REVISTA
CADERNO
VIRTUAL

PROTEÇÃO DE DADOS PESSOAIS: UMA ANÁLISE DOS EFEITOS DA PANDEMIA DA COVID-19 NA PROTEÇÃO DOS DADOS

Guilherme Ornelas Monteiro[1]

Resumo

O presente artigo tem por objetivo analisar se o cenário de pandemia pode se tornar pretexto para que o direito de proteção de dados seja inutilizado. Sob esse contexto, analisou-se como o consentimento e métodos de anonimização de dados são basilares para a proteção da identidade do titular dos dados. Ademais, investigou-se como a Lei Geral de Proteção de Dados garante legitimidade para que o governo realize o tratamento de dados pessoais com vistas a tutelar a saúde, estudou-se os fundamentos pelos quais potencializou-se a defesa pela prorrogação da Lei Geral de Proteção de Dados e os possíveis desarraigamentos dessa prolação.

Palavras-chave: Lei Geral de Proteção de Dados. Consentimento. Dados Anonimizados. Coronavírus.

PERSONAL DATA PROTECTION: AN ANALYSIS OF THE PANDEMIC EFFECTS OF COVID-19 ON DATA PROTECTION

Abstract

The purpose of this paper is to analyze whether the 2020 pandemic scenario can serve as a pretext to data protection rights being weakened. In this sense, this study focuses on the importance of consent and how the provision of the techniques of data anonymization are fundamental for protecting the identity of the data subject. Additionally, an analysis of how Brazil's General Data Protection Law guarantees legitimacy for the government to process personal data in order to protect health was conducted. The arguments behind the defense of the postponement of Brazil's General Data Protection Law enforcement was studied, as well as the possible implications of this suspension.

Keywords: *Brazil's General Data Protection Law. Consent. Data Anonymization. Coronavirus.*

1. INTRODUÇÃO

A crise mundial fomentada pela proliferação da Covid-19 potencializou a consolidação de um cenário cujo direito à proteção de dados torna-se frágil: a coleta dos

[1] Acadêmico de Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Pesquisador do grupo de Direito e Ciência Comportamental (IDP/CNPq). Integrante da Clínica de Direitos Humanos IDP. Membro do Grupo de Estudos em Direito e Economia (GEDE UnB/IDP).

dados pessoais e seu uso para a elaboração de políticas de saúde pública e de pesquisas científicas de combate à doença são cada vez mais aceitos como matéria prima e logrados por instituições públicas e privadas (DONEDA,2020). O contexto de calamidade pública global acentua o interesse estatal em coletar massivamente dados dos cidadãos e aumenta a aceitação de instrumentos jurídicos, políticos e tecnológicos para fazê-lo: na Rússia, por exemplo, já se verifica a identificação de localização de infectados por câmeras de reconhecimento facial[1]; na China, o governo exigiu que pessoas utilizassem o aplicativo *The Alipay Health Code* em seus celulares para monitorá-las e informá-las, por meio de três indicativos de cores, se devem se manter em isolamento ou se estão autorizadas a frequentar espaços públicos[2]; em Hong Kong, alguns cidadãos tiveram que usar um *smartwatch*[3] que, semelhante a uma tornozeleira eletrônica, avisa as autoridades se a pessoa fugir da quarentena; na Coreia do Sul, o governo utilizou do histórico de transações de crédito, de localização do celular e até câmeras de segurança para mapear a rota de pessoas portadoras do vírus[4].

A partir desse cenário, o acentuado número de mortes provocadas pelos desarraigamentos da infecção do vírus propicia que as pessoas assentem com o tratamento de seus dados por uma expectativa de salvaguarda: a privacidade se expressa como um direito de menor relevância ante a necessidade e urgência de combate à pandemia. Sistemas desenvolvidos em parceria com empresas privadas (*Covid-19 apps*[5], por exemplo), por vezes não projetadas à vista de um *privacy by design*[6], transformam a programação dos aplicativos em verdadeiras caixas-pretas, não disponibilizando

[1] Coronavírus e proteção de dados pessoais. Folha de S.Paulo. Disponível em: https://www1.folha.uol.com.br/opiniao/2020/03/coronavirus-e-protecao-de-dados-pessoais.shtml. Acesso em: 2 abr. 2020.

[2] 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: 2 abr. 2020.

[3] Hong Kong is putting electronic wristbands on arriving passengers to enforce coronavirus quarantine. Disponível em: https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html. Acesso em: 2 abr. 2020.

[4] Mapa sul-coreano de pessoas portadoras do vírus. Disponível em: https://coronamap.site/ Acesso em: 2 abr.2020

[5] Aplicativos desenvolvidos por instituições privadas e públicas vocacionados para o rastreamento de pessoas suspeitas ou portadoras do coronavírus.

[6] Acepção de que o respeito à privacidade deve estar intrínseco à formulação de aplicativos. A privacidade se torna basilar desde a engenharia do sistema até a sua aplicação. (CAVOUKIAN, 2012)

informações suficientes para aferir se são aptas e seguras para o tratamento dos dados pessoais (PASQUALE, 2016).

É nesse sentido que as leis e regulamentos cujos objetos versam sobre a proteção às informações pessoais se tornam basilares para a averiguação desses procedimentos: evitar que a pandemia se torne mais um pretexto para a formação de uma sociedade ainda mais monitorada e vigiada (LYON, 2018). Roberto Gargarella e Jorge Ernesto apontam que " *Por las mismas razones, deberíamos oponernos a que se utilice la pandemia como excusa para realizar o intensificar actividades de ciber-patrullaje*" (GARGARELLA, ROA ROA 2020, p.20). No contexto brasileiro, a pandemia da Covid-19 propiciou não apenas a criação de serviços de monitoração para mitigar a proliferação do vírus, como também propiciou debate no Congresso Nacional sobre a prorrogação da Lei Geral de Proteção de Dados Pessoais (LGPD).

O objetivo geral deste artigo é analisar e problematizar a ressignificação do direito à proteção de dados no atual contexto de múltiplas crises. O argumento principal é que a não priorização do direito de proteção de dados pode ter implicações deletérias de longo prazo para o regime democrático brasileiro. À vista do objetivo geral, o artigo propôs estudar três aspectos necessários para refletir sobre os reflexos da pandemia no direito à proteção de dados: (i) o consentimento do titular dos dados pessoais para o tratamento de suas informações; (ii) os dados de geolocalização enquanto anonimizados para a contenção do vírus; e (iii) a prorrogação da LGPD. A análise projetada objetivou estudar se a postura do governo brasileiro frente à crise representaria atenuação ou ab-rogação ao direito de preservação e segurança dos dados.

A metodologia adotada consistiu na revisão bibliográfica sobre a Lei Brasileira Geral de Proteção de Dados, o Regulamento Geral Europeu sobre a Proteção de Dados, estudos empíricos sobre o comportamento dos usuários no ambiente digital, investigações sobre a efetividade da anonimização de dados e o usufruto de dados de localização para a contenção de epidemias. Além disso, por meio de um panorama exploratório, foi investigado os argumentos que fundamentam a defesa pela prorrogação da LGPD, destacando o posicionamento do governo brasileiro, sociedade, setor privado, público e comunidade acadêmica.

Assim, o estudo se divide em quatro partes. Na primeira parte foram apresentados conceitos técnicos: buscou-se mostrar a definição, à luz da LGPD, dos dados pessoais, dados anonimizados, dos dados sensíveis e das hipóteses de seu tratamento. Trabalhou-

se, na segunda parte, com a complexidade do consentimento, buscando refletir, à vista de estudos empíricos e de revisão bibliográfica, desafios para o gozo substancial desse instituto face à pandemia, destacando as hipóteses em que a administração pública brasileira está autorizada a coletar dados para fins de saúde coletiva, inclusive em situações que o consentimento do titular não é necessário para o tratamento de suas informações. Na terceira parte, evidenciou-se a atuação dos governos estaduais com o tratamento de dados frente à crise e, assim, buscou-se entender como os dados de geolocalização são mecanismos importantes para o enfretamento de epidemias, ao passo que transparência e especificação das técnicas de anonimização utilizadas no tratamento dos dados pessoais são basilares para a proteção da privacidade do seu titular. Na quarta e última parte, refletiu-se sobre a prorrogação da LGPD, os argumentos os quais fundamentam seu adiamento e os possíveis desarraigamentos de sua protelação. Por fim, a conclusão.

2. O QUE SÃO OS DADOS PESSOAIS E POR QUE É IMPORTANTE PROTEGÊ-LOS?

Para se compreender a importância de existir fundamentos normativos de proteção aos dados pessoais, é necessário entender o conceito. Afinal, o que seriam os dados pessoais? Os dados pessoais[1] são os fragmentos de informações que agrupados, disciplinados ou não, relacionam-se direta ou indiretamente com a identificação de uma pessoa, isto é, fotos, nome, endereço de e-mail, dados bancários, dados médicos, estado civil, orientação sexual, religião, profissão, histórico de navegação on-line, informações sobre origem racial ou étnica, CPF, RG, endereços, histórico de compras. Estas ainda são suscetíveis de serem coletadas, processadas, armazenadas e transferidas a um terceiro. À luz da LGPD, art.5, I, dado pessoal é a informação "relacionada a pessoa natural identificada ou identificável".

Cada informação possui um grau de potencialidade a estimar a identidade do indivíduo, veja: nome, CPF, RG e endereço são informações com um grau de objetividade extremamente maior quando comparado a um histórico de navegação ou a uma

[1] O dado, isoladamente, não aferi compreensão sobre algo. São considerados o conteúdo quantificável, isto é, a unidade básica da informação. A informação é o dado processado, é a consequência/resultante do processamento de dados, esta nasce por meio da qualificação dos dados (FEDELI ; POLLONI ; PERES, 2010).

informação relacionada a uma compra – algumas informações estão diretamente ligadas à identidade do indivíduo. É laborioso apenas com os dados de que uma pessoa é solteira e advogada saber especificamente sua identidade; entretanto, uma vez tendo acesso a dados como, fotos, o endereço, ou o nome da pessoa, tornará essa identificação mais célere e objetiva. É nesse sentido que os dados pessoais são todas as informações que direta ou indiretamente podem apontar a identidade de alguém. O limite e alcance da regulação de proteção aos dados dar-se-ão pela própria definição do que venha a ser dado pessoal – as legislações precisam pautar cirurgicamente o que é considerado dado pessoal, pois o que não for considerado, também não terá a mesma proteção (como será disposto posteriormente, no caso dos dados anonimizados).

A LGPD, além disso, confere entendimento ao chamado dado anonimizado (art.5, III) que é aquele relativo ao titular que não possa ser identificado. Embora os dados anonimizados sejam relativos a uma pessoa – como os dados estatísticos –, eles também são dados que não viabilizam a identificação do titular.

Para um dado se tornar anônimo, é necessário que passe por um processo de anonimização que consiste na utilização de técnicas que, no momento do tratamento, possam ser aplicadas para que o dado perca a possibilidade de associação direta ou indireta a um indivíduo (art.5, XI). Assim, uma vez o dado anonimizado não sendo apto a viabilizar a identificação direta ou indireta do seu titular, a LGPD não o considera como dado pessoal, salvo se o processo de anonimização ao qual o dado pessoal fora submetido for incipiente, ao passo que, com esforços razoáveis, poderá ser revertido e viabilizar a identificação da pessoa (art.12).

2.1 DADOS SENSÍVEIS

Em contexto de pandemia, os dados que são tratados por instituições a fim de zelar pela saúde coletiva, por vezes, tratam dos chamados dados sensíveis. Os dados sensíveis são as informações que, expostos à coleta, ao armazenamento e submetidas a tratamento, expressam grande potencial de discriminação com vistas a causar lesões (DONEDA, 2020). São os dados que oferecem conteúdo de vulnerabilidade: estes são relacionados a

características da personalidade do indivíduo e seus hábitos pessoais. São os dados referentes à opinião política, origem racial ou étnica, a dado genético, dado biométrico, dados alusivos à saúde ou à orientação sexual, a de caráter religioso ou filosófico – são os que possibilitam de alguma forma fazer distinção ou diferenciação: trata-se, aqui, daqueles relacionados à personalidade, honra e imagem do indivíduo (art.5, II; LGPD).

Para compreender como os dados pessoais podem se tornar instrumentos discriminatórios, insta ressaltar um julgado do Tribunal Superior do Trabalho (TST). O TST, em 2008, reconheceu que havia a necessidade de indenização por dano moral aos trabalhadores que tiveram o nome inserido em listas por empregadores após acionarem a Justiça do Trabalho[1]. Empregadores mal-intencionados criaram listas, em forma de "banco de dados", para servir de fonte de consulta a outros empregadores que queiram conferir a conduta de pessoas que já se candidataram a vagas, em processos de seleção de trabalho, com o objetivo de identificar se, entre aqueles candidatos, há algum com tendência a reivindicar direitos (MENDES, 2014).

Aqui há claramente um exemplo de como os dados uma vez postos à correlação podem servir de instrumento discriminatório: os trabalhadores que acionavam a justiça do trabalho em busca de reparação de direitos eram, pelos seus empregadores, expostos em listas a fim de torná-las pessoas não confiáveis para se trabalhar, pois, as empresas ao contratarem novos empregados, poderiam aferir nessas listas se o candidato possui esse tipo de conduta ou não.

A LGPD, nesse sentido, além de conferir especial proteção normativa aos dados sensíveis, dispõe que aos dados pessoais, que em primeiro momento não são considerados dados sensíveis, mas se tratados e correlacionados puderem revelar tanto da vida privada do indivíduo de modo a discriminá-lo, aplicar-se-ão os mesmos zelo e cuidado como se sensíveis fossem (art. 11, §1).

3. CONSENTIMENTO

O consentimento constitui elemento fundamental para o recolhimento dos dados pessoais. Para a LGPD, o consentimento consiste em um ato de manifestação do titular

[1] Laura Mendes destaca em ''Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental'', página 77, o julgado de 2-4-2008, de relatoria da Ministra Maria de Assis Calsing, da quarta turma, DJ 18-4-2008 (RR 325/2004-091-09-00.7), no sentido de evidenciar que dados pessoais podem ser utilizados com vistas a constranger os indivíduos.

de cunho informado, livre, inequívoco na qual o próprio titular concorda com o tratamento dos seus dados para uma finalidade específica (art. 5º, XII; LGPD). Consentimento como manifestação livre é a expressão autêntica da vontade do indivíduo, sem qualquer tipo de vício, fraude ou coação. Por consentimento informado, compreende-se a pessoa ter acesso às formas pelas quais os seus dados serão tratados, ou seja, ter noção de forma clara, adequada e ostensiva do trato que será aferido (art.9; LGPD). Assim, o consentimento elencado pela LGPD busca garantir completa cognição do titular ante o tratamento dos seus dados. É a partir do consentimento que a pessoa pode usufruir da autodeterminação informativa (art.2, II) que se funda num cenário no qual o titular dos dados possui completo controle sobre o tratamento das informações que lhe pertence, isto é, além de saber do tratamento aferido, é autônomo para interromper esse tratamento – inclusive requisitar a exclusão desses dados.

O consentimento aliado à autodeterminação informativa[1] pressupõe o direito dos indivíduos de decidirem dentro de quais limites seus dados podem ser utilizados – consistindo em fundamento para a criação da LGPD (art. 2, II).

3.1 A COMPLEXIDADE DO CONSENTIMENTO INFORMADO

Os princípios trazidos pela LGPD[2] norteiam o emprego e proveito dos dados, ao passo que também aferem transparência inclusive nas hipóteses cujo consentimento não precisa ser solicitado. Ao assentir pela concessão dos dados pessoais, o titular não confere abnegação ou abandono pela sua autodeterminação informativa, mais claramente, não se trata de renúncia do direito de controlar esses dados pessoais, o consentimento somente representa um movimento de aceitar a coleta desses dados à vista da autonomia individual do titular da informação (MENDES, 2014).

Deve-se considerar, porém, que a autodeterminação informativa está em direta relação com os conhecimentos da pessoa acerca da importância em proteger os dados que lhe pertence. Revela-se, assim, que não é possível gozar do consentimento elencado pela LGPD e da autodeterminação informativa se não vislumbrando a importância disto.

[1] Entende-se por autodeterminação informativa a liberdade e capacidade de decisão do indivíduo sobre as ações a serem realizadas com seus dados.

[2] Art. 6º; LGPD dispõe os princípios os quais devem ser observados para o tratamento de dados pessoais: ‘’finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas’’.

Destaca-se[1], aqui, dois estudos empíricos que evidenciam importantes reflexões acerca do consentimento: (a) As pesquisadoras Aleecia McDonald e Lorrie Cranor realizaram uma pesquisa[2] empírica para avaliar e estudar os modelos mentais dos usuários ao usufruírem do ambiente on-line; para isso, em um primeiro momento, com um grupo de 14 pessoas e, posteriormente, com um grupo maior de 314 pessoas[3].

Na primeira parte da pesquisa, observou-se como as pessoas agem em relação aos *cookies* de navegação no ambiente on-line; quando questionados, verificou-se que apenas 23% dos entrevistados utilizam a navegação privada nos navegadores de internet para impedir a coleta dos dados pessoais pelos *cookies* de navegação; 50% dos usuários não utilizam dessa navegação, ao passo que 27% não tinham certeza[4].

Quando questionados se realizam a exclusão dos *cookies*, somente 17% dos usuários realizam essa ação e, deste reduzido grupo, somente 8% os apagam toda vez ao fechar o navegador de internet. Posteriormente, os 314 entrevistados listaram 390 motivos para excluir ou não os *cookies* de navegação: das 80 razões para não os excluir, 20% disseram não fazer, pois não compreendiam o que eram os *cookies*, 19% não sabiam como os excluir, 31% não se importavam com eles, ao passo que, das 278 razões para os excluir, somente 30% dos participantes os apagam por razões de privacidade e segurança.

As pesquisadoras relatam ainda que os entrevistados tiveram enorme dificuldade de diferenciar os *cookies* com o histórico de navegação, além de observar que mesmo os participantes desejando excluir os cookies, não saberiam como fazê-lo[5]. Interessante notar a aversão que os entrevistados possuíam em ser monitorados no ambiente on-line; quando questionados sobre o rastreamento que os websites fazem sobre as atividades dos clientes: 64% dos entrevistados concordaram em ser hostil tal ação, além de que 40% concordam que teriam mais cuidado no ambiente digital se soubessem que anúncios podem coletar seus dados[6].

---

[1] Bruno Bioni na obra ‘’*Proteção de Dados Pessoais - A Função e os Limites do Consentimento’’* destaca quatro estudos importantes para entender a problemática do consentimento. No presente artigo resolveu-se destacar dois desses para evidenciar que as pessoas estão propensas a fornecer seus dados sem de fato ter conhecimento do ato.

[2] *McDonald, Aleecia and Cranor, Lorrie Faith, Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising (August 16, 2010). TPRC 2010.* Disponível em SSRN: https://ssrn.com/abstract=1989092

[3] Ibdem p.4-5

[4] Ibdem p.11

[5] Ibdem p.12-13

[6] Ibdem p.23

Perante a esse estudo, dentre as conclusões apontadas pelas pesquisadoras, destaca-se que as pessoas não conseguem perceber a necessidade de proteger os dados no ambiente on-line, uma vez que não entendem quais seriam as consequências em não fazer, não há, assim, como valorar a privacidade e a segurança dos dados pessoais e qual seria o real impacto[1]. Os usuários não possuem conhecimento suficiente para tomar decisões esclarecidas e informadas: não sabem os riscos provenientes do compartilhamento de dados nem quais são os dados sujeitos a coleta.

A Universidade da Pensilvânia[2] (b), a partir de entrevistas com grupo de 1.506 pessoas, permitiu entender a conduta das pessoas sobre o recolhimento dos dados sem consentimento e também sobre o fluxo de informações nesse contexto. Os pesquisadores delinearam alguns cenários a fim de obter a opinião das pessoas: (i) é justo que a partir de um fornecimento de desconto, as empresas coletassem seus dados pessoais sem o seu conhecimento; (ii) é justo que, em troca de um fornecimento gratuito de internet, as lojas pudessem coletar seus dados pessoais; e (iii) é plausível que as lojas coletem dados pessoais dos clientes em troca da criação de um perfil personalizado que irá melhorar o serviço prestado. Observou-se que no primeiro cenário, 91% não concordam que as lojas coletem dados pessoais sem o consentimento do titular; no segundo cenário, 71% dos entrevistados discordam com o fornecimento gratuito de internet em troca dos dados; e, no terceiro cenário, 55% das pessoas discordam que é plausível utilizar dados pessoais para a criação de um perfil personalizado[3]. Observa-se que, nessas hipóteses, quando há claramente evidenciado que haverá a coleta de dados pessoais, as pessoas tendem a não concordar com a oferta, isso pois estariam inclinadas a valorar mais a privacidade do que as benesses ofertadas.

Posteriormente, os pesquisadores investigaram o que eles chamam de paradoxo da privacidade[4], a partir de um cenário fictício: pediu-se que as pessoas pensassem em um supermercado pelo qual se frequenta constantemente; assim, os entrevistados foram indagados se permitiriam que o supermercado escolhido coletasse suas informações

[1] Ibdem p. 27 *''We find a gap between the knowledge users currently have and the knowledge they would need to possess in order to make effective decisions about their online privacy.''*

[2] *The tradeoff fallacy - how marketers are misrepresenting american consumers and opening them up to exploitation. Joseph Turow, Michael Henness, Nora Draper. University of Pennsylvania.*. Disponível em: https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

[3] Ibdem p.11 -12

[4] O paradoxo da privacidade, em âmbito de *trade-off*, consiste quando um indivíduo embora saiba do perigo de fornecer seus dados pessoais e a importância em os proteger, anui deles sabendo que gozará de benesses, pois, caso não fizesse, não usufruiria dos serviços.

pessoais em troca de descontos em produtos. Nesse sentido, 45% das pessoas concordariam com a oferta. Subsequentemente, os pesquisadores apenas com o grupo de pessoas que concordaram com a oferta, passaram a elencar outras hipóteses a fim de compreender se haveria ainda anuência dos dados.

Os pesquisadores elencaram diversas situações em que, a partir da coleta dos dados, o supermercado pudesse identificar aspectos específicos sobre a vida do seu titular: (i) se você possui tendência a comprar alimentos menos gordurosos; (ii) quando ocorrerão as próximas férias; (iii) a origem racial; (iv) informações sobre a condição da própria saúde e da família; (v) se há filhos e quais seriam as respectivas idades; (vi) quais são os afazeres fora do ambiente de trabalho; (vii) a renda financeira; e (viii) se se está passando por algum momento importante na vida. Os pesquisadores, assim, realizaram novamente a mesma oferta, porém, agora, fornecendo uma visão macro de como o supermercado pode saber detalhes da vida privada do titular dos dados: dessa forma, observou-se que houve uma redução média de 20%[1], isto é, as pessoas estariam menos propensas a concordar com ofertas desse feitio. Embora a pesquisa aponte que até as pessoas conhecedoras de segurança digital são suscetíveis a fornecer seus dados por benesses (pois acreditam ser inevitável o controle de seus dados por parte das empresas), observa-se que, quando há maior detalhamento sobre as implicações do processamento de dados, elas tendem a declinar dessa permissão.

Sob esse cenário, embora as pessoas alcancem a compreensão em abstrato da necessidade de preservação de sua privacidade, acabam sendo contraditórias e incoerentes frente às propostas econômicas (BIONI, 2019). Na prática, não percebem como sua privacidade está sendo violada a partir de pequenos atos de coleta de informações que, vistos por si só, podem parecer inofensivos, mas que em seu conjunto acabam se tornando um poderoso instrumento de influenciar e moldar comportamentos. As pessoas estão inclinadas a fornecer seus dados quando confrontadas com propostas, pois não possuem compreensão completa das consequências que podem ser geradas a partir de seu fornecimento, isto é, não há como valorar a privacidade sem conhecer as irradiações do tratamento dos dados.

Assim, a base normativa do consentimento torna-se incerta quando fatores externos influenciam na tomada de decisão do titular: o consentimento livre e informado dos cidadãos não é notável, pois podem consentir sem ao menos saber o que poderá ser

[1] Ibdem p.13-14

gerado com esse ato. Trata-se de um consentimento meramente formal e não substancial, pois serve mais como uma licença moral para que empresas se protejam ao coletar informações pessoais do que para proteger os próprios indivíduos.

O cidadão constitui a parte do elo frágil na relação do mercado informacional, pois essas relações comumente conferem a possibilidade de prestação de serviço somente a partir da aceitação do indivíduo em fornecer os dados, do contrário, não gozaria de benesses – veja, por exemplo, as plataformas de redes sociais, as quais só fornecem seus serviços caso o indivíduo concorde com os termos e condições (BIONI, 2019). Não é possível o indivíduo exercer total poder na sua liberdade de deliberação sobre o tratamento dos dados sem ter conhecimentos prévios de privacidade e de como suas informações pessoais podem ser utilizadas para, no futuro, manipular suas percepções e comportamentos. É necessário existir uma linguagem clara[1] e transparente dos termos de uso dos serviços das empresas a fim de que o cidadão possa consentir de forma livre, informada e genuína no fornecimento dos dados e desfrutar da autodeterminação informativa. Os entrevistados na pesquisa de Stanford poderiam, talvez, negarem pelo fornecimento dos seus dados, caso já fossem, desde o início da pesquisa, informados de modo claro e inteligível sobre o alcance e risco que o tratamento dos dados poderia ocasionar.

Percebe-se que, na realidade, os termos de uso e privacidade carecem de inteligibilidade: são extensos, prolixos, além de serem recheados de termos técnicos jurídicos e de tecnologia tal como evidencia matéria investigativa do *New York Times*[2] que constatou como necessário ter um nível de escolaridade de ensino superior ou até ser um profissional da área para compreender esses textos devido ao extenso uso de linguagem técnica especializada. As pessoas aceitam os termos de privacidade, propiciando o tratamento de seus dados pessoais, mas sem de fato entendê-los (LITMAN-NAVARRO, 2019).

[1] O RGPD, por exemplo, estabelece que as instituições utilizem linguagem inteligível, sem jargões técnicos ou jurídicos. Disponível em: https://gdpr.eu/gdpr-consent-requirements/?cn-reloaded=1

[2] LITMAN-NAVARRO, Kevin. We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. The New York Times., 12 jun. 2019. Disponível em: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html. Acesso em: 11 jun. 2020.

Na pesquisa *The Cost of Reading Privacy Polices*[1], Aleecia McDonald e Lorrie Faith Cranor evidenciaram, em 2008, que ler termos de privacidade custam tempo e dinheiro, pois, analisando os termos de privacidade de 75 websites mais populares no ano de 2005, as pessoas teriam que dispor muito tempo para analisá-los, posto que em média possuem 2,514 palavras[2] o que demandaria, pelas estimativas das pesquisadoras, uma média de 244 horas anuais por pessoa[3] para lê-los. Em vista de uma média salarial de US$ 17,93 nos Estados Unidos, as pesquisadoras calcularam que ler os termos de compromisso dos websites demandariam US$ 35,86 por hora, se lidos no ambiente de trabalho, ao passo que demandaria US$ 4,48 se lidos em casa.

Assim, em uma situação em que, num ambiente on-line, os cidadãos americanos lessem "palavra por palavra" todos os termos dos websites que visitam, o país passaria a dedicar 54 bilhões de horas anuais para essa atividade que custaria US$ 781 bilhões anualmente pelo tempo perdido. Em termos individuais representaria US$ 3.534 anuais de custo pelo tempo. Esses dados mostram que tornar os termos de privacidade objetivos, inteligíveis e de leitura célere representaria mais do que uma vantagem para com o consentimento do titular dos dados, também proveria redução de custos e, consequentemente, atenuação de capital pelo tempo aproveitado.

Em contexto de pandemia, com a LGPD até o presente momento (junho de 2020) não vigente, o consentimento e a autodeterminação informativa se tornam ainda mais necessárias e imprescindíveis (art 2º, II e o art 5º, XII; LGPD).

O combate à pandemia serve de pretexto para que governos criem políticas de recolhimento de dados pessoais de modo a induzir que pessoas assentem pelo processamento desses dados sem que tenham uma real percepção dos desarraigamentos da provisão destes, isso porque estariam essas pessoas anestesiadas pela promessa de salvaguarda sanitária pelo Estado. É a acepção do paternalismo libertário ou arquitetura de escolha em que mesmo havendo a preservação de autonomia (o indivíduo pode escolher entre prover ou não os dados), existem muitos *Nudges* para que os indivíduos sejam instigados a realizar determinadas ações (SUNSTEIN; THALER, 2008). Em tempos de calamidade pública, as pessoas estão suscetíveis e fragilizadas para dispor dessas informações sem questionar os seus reflexos: se tornam resignadas.

[1] I/S: A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568. Disponível em: https://kb.osu.edu/handle/1811/72839. Acesso em: 14 jul. 2020.
[2] Ibdem p.554
[3] Ibdem p.562,563, 564

4. O ESTADO PODE COLETAR DADOS PARA FINS DE SAÚDE COLETIVA?

As bases normativas da LGPD proporcionam legalidade para a coleta, armazenamento e tratamento dos dados em períodos emergenciais. A LGPD relaciona as hipóteses de tratamento de dados pessoais sensíveis, sempre quando o titular ou seu responsável consentir de forma destacada, específica e para fins específicos (art. 11, I). Assegura, porém, que, em alguns cenários, o tratamento desses dados pode ocorrer inclusive sem o fornecimento de consentimento do titular: em cenário que seja essencial para o cumprimento de obrigação legal ou regulatória pelo controlador, para execução de políticas públicas pela administração pública, realização de estudos por órgão de pesquisa, proteção da vida ou da incolumidade física do titular ou de terceiro, tutela da saúde (art. 11, II). Este é um elemento fundamental para se entender: o consentimento pode ser relativizado nas hipóteses do inciso II, do artigo 11, e a própria existência de uma lei de proteção aos dados aponta que esse recolhimento, ainda que sem o consentimento, seja norteado pelos princípios elencados pela lei, isto é, torna o processo mais seguro, zelando pela privacidade da pessoa.

Ainda sob esse mesmo prisma, em 6 de fevereiro de 2020, a Lei n. 13.979 foi promulgada no Brasil. Este regulamento estabelece, em seu artigo 6º, que seja obrigatório o compartilhamento de dados essenciais entre órgãos e entidades da administração pública para identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus com finalidade exclusiva de evitar proliferação, veja: aqui, a lei, à luz do princípio da finalidade, diz expressamente que o compartilhamento de dados terá finalidade exclusiva, portanto, em consonância com a LGPD. A lei ainda aponta que a obrigação de compartilhar dados essenciais também se estende às pessoas jurídicas de direito privado, quando solicitado por autoridade sanitária (art.6, § 1º).

Diante desse cenário, a LGPD e a lei 13.979 possibilitam o tratamento dos dados com vistas para a preservação da saúde coletiva; o Estado, portanto, pode fazer uso de dados quando vocacionado para uma finalidade específica, inclusive em hipóteses em que o consentimento do titular não seja necessário.

4.1 BRASIL, DADOS DE LOCALIZAÇÃO E PROBLEMÁTICAS

No intuito de conter a proliferação do vírus, o uso de dados de geolocalização[1] se tornou importantes matérias primas na identificação das rotas de transmissão oriundas do deslocamento das pessoas. A empresa pernambucana In Loco[2] projetou uma tecnologia apta a localizar 60 milhões de brasileiros e entender o seu comportamento; a instituição coleta dados de geolocalização de celulares por meio de aplicativos parceiros que utilizam o seu serviço.

Quando um indivíduo que possui algum aplicativo parceiro da In Loco ativa a funcionalidade de geolocalização do dispositivo, a empresa coleta os dados de localização que são consolidados, agregados, organizados em grupos de usuários por padrões – assim, a empresa consegue estabelecer métricas de comportamento, a partir de um mapa que indica o índice de isolamento social no país[3].

A empresa alega que oferece dados anônimos, estatísticos e cartográficos aptos a ajudar os pesquisadores a elaborarem pesquisas promissoras e auxiliar as instituições públicas a programarem políticas públicas – portanto, não considerados dados pessoais para a LGPD. O Governo de São Paulo[4], nesse mesmo sentido, estabeleceu o Sistema Monitoramento Inteligente de São Paulo (Simi-SP) que, diante de parcerias com as operadoras Vivo, Claro, Oi e Tim, utilizará dos dados de geolocalização para estudar como a sociedade está se conduzindo no contexto de calamidade pública, dessa forma, o Simi-SP averigua quais são as regiões, em que há grande concentração de pessoas, suscetíveis de haver disseminação do vírus.

É nesse sentido que, para que essas parcerias se tornem consonantes à LGPD, precisam, à luz do princípio da transparência (art. 6º, VI; LGPD), disponibilizar as informações oficiais detalhadas do tratamento de dados, pois, como será discorrido posteriormente, os dados anônimos, se submetidos a um processo de anonimização fraco, podem ainda identificar o seu titular; ademais, é necessário que haja a eliminação dos dados quando o propósito inicial tiver sido almejado.

---

[1] Os dados de geolocalização, quando agregados, são capazes de fornecer índices sobre a eficácia das medidas de distanciamento social, identificando possíveis pontos de risco de transmissão.

[2] Controle à COVID-19 preservando a privacidade. In Loco. p. 1-24. Disponível em: https://content.inloco.com.br/blog/controle-a-covid-19-preservando-a-privacidade. Acesso em: 11 jun. 2020

[3] Mapa brasileiro da COVID-19. In Loco. Disponível em: https://mapabrasileirodacovid.inloco.com.br/. Acesso em: 11 jun. 2020.

[4] Governo de SP apresenta Sistema de Monitoramento Inteligente contra coronavírus. Disponível em: https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus/ Acesso em: 1 jun.2020

Não há consenso, todavia, de que os sinais de GPS fornecem estimativas de localização no nível de exatidão que é necessário para prever o risco de transmissão da Covid-19[1]. A coleta dos dados de localização para contenção de epidemias não garante que haja eficiência no rastreamento da rota de disseminação do vírus: em nota técnica, o Laboratório de Políticas Públicas e Internet evidencia que, à época da epidemia da Ebola na África Ocidental, o tratamento de dados de geolocalização com vistas a rastrear e monitorar o percurso que a doença se disseminava não foi aferido, isso porque os mecanismos tecnológicos utilizados eram incipientes ante ao objetivo pré-estabelecido.

Analogamente, estudos mostram que, em 2014 – 2016, em cenário de epidemia da Ebola em Serra Leoa, foram observadas insuficiências e limitações no uso de dados de geolocalização para conter a disseminação do vírus (ERIKSON, 2018). Como observa Susan Landau[2]- matemática, especialista em políticas de segurança cibernética e professora na Fletcher School of Law and Diplomacy and the School of Engineering, Department of Computer Science, Tufts University – os sinais de GPS poderiam indicar que "um indivíduo portador do vírus esteve na mesma estação de metrô que uma pessoa não portadora, mas não é capaz de apontar que essas pessoas andaram no mesmo vagão[3]".

Estudo publicado na *nature*[4], que investigou o uso de dados de localização na epidemia da Cólera no Haiti, evidenciou, entretanto, que os dados de telefones móveis, ainda que não completamente exatos, podem representar uma forma fundamental para a compreensão de como se dissemina os agentes infecciosos e, assim, servindo de parâmetro para a criação de políticas mais sólidas. O uso de dados e algoritmos, na luta contra a pandemia da Covid-19, se utilizados segura e prudentemente, certamente representam os instrumentos mais efetivos vocacionados a mitigar os reflexos da proliferação (IENCA, 2020).

4.2 SOBRE OS DADOS ANÔNIMOS

[1] GPS Accuracy. GPS gov, Disponível em: https://www.gps.gov/systems/gps/performance/accuracy/. Acesso em: 11 jun. 2020.

[2] LANDAU, Susan. Location Surveillance to Counter COVID-19: Efficacy Is What Matters. Law Fare, 25 mar. 2020. Disponível em: https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters. Acesso em: 11 jun. 2020.

[3] Tradução autoral.

[4] Bengtsson, L., Gaudart, J., Lu, X. et al. Using Mobile Phone Data to Predict the Spatial Spread of Cholera. Sci Rep 5, 8923 (2015). Disponível em: https://doi.org/10.1038/srep08923 Acesso em: 11 jun.2020

Como observado, os dados a serem coletados por governos e empresas para o combate à pandemia são anônimos, agregados e estatísticos. Porém, mesmo que anônimos, os dados de localização propiciam a identificação da rotina de um indivíduo que consequentemente pode apontar sua identidade. O *New York Times*[1] recebeu de fontes anônimas mais de 50 bilhões de *pings* anonimizados de localização de celulares de mais de 12 milhões de estadunidenses (entende-se por pings os pacotes de localização transmitidos isoladamente por um dispositivo celular e recebido por uma torre de transmissão, propiciando, por exemplo, a triangulação. Estes agrupados e correlacionados são passíveis de mapear a rotina de um indivíduo.). Com esses dados, os jornalistas passaram a investigar os possíveis desarraigamentos do seu tratamento, ao passo que também entrevistaram e consultaram especialistas em computação.

Os jornalistas elencaram as principais premissas utilizadas por instituições privadas para coletar os *pings*: "as pessoas consentem com o fornecimento desses dados, os dados são anônimos e são seguros[2]". Acerca do consentimento, não é possível afirmar que as pessoas consentem completamente com o fornecimento de suas informações (como discorrido anteriormente).

Sobre os dados serem seguros, essa afirmação não se sustenta, uma vez que o próprio veículo *New York Times* obteve acesso a um banco de dados expressivo. Em relação a serem anônimos, de fato os *pings* de geolocalização não contém informações como nome ou endereço de e-mail (o que em primeiro momento não identifica quem é o titular), mas uma vez tratados singularmente podem se tornar dados pessoais, ou seja, que identificam uma pessoa.

Para evidenciar esta fragilidade, os jornalistas acessaram o banco de dados e isolaram *pings* de geolocalização provenientes de apenas um dispositivo celular e, assim, os analisaram durante o período de 2016 e 2017. A partir dessa análise, os jornalistas conseguiram observar que esses *pings* curiosamente estavam sendo transmitidos sempre nas mesmas localidades: o que evidenciava a rotina do dono desse dispositivo móvel, pois uma vez observando todos os lugares (lojas, casas, instituições) pelos quais os *pings* foram transmitidos, era possível aferir por onde o titular se deslocou durante esse período.

[1] THOMPSON, Stuart; WARZEL, Charlie. Twelve Million Phones, One Dataset, Zero Privacy. The New York Times, 19 dez. 2019. Disponível em: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. Acesso em: 31 maio 2020.

[2] Tradução autoral.

Desse ensaio, já é possível concluir que, mesmo os *pings* não provendo informações como nome ou e-mail de quem estava utilizando o dispositivo móvel, é possível ter conhecimento de todos os lugares pelos quais esse dispositivo se deslocara durante o período; assim, não é difícil aferir quem seria o titular desse dispositivo móvel que transitou nos lugares verificados.

Os jornalistas realizaram o mesmo isolamento, mas agora em uma dimensão maior, conseguindo traçar a rotina de diversas pessoas; por exemplo, os jornalistas identificaram membros do governo e manifestantes em seus afazeres diários, como levar as crianças às escolas, ir ao trabalho, voltar para casa – tudo a partir dos dados recebidos que são tidos como supostamente anônimos.

Um célebre exemplo da investigação é o caso do Ex-engenheiro da *Microsoft:* os jornalistas novamente isolaram os *pings* gerados de um único dispositivo celular e puderam observar a rotina e o deslocamento de um indivíduo que se encontrara na sede da *Microsoft* (que depois descobriu se tratar de Ben Broili). Observou-se que o dono desse dispositivo móvel em certo dia se deslocara até a outra extremidade da sua região de trabalho chegando até à *Amazon* e permaneceu certo tempo na empresa. No mês seguinte, esse indivíduo começou um novo emprego na empresa *Amazon.*

Se, em um cenário hipotético, a Microsoft estivesse analisando esses dados, certamente evitaria deixar que Ben tivesse acesso aos novos projetos da empresa, uma vez sabendo que este poderia a qualquer momento começar um emprego na instituição concorrente. Os dados são passíveis de apontar informações sensíveis sobre a vida privada de um indivíduo: *"They can see the places you go every moment of the day, whom you meet with or spend the night with, where you pray, whether you visit a methadone clinic, a psychiatrist's office or a massage parlor."*.

Daí a importância de existir marco normativo que impeça as empresas de se basearem no pretexto de "dados anônimos" para não impor a mesma proteção que os dados pessoais requereriam, uma vez que as legislações de proteção aos dados não reconhecem os dados anônimos como sendo pessoais; porém, como observado nas matérias investigativas da *Times Opinion*, os dados anônimos podem se tornar pessoais se forem incipientes.

A LGPD dispõe que os dados anonimizados serão considerados dados pessoais quando o processo de anonimização ao qual forem submetidos se constituírem fracos e puderem indicar direta ou indiretamente a identidade da pessoa (art.12), portanto, já há

previsão para que os dados dos cidadãos passem por um processo de anonimização seguro e complexo para que, de fato, torne sigilosa a identidade do indivíduo, evitando, assim, que, com "esforços razoáveis[1]"possam esses dados serem revertidos à condição de dados pessoais.

Nesse sentido, é de imprescindível importância que o governo e empresas, que tratem dados de geolocalização para o combate ao vírus, forneçam detalhes acerca do processo de anonimização ao qual os dados de localização estão sendo submetidos, justamente para apontar se o processo é inábil ou não.

A Autoridade Nacional de Proteção de Dados (ANPD) poderia dispor sobre padrões e técnicas seguras para o processo de anonimização (art.12, § 3º), mas o órgão federal não está efetivamente implementado.

5. PRORROGAÇÃO DA LGPD: REALMENTE NECESSÁRIO?

O Projeto de Lei (PL) 1179/2020 tramitou no Congresso Nacional de modo a tratar de diversas matérias sobre direito privado durante o período de pandemia e, dentro as temáticas, dispõe sobre alteração na *vacatio legis* da LGPD para janeiro de 2021. Nesse mesmo sentido, a Medida Provisória n. 959, editada pelo poder executivo em 20 de abril de 2020, adiara a entrada em vigor da LGPD para maio de 2021.

A premissa por trás do adiamento da lei se baseia em que é preciso proteger as empresas que não teriam orçamento para adaptar sua estrutura à LGPD (uma vez que a lei traz diversas mudanças pelas quais as empresas deverão aderir) e, uma vez em estado de isolamento social, cuja circulação de capital ficara prejudicada, essas adaptações, assim como as punições trazidas pela lei (em caso de descumprimento às especificações), deveriam ser impostas em período posterior à pandemia. Como justifica a relatora do PL, senadora Simone Tebet (MDB-MS):

> "(...) inúmeras empresas estão impossibilitadas de, nesse momento, adotar as medidas necessárias para cumprir as obrigações constantes da Lei Geral de Proteção de Dados, pois muitos desses deveres envolvem

[1] Esforços razoáveis é a expressão pela qual a LGPD utiliza para dizer que será considerado dado pessoal aquele dado anônimo pelo qual se submeteu a um processo que com esforços razoáveis pode ser revertido. Art. 12

> a necessidade de contratar outras empresas responsáveis pela gestão de dados pessoais"[1].

Nesse sentido, pesquisa realizada pela Serasa Experian[2] mostrou que, em 2019, 85% das empresas no Brasil afirmaram não estarem prontas para adotar os requisitos da LGPD, isto é, não estarem preparadas para garantir os deveres e direitos impostos pela lei.

O estudo entrevistou 508 companhias de diferentes portes e nichos de atuação em todo país. Interessante notar que, dentre as firmas com mais de 100 funcionários, 72% pretendem contratar pessoas ou consultoria especializada para adequar a estrutura da empresa à lei, pretendem, assim, custear a contratação de terceiros. Já as empresas com menos de 100 funcionários (talvez por questões orçamentárias) tendem a utilizar o próprio quadro atual de funcionários para realizar essa adequação e, portanto, não têm a intenção de custear a contratação de terceiros para essa restruturação.

É nesse sentido que a própria LGPD, em seu art. 55-J, XVIII, dispõe que as Pequenas e Microempresas (PMEs) receberão tratamento simplificado e diferenciado, inclusive quanto a prazos, para que possam se adequar à mencionada lei. Esses mesmos direitos se estendem às iniciativas de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação. Veja, pois, que mesmo havendo ônus de custos, a própria LGPD confere procedimentos simplificados e diferenciados para as PMEs, justamente para que estas não sejam fortemente lesadas ao ponto de arruinar seus negócios. Em cenário em que as PMEs geram 27% do PIB do país e representam 99% dos estabelecimentos brasileiros[3], como informa pesquisa do SEBRAE, em uma visão macro, a vigência da LGPD não representava perigo às empresas brasileiras. Com a

---

[1] VALOR ECONÔMICO. Câmara avalia adiar lei de proteção de dados, após decisão do Senado, 6 abr. 2020. Disponível em: https://valor.globo.com/empresas/noticia/2020/04/06/camara-avalia-adiar-lei-de-protecao-de-dados-apos-decisao-do-senado.ghtml. Acesso em: 27 jun. 2020.

[2] SERASA EXPERIAN. 85% das empresas declaram que ainda não estão prontas para atender às exigências da Lei de Proteção de Dados Pessoais. Serasa Experian,, 8 ago. 2019. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian. Acesso em: 12 jun. 2020.

[3] SEBRAE. Pequenos negócios em números. Disponível em: https://m.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD#:~:text=COMPARTILHAR&text=Os%20pequenos%20neg%C3%B3cios%20empresariais%20s%C3%A3o,e%20pequenas%20empresas%20(MPE). Acesso em: 12 jun. 2020.

prorrogação, o Brasil se torna um país atrasado na inserção na economia global digital, pois, sem um marco regulatório de proteção aos dados, o país fica em desconformidade com boa parte das democracias ocidentais.

O impacto, portanto, também é comercial: as empresas brasileiras, com a prorrogação da lei, encontrarão dificuldades em realizar intercâmbio de dados com vistas a relações comerciais, uma vez que a falta de uma lei de proteção de dados no Brasil afastará competitividade e credibilidade nas relações com companhias internacionais (MANSO, 2020); gera-se insegurança às relações comerciais de serviços que necessitam do fluxo de dados, como menciona o Ministério Público Federal em nota técnica[1]. O Regulamento Geral de Proteção de Dados da União Europeia (RGPD) [2], por exemplo, exige que o país de destino do fluxo de dados esteja adequado ao regulamento com todas as diretrizes de segurança aos dados e, visto que a LGPD está em conformidade com o marco normativo europeu, sua prorrogação impedirá oportunidades de negócio entre empresas brasileiras e europeias no cessar da crise pandêmica.

Argumentar-se-ia que as empresas brasileiras no atual momento (2020) poderiam sofrer encargos desproporcionais relativos às multas previstas na LGPD por tratamento indevido de dados e, assim, dificultando sua recuperação econômica. Mesmo com a prorrogação da LGPD, há no Brasil marcos normativos que conferem responsabilidade civil às empresas por possíveis prejuízos e dispêndios causados a consumidores quando, na prestação serviços, indevidamente tratarem dados – o Código de Direito do Consumidor, o Marco Civil da Internet, a própria Constituição Federal são exemplos.

Em suma, esses marcos já dispõem sobre responsabilização civil por danos causados a consumidores ou terceiros no desenvolvimento de atividades com dados (FILHO, 2020). Daí que em caso de dano causado por manipulação, compartilhamento indevido ou algum tipo de acidente com os dados no desenvolvimento das atividades, que ocorrerem em contexto de pandemia, ensejará responsabilização do controlador. O próprio Marco Civil da Internet prevê "multa de até 10% do faturamento do grupo econômico no Brasil" em caso de qualquer acidente que ocorra desde a coleta, armazenamento, guarda até o tratamento de dados pessoais (art.11 e 12, II).

A prorrogação da LGPD, na realidade, representará insegurança jurídica, dado que as empresas serão responsabilizadas a partir de leis esparsas: os juízes poderão aferir

[1] Disponível em: https://www.conjur.com.br/dl/nota-tecnica-lgpd.pdf. Acesso em: 12 jun. 2020.
[2] RGPD, 101

punições a partir de princípios e normas abstratas, ao passo que os tribunais poderão ter entendimentos divergentes sobre a interpretação das leis (FILHO, 2020).

A criação da ANDP, portanto, é de suma importância para que se evite insegurança jurídica: esta possui em suas atribuições, elaborar diretrizes para a aplicação da lei, além de indicar requisitos necessários e padrões para o cumprimento, isto é, difundir parâmetros a serem obedecidos pelos indivíduos, instituições privadas e públicas. A ANPD (que já haveria de ter sido efetivamente implementada[1]) como principal autoridade brasileira de proteção de dados poderá fornecer parâmetros para os tribunais se nortearem e uniformizarem o entendimento para a aplicação de multas (55-J LGPD).

Sem a uniformização dessa interpretação, o judiciário poderá aplicar sanções não adequadas, sujeitando as empresas ao pagamento de multas impostas a partir de interpretações arbitrárias, ao passo que os empresários também terão dificuldades em saber quais modelos e parâmetros seguir para estruturar suas atividades de tratamento de dados, estarão sujeitos, dessa forma, a modelos criados a partir de interpretações não especializadas sobre o tema.

Em âmbito de relações governamentais, pode-se pensar até em repercussões na esfera criminal, pois a LGPD confere reciprocidade de transferência de dados com vistas a subsidiar procedimentos criminais com outros países (art 33, III) e, a partir do adiamento da lei, essa cooperação internacional poderá ficar prejudicada.

Em contexto de isolamento social, período em que o trabalho remoto se acentua drasticamente e instituições particulares, assim como públicas, passaram a utilizar plataformas on-line para continuar com seus serviços, a vigência da LGPD novamente se mostra necessária.

O Senado Federal, para ilustrar, utilizou dos serviços da plataforma Zoom[2] para realizar seus trabalhos legislativos durante o período de isolamento, essa mesma plataforma admitiu falhas de segurança que comprometeram a privacidade de seus usuários[3]. A proteção de dados, no atual contexto de pandemia (2020), configura-se

[1] Ver Art. 65, I; LGPD

[2] Orientações para implantação e operação do sistema de deliberação remota do Senado Federal, p. 1-41. Disponível em: http://www.senado.leg.br/senado/hotsites/sdr/pdf/SDR_SF_DS_V162.pdf. Acesso em: 12 jun. 2020.

[3] Nota oficial da plataforma Zoom. Disponível em: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/. Acesso em: 12 jun. 2020.

essencial: dados sensíveis são passíveis de discriminação e podem ser obtidos por meio das falhas de privacidade das plataformas digitais.

Em momento que a telemedicina passa a vigorar no Brasil para atender pacientes em isolamento[1], em que as plataformas digitais passam a coletar indiscriminadamente dados de saúde (portanto sensíveis) das pessoas, sem ao menos terem passados por testes de segurança oficiais validando suas defesas contra invasões digitais, torna-se essencial o reforço pela aplicação da LGPD inclusive para averiguar que essas empresas realizem a exclusão dos dados pós-pandemia.

6. CONCLUSÃO

Depreende-se, portanto, do presente artigo, que o marco normativo da Lei Geral de Proteção de Dados ao garantir que o consentimento seja uma manifestação livre, informada, inequívoca e com vistas a uma finalidade específica, procura garantir que haja usufruto substancial do consentimento, posto que as pessoas ao anuírem pelo fornecimento dos seus dados, saberiam o porquê e quais os procedimentos que serão utilizados para tratar suas informações. Muito embora o marco normativo estabeleça a necessidade do consentimento e, consequentemente, da fruição da autodeterminação informativa, as razões pelas quais induzem as pessoas a não assentirem pelo provimento de seus dados, como demonstra as pesquisas empíricas suscitadas no item 3.1, não se situam associadas a uma real percepção dos desarraigamentos na esfera da privacidade.

A carência sobre entendimento de segurança digital se verifica reconhecível quando os indivíduos confrontados por ofertas econômicas estão mais suscetíveis a anuírem pelos seus dados, ao passo que, no momento em que alcançam a compreensão da magnitude de previsões que podem ser realizadas, a partir desses mesmos dados, sobre a vida privada, recuam dessa anuência.

O impasse se exacerba ainda quando os termos de compromisso das plataformas digitais não são amoldados à vista de uma linguagem inteligível; na prática são textos que requerem conhecimento técnico e excluem as pessoas de uma completa cognição. Importante destacar o consentimento em período de Covid-19 quando (i) aplicativos de

[1] Câmara aprova projeto que autoriza telemedicina durante pandemia de coronavírus. Disponível em: https://www.camara.leg.br/noticias/648408-CAMARA-APROVA-PROJETO-QUE-AUTORIZA-TELEMEDICINA-DURANTE-PANDEMIA-DE-CORONAVIRUS. Acesso em: 12 jun. 2020.

telefones celulares, não submetidos a um processo de segurança oficial, estão sendo produzidos para ajudar no rastreamento de identificação de portadores da COVID-19 – *digital tracking*- e, as pessoas sensibilizadas ante o número expressivo de mortes pelo desarraigamento da infecção, estão dispostas a aceitar os termos dos aplicativos, ceder seus dados – sem conceber as decorrências do ato – por uma expectativa de salvaguarda.

O fundamento de proteção à saúde coletiva constitui estímulo para que os indivíduos acordem pelo provimento de suas informações. A problemática do consentimento se expressa quando se delega exclusivamente aos titulares dos dados pessoais o ônus de protegê-los, posto que, em contexto de fluxo informacional, as pessoas são parte do grupo frágil da relação assimétrica (BIONI, 2019).

Posteriormente, o artigo traçou as possibilidades pelas quais o governo pode coletar dados sensíveis, inclusive sem consentimento do titular, com desígnios de verificar como o governo brasileiro atuou nesse sentido e como essas ações podem influenciar na supressão ao direito de proteção de dados.

Concluiu-se desse aspecto que (i) as ações governamentais carecem em fornecer detalhes sobre o tratamento desses dados (como observado no caso do governo de São Paulo), pois (ii) mesmo que os dados de geolocalização (coletados e utilizados para mapear a rota do vírus) estejam supostamente sendo submetidos a um processo de anonimização e agregação, deve-se fornecer detalhes desses processos que, como observado no item 4.2, não podem ser compreendidos como isentos de insegurança.

A LGPD, ao não considerar dado anonimizado como dado pessoal, estabelece que se o processo de anonimização pelo qual o dado fora submetido for incipiente, esse dado por sua vez tornar-se-á pessoal novamente. Daí que um detalhamento desses processos pelos governos estaduais é fundamental para garantir que o processo de anonimização é seguro e impede a identificação direta ou indireta do seu titular.

A prorrogação da LGPD passou, devido à crise econômica, ser pauta de discussão no Congresso Nacional. Sobre fundamento de proteção econômica às atividades empresariais, parlamentares e setores da indústria alegam que as empresas brasileiras não possuem orçamento para adequar sua estrutura às particularidades da LGPD.

Como disposto no item 5, de fato, as empresas que já não estavam adequadas à LGPD (mesmo após quase dois anos da promulgação da lei), com a crise no setor econômico estarão inaptas a se reestruturarem. Conquanto, prorrogar a lei agravará esse problema uma vez que, além da LGPD já prever procedimentos especiais para as PMEs,

(i) as empresas de diferentes nichos e tamanhos, pós-período de isolamento social, encontrarão mais dificuldades em se adaptarem visto os reflexos gerados da crise; (ii) depararão com dificuldades em firmar negócios internacionais que necessitam de fluxo de informações; (iii) estarão suscetíveis aos reflexos da insegurança jurídica provocada pela prorrogação; e (iv) não encontrarão parâmetros oficiais para tratar dados pessoais sem a implementação da ANPD.

Delongar a *vacatio legis* da lei, adido pela ausência da ANPD, suscitará também risco no ambiente digital, posto que os fluxos de informações transmitidos por meio das plataformas digitais, acentuados pelo teletrabalho e a telemedicina, carecerão de fiscalização pela ANPD.

Veja, pois, que a vigência da LGPD se evidencia como notadamente essencial para a proteção da democracia do país, ao passo que não apenas as instituições privadas, mas os poderes da república estão sujeitos a violações na esfera de proteção de dados, passíveis de terem dados sensíveis, assim como informações sigilosas, comprometidas pela incipiência na segurança das plataformas digitais.

REFERÊNCIAS BIBLIOGRÁFICAS

ARDUINI, Laís. As consequências da prorrogação da LGPD para as startups. **Nunes Duarte & Maganha**, 4 maio 2020. Disponível em: https://ndmadvogados.com.br/artigos/consequencias-da-prorrogacao-da-lgpd-para-startups. Acesso em: 21 maio 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. rev., atual., reformul Rio de Janeiro: Forense, 2019. Livro. (1 recurso on-line). ISBN 9788530988777. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788530988777. Acesso em: 24 jun. 2020.

BRASIL. Lei no 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 jul. 2020

BRASIL. Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 jul. 2020

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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm. Acesso em: 15 jul. 2020

BRASIL. Medida Provisória no 959, de 29 de abril de 2020. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 15 jul. 2020

BRASIL. Projeto de Lei no 1179, de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do Coronavírus (Covid-19). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141306. Acesso em: 15 jul. 2020

Cavoukian, "Privacy by Design [Leading Edge]," in *IEEE Technology and Society Magazine*, vol. 31, no. 4, pp. 18-19, winter 2012, doi: 10.1109/MTS.2012.2225459. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6387956 Acesso em: 14 jul. 2020.

DONEDA, Danilo. A proteção de dados em tempos de coronavírus: A LGPD será um elemento fundamental para a reestruturação que advirá após a crise. **JOTA**, [*S. l.*], p. S.I, 25 mar. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020. Acesso em: 27 jun. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei geral de proteção de dados. São Paulo: Revista dos Tribunais, 2019. E-book. 1 Recurso Eletrônico. ISBN 978-85-5321-9049.Disponível em:

https://signon.thomsonreuters.com/?productid=EREAD&viewproductid=EREAD&returnto=https%3A%2F%2Fproview.thomsonreuters.com%2Flogin.html&culture=pt-BR&lr=0&bhcp=1. Acesso em: 24 jun. 2020.

ERIKSON, Susan. Cell Phones ≠ Self and Other Problems with Big Data Detection and Containment during Epidemics. Medical Anthropology Quarterly Journal, Disponível em: https://anthrosource.onlinelibrary.wiley.com/doi/abs/10.1111/maq.12440. Acesso em: 14 jul. 2020

EUROPEAN UNION LAW. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 15 jul. 2020

FEDELI , Ricardo Daniel; POLLONI , Enrico Giulio Franco; PERES, Fernando Eduardo. **Introdução à Ciência da computação**. 2a edição. 2010. 270 p. Disponível em: https://www.cairu.br/biblioteca/arquivos/cc_ead/Introducao_a_Ciencia_Da_Computacao.pdf. Acesso em: 29 jun. 2020.

FILHO, Demócrito Reinaldo. Prorrogação da vigência da LGPD coloca em risco a sociedade brasileira. **ConJur**. 15 maio 2020. Disponível em: https://www.conjur.com.br/2020-mai-15/democrito-reinaldo-filho-prorrogacao-lgpd-risco-sociedade. Acesso em: 28 maio 2020.

Gargarella, Roberto and Roa Roa, Jorge, Diálogo democrático y emergencia en América Latina (Democratic Dialogue and Emergency in Latin America) (June 10, 2020). Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper No. 2020-21, Disponível em: https://ssrn.com/abstract=3623812 ou http://dx.doi.org/10.2139/ssrn.3623812 Acesso em: 14 jul. 2020.

HUMAN RIGHTS WATCH. Governments Should Respect Rights in COVID-19 Surveillance. **Human Rights Watch**, 2 abr. 2020. Disponível em: https://www.hrw.org/news/2020/04/02/governments-should-respect-rights-Covid-19-surveillance. Acesso em: 29 maio 2020.

HUMAN RIGHTS WATCH. Mobile Location Data and Covid-19: Q&A. **Human Rights Watch**. 13 maio 2020. Disponível em: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-Covid-19-qa. Acesso em: 29 maio 2020

Ienca, M., Vayena, E. On the responsible use of digital data to tackle the COVID-19 pandemic. *Nat Med* **26,** 463–464 (2020). Disponível em: https://doi.org/10.1038/s41591-020-0832. Acesso em: 11 jun. 2020

LANDAU, Susan. Location Surveillance to Counter COVID-19: Efficacy Is What Matters. **Lawfare**, p. S.I, 25 mar. 2020. Disponível em: https://www.lawfareblog.com/location-surveillance-counter-Covid-19-efficacy-what-matters. Acesso em: 12 maio 2020.

LAPIN. Nota Técnica PLS 1.179/2020: Contra a prorrogação da LGPD pelo art.21 do PLS 1.179/2020. **Laboratório de Pesquisa em Direito Privado e Internet da Universidade de Brasília (Lapin-UnB)**, p. 1-12. 2020. Disponível em: https://www.lapin.org.br/. Acesso em: 13 jun. 2020.

LAPIN. Uso de Dados de Localização No Combate Ao Covid-19: Considerações sobre privacidade e tutela da saúde durante a pandemia. **Laboratório de Pesquisa em Direito Privado e Internet da Universidade de Brasília (Lapin-UnB)**, p. 1-19, 14 maio 2020. Disponível em: https://www.lapin.org.br/. Acesso em: 9 jun. 2020.

LILLA, Paulo. Prorrogação da vigência da LGPD: ilusões e incertezas em meio à Covid-19. **ConJur**, 21 abr. 2020. Disponível em: https://www.conjur.com.br/2020-abr-21/paulo-lilla-ilusoes-incertezas-prorrogacao-lgpd. Acesso em: 6 maio 2020.

LYON, David. The Culture of Surveillance: Watching as a Way of Life. Polity Press, 2018. 172 p.

MANSO, Carla Prado. Adiamento da LGPD pode trazer sérios riscos para os negócios brasileiros. **CIO Magazine Brasil**, 2 jun. 2020. Disponível em: https://cio.com.br/adiamento-da-lgpd-pode-trazer-serios-riscos-para-os-negocios-brasileiros/#:~:text=Por%20Carla%20Prado%20Manso*&text=O%20novo%20prazo%20de%20vig%C3%AAncia,inicialmente%20aprovado%20pelo%20Governo%20Federal. Acesso em: 27 jun. 2020.

MCDONALD, Sean Martin. Ebola: a Big Data Disaster. India: The Centre for Internet and Society, 1 mar. 2016. Disponível em: https://cis-india.org/papers/ebola-a-big-data-disaster. Acesso em: 14 jul. 2020

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. E-book. (1 recurso on-line). (IDP. Linha de pesquisa acadêmica). ISBN 9788502218987. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788502218987. Acesso em: 24 jun. 2020.

MENDONÇA, Suzana. A autodeterminação informativa no contexto de proteção de dados pessoais. **ConJur**. 20 out. 2019. Disponível em: https://www.conjur.com.br/2019-out-20/suzana-mendonca-autodeterminacao-informativa-protecao-dados. Acesso em: 12 maio 2020.

PASQUALE, Frank. **The Black Box Society – The Secret Algorithms That Control Money and Information**. Harvard University Press, 2016. 320 p.

PINHEIRO, Patríci Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2018. Livro. (1 recurso on-line). ISBN 9788553608324. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788553608324. Acesso em: 24 jun. 2020.

SCHWARTZ, Paul. Protecting privacy on COVID-19 surveillance apps. **Berkeley Blog**, [*S. l.*]. 14 maio 2020. Disponível em: https://blogs.berkeley.edu/2020/05/14/protecting-privacy-on-Covid-19-surveillance-apps/. Acesso em: 24 jun. 2020.

THALER, Richard; SUNSTEIN, Cass. Nudge: Como tomar melhores decisões sobre saúde, dinheiro e felicidade.Objetiva; Edição:, 2019. 408 p.