da-pandemia.shtml>, acesso em: 12 abr. 2020.
186 GARCIA, Diego, Informalidade supera 50% em 11 estados do país, diz IBGE, Folha de S.Paulo, disponível em: <https://www1.folha.uol.com.br/mercado/2020/02/informalidade-atinge-recorde-em-19-estados-e-no-df-diz-ibge.shtml>, acesso em: 12 abr. 2020.

suas atividades laborais, estando, ainda, afastada de eventuais programas sociais do governo.

Diante de tão grave cenário, foi publicada a lei federal de número 13.982, cujo artigo 2º trouxe a figura denominada "auxílio emergencial", que consiste no pagamento de R$ 600,00 (seiscentos reais) durante um período de três meses, desde que preenchidos os requisitos do mesmo dispositivo. Logo após a publicação da lei, diante da omissão do texto legal acerca do modo de operacionalização do pagamento do auxílio emergencial, teve início grande especulação sobre a forma que seria utilizada para tanto[187]. A solução foi apresentada apenas em 07 de abril de 2020[188], com o cadastramento dos beneficiários por meio de aplicativo para celular e por site específico. O pagamento se daria por meio de depósito em conta informada pelo beneficiário no momento do cadastro, ou, para os que já estavam inscritos em programas sociais do governo, na conta em que recebem os demais benefícios.

Contudo, no mesmo anúncio, foi apresentada a solução para aqueles que não estavam cadastrados em programas sociais e que tampouco possuíam contas bancárias para recebimento dos valores. Nestes casos, a Caixa Econômica Federal, após o cadastro do beneficiário para recebimento do auxílio, realizou a abertura de uma conta poupança digital, sem custo para o titular, com o que, num único movimento, a instituição financeira trouxe para seu portifólio mais de 30 milhões de pessoas[189] que estavam fora do

187 ANDRADE, Hanrrikson de, Coronavoucher atrasa, e Bolsonaro admite receio de criar "cheque sem fundo", disponível em: <https://economia.uol.com.br/noticias/redacao/2020/04/02/bolsonaro-beneficio-600-reais.htm>, acesso em: 13 abr. 2020.
188 MINISTÉRIO DA CIDADANIA, Auxílio Emergencial de 600 — Secretaria Especial do Desenvolvimento Social, Secretaria Especial do Desenvolvimento Social, disponível em: <http://desenvolvimentosocial.gov.br/auxilio-emergencial/auxilio-emergencial-de-600>, acesso em: 13 abr. 2020.
189 Caixa abrirá 30 milhões de poupanças para pagamento de auxílio de R$ 600, EXAME, disponível em: <https://exame.abril.com.br/seu-dinheiro/caixa-abrira-30-milhoes-de-poupancas-para-pagamento-de-auxilio-de-r-600/>, acesso em: 13 abr. 2020.

mercado bancário brasileiro. Trata-se de efeito fático não previsto na lei, com repercussões que ultrapassam a situação presente de emergência econômica e de sérias consequências no tocante à exposição de dados pessoais dos beneficiários do auxílio.

CONTAS DIGITAIS: DO "ESTADO DE EXCEÇÃO" À VIGILÂNCIA CRÔNICA DO CRÉDITO

A criação das contas-poupança digitais revelou-se, em princípio, ferramenta efetiva para a solução da problemática enfrentada pelo governo federal para alcançar a parcela da população que se encontrava afastada do sistema bancário formal, composta, expressivamente, de pessoas que possuem ocupações informais e que, por isso, acabavam passando à margem das regulações governamentais e mercadológicas.

Nesse contexto, apresenta-se preocupação acerca da normalização de uma medida que surgiu como solução apenas para o "estado de exceção", sem considerar o efeito de incremento na vigilância crônica já existente no mercado de consumo e de crédito brasileiro, decorrente da inclusão de 30 milhões de cidadãos no sistema bancário nacional.

A vigilância crônica do mercado de consumo, em especial, no tocante ao poder de compra e ao crédito dos consumidores brasileiros, vem em trajetória ascendente, independentemente da orientação política dos atores que estejam em posição de chefia dos poderes da república, desde o início da segunda década do século XXI, mais especificamente, desde 30 de dezembro de 2010, com a edição da Medida Provisória 518, pela qual se deu vida ao chamado "Cadastro Positivo de Crédito", apresentada como uma

importante ferramenta a ser utilizada no mercado de crédito para a garantia de concessão de menores taxas de juros para os bons pagadores[190]. Posteriormente, em 09 de julho de 2011, a Medida Provisória foi convertida na lei de número 12.414, instituindo, de forma definitiva, a possibilidade de criação de cadastros para a análise do histórico de crédito dos consumidores brasileiros.

A criação dos cadastros positivos seguiu a tendência mundial de detalhamento do padrão de comportamento dos consumidores para permitir aos fornecedores a formação de uma imagem mais completa sobre seus clientes, com vistas à oferta de produtos com maior chance de aceitação, bem como à possibilidade de uma melhor manipulação do comportamento de consumo. Este movimento, que busca transformar os consumidores e seus hábitos diários em mercadorias a serem oferecidas para outras empresas fornecedoras, foi analisado e descrito, exemplarmente, pelo sociólogo Zygmunt Bauman[191].

Ocorre que o meio eleito para a criação desses perfis de consumo – um cadastro em que o consumidor optava pela adesão – não alcançou o objetivo pretendido, sendo desconhecido pela maior parte da população[192]. Além desse desconhecimento social, já se questionava a legalidade da referida lei[193]. Diante desse cenário, as empresas de análise de crédito optaram por uma nova abordagem: a criação do chamado "credit score"

---

[190] BARRETO, Luiz Paulo Teles Ferreira; MANTEGA, Guido, Exposição de Motivos Interministerial n° 171/2010 - MF/MJ.
[191] BAUMAN, Zygmunt, **Vida para consumo: A transformação das pessoas em mercadoria**, Rio de Janeiro: Zahar, 2008.
192 Neste sentido: Um tal "Cadastro Positivo", Revista do IDEC, n. 186, p. 16–16, 2014; ALEGRETTI, Laís; ALVES, Murilo Rodrigues, Bancos 'travam' cadastro positivo - economia - Estadao.com.br, Estadão, disponível em: <http://economia.estadao.com.br/noticias/economia-geral,bancos-travam-cadastro-positivo,176835,0.htm>, acesso em: 4 fev. 2014.
193 Neste sentido: BESSA, Leonardo Roscoe, Responsabilidade civil dos bancos dos dados de proteção ao crédito: diálogo entre o Código de Defesa do Consumidor e a Lei do Cadastro Positivo, Revista de Direito do Consumidor, v. 92, p. 49, 2014; CUNHA E CRUZ, Marco Aurélio Rodrigues da; OLIVA, Afonso Carvalho de, A defesa constitucional do consumidor e a lei no 12.414/2011 (cadastro positivo): Banco de dados, proteção de dados pessoais e relações de consumo., in: MEIRELLES, Delton R. S.; PIMENTEL, Fernanda (Orgs.), Processo e Conexões Humanas, 1. ed. Petrópolis: Sermograf, 2014, p. 130–158.

– uma nota (ou classificação) conferida aos consumidores com base numa série de informações coletadas das mais diversas fontes[194], resultante do "risco" que ele representaria para a concessão de crédito.

A prática, realizada, inicialmente, sem o conhecimento dos consumidores, foi levada aos tribunais brasileiros, tendo chegado até o Superior Tribunal de Justiça[195], que reconheceu sua legalidade e editou a súmula 550[196], para firmar o entendimento delineado no acórdão do processo sobre a questão.

Imperioso destacar que o julgamento e a posterior súmula editada foram objetos de críticas da doutrina[197], uma vez que o reconhecimento estatal desta prática apenas fortalecia a manipulação do mercado de consumo, autorizando uma ampliação da coleta indiscriminada de dados pessoais dos consumidores, o que permitia às empresas de análise de crédito o acompanhamento personalíssimo dos consumidores.

Em 2019, um novo movimento no sentido de aprofundamento da "vigilância crônica" no mercado de consumo brasileiro foi verificado com a publicação da Lei Complementar nº. 166, que trouxe sensíveis alterações à lei 12.414/2011, sendo a mais alarmante a mudança na forma de constituição dos cadastros positivos de crédito. O que antes dependia de uma posição ativa do consumidor, que escolhia participar – caso em

194 OLIVA, Afonso Carvalho de. Direitos do Consumidor: proteção de dados pessoais, 1. ed. Aracaju: DireitoMais, 2016, p. 149–150.
195 BRASIL, Superior Tribunal de Justiça, Inteiro Teor do Acórdão do Recurso Especial no. 1.419.697 - RS, Diário da Justiça Eletrônico, 1632. ed. 2014, p. 419.
196 Súmula 550-STJ: A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. STJ. 2ª Seção. Aprovada em 14/10/2015, DJe 19/10/2015.
197 Cf. GOMES, Gustavo Gonçalinho da Mota et al, ANÁLISE DA PRÁTICA DE CREDIT SCORE E AVALIAÇÃO DE ATUAÇÃO NOS AUTOS DO RESP 1.419.697/RS. NOTA N. 104/CGEMM/DPDC/SENACON/2014 - Ministério da Justiça Secretaria Nacional do Consumidor Departamento de Proteção e Defesa do Consumidor Coordenação Geral de Estudos e Monitoramento de Mercado, Revista de Direito do Consumidor, v. 96, p. 383–399, 2014; OLIVA, Direitos do Consumidor: proteção de dados pessoais.

que era chamado de opt-in – passou a ser compulsório, podendo o consumidor optar por se retirar destes cadastros – modelo opt-out.

A escola da Análise Econômica do Direito já se ocupou da análise da ineficácia dos modelos opt-out em contratos de consumo. Bar-Gill e Ben-Shahar[198] demonstram como o custo envolvido nesses modelos dificilmente supera, numa análise superficial dos consumidores, os benefícios que estes podem auferir. O "transactional cost" é negativo, e o consumidor irá "gastar" seu tempo para tomar conhecimento do cadastro e buscar os meios para sair de um serviço que não irá representar qualquer ganho, financeiro ou de bem-estar, para ele.

Essas são algumas das preocupações com as medidas adotadas neste momento de exceção, decorrentes da criação de 30 milhões de novas contas bancárias. Indiscutível, também, a inclusão de 30 milhões de novos consumidores nas bases de dados dos cadastros positivos de crédito, com uma informação adicional: a certeza de que se trata de indivíduos que preenchem os requisitos previstos na lei de concessão do auxílio emergencial, o que garante uma maior categorização desses consumidores. Resulta disso um possível impacto direto na concessão de crédito, uma vez que, se antes os consumidores poderiam representar uma incógnita para os sistemas de análise de risco, já que não possuíam movimentações financeiras, agora, podem ser facilmente identificados como consumidores que representam um "potencial risco", ante a caracterização como pessoa em situação de "dificuldade financeira".

Destaca-se, ainda, que, quando do cadastramento para abertura da conta, não é aventada a possibilidade de abertura de cadastro positivo, ou mesmo a utilização dos

[198] BAR-GILL, Oren; BEN-SHAHAR, Omri, **Optimal Defaults in Consumer Markets**, Rochester, NY: Social Science Research Network, 2016.

dados ali captados para o oferecimento de novos produtos ou serviços, embora essa possibilidade seja confirmada pela própria instituição financeira[199], mediante o oferecimento de produtos e serviços "moldados" para os perfis de consumo de cada um desses cidadãos. Viola-se, com isso, a autodeterminação informativa do consumidor brasileiro[200], o que agrava sua posição de mera "mercadoria", a ser negociada entre diversos fornecedores.

Com essas palavras, reforça-se a característica excludente do mercado creditício, em que as ferramentas e tecnologias são apresentadas como soluções para facilitar o acesso dos consumidores aos produtos, maquiando seu real propósito, o de servirem como mecanismos de classificação e filtragem desses clientes, agora compartimentalizados e segregados. Assim, "garantindo-se a desigualdade, permanece a possibilidade de domínio social pelos grupos políticos, que são, em última análise, dominados por grupos de grande poder econômico"[201], em reforço ao objetivo do mercado de consumo, de buscar tomar posse de todos os dados produzidos pelos consumidores[202], para compreendê-los e, em seguida, moldar o seu comportamento de modo a adequá-lo aos objetivos das empresas fornecedoras.

---

199 FLACH, Natália; MAMONA, Karla; ALMEIDA, Marília, Caixa pretende rentabilizar os clientes que não têm conta bancária, EXAME, disponível em: <https://exame.abril.com.br/negocios/caixa-pretende-rentabilizar-os-clientes-que-nao-tem-conta-bancaria/>, acesso em: 13 abr. 2020.

200 Neste sentido: BIONI, Bruno Ricardo, O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo "Lulu", Revista de Direito do Consumidor, v. 94, p. 283–324, 2014; NAVARRO, Ana Maria Neves de Paiva, O Direito Fundamental à Autodeterminação Informativa, in: CONPED/UFF (Org.), Direitos fundamentais e democracia II, Florianópolis: FUNJAB, 2012, p. 410–438; CARVALHO, Ana Paula Gambogi, O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos, Revista de direito do consumidor, v. 46, p. 77–119, 2003.

201 OLIVA, Afonso Carvalho de; PESSOA, Flávia Moreira Guimarães, Bancos de Dados e a Proteção do Consumidor Brasileiro: o Panóptico Pós-Moderno, **Prim@ Facie**, v. 15, n. 28, p. 01–43, 2016.

202 Idem.

CONSIDERAÇÃO FINAL

A urgência econômica, tão pandêmica quanto a própria doença que a causa, faz bem vindo o auxílio emergencial no Brasil, mas não se pode ignorar que se trata de medida de efeitos colaterais previsíveis no tocante ao futuro (não distante) do tratamento e da utilização dos dados pessoais informatizados, seja daqueles já cadastrados nos programas assistenciais governamentais, seja dos recém-cadastrados para recebe-lo.

Que a presente provocação seja capaz de despertar o interesse em pesquisas mais aprofundadas, a respeito dos impactos que a abertura de contas digitais pode ocasionar para o futuro creditício dos consumidores brasileiros e para o monitoramento destes pelo mercado de consumo, invariavelmente, com reflexos sobre a oferta orientada de produtos e serviços, (re)desenhados de acordo com o perfil traçado por meio dos dados pessoais coletados e processados.

CORONAVÍRUS: UM INTENSIFICADOR DO ESTADO DE VIGILÂNCIA

Fabricio Barili

Dados pessoais e governos possuem uma relação estreita. Do sujeito censor do Império romano ao surgimento da estatística como uma Ciência do Estado[203], a necessidade de obter dados dos seus cidadãos permanece e se aperfeiçoa. No Brasil, para se ter conhecimento sobre a população, a fim de estudos ou tomada de ações, os censos

203 BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. Revista FAMECOS, [s. l.], v. 15, n. 36, p. 10, 2008.

são realizados há anos pelo IBGE, um órgão estatal que tem como principal objetivo fazer o levantamento periódico acerca de dados socioeconômicos do país. Contudo, o órgão não se prende à análise de dados sensíveis – aqueles que podem identificar um cidadão – e assim impossibilita que medidas de vigilância sejam impostas.

O período de exceção derivado da disseminação massiva do novo Coronavírus levaram o Estado a tomar medidas que afetam diretamente a vida do cidadão: restrição na circulação, fechamento de estabelecimentos, interrupção no tráfego de interestaduais, entre outras. Seja pela via biopolítica, como em Foucault[204], ou pela necropolítica, como em Mbembe[205], há uma governamentalidade dos corpos pelo Estado, por meio de tecnologias de vigilância e a partir da naturalização de um Estado de exceção. Para o monitoramento, utiliza massivamente a tecnologia disponível, que depende exaustivamente de coleta e processamento de dados. É invisível e não possui seus processos claros, levantando uma série de perigos.

Questões como a privatização de instituições públicas, histórico de vazamento de dados, os vieses por trás de cada estrutura algorítmica e a forma como são processadas essas informações são de interesse de toda a população e devem ser discutidas abertamente. Assim, neste ensaio, irei discutir questões que possam elucidar a maneira com que um Estado de exceção pode se aproveitar do novo Coronavírus para fortalecer políticas de vigilância praticados durante a pandemia e após ela.

204 FOUCAULT, Michel. O Nascimento da Biopolítica. São Paulo: Martins Fontes, 2008.
205 MBEMBE, Achille. Necropolítica: biopoder, soberania, estado de exceção, política da morte. São Paulo: N-1, 2018.

GOVERNO E DADOS

Diante de cenários de exceção como a pandemia do CoVid-19, a China demonstrou sua capacidade de rastrear indivíduos por meio de câmeras, aplicações móveis e utilização de serviços públicos, tentando mapear os possíveis contaminados pela doença. A obtenção de tais informações somente se tornou viável devido à vasta infraestrutura de câmeras, algoritmos de reconhecimento facial e integração das bases de dados do governo. Estruturas dessa complexidade não são vistas no Brasil, no entanto, em momentos ímpares como Olimpíadas, Pan Americano e Copa do Mundo, houve a necessidade de um aperfeiçoamento na infraestrutura de monitoramento nacional. Batista[206] fez um estudo das práticas de Smartsurveillance praticadas durante a Copa do Mundo de 2014 e sinalizou que nas cidades do Recife e Curitiba foram implementados Centros Integrados de Comando e Controle, além de ações envolvendo as empresas Cisco e Nec, junto ao poder público da cidade de Recife. Percebemos, nesse caso, a importância que os governos deram para uma coleta automatizada de dados e de vigilância para um fim específico.

O que desejo chamar a atenção é: após um Estado de exceção, os investimentos realizados e os poderes cedidos para a obtenção e coleta de informações não retornam ao ponto anterior[207]. O autor dessa frase, no seu texto intitulado **O coronavírus tirou qualquer freio à invasão da tecnologia na sociedade** faz referência ao Patriot Act que, na ocasião dos ataques terroristas de 11 de setembro, foi aprovado, permitindo que o governo norte-americano pudesse coletar todo e qualquer tipo de dado dos seus cida-

206 BATISTA, Marcela de Moraes; FARINIUK, Tharsila Maynardes Dallabona; MELLO, Sérgio Carvalho Benício De. SMARTSURVEILLANCE EM APLICAÇÕES RECENTES NO BRASIL: UM ESTUDO DE CASO NAS CIDADES DE RECIFE E CURITIBA. [s. l.], p. 34, 2016.
207 FELITTI, Guilherme. O coronavírus tirou qualquer freio à invasão da tecnologia na sociedade. 2020. Disponível em: https://manualdousuario.net/podcast/tecnocracia-30. Acesso em 11 de abril de 2020.

dãos, sem a permissão do congresso, para fins de segurança pública. Anos após o acontecimento, veríamos essa prática ser levada ao extremo após as denúncias de Edward Snowden ao jornal The Intercept. A premissa apresentada por Felitti acerca das regras de um Estado de exceção se tornarem permanentes, e é reforçada pela recente entrevista de Edward Snowden[208] e pelo estudo de Batista[209]: "após o término da Copa do Mundo, o CICC-PE permaneceu em pleno funcionamento todos os dias da semana. Entretanto, passou por algumas mudanças em nível estratégico, sendo também utilizado em ações de monitoramento cotidiano".

Os dados coletados de todos os cidadãos, seja pelo IBGE nos censos ou através da utilização de serviços públicos como SUS, seguro desemprego, financiamentos de diversos tipos ou até mesmo o fornecimento do CPF no cupom fiscal, enriquecem a base de dados do Estado. Isso permite o conhecimento de cada movimento do cidadão compondo, de certa forma, um laboratório-mundo, nos termos de Bruno[210]. Cada um desses inputs tem de ser eficientes na sua função para coletar cada vez mais dados. Isso significa ter agilidade, sem fricção e extrair dados com mais qualidade. Essa estrutura ganha um salto no conhecimento humano por meio dos dados pois passa, além de coletar, a alimentar bases de dados que possuem por finalidade conhecer, fazer previsões e até mesmo intervenções em nosso comportamento[211].

Com a pandemia, mais uma série de iniciativas coletoras entraram na jogada. Aplicativos do governo foram criados e oferecidos à população com diversas finalidades,

---

208 Edward Snowden prevê futuro distópico após a epidemia de COVID-19. Disponível em: <https://medium.com/@andrmiguis/edward-snowden-prev%C3%AA-futuro-sombrio-ap%C3%B3s-a-epidemia-de-covid-19-805c2bedb1cc>. Acesso em 13 de abril de 2020.

210 211 227 BRUNO, Fernanda Glória; BENTES, Anna Carolina Franco; FALTAY, Paulo. Economia psíquica dos algoritmos e laboratório de plataforma: mercado, ciência e modulação do comportamento. Revista FAMECOS, [s. l.], v. 26, n. 3, p. 33095, 2019.

por exemplo, ferramenta de cadastro e acompanhamento da distribuição de renda[212], aplicativo para monitoramento de infectados e suspeitos[213], informações gerais[214] e até autoavaliação[215]. Esses apps já contabilizam mais de 1 milhão de downloads.

Essas ferramentas – versões simplificadas do mecanismo chinês de vigilância e controle da população[216] durante a pandemia – permitem que se insira na sociedade uma política de controle e vigilância ativa do Estado. A iniciativa privada também atua fornecendo dados geolocalizados para auxiliar o Estado a entender o fluxo e aglomerações de pessoas[217]. Exemplos como esse são vistos em discursos das smart cities, em que o setor privado atua junto ao Estado, a fim de viabilizar meios de interferir na organização e gerenciamento das cidades. Essas iniciativas vão além da organização da cidade, visando o bem-estar social mas, acima de tudo, o lucro. É através deste que o usuário deixa de ser apenas usuário e passa a ser fonte de dados e de lucro para as empresas parceiras.

Ora, ali encontramos alguns pontos interessantes para serem observados. A porteira da vigilância escancarada do Estado foi aberta. O uso da tecnologia das empresas de telefonia, junto ao Estado, fornecerá uma gama de dados que, se analisados em conjunto com uma série de informações já existentes, possibilitam realizar a engenharia

212 CAIXA | Auxílio Emergencial. Disponível em: <https://play.google.com/store/apps/details?id=br.gov.caixa.auxilio > Acesso em 08 de abril de 2020.
213 Coronavírus Ceará. Disponível em: <https://play.google.com/store/apps/details?id=com.saude.ceara.gov.ce.br.corona_app>. Acesso em 08 de abril de 2020.
214 Coronavírus – SUS. Disponível em: <https://play.google.com/store/apps/details?id=br.gov.datasus.guardioes>. Acesso em 08 de abril de 2020.
215 Coronavírus SP. Disponível em: <https://play.google.com/store/apps/details?id=br.gov.sp.prodesp.coronavirussp>. Acesso em 08 de abril de 2020.

216 In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. Disponível em: <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>. Acesso em 08 de abril de 2020.
217 CNN - Governo diz que vai usar dados de celulares para monitorar aglomerações. Disponível em:

reversa e identificar um indivíduo, como explica Bioni[218]. A tecnologia de comunicação móvel possui caráter de utilização individual. São raras as vezes que uma pessoa compartilha o seu aparelho e, como menciona Yeregui[219] o dispositivo é potencialmente móvel; quem dá o sentido de locomoção é o ser humano.

A diversidade de aplicativos cedidos por cada Estado ou cidade exigem que os cidadão forneçam informações para utilizá-los. O aplicativo Coronavírus Ceará, por exemplo, possui campos de CPF ou RG. Esses dados, por si só, possibilitam vincular uma pessoa a um dispositivo que, por sua vez, poderá manter a situação de vigilância por tempo indeterminado, mesmo que o usuário troque de aparelho. O destino dessas informações não é claro, visto que não há nenhuma explicação sobre a forma que os dados serão utilizados pelos desenvolvedores e proprietários.

Se não bastasse a entrada massiva de dados do cidadão, voluntária ou involuntariamente, há outro agravante para essa situação: a forma como o governo lida com os nossos dados. Há históricos preocupantes que mostram a ineficiência dos gestores de dados públicos em mantê-los em segurança, zelar pela boa utilização ou, simplesmente, por privatizar órgãos públicos que possuem dados sensíveis. Trago alguns exemplos.

A atitude do então prefeito de São Paulo João Dória em ofertar ao capital estrangeiro os dados de usuários de transporte público em 2017 causou repercussão na mídia e a proposta logo foi barrada[220]. A transação não foi efetivada, mas o alerta foi dado: o Estado possui essas informações, pois oferece serviços públicos ao cidadão e,

218 BIONI, Bruno Ricardo. Proteção de dados pessoais, 2019.
219 YEREGUI, Mariela. Móveis em movimento: corpo e território na cena pós-midiática. In: Nomadismos tecnológicos. [s.l: s.n.]. p. 278.
220 Folha de São Paulo - Lei de Dados barra planos da Prefeitura de vender informações do Bilhete Único. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/07/lei-de-dados-barra-planos-da-prefeitura-de-vender-informacoes-do-bilhete-unico.shtml>. Acesso em 10 de abril de 2020.

claramente, pretendia oferecer à iniciativa privada, a fim de remunerar essa massa de dados em capital. A lógica do Estado empreendedor, da autora Mariana Mazzucatto[221], nos leva a perceber como os governos se aliam às empresas privadas com o objetivo de financiar pesquisas, oferecer insumos – os dados – para o desenvolvimento de produtos e soluções. Somado à tentativa do ex-governador de São Paulo Márcio França, em 2017, de também fornecer os dados de mais de 30 milhões de contribuintes, e do episódio da disponibilização de dados sensíveis de IPTU pelo então prefeito Fernando Haddad, em 2015, mostram como o databroker mor dos dados do cidadão – destino de todos os dados resultantes da utilização de serviços públicos e transações com o governo – é incapaz de respeitar sua responsabilidade sobre as informações que possui e carrega consigo, permitindo que informações sejam expostas ou oferecidas a terceiros.

CIDADÃOS E CONSEQUÊNCIAS

A situação, num primeiro olhar, parece igual para todos, afinal, o governo atua coletando os dados de todos os cidadãos, sejam brancos, negros, ricos ou pobres. Bem, não é por aí. Como Felitti[222] pressupõe, são os mais pobres que utilizam os serviços do Estado e, como consequência, fornecem mais dados a ele. Assim, quanto mais dependem de programas de assistência, como SUS, auxílio desemprego, bolsa família e até mesmo o programa de remuneração do Covid-19, mais suscetíveis às falhas eles estarão.

A maneira como o Estado utiliza os dados coletados durante a pandemia e também os já armazenados tende a impactar de forma distinta as populações, de acordo com a faixa de renda. Conforme Eubanks[223] retrata em seu livro **Automating Inequality:**

221 MARZUCATTO, Mariana. O Estado empreendedor. 1ª ed., 2014.
222 FELITTI, Guilherme. O governo deveria proteger seus dados, mas é excelente em expô-los. 2019. Disponível em: <https://manualdousuario.net/podcast/tecnocracia-24>. Acesso em 10 de abril de 2020.
223 EUBANKS, Virginia. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: St Martin's Press, 2018.

How High-Tech Tools Profile, Police, and Punish the Poor, os mais pobres tendem a sofrer mais com o que os designers entrevistados chamam de "triagem". Nesse processo, baseado em dados já inseridos e algoritmos de IA treinados – com os olhos voltados para episódios que já ocorreram, ou seja, para o passado – tende a replicar, ou pior, potencializar os efeitos de racismo, desigualdade social e exclusão. A autora, em entrevista para o site Digilabour[224], refere-se aos sistemas informatizados em ações sociais da seguinte maneira: "nós vemos que essas ferramentas são muito mais casos de evolução do que de revolução". A afirmação de Eubanks reforça que os efeitos diretos de uma automação e os processos de atendimento à população tendem a potencializar todo um histórico de segregação entre ricos e pobres, brancos e negros, aumentando, assim, o abismo socioeconômico.

Outro ponto é um cenário do livro 1984, de George Orwell. A situação mencionada no romance é de guerra. Esse mesmo termo, guerra, é utilizado para nos referirmos à batalha contra a pandemia. Por outro lado, a tecnologia de vigilância passa quase imperceptível pela população. Além disso, a possibilidade de utilizar algoritmos para moldar e controlar a vida das pessoas não será aquela em que andaremos por várias filas e teremos a ciência de que estamos sendo levados para algum lugar por uma força maior. Na verdade, será cada um seguindo seu fluxo, individualmente, e "seguindo os seus próprios desejos" – que foram estimulados por algoritmos. O Estado poderá punir ou beneficiar cada cidadão por meio de decisões que códigos exibem.

O cenário de uma vigilância estatal automatizada e que puna seus cidadãos não é impossível e nem está longe de ser concretizada. Desde o dia 1º de abril de 2020, o

224 Digilabour - Automatizando as Desigualdades: entrevista com Virginia Eubanks. Disponível em: <https://digilabour.com.br/2019/09/01/eubanks-automatizando-as-desigualdades>. Acesso em 11 de abril de 2020.

governador de São Paulo, João Dória, possui acesso ao deslocamento massivo dos cidadãos e pretende aplicar multa[225] para quem desrespeitar o isolamento. O governo tem o objetivo de obter 70% do isolamento social e, caso isso não ocorra, o Dória afirmou que poderá multar e até prender quem desrespeitar a medida.

Em paralelo, a Google e a Apple fecharam uma parceria para possibilitar o "desenvolvendo uma solução que usa o Bluetooth do celular para rastreamento de contato[226]". Ainda segundo a reportagem, a tecnologia será disponibilizada via API para aplicativos de autoridades de saúde pública. O grande salto e principal diferença entre a iniciativa das desenvolvedoras e das telefonias é a precisão. Com Bluetooth, é possível analisar a aproximação com precisão de 1 a 20 metros, podendo alertar também se o indivíduo teve proximidade com um infectado.

Há também o perigo iminente de um laboratório de plataforma, nos termos de Bruno, Bentes e Faltay[227]. A massa de dados que alimenta as bases do Governo permite que este crie movimentos que estimulem a população à determinados objetivos sem que os cidadãos tenham ciência. Da mesma forma que algoritmos e o modelo Big Five foram aplicados para criar discursos direcionados e influenciar as eleições norte-americanas, não há nada que impeça de que estes sejam aplicados com o fim de alterar a opinião pública por meio de discursos "feitos sob medida" para cada tipo de personalidade. Como cada indivíduo possui uma experiência única ao consultar um site de rede

225 Carta Capital - Doria cogita aplicar multa e prisão para quem desrespeitar isolamento. Disponível em: <https://www.cartacapital.com.br/saude/doria-cogita-aplicar-multa-e-prisao-para-quem-desrespeitar-isolamento/>. Acesso em: 11 de abril de 2020.
226 Tecmundo - Apple e Google se unem para criar tecnologia de combate ao coronavírus. Disponível em: https://www.techtudo.com.br/noticias/2020/04/apple-e-google-se-unem-evitar-propagacao-do-covid-19-com-nova-tecnologia.ghtml. Acesso em 11 de abril de 2020.

social, por exemplo, o discurso exibido pode moldar individualmente a opinião. No entanto, aplicando este procedimento massivamente, uma quantidade enorme de pessoas pode ter seu humor, relações sociais e até mesmo suas opiniões afetadas acerca de temas de interesse público, causando efeitos em larga escala.

A situação não é nova à nível global, dado o exemplo da China, que lida com seus cidadãos monitorando-os cotidianamente. O que se espera do Brasil – e se torna perigoso – é a força que o Estado ganha com esses artefatos vigilantes, somados a um passado de ditadura militar severa, ineficiência do Estado em proteger as informações do seu cidadão – relacionado ao dever de não fornecer para terceiros e manter a segurança nacional – e, principalmente, o descaso que o país tem com a população negra que há anos é marginalizada e excluída. Com o algoritmo e a automação, se for diferente, acontecerá uma intensificação dessas desigualdades com uma fachada de "objetividade" e "neutralidade". Com tecnologias móveis, aplicativos criados para a pandemia e união do Estado com a iniciativa privada, a tendência é que o monitoramento sistemático fique mais eficiente, o poder siga concentrado nos detentores dos meios de vigilância, dos algoritmos e poder intelectual para desenvolver tais aplicações, deixando a população à mercê das decisões políticas envolvidas na construção e circulação de algoritmos.

"QUIS CUSTODIET IPSOS CUSTODIES?": A NATURALIZAÇÃO DA VIGILÂNCIA EM MASSA EM TEMPOS DE EMERGÊNCIA

Raphael Marques de Barros

É certo que, em períodos de turbulência social, nos quais a segurança percebida pelas pessoas se encontra ameaçada, há uma maior flexibilidade legislativa para conter tal turbulência. Em emergências, com a esperança e o medo guiando muitas decisões, às vezes com nobres intenções, passam a vigorar leis abusivas cujas consequências, por

vezes dificilmente previstas, se alastram por muito depois da crise que as originou. Em geral, comunidades tendem a buscar maneiras de limitar a direitos e liberdades individuais que possam de algum modo embaçar o combate a um mal coletivo.

Este debate sobre a sobreposição de um suposto interesse coletivo certamente não é nada novo. Escrevendo em 1979, Michel Foucault ao detalhar essa sobreposição disciplinaria em contenções de epidemias no século XVI afirmava o seguinte:

> *"It [the plague] lays down for each individual his place, his body, his disease and his death, his well-being, by means of na aracterizes and aracterize power that subdivides itself in a regular, uninterrupted way even to the ultimate determination of the individual, of what aracterizes him, of what belongs to him, of what happens to him."*[228]

Em 1890, quando Louis Brandeis e Samuel Warren escreveram um dos artigos fundadores da nossa presente concepção sobre o Direito à Privacidade[229], um outro cenário sobre os perniciosos efeitos da invasão à vida íntima se apresentava. À época, eles escreviam sobre as recém-inventadas máquinas fotográficas e como a sua utilização por tabloides explorava e limitava o pleno desenvolvimento pessoal.

O que é relativamente novo, entretanto, são as limitações e cerceamentos realizados ao direito à privacidade e ao direito à proteção de dados por meio da vigilância eletrônica. Em 2001, com o atentado terrorista às Torres Gêmeas e a intenção de combater essa "ameaça invisível", o governo dos Estados Unidos promulgou diversas peças legislativas (PATRIOT Act, Presidential Surveillance Program, e diversos outros), que permitiam, dentre outras coisas, a espionagem de cidadãos americanos sem expedição de

228 FOUCAULT, Michel. Discipline and Punish: The Birth of the Prison. Vintage Books, 2nd ed. 1979, pp. 197.
229 BRANDEIS, Louis D., WARREN, Samuel D. The Right to Privacy. Harvard Law Review, v. 4, nº 5. Dez. 1890. pp. 193-220. Disponível em <http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C>.

qualquer mandado ou atribuição de responsabilidade para as autoridades[230]. Famosa é a secreta sala 641A.[231]

Atualmente, com a emergência causada pela pandemia de infecção humana pelo vírus SARS-Cov-2, presenciamos reflexos jurídicos que naturalmente seguem nos largos passos da flexibilidade legislativa permitida por emergências, que aceleram processos sociais em nome do seu combate. O Congresso Nacional aprovou a Lei 13.979/2020, cujo artigo 6º dispõe sobre a utilização por autoridades da saúde de quaisquer dados essenciais para a identificação de casos confirmados ou até suspeitos. A Câmara dos Deputados recentemente postergou a vigência da Lei Geral de Proteção de Dados para 2021 dada a necessidade de monitoramento[232]. O parlamento húngaro permitiu ao presidente Viktor Órban governar por decreto porquanto durar a epidemia[233]. O governo sul-coreano passou a utilizar dados de telefonia móvel para monitorar o espalhamento da epidemia[234] e o governo russo requer autorização digital por meio de QR codes para sair às ruas[235].

Essas erosões ao direito à privacidade devidas à nova pandemia certamente não vem somente de governos e de seus interesses políticos, mas também de empresas e

---

230 ESTADOS UNIDOS. Public Law 107-26, 2001. 107th Congress. Washington, D.C., Sec. 213, pp. 285-286. Disponível em: <https://www.congress.gov/bill/107th-congress/house-bill/3162/text>.

231 Em síntese, Room 641A era uma sala operada pela agência de telecomunicações AT&T em uma de suas sedes a serviço do governo americano para captar dados telefônicos e de internet por meio de acesso ao backbone de transmissão de dados tanto domésticos quanto internacionais. Para mais detalhes, ver <https://en.wikipedia.org/wiki/Room_641A>.

Luciana Marinelli. Governo adia para maio de 2021 vigência da Lei Geral de Proteção de Dados. Valor Econômico, São Paulo, 29 abr. 2020. Disponível em: <https://valor.globo.com/empresas/noticia/2020/04/29/governo-adia-para-maio-de-2021-vigncia-da-lei-geral-de-proteo-de-dados.ghtml>.

233 PICHETA, Rob. HALASZ Stephanie. Hungarian parliament votes to let Viktor Orban rule by decree in wake of coronavirus pandemic. CNN. 30 mar. 2020. Disponível em: <https://edition.cnn.com/2020/03/30/europe/hungary-viktor-orban-powers-vote-intl/index.html>.

234 KASULIS, Kelly. S Korea's smartphone apps tracking coronavirus won't stop buzzing. Al Jazeera. 8 abr. 2020. Disponível em: <https://www.aljazeera.com/news/2020/04/korea-smartphone-apps-tracking-coronavirus-won-stop-buzzing-200408074008185.html>.

235 ILYUSHINA, Mary. Moscow rolls out digital tracking to enforce lockdown. Critics dub it a 'cyber Gulag'. CNN. 14 abr. 2020. Disponível em: <https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html>.

de seus interesses econômicos (que muitas vezes se misturam). O Google recentemente criou uma ferramenta chamada Relatórios de Mobilidade Comunitária, para verificar a eficácia de medidas de confinamento e quarentena[236]. Além de mostrar se as pessoas estão ficando em casa ou não, a ferramenta também mostra fluxos de transporte e de estabelecimentos comerciais. Não é preciso ir muito fundo para perceber os incentivos econômicos deste tipo de vigilância.

Telefones agora servem de tornozeleiras eletrônicas, informando às autoridades quem vai aonde, quem fala com quem, o que é, no mínimo, razão para encará-los com preocupação.

Essas erosões, entretanto, há tempos são de conhecimento público. As revelações de Edward Snowden a respeito da vigilância realizada pela Agência Nacional de Segurança em 2013, a utilização de dados de usuários do Facebook para análises políticas de campanha na eleições americanas de 2016 sem o seu consentimento[237], as escutas realizadas pela Amazon e pelo Google em aparelhos de smartphones (é possível baixar esses dados coletados e se arrepiar)[238]. Nada disso é novidade, mas está se tornando o novo normal e as consequências disso para as nossas liberdades e para o mundo democrático são patentes – transmissão de fake news por autoridades políticas, manipulação de dados em campanhas e votações dentre inúmeras outras que ainda não somos capazes de perceber.

---

236 CONCEIÇÃO, Ana. Google cria ferramenta para checar isolamento social. Valor Econômico. São Paulo. 06 abr. 2020. Disponível em: <https://valor.globo.com/brasil/noticia/2020/04/06/google-cria-ferramenta-para-checar-isolamento-social.ghtml>.
237 O escândalo de utilização de dados de milhões de usuários da rede social pela empresa Cambridge Analytica foi descoberto em 2018, anos após as invasões à privacidade já terem seus efeitos consolidados. Para mais informações, ver <https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal>.
238 CRIST, Ry. Amazon and Google are listening to your voice recordings. Here's what we know about that. CNET. 13 jul. 2019. Disponível em: <https://www.cnet.com/how-to/amazon-and-google-are-listening-to-your-voice-recordings-heres-what-we-know/>.

Numa escala pandêmica, em que centenas de milhares de pessoas se encontram contaminadas em uma dada localidade, monitoramentos muito generalizados, abstratos, falham em perceber as nuances humanas da contaminação. Dessa forma, qualquer monitoramento que se leve a sério em observar os fluxos de contágio acaba por vigiar de maneira tão profunda esses fluxos que qualquer tentativa de anonimizar os dados coletados cai por terra. Os sets de dados criados com esse monitoramento em uma escala sem precedentes (e com uma candidez também sem precedentes, dada a facilidade de instituições em afirmar sua vigilância) são inimagináveis e, logicamente, a justificativa é a de monitorar o contato de pessoas infectadas mas é certamente de se questionar se essa coleta de informação se limitará à pandemia (não se limitará). Um estudo publicado pela revista Nature concluiu que apenas 15 atributos demográficos são necessários para identificar 99.98% da população americana em qualquer set de dados, explicitando a dificuldade de uma anonimidade verdadeira vinda destas coletas de dados.[239]

É até de se estranhar a falta de comparações de governos e empresas ao Grande Irmão nessa pandemia, especialmente em tempos de Big Brother. A capacidade de saber como e com quem as pessoas se reúnem facilmente permite inferir consequências políticas para esses conjuntos de dados coletados na pandemia. Afinal, que facilidade maior existe para manipular alguém quando o conhece melhor do que ele mesmo, sabe como pensa no íntimo de sua casa e o que procura saber "quando ninguém mais está olhando"?

239 ROCHER, Luc, HENDRICKX, Julien M., DE MONTJOYE, Yves-Alexandre. Estimating the success of re-identifications in incomplete datasets using generative models. Nature Communications, v. 10, n. 3069. Jul 2019. Disponível em: <https://www.nature.com/articles/s41467-019-10933-3>.

Existe sim o risco dessa vigilância em massa se tornar algo constante, como as tendências recentes vem apontando. A justificativa de que a vigilância pela qual passamos agora irá se extinguir com o fim da pandemia exige certa ingenuidade para ser crível. Estes conjuntos de dados e sistemas de vigilância certamente não serão descartados com o passar do tempo, mas sim aperfeiçoados e colocados a disposição de outras entidades para outros fins, os quais hoje ainda não conseguimos ver. Ainda que se possa, por um instante, crer que esses dados não serão hoje ou amanhã utilizados para fins nefastos pelas pessoas em quem "confiamos", é impossível ter certeza de que nunca serão por terceiros desconhecidos.

O problema cerne é a mudança paradigmática que estas decisões emergenciais tomadas hoje acarretam. Seu estabelecimento cria um novo "normal", em que os cerceamentos abusivos ao direito à privacidade e à proteção de dados pessoais se tornam as novas fronteiras naturais destes direitos. Já hoje entende-se como o novo normal, apesar de incômodo para alguns, o monitoramento constante de informações pessoais por meio de celulares para a "personalização de anúncios" e "melhora de serviços".

Devemos, é claro, combater a pandemia da maneira mais responsável possível, respeitando regras instituídas por autoridades sanitárias para a mais ágil e mais segura resolução, limitando perdas desnecessárias. Obviamente, isso significa alguma perda momentânea de liberdade (especialmente ao ficarmos em quarentena).

Isso não significa que devemos permitir, entretanto, que medidas invasivas de vigilância com eficácia e consequências questionáveis arrisquem danos permanentes à sociedade e à democracia. Isso, pois, quando este começo da epidemia tiver passado e se tornar uma memória distante, a conjuntura estabelecida por estas decisões será na-

turalizada e questionamentos a elas serão questionamentos contra a suposta necessidade coletiva. Por isso, é necessário ter em mente que essas decisões que tomamos hoje terão profundos impactos e que essa crise e esse inimigo invisível têm um fim que a maioria de nós em alguns anos presenciaremos, não podendo nós arriscarmos nossas liberdades e processos democráticos no seu combate. A nossa privacidade é um dos fundamentos dessas liberdades, é o potencial de realização plena do indivíduo com a segurança de não ser indevidamente julgado ou molestado pelos seus pares ou pelo Estado, é uma das pedras fundamentais do erodido conceito da democracia moderna, é um direito individual de efeitos coletivos.

Não devemos deixar que o nosso medo desse combate nos leve a decisões das quais nos arrependeremos no futuro. Tampouco devemos deixar que interesses políticos e econômicos tomem estas decisões em nosso lugar e ameacem nossas liberdades civis. Discursando em 1961 sobre essa perigosa combinação de interesses, o então presidente dos Estados Unidos e ex-Comandante Supremo das forças aliadas na Segunda Guerra, Dwight Eisenhower afirmou:

> *"The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted."*[240]

Em tempos de quarentena, em que o contato humano e a transmissão de informações se dá principalmente por meios digitais, quando quase se pode afirmar a fundamentalidade do direito de acesso à internet, é necessária a vigilância contra a vigilância. Para evitarmos a naturalização destes abusos contra a nossa privacidade e obtermos o

240 EISENHOWER, Dwight D. Farewell Speech. Library of Congress. Washington D.C. 1961 Disponível em: <https://www.eisenhowerlibrary.gov/sites/default/files/file/farewell_address.pdf>.

controle sob a utilização de nossos dados, precisamos estar sempre alertas acerca das graves consequências escondidas por debaixo de nobres intenções.

Precisamos de agentes independentes que monitorem e reportem estes abusos de maneira objetiva e de leis que assegurem nossos direitos fundamentais. O trabalho de *watchdogs* da sociedade civil – vigias e organizações independentes de monitoramento de abusos – e de legislações fortes e contundentes que limite os poderes de coleta de dados e de vigilância e os torne transparentes e responsáveis perante aqueles que são vigiados se mostra precioso mais uma vez.

SAÚDE E PROTEÇÃO DE DADOS – FUNDAMENTOS DA VIGILÂNCIA EPIDEMIOLÓGICA SOCIAL

Marco Aurélio Fernandes Garcia[241]

É de tal forma inegável a importância de um regime jurídico sólido para proteção de dados na sociedade moderna que, em uma Lei emergencial e enxuta para combater a recente pandemia de Covid-19[242], vislumbrou-se a necessidade de dedicar uma disposição que regulasse a transferência de dados pessoais entre as entidades da Administração Pública e entre entes privados e a Administração Pública, quando solicitados pela última.

241 Mestrando em Direito Internacional pela Faculdade de Direito da Universidade de São Paulo. Mestrando em Direito Europeu pela Université du Luxembourg. Especialista em Direito Empresarial pela Escola de Direito da Fundação Getulio Vargas. Bacharel em Direito pela Faculdade de Direito da Universidade de São Paulo. Advogado em São Paulo.

242 BRASIL. Lei n. 13.979, de 6 de fevereiro de 2020. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L13979.htm>, acessado em 02/04/2020.

Ocorre que, ao invés do Artigo 6º da nova Lei nº 13.979/2020 regular a transferência de dados sob bases jurídicas sólidas, ele caminha na direção oposta e torna *obrigatório* o compartilhamento de dados essenciais à identificação das pessoas suspeitas ou infectadas com Covid-19.

Neste breve ensaio, discutiremos pontos selecionados acerca da intersecção entre as medidas públicas de contenção da Covid-19 e o regime jurídico brasileiro de proteção de dados. Em primeiro lugar, traçaremos considerações sobre privacidade e saúde. Em segundo lugar, abordaremos brevemente o regime brasileiro de notificação de patologias. Por fim, discutiremos a abrangência do Artigo 6º, da Lei 13.979/2020 e a transferência compulsória de dados de pacientes em um estado de vigilância epidemiológica e social.

SAÚDE E PRIVACIDADE

A proteção da saúde é um tema de destacada importância nos regimes jurídicos de proteção de dados. Em particular, a definição de dados pessoais sensíveis e de categorias especiais de dados na Lei Geral de Proteção de Dados ("LGPD")[243] e o Regulamento Europeu sobre a Proteção de Dados[244], em seus artigos 5º, II, e 9º, 1, respectivamente, engloba a abrangente categoria de "dados relativos à saúde". Não causa surpresa que assim seja, porquanto a saúde do indivíduo é um tema umbilicalmente ligado à sua privacidade e dignidade.

243 BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>, acessado em 02/04/2020.
244 UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679>, acessado em 02/04/2020.

O principal documento que congrega dados relativos à saúde do indivíduo é o prontuário médico, que congrega obrigatoriamente a identificação do paciente, anamnese e evolução diária do paciente[245]. Não é incomum que este documento contenha uma pletora de informações sensíveis sobre o paciente e família e que o ele permaneça fisicamente em lugares de acesso ao público que frequentava os andares de internação do hospital, por exemplo, com acesso por todos profissionais médicos, enfermeiros, assistentes e familiares de outros pacientes[246]. Além disso, também não é raro que médicos enviem documentos e exames entre si por meio de aplicativos e dispositivos eletrônicos.

Estas práticas reprováveis persistem pelo simples fato que a Medicina não coloca, e não deve colocar, a privacidade do paciente antes da sua cura. A primeira disposição do Código de Ética Médica define a Medicina como uma profissão a serviço do ser humano[247]. A saúde é direito de todos (e dever do Estado)[248] porque está ligada à própria condição humana. Não obstante, o mesmo Juramento Hipocrático que determinada a preservação da saúde do paciente de tal forma que nunca seja causado mal a alguém prevê que o médico não deve divulgar o que tenha visto ou ouvido, mantendo-o inteiramente secreto. Apesar de passar despercebido em algumas circunstâncias, a privaci-

245 CONSELHO FEDERAL DE MEDICINA. Resolução 1.638, de 9 de agosto de 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm>, acessado em 02/04/2020.

246 Por diversas razões técnicas e administrativas, como a digitalização de documentos e práticas médicas, os prontuários ainda são, via de regra, físicos. A digitalização dos prontuários é tema ainda recente e regido pela Lei nº 13.783/2018, que determina, inter alia, o uso de certificado digital e regras sobre armazenamento de prontuário (no mínimo 20 anos).

247 CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.931, 17 de setembro de 2009. Código de Ética Médica. Disponível em: <https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf>, acessado em 02/04/2020.

248 BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm>, acessado em 02/04/2020. Artigo 196.

dade e confidencialidade também são fundamentais na Medicina. Compreender privacidade na Medicina passa, então, a ser uma questão de como integrar preocupações de privacidade na atividade médica

NOTIFICAÇÃO COMPULSÓRIA DE COVID-19

A administração da saúde exige que eventos de saúde pública, doenças e agravos sejam reportados para as autoridades da Administração Pública, sob a égide do Sistema Nacional de Vigilância em Saúde[249]. Trata-se de medida voltada à elaboração de políticas públicas que demanda esforço dos profissionais da saúde para que moléstias graves ou contagiosas, assim como incidentes de agressão doméstica, venham ao conhecimento da Administração Pública. A lista não é particularmente extensa e possui 49 entradas com prazos diferenciados de notificação (24 horas e semanal) e para autoridades distintas (Ministério da Saúde, Secretaria Estadual da Saúde e Secretaria Municipal da Saúde).

Naturalmente, os casos identificados ou suspeitos de Covid-19 são de notificação compulsória no Sistema de Informação de Agravos de Notificação[250]. Em particular, a notificação de Covid-19 deve ocorrer em menos de 24 horas e ser direcionada também à Secretaria Estadual de Saúde e à Secretaria Municipal de Saúde.

249 O regulamento das moléstias de notificação compulsória, eventos de saúde pública e agravos se encontra no Anexo V do Anexo I da Portaria de Consolidação do Ministério da Saúde nº 4, de 28 de setembro de 2017. Eventos de saúde pública são definidos como a "situação que pode constituir potencial ameaça à saúde pública, como a ocorrência de surto ou epidemia", doenças são classificadas como "enfermidade ou estado clínico", ao passo que agravo é "qualquer dano à integridade física ou mental do indivíduo, provocado por circunstâncias nocivas, tais como acidentes, intoxicações por substâncias químicas, abuso de drogas ou lesões decorrentes de violências interpessoais".

250 O item 43 ("Síndrome Respiratória Aguda Grave associada a Coronavírus. SARS-CoVb. MERS-CoV) está presente na lista de doenças de notificação compulsória ao menos desde 17 de fevereiro de 2020. MINISTÉRIO DA SAÚDE. Portaria nº 264, 17 de fevereiro de 2020. Altera a Portaria de Consolidação nº 4/GM/MS, de 28 de setembro de 2017, para incluir a doença de Chagas crônica, na Lista Nacional de Notificação Compulsória de doenças, agravos e eventos de saúde pública nos serviços de saúde públicos e privados em todo o território nacional. Disponível em: <http://www.in.gov.br/en/web/dou/-/portaria-n-264-de-17-de-fevereiro-de-2020-244043656>, acessado em 02/04/2020.

A notificação não visa identificar o paciente, mas apenas informar a ocorrência da moléstia em determinada unidade hospitalar. A ficha de notificação[251] contém entradas numéricas para o total de casos suspeitos e confirmados, o local de ocorrência do evento e os dados do notificador. Orienta-se sejam adicionadas informações sobre o paciente, tais como a nacionalidade, se é viajante, contatos e aspectos clínicos, assim como dados pessoais, tais como nome, sexo, data de nascimento, idade, nome da mãe, telefone e domicílio[252].

A pessoalidade do dado é dirigida pela identificabilidade de uma pessoa natural, de tal forma que o dado de titular não identificável é considerado dado anonimizado[253]; o dado, por si só, é "fato bruto"[254]. O propósito da transmissão destes dados às autoridades públicas é evidentemente relacionado à necessidade de instituição de políticas públicas, direcionamento de leitos e fármacos, utilização de orçamento, entre outros. Embora a confirmação ou suspeita de Covid-19 seja um dado referente à saúde, se não for possível conectar esta informação a uma pessoa natural identificável, os dados deverão ser considerados meramente estatísticos e para fins de execução de políticas públicas.

Entretanto, diante da transmissão de dados pessoais, esta situação é um pouco mais nuançada. A qualificação pessoal é necessária para certificar a veracidade das informações fornecidas, porquanto é possível cruzar estes dados com os dados mantidos

251 Minuta disponível em: <http://formsus.datasus.gov.br/site/formulario.php?id_aplicacao=6742>, acessado em 02 de abril de 2020.
252 Cf. formulário disponível em: <http://cveantigo.saude.sp.gov.br/sistemas/central/not_ind.asp>, acessado em 02/04/2020.
253 Artigo 5º, I e II, III, da Lei Geral de Proteção de Dados.
254 BIONI, Bruno. Proteção de dados pessoais – A função e os limites do consentimento. São Paulo: Forense, 2019. p. 36.

pelos hospitais em prontuário para determinar a existência ou não da moléstia. O endereço do paciente, por exemplo, pode servir para identificar a origem dos casos, assim como para estabelecer bloqueios locais em casos de epidemia.

Salvo quando notificado, apenas os centros hospitalares (e assimilados) possuem acesso simultâneo à patologia e à qualificação completa do paciente, inscritas em prontuário. Prontuários são documentos que já foram de guarda permanente pelo hospital, sendo atualmente necessária sua manutenção pelo prazo mínimo de 20 anos[255]. O centro de interesses natural em relação à proteção da privacidade referente a Covid-19 certamente se encontra no hospital, que é um controlador quase permanente de uma infinidade de dados pessoais sensíveis dos pacientes. Contudo, após a notificação compulsória, as autoridades públicas passam a controlar dados pessoais (qualificação completa) e pessoais sensíveis (suspeita ou confirmação de patologia) dos pacientes.

A AMBÍGUA ESCRITA DO ARTIGO 6º DA LEI Nº 13.979/2020

Se os dados pessoais e pessoais sensíveis referentes aos casos suspeitos ou confirmados de Covid-19 são comunicados às autoridades públicas de forma compulsória, quais seriam as preocupações com relação ao sistema de comunicação obrigatória previsto no Artigo 6º, *caput*, da Lei nº 13.979/2020?

Em primeiro lugar, o *caput* do Artigo 6º comete uma gafe preocupante ao se referir aos "dados essenciais à identificação de pessoas infectadas". Isto porque a identificabilidade, conforme asseverado, é o critério fundamental para a determinação da pessoalidade dos dados. Passa-se a impressão de que se deseja identificar o paciente e não colher estatísticas sobre a doença. Quando a Lei afirma tratar de dados essenciais à

255 CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.821, de 23 de novembro de 2007. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2007/1821_2007.pdf>, acessado em 02/04/2020.

identificação, sendo que os dados necessários para o propósito definido (prevenção do Covid-19) são majoritariamente dados anonimizados, duas hipóteses podem ser levantadas: trata-se de uma imprecisão jurídica ou uma ambiguidade proposital. Vejamos.

A nova Lei nº 13.979/2020 certamente não foi redigida por especialistas em proteção de dados pessoais. Neste sentido, não seria anormal verificar que a Lei falharia ao se referir à identificabilidade de dados anonimizados. É igualmente possível que a interpretação pretendida pelo redator da Lei fosse que a identificação se referisse à contagem de casos suspeitos ou confirmados, mas não ao nome, CPF e endereço dos indivíduos. Isto porque o texto aprovado é ambíguo em relação a este ponto, já que pode tanto significar os dados essenciais *à identificação da pessoa,* quanto dados essenciais *à identificação do contágio em uma região*.

Esta ambiguidade pode também não ser o resultado de uma atecnia, mas sim de uma intenção em deixar o texto aberto para que seja possível tanto identificar o *contágio*, quanto para qualificar o *indivíduo contagiado*. Se a Lei pretende, de fato, seja feita a identificação do indivíduo contagiado, a obrigação de entidades públicas e privadas de comunicar obrigatoriamente (Artigo 6º, §1º) certamente levanta preocupações de vigilância social mais profundas, tendo em vista que permitiria às autoridades públicas colherem dados pessoais e pessoais sensíveis de virtualmente toda a população brasileira por meio de via transversa, na qual não haveria a efetiva possibilidade do titular de dados de exercer os seus direitos e se opor à transferência.

Neste diapasão, a abertura da redação do dispositivo daria vazão para abusos, tendo em vista que as Autoridades Públicas poderiam requisitar sejam informados dados pessoais e sensíveis do indivíduo, já que não está claro se a Lei se refere somente a

dados anonimizados. Não é demais lembrar que hospitais são entidades públicas e privadas no Brasil que controlam dados de vida e morte de indivíduos e o quão pernicioso seria se a Administração Pública tivesse acesso absoluto e sem a ciência do titular dos dados sobre os seus dados pessoais.

Esta ambiguidade não se resolve completamente, já que a Lei não aponta com precisão os dados que seriam transmitidos, embora o §2º do Artigo 6º indique uma possível solução para este ponto, já que ele apresenta dois pontos contextuais fundamentais para sua interpretação. O primeiro ponto se refere ao fato de que o Ministério da Saúde manterá públicos os dados colhidos acerca da contaminação, sendo improvável que dados pessoais sejam tornados públicos, já que o nome e CPF em nada se relacionam e em nada auxiliam o combate ao Covid-19. O segundo ponto é que está previsto que será resguardado o sigilo das informações pessoais.

Isso significaria reconhecer que embora a nova Lei preveja o compartilhamento obrigatório de dados pessoais com as autoridades públicas, estes dados não ultrapassariam aqueles já rotineiramente comunicados no sistema de notificação obrigatória e não devem implicar sejam tornados públicos dados pessoais ou pessoais sensíveis.

VIGILÂNCIA EPIDEMIOLÓGICA E VIGILÂNCIA SOCIAL

Apesar de não encontrarmos pontos fundamentalmente incorretos em relação ao novel Artigo 6º, é necessário reconhecer a falta de controle pelo titular e ausência de remédios jurídicos contra abusos possivelmente praticados pela Administração Pública. Se a compulsoriedade de transmissão de informação não é o ponto central, porquanto já existente neste subsistema específico da saúde, a inexistência de proteção ao titular de dados resta patente.

É fundamental que a vigilância epidemiológica – natural e necessária numa sociedade democrática – não seja fundamento de vigilância social. Não é distópico imaginar um cenário no qual o governo coleta informações extremamente invasivas sob subterfúgios de administração da saúde, mas utiliza os dados para propósitos diversos. À guisa de exemplo, bancos de dados interoperáveis permitiram autoridades policiais encontrarem o endereço de suspeitos com base no domicílio informado por um profissional da saúde em uma doença de notificação compulsória.

O escudo do titular de dados é o regime jurídico de proteção de dados. Em particular, o seu rol de direitos, os remédios jurídicos disponíveis e a atuação incisiva dos órgãos de fiscalização e da autoridade nacional são a sua linha de proteção contra a vigilância abusiva e contra aqueles que obrigam o titular de dados a revelar pontos tão sensíveis relacionados à vida e saúde.

QUAIS OS LIMITES DE ATUAÇÃO DOS GOVERNOS EM TEMPOS DE CORONAVÍRUS E QUAIS OS DEVERES DOS CIDADÃOS VIGILANTES?

Fernando Bottega Pertile[256]

Nesta que é tida como a "maior crise sanitária mundial da nossa época" pela Organização Mundial da Saúde (OMS)[257], tanto autoridades civis quanto especialistas das mais diversas áreas não estão medindo esforços para procurar soluções ou atenuações

256 Bacharel em Direito pela Universidade Federal de Santa Maria.
257 Tradução livre de "This is the defining global health crisis of our time". WORLD HEALTH ORGANIZATION. WHO Director-General's opening remarks at the media briefing on COVID-19 - 16 March 2020. Disponível em: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---16-march-2020. Acesso em: 15 abr. 2020.

às consequências sanitárias e econômicas advindas da pandemia do coronavírus. Além da discussão sobre o *trade-off* de manter quarentenas para diminuir a circulação do vírus, tendo de se arcar com o desastre econômico decorrente da redução de transações econômicas e de circulação de pessoas (discussão que, aliás, também poderia ter acontecido caso o surto tivesse ocorrido há algumas décadas), um tópico bastante atual se coloca como um dos mais importantes nessa luta: o da proteção de dados.

Estima-se que a humanidade gera, por dia, cerca de 2,5 exabytes de dados[258]. Em 2018, um estudo mostrou que mais de 90% dos dados existentes no mundo haviam sido gerados somente nos dois anos anteriores[259]. Isso significa não somente que há uma quantidade gigantesca de informações sobre praticamente todas as pessoas que fazem uso de dispositivos eletrônicos, mas que a cada dia novas ferramentas são criadas para melhor lidar e processar tais dados. Em tempos de crise, é natural esperar que saídas venham de soluções tecnológicas que façam uso desses dados, especialmente porque a utilização de dispositivos eletrônicos para a localização de pessoas com o fim de enfrentar doenças não é algo novo.

Em 2007, a OMS lançou uma iniciativa para eliminar a malária em Zanzibar, na Tanzânia, que utilizava os dados de localização dos celulares nas regiões onde casos da doença eram encontrados[260]. Esse projeto acabou sendo replicado na própria África pra combater outras doenças, como o ebola[261]. Os responsáveis pelo projeto afirmam que

258 MARR, Bernard. How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. Disponível em: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2ea5b1ae60ba. Acesso em: 15 abr. 2020.
259 Ibidem.
260 FILDES, Nic; ESPINOZA, Javier. Tracking coronavirus: big data and the challenge to privacy. Disponível em: https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987. Acesso em: 14 abr. 2020.
261 Ibidem.

"utilizar dados de celulares para entender como doenças e patogênicos fluem pela população é vital"[262].

Assim, com o coronavírus, é natural o surgimento de iniciativas que busquem utilizar dados pessoais, especialmente aqueles gerados pelos celulares, para guiar a construção de políticas públicas. A Coréia do Sul, tida como um dos países que melhor está controlando a disseminação do vírus, realiza um profundo monitoramento da população, especialmente dos infectados e daqueles que entraram em contato[263]. De acordo com as autoridades, o objetivo ao lutar contra o vírus é "criar uma rede abrangente de diagnóstico e de redução da taxa de mortalidade"[264]. Para isso, precisa-se detectar a doença nos estágios iniciais, e então impedir ou atrasar a disseminação do vírus para outras pessoas. Além da testagem em massa, uma das formas mais eficientes encontrada foi a utilização de dados dos smartphones da população.

Na prática, os cidadãos recebem em seus celulares, de acordo com o bairro em que residem, informações sobre a trajetória dos novos diagnosticados pela cidade. "Com a geolocalização dos celulares, mostram por onde cada novo infectado andou, as linhas de metrô que tomou, onde almoçou, por quais ruas transitou até o momento da confirmação da infecção"[265]. Assim, quem passou pelos mesmos locais que algum infectado pode tomar as devidas medidas pra verificar se, de fato, foi contaminado, bem como para evitar novos contágios. Informações de transações de cartão de crédito e

262 Tradução livre de "Understanding how diseases and pathogens flow through populations using mobile phone data is vital". Ibidem.
263 BBC. Coronavírus:o que está por trás do sucesso da Coreia do Sul para salvar vidas em meio à pandemia. https://www.bbc.com/portuguese/internacional-51877262. Acesso em: 14 abr. 2020.
264 Ibidem.
265 MOREIRA, Thiago Mattos. As lições da Coreia do Sul no combate ao coronavírus. Disponível em: https://epoca.globo.com/mundo/as-licoes-da-coreia-do-sul-no-combate-ao-coronavirus-1-24315715. Acesso em: 14 abr. 2020.

geolocalização de smartphones têm apoio legal no país desde o surto de Mers, em 2015[266].

Com uma vigilância tão profunda, inevitável a existência de efeitos colaterais negativos. Mesmo que não haja a exibição dos nomes dos infectados, é possível identificá-los "pela trajetória apresentada, pela idade e pelo gênero"[267]. De acordo com uma pesquisa, mais sul-coreanos temiam "a represália social de terem se contaminado e espalhado o vírus do que os sintomas e consequências da doença"[268]. Países como China, Israel[269] e Singapura adotaram medidas semelhantes de vigilância no combate ao vírus.

Na China, a vigilância ocorre em outro nível - desde antes da pandemia[270]. A movimentação das pessoas é limitada por softwares, que fazem análises e atribuem a cada um dos cidadãos uma cor, a depender da sua relação com o vírus[271]. Os contaminados, ou com grande chance de assim estarem, recebem a cor vermelha; quem teve contato com alguém contaminado também deve ficar em observação, e recebe a cor amarela. Somente os de cor verde podem sair.

Na Europa, tratando-se do continente que conta com a legislação de proteção de dados mais avançada do mundo, o monitoramento não é tão profundo. Assim como em algumas iniciativas no Brasil[272], utiliza-se dados agregados de localização para rastrear a

266 Ibidem.
267 Ibidem.
268 Ibidem.
269 Israel passou a utilizar no rastreamento do coronavírus sistemas de coleta de dados criados para o combate ao terrorismo. TIDY, Joe. Coronavírus leva governo de Israel a se dar 'poderes especiais' de espionagem. Disponível em: https://www.bbc.com/portuguese/geral-51938946. Acesso em: 15 abr. 2020.
270 CAMPBELL, Charlie. How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens. Disponível em: https://time.com/collection/davos-2019/5502592/china-social-credit-score/. Acesso em: 15 abr. 2020.
271 MOZUR, Paul. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 15 abr. 2020.
272 TILT. Quarentena: entenda a polêmica do monitoramento de celular no Brasil. https://www.uol.com.br/tilt/noticias/redacao/2020/04/14/monitoramento-de-celular-perguntas-e-respostas.htm. Acesso em: 15 abr. 2020.

transmissão do vírus e identificar locais que mais precisam de ajuda. Em cidades como Madri e Milão, as "operadoras de telefonia criaram mapas de calor que mostram como as restrições de movimentação estão funcionando e se a presença da polícia nas ruas possui efeito no comportamento [das pessoas]"[273]. Dessa forma, é possível analisar o (des)cumprimento do isolamento social. O rastreamento do avanço da pandemia através de mapas de calor gerados a partir dos dados de múltiplos celulares, sobrepostos com dados médicos, é recomendado por especialistas[274].

De acordo com os responsáveis brasileiros[275] e europeus[276], tais dados são anonimizados. Isso é, não podem ser ligados a nenhuma pessoa específica, o que, em tese, protege os cidadãos de ter eventuais dados de geolocalização utilizados sem seu consentimento. Há de se ter, contudo, certo cuidado em relação aos dados compartilhados, mesmo que anonimizados.

Um estudo feito pela Universidade Católica de Louvain em parceria com o Imperial College de Londres sugere que a anonimização de dados pessoais ainda pode ser revertida, utilizando-se inteligência artificial para re-identificar os indivíduos a quem determinados dados se referem[277]. Na pesquisa, 99,98% das pessoas de bancos de dados anonimizados foram corretamente re-identificadas apenas utilizando-se de quinze características, como data de nascimento, sexo e estado civil. Dessa forma, mesmo ausentes informações como nome e endereço de e-mail, foi possível a identificação do titular. Determinadas informações tidas como anônimas, portanto, podem acabar sendo dados

273 FILDES, Nic; ESPINOZA, Javier. Tracking coronavirus: big data and the challenge to privacy. Disponível em: https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987. Acesso em: 14 abr. 2020.
274 Ibidem.
275 TILT. Op cit.
276 FILDES, Nic; ESPINOZA, Javier. Op cit.
277 ROCHER, Luc; HENDRICKX, Julien; MONTJOYE, Yves-Alexandre de. Estimating the success of re-identifications in incomplete datasets using generative models. Disponível em: https://www.nature.com/articles/s41467-019-10933-3. Acesso em: 15 abr. 2020.

pessoais. Ainda que pareça menos provável a possibilidade de reversão somente com os dados de geolocalização para mapas de calor, é dever da população e dos órgãos de vigilância permanecerem atentos.

Uma segunda forma de monitorar a transmissão do vírus é utilizando-se da tecnologia *bluetooth* dos aparelhos celulares. Sendo essa uma tecnologia de curto alcance, as empresas pretendem utilizá-la para registrar o contato ou a proximidade com outras pessoas. Assim, caso nos dias seguintes alguma das pessoas com quem os celulares trocaram informações foi diagnosticada com o coronavírus, as outras serão informadas[278]. Nesse caso, há necessidade do consentimento do infectado, que voluntariamente envia as suas informações.

Há uma clara distinção entre as medidas adotadas por China, Coreia do Sul e Israel daquelas feitas pelos países ocidentais: nestes, a vigilância preza por uma maior proteção dos dados pessoais. Sendo os Estados Unidos conhecidos como o bastião das liberdades individuais e a Europa tendo a liderança nas legislações protetivas de dados, não poderia ser diferente. No Brasil, a aprovação da Lei Geral de Proteção de Dados (LGPD) há dois anos tem papel fundamental: apesar de ainda não ter entrado em vigor, suas diretrizes norteiam as ações.

As medidas de monitoramento auxiliam no combate ao vírus, mas medidas como teste em massa[279] e cooperação entre as pessoas também são capazes de combater

278 MARQUES, Eduardo. Como funcionará o rastreamento de pessoas com Coronavírus no iOS e no Android. Disponível em: https://macmagazine.uol.com.br/post/2020/04/11/como-funcionara-o-rastreamento-de-pessoas-com-coronavirus-no-ios-e-no-android/. Acesso em: 15 abr. 2020.
279 EXTRA. Coronavírus: ranking aponta Israel, Cingapura e Nova Zelândia como os países mais seguros para se estar durante a pandemia. Disponível em: https://extra.globo.com/noticias/saude-e-ciencia/coronavirus-ranking-aponta-israel-cingapura-nova-zelandia-como-os-paises-mais-seguros-para-se-estar-durante-pandemia-rv1-1-24346109.html. Acesso em: 15 abr. 2020.

eficazmente a proliferação do vírus[280]. Tratando-se de uma situação bastante excepcional, que exige medidas excepcionais para sua contenção, é necessário o equilíbrio entre a busca pela diminuição da propagação do vírus e as liberdades individuais, a fim de que as tentativas de solução tomadas não prejudiquem em demasia os direitos de seus titulares. A luta pelo direito à privacidade e à proteção de dados não pode ser em vão. Há de se ter um equilíbrio entre a saúde pública, o combate à doença, a proteção de dados e a privacidade dos cidadãos. Todos são importantes, e um balanço é necessário.

No contexto europeu, o Comitê Europeu para a Proteção de Dados (European Data Protection Board - EDPB) destacou, em manifestação sobre o uso de dados pessoais no combate ao COVID-19, que o Regulamento Europeu de Proteção de Dados (General Data Protection Regulation - GDPR) permite às autoridades públicas sanitárias o tratamento de dados pessoais em contexto de epidemia sem necessidade de consentimento, contanto que seja feito de acordo com as leis nacionais e dentro das condições estabelecidas no próprio regulamento[281]. No Brasil, a anonimização garante o direito à privacidade e à proteção de dados, dada a incapacidade de ligação ao indivíduo que gerou a informação, ao mesmo tempo em que se teria previsão e controle da movimentação do vírus. Contudo, faz-se necessária atenção por parte dos titulares, uma vez que a ausência da Autoridade Nacional de Proteção de Dados (ANPD) e o possível adiamento da entrada em vigor da LGPD[282] facilitam o uso abusivo de dados.

---

280 HARARI, Yuval Noah. Yuval Noah Harari: the world after coronavirus. Disponível em: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?shareType=nongift. Acesso em: 15 abr. 2020.

281 EUROPEAN DATA PROTECTION BOARD. Statement on the processing of personal data in the context of the COVID-19 outbreak. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en. Acesso em: 15 abr. 2020.

282 Em recente nota, o Ministério Público Federal sustentou a importância de não prorrogar-se o início da entrada em vigor da LGPD, especialmente pelo seu importante papel na garantia e defesa dos direitos individuais. A nota ressalta que a própria lei já prevê situações como a presente pandemia, e dá norte sobre como deve ser o tratamento de dados pessoais. BRASIL. Nota Técnica Conjunta: PFDC & Câmara Criminal, Epidemia covid-19 e PLS(Substitutivo) 1179/20: Manutenção do prazo de entrada em vigor da

É inegável que o medo de estar cada vez mais vigiado não é infundado, especialmente pelo uso posterior que os dados podem ter assim que a crise acabar, bem como quanto à sua real anonimização[283]. É momento de reacender o debate entre liberdade e vigilância. Infelizmente, "medidas temporárias tem o hábito de se tornarem medidas permanentes, até mesmo porque sempre há uma nova emergência no horizonte"[284]. Não é difícil imaginar que alguns governos possam querer manter determinados dados pessoais coletados para se prepararem contra uma segunda onda de coronavírus. Nessa situação, convém que cidadãos vigilantes cobrem as autoridades competentes por uma atuação justa e direta na proteção de seus dados pessoais.

COVID-19 E AS ENTRANHAS DO CAPITALISMO DE VIGILÂNCIA

Maurício Requião[285]

Em praticamente todo filme norte-americano de investigação policial há aquela cena em que um suspeito é interrogado numa sala em que há um espelho falso que não o permite ver o que está do outro lado, enquanto através dele os demais investigadores ocultos estão assistindo ao interrogatório. É também nessa dualidade de transparência e opacidade[286] que funcionam as atuais bases do capitalismo de vigilância.

LGPD. Ministério Público Federal. 2020. Disponível em: https://www.migalhas.com.br/arquivos/2020/4/E3A4099956E262_PR-SP-00039100.2020.pdf. Acesso em: 15 abr. 2020.

283 FILDES, Nic; ESPINOZA, Javier. Tracking coronavirus: big data and the challenge to privacy. Disponível em: https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987. Acesso em: 14 abr. 2020.

284 Tradução livre de "temporary measures have a nasty habit of outlasting emergencies, especially as there is always a new emergency lurking on the horizon". HARARI, Yuval Noah. Yuval Noah Harari: the world after coronavirus. Disponível em: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?shareType=nongift. Acesso em: 15 abr. 2020.

285 Doutor em Direito. Professor de Direito Civil da UFBA e da Faculdade Baiana de Direito. Líder do grupo de pesquisa "Autonomia e Direito Civil contemporâneo". Advogado.

286 LEMOS, André. MARQUES, Daniel. Privacidade e Internet das Coisas: uma análise da rede Nest a partir da Sensibilidade Performativa. In: E-compos. v.22, 2019. Disponível em: <https://www.e-compos.org.br/e-compos/article/view/1611>. Acesso em 08 jan 2020.

Este modelo, que de acordo com Shoshana Zuboff pode ser definido de diversas maneiras, pode ser explicado como "uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, predição e vendas"[287] (tradução livre).

Não que a ideia de um observador que não pode ser visto seja nova[288], mas os cada vez mais rápidos avanços tecnológicos na área de captura de dados têm elevado esta dualidade a níveis nunca vistos. Não se trata nem da ideia de que os usuários, ao utilizarem seus smartphones, não tenham noção de que seus dados pessoais são capturados; a maioria o tem, do mesmo modo que o suspeito interrogado sabe que do outro lado do espelho deve haver alguém. O que normalmente passa desapercebida é a dimensão dessa vigilância.

A crise provocada pela pandemia do COVID-19 tem mobilizado esforços dos mais diversos campos para seu enfrentamento. Dentre estes, devido à facilidade de transmissão da doença, se encontram os de monitoramento e vigilância, com objetivos de rastrear com maior eficácia as pessoas infectadas e de fiscalizar a realização do isolamento social.

287 ZUBOFF, Shoshana. The age of surveillance capitalism: the fight for the future at the new frontier of power. Profile Books: London, 2019, posição 69, e-book Kindle.
288 BENTHAM, Jeremy. O panóptico. 2.ed. Belo Horizonte: Autêntica, 2000.

As notícias sobre as práticas de vigilância, normalmente veiculadas pela mídia[289] e mesmo pela academia[290] de maneira positiva, não são novas, mas tão somente desveladas ou implementadas em função do momento da crise. Em outras palavras, tudo que se está fazendo para monitorar milimetricamente a vida dos sujeitos, com fito de combater a pandemia, já estava ocorrendo ou já era implementável. O que a pandemia proporciona é somente a exposição das entranhas da estrutura do capitalismo de vigilância.

O Google, que se cita aqui como exemplo por ser uma das empresas com maior poder de coleta de dados pessoais, divulgou recentemente quadro comparativo mostrando as diversas frequências de pessoas em ambientes definidos como "trabalho", "supermercados e farmácias", "parques" e "residências", separados por países e regiões, antes e durante a pandemia291. A simples possibilidade de criação de quadro comparativo já denota claramente que a vigilância por parte de tal empresa não é algo novo.

Na China, ponto inicial da pandemia, são utilizados drones, tecnologia de reconhecimento facial, scanners infravermelhos, além da implementação de aplicativo para

289 ROSA, João Luiz; BRIGATTO, Gustavo. Companhias dão, de graça, tecnologia contra surto. In: Valor Econômico. Disponível em: <https://valor.globo.com/empresas/noticia/2020/03/30/companhias-dao-de-graca-tecnologia-contra-surto.ghtml>. Acesso em 31 mar 2020.
290 BOULOS, Maged N. Kamel. Geographical tracking and mapping of coronavirus disease COVID-19/severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) epidemic and associated events around the world: how 21st century GIS technologies are supporting the global fight against outbreaks and epidemics. In: International Journal of Health Geographic, v. 19, 2020. Disponível em: <https://ij-healthgeographics.biomedcentral.com/articles/10.1186/s12942-020-00202-8>. Acesso em 06 abr 2020.
291 Google. See how your community is moving around differently due to COVID-19. Disponível em: <https://www.google.com/covid19/mobility/>. Acesso em 03 abr 2020.

classificar as pessoas de acordo com o risco de contágio, sendo tal informação transmitida às autoridades competentes[292]. As notícias dão conta até mesmo da possibilidade de instalação de câmeras dentro das casas das pessoas para fins de monitoramento[293].

A Coreia do Sul, por sua vez, rastreia os celulares dos usuários para criar um mapa que fica disponível publicamente para que todos cidadãos possam consultar por onde passaram as pessoas infectadas. Diversas outras medidas de monitoramento, em maior ou menor grau das acima narradas, já foram adotadas também no Irã, Israel, Taiwan, Áustria, Polônia, Bélgica, Alemanha e Itália[294].

Para Byung-Chul Han, China e Coreia do Sul, por exemplo, adotaram práticas de vigilância em geral mais pesadas e com maior aceitação por parte da população do que suas contrapartes ocidentais. Para o autor, isso se explica, em parte, por conta de que, ao contrário da cultura ocidental, a oriental seria mais voltada para o coletivo do que para o individual, sem que isso necessariamente indique se tratar de uma cultura com menor grau de egoísmo[295].

---

292 Ehrhardt Júnior, MARCOS; SILVA, Gabriela Buarque Pereira. Privacidade e proteção de dados pessoais durante a pandemia da COVID-19. Disponível em <https://direitocivilbrasileiro.jusbrasil.com.br/artigos/824478175/privacidade-e-protecao-de-dados-pessoais-durante-a-pandemia-da-covid-19>. Acesso em 31 mar 2020.

293 ROBITZSKI, Dan. China is installing surveillance cameras inside people's homes. In: the_byte. Disponível em: <https://futurism.com/the-byte/china-installing-surveillance-cameras-inside-peoples-homes>. Acesso em 28 abr 2020.

294 MOURA, Raíssa; FERRAZ, Lara. Meios de Controle à Pandemia da COVID-19 e a Inviolabilidade da Privacidade. Disponível em: <https://content.inloco.com.br/hubfs/Estudos%20-%20Conte%C3%BAdo/Coronavirus/Meios%20de%20controle%20a%CC%80%20pandemia%20da%20COVID-19%20e%20a%20inviolabilidade%20da%20privacidade.pdf?hsCtaTracking=ad1577ba-e5bc-4ff3-afdd-54a896891088%7C07ab4d6b-53d3-4a06-9f43-fb43621df88f>. Acesso em 31 mar 2020.

295 HAN, Byung-Chul. O coronavírus de hoje e o mundo de amanhã. In: El País. Disponível em: <https://brasil.elpais.com/ideias/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html?rel=mas>. Acesso em 30 mar 2020.

No Brasil[296], bem recentemente, uma empresa nacional, que trabalha com geolocalização, e da qual provavelmente a maior parte dos leitores jamais ouviu falar, se ofereceu para auxiliar no monitoramento durante a pandemia e já está sendo utilizada pela prefeitura de Recife com tal intuito. A referida empresa declarou que atualmente 60 milhões de smartphones carregam algum app com seu algoritmo, que os permite dizer onde cada uma dessas pessoas está, com uma margem de erro de dois a três metros[297].

Também no Brasil, o Governo Federal já anunciou seu interesse na adoção de medidas de monitoramento de celulares, similares às realizadas na China, o que encontra, inclusive, alguns óbices legais. Por enquanto, de acordo com o SindiTelebrasil (Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal), dentro de cerca de duas semanas deverá começar o repasse de dados de quase 220 milhões de aparelhos celulares, "com um dia de atraso de modo aglomerado, estatístico e anonimizado, a partir da coleta de informações por quase cem mil antenas"[298-299].

Mantendo o foco no cenário brasileiro, o acesso ao recentemente aprovado "auxílio emergencial ao cidadão" se dá através de cadastro na Caixa Econômica Federal[300]. A página inicial enumera os requisitos que devem ser atendidos pelo cidadão para ter

---

296 Saliente-se que, por meio da Medida Provisória (MP) 959/2020, lamentavelmente, a Lei Geral de Proteção de Dados (LGPD) teve sua vacatio legis ampliada, só devendo entrar em vigor em 03 de maio de 2021.

297 ROSA, João Luiz; BRIGATTO, Gustavo. Companhias dão, de graça, tecnologia contra surto. In: Valor Econômico. Disponível em: <https://valor.globo.com/empresas/noticia/2020/03/30/companhias-dao-de-graca-tecnologia-contra-surto.ghtml>. Acesso em 31 mar 2020.

298 MAGENTA, Matheus. Coronavírus: governo brasileiro vai monitorar celulares para conter pandemia. In: BBC News Brasil. Disponível em <https://www.bbc.com/portuguese/brasil-52154128>. Acesso em 03 mar. 2020.

299 Durante o período de ajustes para redação final deste texto, foi editada a MP 954/2020, que "Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020". A referida MP foi alvo de cinco Ações Diretas de Inconstitucionalidade e felizmente se encontra com sua eficácia suspensa, em caráter cautelar, vinculada à Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387/DF, por decisão da Ministra do Supremo Tribunal Federal, Rosa Weber.

300 CAIXA ECONÔICA FEDERAL. Auxílio emergencial ao cidadão. Disponível em: <https://auxilio.caixa.gov.br/#/destinacao>. Acesso em 07 abr 2020.

acesso aos benefícios e, para que possa prosseguir, exige a aceitação através de clique em duas caixas.

A primeira é de declaração de leitura e ciência de enquadramento do sujeito nas condições enumeradas na própria página. Já a segunda o cidadão deve indicar que autoriza o acesso e uso dos seus dados para validar as informações enumeradas. Não há qualquer explicação sobre que dados seriam coletados ou a partir de que bases de dados isso se daria. Fato é que, sem aceitar ambas opções a partir de um clique, não é possível prosseguir no cadastro.

Diante da premente necessidade de renda pela qual passam muitos cidadãos no momento, não é difícil chegar à conclusão de que o aceite se dará sem maiores reflexões sobre a proteção de seus dados pessoais. A situação parece ainda mais absurda quando se considera que é justamente a população mais vulnerabilizada que necessitará dar seu aceite incondicional e sem que lhe sejam prestadas maiores explicações.

Por fim, ainda no Brasil, foi aprovada a Lei n. 13.979/2020, que dispõe sobre as medidas de combate ao coronavírus no país. Em seu art. 6°, a referida Lei torna obrigatório

o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação.

Obrigatoriedade essa que ultrapassa a esfera dos órgãos públicos e "estende-se às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária", como determinado no parágrafo 1°, do mesmo artigo.

Como se nota pela narrativa delineada, não apenas a pandemia trouxe a público ou acelerou medidas de vigilância já adotadas pelas empresas privadas e Estados ao redor do globo, como também estabeleceu, por vezes de modo compulsório, como no caso do parágrafo acima citado da Lei brasileira, a cooperação, em falta de palavra mais adequada, na transmissão de informações sobre dados pessoais entre entes privados e Estado.

Embora se tenha divulgado a ideia de que o aumento da vigilância gera ganhos para a saúde, não se tem ainda prova de que esse custo-benefício exista de maneira substancial, como admitido recentemente pelo Primeiro Ministro de Singapura[301]. Mais do que vigilância, o que se prova até então efetivo é o isolamento social voluntário e a simples medida sanitária de lavar as mãos. Por outro lado, o que é certo é que esta pandemia traz como saldo a exposição da sociedade de vigilância que desde antes já está instalada e sua, ao menos momentânea, aceitação em maior grau por parte dos cidadãos em geral.

Entretanto, terminada a crise, qual será seu reflexo no que toca às práticas de vigilância?

No plano das estruturas sociais, uma das principais preocupações diz respeito à escalada do autoritarismo e dos riscos à democracia[302], facilitadas pela obtenção massiva por parte dos governos de dados dos cidadãos. Por um lado, porque terão obtido dados massivamente facilitando o controle futuro, por outro porque não há qualquer

301 CHEONG, Danson. Coronavirus: Most workplaces to close, schools will move to full home-based learning from next week, says PM Lee. In: The Straits Times. Disponível em <https://www.straitstimes.com/singapore/health/most-workplaces-to-close-schools-will-move-to-full-home-based-learning-from-next>. Acesso em 07 abr 2020.
302 HARARI, Yuval Noah. The world after coronavirus. In: Financial Times. Disponível em: <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75>. Acesso em 26 mar 2020. BIEBER, Florian. Authoritarianism in the Time of the Coronavirus. In: Foreign Police Magazine. Disponível em <https://foreignpolicy.com/2020/03/30/authoritarianism-coronavirus-lockdown-pandemic-populism/>. Acesso em 31 mar 2020.

garantia de que, encerrada a crise, os níveis de monitoramento caiam. Encontrar outro inimigo que justifique a manutenção do monitoramento não parece ser tão difícil e, como já dito, tais práticas de vigilância já aconteciam antes da crise, inclusive para controle de fronteiras[303].

Na China, para voltar a um exemplo já citado neste texto, se estabeleceu um "gigantesco panóptico militar e sanitário, que limita a população a viver trancada e sob permanente vigilância"[304]. No futuro, acabada a pandemia, não há como precisar qual será o impacto do atual modelo para a tolerância, já antes alta, à vigilância, nem que força dará ao autoritarismo.

No plano das práticas individuais resta a incógnita: com maior conhecimento sobre a dimensão do tratamento de dados as pessoas mudarão suas práticas a este respeito? Haverá mudança de comportamento e exigência de maior restrição à vigilância e consequente tratamento de dados depois de se saber o que há do outro lado do espelho?

Embora o desejo seja de que a pandemia venha a mudar as práticas dos sujeitos, gerando reação ao capitalismo de vigilância, o mais provável é que isso não aconteça. Passada a crise, os olhos provavelmente se desviarão das suas entranhas estruturais, buscando se adequar ao que for o novo paradigma de normalidade, ainda que seja este um paradigma de maior vigilância.

---

303 SÁNCHEZ-MONEDERO, Javier; DENCIK, Lina. The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl. Disponível em: <https://datajusticeproject.net/resources/>. Acesso em 29 dez. 2019.
304 ZIBECHI, Raul. Coronavírus: a militarização das crises. In: DAVIS, Mike et al. Coronavírus e a luta de classes. Brasil: Terra sem Amos, 2020, p. 31. Em sentido contrário, indicando que as críticas feitas ao cenário da China se fundam em desconhecimento e preconceito: JABBOUR, Elias. A China (muito) além da "Sopa de Wuhan". In: Le Monde Diplomatique Brasil. Disponível em: <https://diplomatique.org.br/a-china-muito-alem-da-sopa-de-wuhan/>. Acesso em 17 abr 2020.

CORONAVÍRUS - SUS: ASPECTOS RELEVANTES DA PRIVACIDADE E PROTEÇÃO DE DADOS E TECNOLOGIA DE VIGILÂNCIA

Laiane Maris Caetano Fantini[305]

INTRODUÇÃO

Governos por todo o mundo têm aderido a medidas tecnológicas de vigilância em massa para monitoramento dos cidadãos, infectados ou não, a partir de dados pessoais relacionados, principalmente, à localização em tempo real registrada no celular.

Os dados pessoais, contudo, estão relacionados às informações individuais da pessoa humana e são protegidos como direito fundamental à privacidade. Dessa forma, a preocupação em torno dessas tecnologias de vigilância reside na coleta não autorizada de dados, no risco de não anonimização e no destino que esses dados terão na medida em que deixar de existir a situação excepcional que justificou a coleta em detrimento de alguns princípios da privacidade e da proteção de dados pessoais.

A privacidade de dados é um limite e não uma barreira para a saúde pública em tempos de pandemia, deve ser usada com cautela e em respeito aos direitos fundamentais do titular e os princípios da proteção de dados. Em razão disso, o presente estudo busca fazer uma breve análise sobre as formas de coleta de dados pessoais dos usuários pelo Governo Federal através do aplicativo **Coronavírus - SUS**.

305 Advogada especialista em Direito Empresarial pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas), pesquisadora bolsista da CAPES na área de Direito Privado pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas), integrante do grupo de estudos DTI-BR (UFMG), membro da Comissão da OAB de Direito para Startups. Lattes: http://lattes.cnpq.br/3423805228534232

A COLETA DE DADOS PESSOAIS NA LEGISLAÇÃO NACIONAL

A Lei Geral de Telecomunicações[306] (Lei n. 9.472/97) já permitia, em seu art. 72, que empresas de telefonia realizassem o tratamento de dados pessoais dos usuários, para a execução de sua atividade-fim e para fins de divulgação, devendo respeitar a anuência expressa do usuário e, se envolvesse disponibilização desses dados para terceiros, a anonimização. Essa lei, até pela época em que foi promulgada, não avançou muito em questões envolvendo o titular de dados pessoais e seus direitos, mas já chamava atenção para a importância da criação de uma cultura de proteção de dados.

O debate sobre a regulamentação específica da proteção de dados pessoais é recente no país e hoje contamos com duas leis relevantes para o debate. Uma delas é o Marco Civil da Internet[307], que alçou como princípio a proteção dos dados pessoais. A outra é a Lei de Proteção de Dados Pessoais (LGPD)[308], que embora tenha tido sua *vacatio legis* prorrogada para maio de 2021, é a norma mais importante sobre o tema no país.

A LGPD, dentre inúmeros dispositivos de grande importância, traz no art. 4º algumas definições relevantes. Considera-se **dado pessoal** toda informação relacionada à pessoa natural identificada e identificável. Dentro dessa categoria existem os dados pessoais sensíveis, relacionados, por exemplo, ao dado genético ou à saúde.

306 BRASIL. Lei 9.472 de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995.Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9472.htm. Acesso em: 11 de abril de 2020.
307 BRASIL. Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 de abril de 2020.
308 BRASIL. Lei n. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 de maio de 2020.

Por **tratamento** entende-se qualquer operação realizada com esses dados, como coleta, produção, acesso, transmissão, arquivamento, dentre outros, e normalmente para qualquer operação de tratamento, é preciso ter o **consentimento** do titular, manifestação livre e informada, autorizando o tratamento para uma finalidade certa.

O art. 7º da LGPD trouxe uma exceção ao consentimento do titular se o tratamento de dados for realizado pela Administração Pública na execução de políticas públicas. É esse o fundamento legal basilar que respalda as diversas medidas adotadas pelo governo nos dias atuais, inclusive em relação ao aplicativo **Coronavírus - SUS**.

Como complemento, o Ministério da Economia publicou duas resoluções acerca do compartilhamento de dados.

A Resolução n. 1[309] criou o Comitê Central de Governança de Dados, órgão permanente e de natureza deliberativa responsável pela solução de controvérsias envolvendo o compartilhamento de dados entre solicitante e gestor público de dados. A Resolução n. 2[310] buscou facilitar o compartilhamento de dados entre os órgãos do governo, buscando reduzir a ambiguidade, categorizar o tipo de dado e adequá-los aos requisitos de segurança, tais como a anonimização, para orientar melhorias nos serviços públicos prestados aos cidadãos. Um desses critérios previstos foi a anonimização, a depender da classificação que esses dados vierem a receber.

As medidas nessas resoluções fundamentam a coleta ordinária de dados pessoais dos cidadãos pelo poder público, levando em conta situações para além da situação

309 BRASIL. Resolução n. 1 de 16 de março de 2020. Aprova o Regimento Interno do Comitê Central de Governança de Dados – CCGD. Ministério da Economia. Brasília.
310 BRASIL. Resolução n. 2 de 16 de março de 2020. Dispõe sobre as orientações e as diretrizes para a categorização de compartilhamento de dados. Ministério da Economia. Brasília.

de pandemia enfrentada no país, de modo a respaldar o tratamento dessas informações pessoais obtidas sem consentimento informado, nos termos do art. 7º III da LGPD.

O USO DE TECNOLOGIAS DE VIGILÂNCIA EM MASSA POR AUTORIDADES PÚBLICAS

A coleta de dados pessoais de geolocalização dos usuários de aparelho móvel pelo Poder Público pode ser feita, principalmente, de duas formas. A primeira delas, até o momento não adotada oficialmente pelo Governo Federal, consiste numa forma indireta de obtenção em que é feita a solicitação às operadoras de telefonia móvel, para o acesso a dados pessoais dos usuários, coletados diretamente pelas empresas para prestar os seus serviços, ou ainda, dados de geolocalização obtidos através ou de triangulação de antenas (o que permite obter de cada portador de aparelho celular informações onde esteve ou está).

O governo de São Paulo adota essa modalidade com o uso do SIMI/SP (Sistema de Monitoramento Inteligente), que, em parceria direta com as principais operadoras de telefonia, utiliza dados de georreferenciamento para monitorar aglomeração de pessoas, respeitando a anonimização.

Outra forma é a obtenção direta desses dados, por meio de aplicativos com autorizações específicas, criados pelo governo ou pela iniciativa privada, que coletam e tratam esses dados. Essa última medida tem sido mais adotada por diversos países, visando controlar a propagação do Covid-19 e monitorar a circulação de pessoas.

Embora os governos, nos casos citados, assumam o compromisso de manter a anonimização dos dados pessoais, a preocupação que muitas pessoas têm – ou ao menos deveriam ter – é com o aumento do Estado vigilante e a falta de informações sobre

a forma com que os dados que são coletados, as finalidades e período para o tratamento.

No artigo publicado pelo *Financial Times*[311], a Coréia do Sul adotou um modelo paradigmático de vigilância dos cidadãos através de dados de telefones celulares para o controle de doenças infecciosas, coletando dados como geolocalização, compras em cartão de crédito, consumo em farmácias, etc., pois "*os dados [coletados] permitiram a rápida implantação de um sistema de notificação alertando os coreanos sobre os movimentos de todas as pessoas potencialmente contagiosas em seus bairros ou edifícios*"[312] (tradução livre).

O mesmo tem ocorrido com países como China e Israel, cujos modelos de monitoramento por aplicativos ignoram a manifestação de vontade do titular dos dados. O aplicativo chinês, por exemplo, controla e restringe a livre circulação dos indivíduos, determinando quem (e quando) alguém poderá ou não deixar a sua residência.

Na Alemanha, o governo desenvolveu um aplicativo junto com o grupo *Berlim Thryve*, que atua na área de saúde digital. O objetivo do aplicativo é mapear a propagação do Covid-19, monitorando dados anonimizados que envolvam a apresentação de comportamentos dos usuários, como pulsação, sono e atividade, para inferir se não suspeitos.

311 FIELDS, Nic; ESPINOZA, Javier. Tracking coronavirus: big data and the challenge to privacy. Financial Times. 2020. Disponível em: https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987. Acesso em: 11 de abril de 2020.

A Áustria desenvolveu o "*StoppCorona*"[313], que permite aos usuários rastrearem pessoas que tiveram em contato com o vírus, notificando-as se algum de seus contatos tiver testado positivo para o vírus.

Em países com menor investimento em tecnologias de ponta, foram adotados meios alternativos. A Polônia[314], por exemplo, lançou o "*Home quarantine app*", mandatório, o qual, essencialmente, envia notificações a usuários aleatórios, exigindo o envio de *selfies* dentro do lugar em que estão cumprindo a quarentena.

O Brasil também adotou medidas próprias, embora em menor escala em termos de vigilância. O aplicativo "**Coronavírus – SUS**", criado pelo **DataSus**, propõe conscientizar a população sobre o Covid-19, indicar unidades de saúde mais próximas do usuário além de orientar o usuário sobre eventual apresentação de sintomas. Aparentemente, se projeta como um serviço intermediário dos modelos citados, já que procura monitorar a circulação do usuário sem enviar nenhum alerta ou fundamentar a aplicação de qualquer sanção administrativa.

Todavia, mesmo com relevantes recursos tecnológicos, muitos dos usuários de aplicativos, enquanto titulares dos dados pessoais fornecidos, desconhecem a abrangência dos dados coletados – muitas vezes, até pela interface do aplicativo - ou, ainda que conheçam, não apresentam oposição por acreditar no alcance de um fim maior.

313 OSTERREICHISCHES ROTES KREUS. Meet the STOPP CORONA APP. Disponível em: https://www.roteskreuz.at/site/meet-the-stopp-corona-app/. Acesso em: 30 de abril de 2020.
314 CHEN, Caleb. Poland´s COVID-19 "selfie app" rises privacy questions – Will everyone eventually be tracked?. 2020. Disponível em: https://www.privateinternetaccess.com/blog/polands-covid-19-selfie-app-raises-privacy-questions-will-everyone-eventually-be-tracked/. Acesso em: 11 de abril de 2020.

LEMOS e MARQUES[315], estudando aplicativos usados pela Prefeitura de Salvador para obter dados pessoais, constaram a presença de interfaces maliciosas, as quais coletam informações sem que o usuário se dê conta ou tenha como evitar. Trata-se do que Harry Bignull cunhou como *Dark Patterns* (DP)[316], utilizado nessas aplicações com o fim de mitigar o consentimento informado e a privacidade dos titulares.

O uso de recursos como esses reforçam a assimetria informacional, pois o usuário não se dá conta dos dados que está fornecendo. Em se tratando ainda da situação gerada pela pandemia do Covid-19, os usuários acabam concordando com o fornecimento de dados pessoais em troca da oportunidade de contribuir com a base de dados do sistema público de saúde e assim, aprimorar medidas de apoio à população.

O APLICATIVO CORONAVÍRUS - SUS E A COLETA DE DADOS PESSOAIS DOS USUÁRIOS

Para usar o "**Coronavírus – SUS**", é necessário baixar o aplicativo e instalá-lo, não sendo exigido nenhum cadastro ou qualquer outra barreira para condicionar o acesso.

Porém, a aplicação solicita permissões para compartilhar informações de localização aproximada (*network-based* – baseada na rede) e para acessar a localização precisa (GPS e *network-based*) para, aparentemente, poder oferecer com precisão o serviço de indicar a unidade de saúde mais próxima. O aplicativo solicita ainda acesso completo à

315 LEMOS, André; MARQUES, Daniel. Interfaces Maliciosas: estratégias de coleta de dados pessoais em aplicativos. São Carlos, n. 19, 2019. [online]. Disponível em: https://www.researchgate.net/publication/337926919_Interfaces_Maliciosas_Estrategias_de_Coleta_de_Dados_Pessoais_em_Aplicativos. Acesso em 12 de abril de 2020.
316 Na pesquisa citada, os autores colocam "Dark Patterns" como sinônimo de interfaces maliciosas, as quais não são necessariamente interfaces ruis, mas usadas com "intencionalidade obscura, desenvolvidos para obtenção de resultados específicos sem explicações ao usuário" (pág. 2).

rede de conexões e ainda, permissão para realizar ligações telefônicas. Isso nos leva a questionar que, se nenhum cadastro prévio é solicitado ao usuário, como essas informações serão colhidas a partir do dispositivo móvel e, ademais, qual a finalidade de se ter acesso ao recurso de chamadas e como isso respeita a anonimização.

De fato, se o objetivo implícito do aplicativo é monitorar a movimentação das pessoas e a formação das ondas de calor para verificar possíveis aglomerações, precisaria apenas da geolocalização dos usuários, não havendo necessidade para acesso a informações como o nome do usuário, aos contatos no celular ou ainda, à permissão para realizar chamadas telefônicas.

Ao acessar o aplicativo, é preciso concordar com os Termos de Uso e conferir determinadas permissões, quando solicitadas. No tópico "Uso das contribuições" desse termo, consta o compromisso na aplicação à LGPD, principalmente às eventuais regulamentações da Autoridade Nacional de Proteção de Dados (ANPD), quando for criada. Todavia, o aplicativo não esclarece se os dados obtidos serão tratados apenas durante esse período emergencial, com o adequado descarte posterior. Dá a entender que esses dados pessoais ficarão permanentemente no banco de dados administrado pelo DataSUS, responsável pelo aplicativo. É um indício de uso de interface maliciosa atrelada à questionável observância ao Princípio da Informação e Necessidade (art. 6º, I e III da LGPD).

A pandemia tornou trouxe à evidência questões importantes sobre a coleta de dados pessoais e o respaldo, na segurança das pessoas, para buscar métodos de monitoramento cada vez mais invasivos e ao mesmo tempo, sutis. A LGPD mostra papel fundamental nesse momento, para orientar as autoridades, empresas e cidadãos e fiscalizar condutas sob o parâmetro da proteção à privacidade.

Conquanto o empenho em cumprir a LGPD, é importante ressaltar que, até a presente data, o fato dessa lei não estar ainda em vigor afeta o direito dos titulares na medida em que, percebendo qualquer violação ou suspeita de violação a seus direitos, a falta de uma autoridade de proteção de dados prejudica a fiscalização desses pontos, deixando vulneráveis os usuários desse aplicativo.

CONCLUSÃO

Os dados pessoais dos titulares, coletados durante a situação excepcional a qual o país está atravessando, devem ser tratados pelo Poder Público apenas para servir de base para a adoção de medidas acautelatórias e de combate à pandemia.

Normas como a Lei Geral de Telecomunicações, o Marco Civil da Internet e a Lei Geral de Proteção de Dados fundamentam o tratamento de dados pessoais e reforçam a necessidade de consentimento ou de informação da finalidade específica para o tratamento do dado que está sendo coletado e servem de respaldo para o aplicativo **Coronavírus - SUS**.

Contudo, embora a Lei Geral de Proteção de Dados ainda não esteja em vigor, deve servir de parâmetro normativo para todas as medidas que têm sido – e que serão – adotadas diante dessa situação o "estado de exceção", buscando preservar os princípios basilares da proteção e privacidade de dados pessoais, principalmente em relação ao aplicativo Coronavírus - SUS. Os usuários não deveriam ter que escolher entre os direitos fundamentais de privacidade e saúde para se sentirem protegidos em relação às medidas adotadas pelo Poder Público.

AS RELAÇÕES DE PRECEDÊNCIA CONDICIONADA COMO LIMITE À VIGILÂNCIA EXTREMA: O REPASSE DE INFORMAÇÕES PELAS OPERADORAS DE TELECOMUNICAÇÃO

Marco Aurélio Rodrigues da Cunha e Cruz[317] *e Luís Henrique Kohl Camargo*[318]

INTRODUÇÃO

No realismo mágico de "Cem anos de solidão", Macondo foi invadida pela "peste da insônia". O patriarca Buendía debochou inicialmente. Seria mais uma das enfermidades inventadas pela superstição indígena: "Se não voltarmos a dormir, melhor. [...] Assim a vida renderá mais". Visitación o advertiu sobre o mais agudo estágio, o esquecimento, pois com estado de vigília, absorvia-se toda e qualquer informação sem a devida reflexão. Macondo ficou infatigavelmente acordada e algumas medidas foram tomadas: 1) medidas exógenas para impedir o contágio: os forasteiros teriam que tocar sinos na entrada do povoado e não se lhes permitiria comer ou beber nada; 2) medidas endógenas para atenuar as evasões de memória: descrições do significante, do significado e da utilidade das coisas: "Esta é a vaca, tem-se que ordenhá-la todas as manhãs para que produza leite, e o leite deve ser fervido para ser misturado com o café e fazer o café com leite". Os habitantes de Macondo "continuaram vivendo numa realidade escorregadia, momentaneamente capturada pelas palavras, mas que fugiria sem remédio quando fosse esquecido o valor da letra escrita", até que tentaram construir a "máquina da memória" [319].

317Doutor em Direito Constitucional, Professor Permanente | PPGD-Unoesc: mar.cunhaecruz@gmail.com.
318Mestrando em Direitos Fundamentais | PPGD-Unoesc, luiskohl@hotmail.com.
319GARCÍA MÁRQUEZ, G. Cem anos de solidão. 18. ed. Rio de Janeiro: Record, 19--. p.39-50.

A alegoria conduz a problematizar duas medidas não-farmacológicas tomadas no Brasil para o enfrentamento do COVID-19 como hipóteses de redução do risco de doença e proteção do direito à saúde [P1]: [M1] o repasse de informações pelas operadoras de telecomunicação sobre a circulação de pessoas[320]; e [M2] o compartilhamento de dados pessoais para a implantação de teleatendimento pelo Ministério da Saúde[321]. Questiona-se uma possível violação à privacidade [P2]. O objetivo deste escrito é defender o argumento das relações de precedência condicionada como limite à vigilância extrema. Com uma metodologia analítica, as conclusões são resultado de uma revisão bibliográfica e documental de natureza descritiva, tendo Robert Alexy como referencial teórico.

AS COLISÕES DOS DIREITOS, A COVID-19 E O ESTADO DEMOCRÁTICO

"A moral reformada; a saúde preservada; a indústria revigorada; a instrução difundida; os encargos públicos aliviados; a economia assentada, como deve ser, sobre uma rocha; o nó górdio da lei sobre os pobres não cortado, mas desfeito – tudo por uma simples ideia de arquitetura!". Estes os objetivos de "vigilância crônica" ou "extrema" que propôs Bentham em 1787, com as variáveis de intensidade, controle, visibilidade e inspeção, alcance e extensão além do sistema penitenciário[322]. Vários modelos pós-panópticos poderiam ser listados com outras variáveis, como na Sociedade Disciplinar[323]

320BRASIL, Agência. Governo usará dados de teles para monitorar circulação de pessoas, Brasília, publicado em 05/04/2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/governo-usara-dados-de-teles-para-monitorar-circulacao-de-pessoas>. Acesso em: 2 maio 2020. Adota-se a distinção entre "dado" e "informação" de Danilo Doneda. Cf.: DONEDA, D. Da privacidade à proteção de dados pessoais. 2. ed. São Paulo: RT, 2019.
321Parecer n. 00281/2020/CONJUR-MCTIC/CGU/AGU.
322BENTHAM, J. O panóptico. [e-book: Kindle]. Autêntica: 2019: "[...] consistiu em tornar 'universalmente aplicável' as 'circunstâncias de aplicação exclusiva' corporificadas no Panóptico de Samuel em Krichev".
323FOUCAULT, M. Vigiar e punir: nascimento da prisão. 42. ed. Petrópolis: Vozes, 2014.

ou na *Scored Society*[324], mas a linha conjuntiva destes evidencia importância no que, quem, como, com qual objetivo, quando e por quanto tempo se monitora[325].

O monitoramento e a regulação de dados pessoais na *data-driven economy*[326] do século XXI tem resposta em leis em ao menos cento e trinta e dois países[327]. "Moderado" é a classificação do Brasil no *Data protection laws of the World*, pressupondo a LGPD[328]. A LGPD inaugurará uma nova abordagem jurídica para o uso de dados pessoais[329], contudo, tem incidência mediata que pode ser prorrogada para 2022[330]. Sem uma regulação específica no nível de regras infraconstitucionais, cabe uma argumentação jurídica para avaliar a juridicidade das duas medidas não-farmacológicas aludidas.

Em um Estado Democrático, Alexy[331] pontua que os direitos fundamentais podem se converter em um problema quando de um mero ideal sejam tornados em algo real. Esta problematização democrática cabe no recorte das duas debatidas medidas de redução do risco de contágio do COVID-19, para responder à colisão de dois direitos fundamentais: saúde e privacidade. Alexy aposta na resolução dos conflitos de direitos fun-

---

324CITRON, D. K.; PASQUALE, F. The Scored Society: Due Process for Automated Predictions. Washington Law Review, v. 89, n.1, p. 1-34, March 2014.

325Em uma remissão parcial ao que questionou o Tribunal Constitucional alemão em 15 de dezembro de 1983, sobre a Lei do censo (Volkszählungsgesetz), (wer, was, wann, bei welchen Gelegenheit). Cf.: PÉREZ LUÑO, A-E. Derechos Humanos, Estado de Derecho y Constitución. Madrid: Tecnos, 2005, p. 358-359.

326UNCTAD. Digital Economy Report 2019. New York: UN Publications, 2019. Disponível em:<https://unctad.org/en/PublicationsLibrary/der2019_en.pdf>. Acesso em: 2 maio 2020.

327GREENLEAF, G. Global Tables of Data Privacy Laws and Bills. Supplement to 157 Privacy Laws & Business International Report, Sydney, 2019. Disponível em: <https://ssrn.com/abstract=3380794>. Acesso em: 11 abr. 2020.

328DLA PIPER. Data protection laws of the World: full handbook. DLA PIPER: 2020. Disponível em: <https://www.dlapiperdataprotection.com/>. Acesso em: 2 maio 2020.

329Sobre a autonomia jurídica do direito à proteção de dados pessoais/autodeterminação informativa: MURILLO DE LA CUEVA, P. L. El derecho a la autodeterminación informativa. Tecnos: Madrid, 1990.

330O Senado Federal aprovou o PL 1179/2020 que prorroga para vigência para 1.1.2021 e aplicação de punições em 1.8.2021. Ainda consta no Senado o PL 1027/20 e na Câmara dos Deputados o PL 5762/2019.

331ALEXY, R. Direitos fundamentais no Estado Constitucional Democrático. Revista de Direito Administrativo, Rio de Janeiro, v. 217, p. 55-66, jul. 1999. ISSN 2238-5177. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/47413/45319>. Acesso em: 2 maio 2020.

damentais pela representação política e pela representação argumentativa: "O parlamento representa o cidadão politicamente, o tribunal constitucional argumentativamente". A representação argumentativa atua negativamente como instância de reflexão (e objeção) do processo político, e positivamente ao se aprovar os argumentos do tribunal, dentro de um discurso jurídico-constitucional racional. A estabilidade dessas representações é o suporte para uma institucionalização dos direitos fundamentais no Estado Constitucional democrático e a reconciliação entre estes e a democracia. Alexy, ainda, observa uma liberdade limitada à argumentação jurídica, com a sujeição à lei (representação política), aos precedentes e seu enquadramento pela dogmática da ciência do Direito[332].

No nível hierárquico extremo, a gramaticalidade do texto de 1988 atribui à saúde (art. 6º, 196 a 200) e à privacidade (art. 5º, inc. X, XI, XII, LX, LXXII,) dupla fundamentalidade (formal e material). Não há regras textual-normativas que estabeleçam relações de restrição. Há possibilidades fáticas e jurídicas para o seu maior grau de otimização, o que deflui da lógica normativo-teórica de princípios. Não há uma relação de precedência absoluta entre estes princípios. A solução para essa colisão levará em consideração o caso concreto [C] para a fixação de condições sob as quais um princípio tem precedência condicionada em face do outro [**P**]. Sob outras condições, é possível que a questão da precedência seja resolvida de outra forma até oposta[333].

Princípios e regras são razões para normas e indiretamente razões para ações. Urge avançar para os demais níveis hierárquicos. Na interpretação sistemática da leitura

332ALEXY, R. Teoria da argumentação jurídica. 3. ed. Rio de Janeiro: Forense, 2013, p.31.
333ALEXY, R. Teoria dos direitos fundamentais. 2. ed. São Paulo: Malheiros, 2011, p.96; ALEXY, R. Direitos Fundamentais Sociais e Proporcionalidade. Trad.: Rogério L. Nery da S. In: ALEXY, R., BAEZ, N. L. X.; NERY DA SILVA, R. L. Dignidade humana, direitos sociais e não-positivismo inclusivo. Florianópolis: Qualis, 2015, p. 165-178.

infraconstitucional e supra-legal, a saúde pública é hipótese textual-normativa de restrição de liberdades protegidas (1) de locomoção, (2) de manifestação religiosa ou de crença, (3) de pensamento e de expressão, (4) de reunião e (5) de associação, tanto no PIDCP[334] como na CADH[335]. Nestes Tratados de Direitos Humanos a interpretação lógica protetivo-normativa do direito a saúde é uma hipótese jurídico-restritiva da dimensão defensiva de liberdades protegidas. Por sua vez, a lógica da dimensão defensiva (direitos a ações negativas) é a que *prima facie* está inscrita nas premissas protetivas da privacidade (inviolabilidade moral, inviolabilidade do domicílio, inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas). E a proteção os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural é o objetivo da LGPD (art. 1º).

Outrossim, a Lei nº 13.979/2020, que dispõe sobre as medidas para enfrentamento da emergência de saúde pública decorrente do COVID-19, no inciso III do §2º, do art. 3º, assegura às pessoas afetadas pelas medidas previstas na lei o respeito à dignidade, aos direitos humanos e às liberdades fundamentais das pessoas. Com o reconhecimento da pandemia em 11.3.2020[336], vários entes federativos brasileiros editaram atos normativos com medidas não-farmacológicas indiretamente restritivas à liberdade de reunião e de mitigação de possibilidades fáticas de liberdade de locomoção para redução do risco de contágio[337], reforçadas com a declaração de estado de transmissão comunitária do COVID-19, pela Portaria nº 454/GM/MS, 20.3.2020.

334Artigos 12, 18, 19, 21 e 22 do Pacto Internacional sobre Direitos Civis e Políticos de 1966, Decreto No 591/92.
335Artigos 12, 13, 15, 16 e 22 da Convenção Americana sobre Direitos Humanos de 1969, Decreto No 678/92.
336WORLD HEALTH ORGANIZATION. WHO Director-General's opening remarks at the media briefing on COVID-19,11 March 2020. Disponível em: <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020>. Acesso em: 2 maio 2020.
337Para exemplificar: DISTRITO FEDERAL. Decreto n. 40.509, de 11 de março de 2020. Disponível em: <http://www.dodf.df.gov.br/index/visualizar-arquivo/?pasta=2020/03_Março/DODF%20025%2011-03-2020%20EDICAO%20EXTRA&arquivo=DODF%20025%2011-03-2020%20EDICAO%20EXTRA.pdf>.Acesso em 2 maio 2020; SÃO PAULO, Governo do Estado

Este é o contexto das notícias de que as operadoras de telecomunicação repassarão informações pessoais para o poder público[338]. Medidas diretamente restritivas de compartilhamento (inconsentido) de informações [P2] estariam sendo utilizadas para aferir as medidas indiretamente restritivas das liberdades de reunião e de locomoção [Objetivo], cuja finalidade seria a redução do risco de contágio de transmissão comunitária do COVID-19 [P1]. Mas há diferenciações entre o [M1] repasse de informações sobre a circulação de pessoas (geolocalização) e o [M2] compartilhamento de dados pessoais junto ao Ministério da Saúde.

AS DUAS RELAÇÕES DE PRECEDÊNCIA CONDICIONADA

Tendo como razão a declaração de estado de transmissão comunitária do COVID-19 e defendendo o conceito expansionista de dados pessoais[339][P2], haverá precedência [**P**] da saúde [P1] no monitoramento da circulação de pessoas (geolocalização) [M1] na seguinte condição de precedência [C1]: se o compartilhamento pelas operadoras for de informações agregadas e proveniente de dados anonimizados segundo o art. 72, §2°, Lei n. 9472/97, com a finalidade exclusiva identificar situações de concentração de pessoas e risco de contaminação, durante a situação de emergência de saúde pública prevista na Lei 13.979/20. Quanto mais e maior o grau de *Privacy Enhancing Technologies* melhor a proteção[P2], na linha do descrito na Recomendação 2020/518 da Comissão Europeia[340].

---

de. Decreto nº 64.862, de 13 de março de 2020. Disponível em: <http://www.legislacao.sp.gov.br/legislacao/dg280202.nsf/69aaa17c14b8cb5483256cfb0050146e/f61eabdde86c24758325852d004f3cf2?OpenDocument&Highlight=0,coronav%C3%ADrus,2020>. Acesso em: 2 maio 2020.

338Não constam publicações no Diário Oficial da União (http://www.in.gov.br/web/guest/inicio).

339BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. R.J.: Forense, 2019.

340 COMMISSION RECOMMENDATION (EU) 2020/518 of 8 April 2020. Disponível em:<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020H0518&from=EN>. Acesso em: 2 maio 2020.

Sobre [M2] o compartilhamento de base de dados simplificada de âmbito nacional com o número do telefone, idade e o município [P2] para implantação de teleatendimento para triagem de identificação de indivíduos com sintomas do COVID-19 (dados sensíveis: art. 5, II, LGPD), o Ofício nº 401/2020/SE/GAB/SE/MS indica que esta triagem à distância objetiva viabilizar a prevenção ativa e o monitoramento dos casos já identificados e "evitar que casos não críticos cheguem às unidades de saúde, impedindo a disseminação do novo vírus aos profissionais de saúde, mantendo maior controle da proliferação da doença, nos locais de sua maior incidência" [P1]. Tendo esta razão, haverá precedência [**P**] da saúde [P1] na seguinte condição de precedência [C2]: se for pedido por autoridade competente (Ministério da Saúde: art. 47, III, Lei nº 13.844/2019), dentro da hipótese da previsão legal (art. 213, Lei n. 9472/97; art. 6º, §1º, Lei n.º 13.979/2020), pode ser feito o compartilhamento de dados pessoais essenciais para finalidade específica (exclusiva) de evitar a propagação do COVID-19 e possível identificação de pessoas infectadas ou com suspeita de infecção, durante a situação de emergência de saúde pública prevista na Lei 13.979/20 e observado o art. 116 da Lei nº 8.666/93. Quanto mais e maior o grau de *Privacy Enhancing Technologies*, maior extensão terá esta regra.

CONSIDERAÇÕES FINAIS

Foi o cigano Melquíades (a ciência) que levou um "frasco com uma substância de cor suave", e a luz se fez na memória de Macondo. Enquanto não há medidas farmacológicas eficazes, cabe no atual momento "descrições do significante, do significado e da utilidade" das normas jurídicas. Uma das primeiras indagações de Rodotá sobre a configuração da "Sociedade da Classificação" é: "Sociedade da vigilância total ou sociedade

da liberação total?[341]". A representação política infraconstitucional aplicada nos suportes fáticos [M1 e M2], segundo a teoria dos direitos fundamentais de Alexy, levou às soluções *C1* e *C2* acima apresentadas, com a fixação de condições sob as quais a saúde [P1] teve precedência condicionada [**P**] em face da privacidade [P2]. Sob outras condições, é possível que a relação de precedência seja resolvida de outra forma até oposta, o que reforça a consistência do argumento das relações de precedência condicionada como limite à vigilância extrema em um Estado Democrático.

341RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p.111.

ISBN: 978-65-87614-02-1