REVISTA JURÍDICA NÚCLEO DE ESTUDO LUSO-BRASILEIRO FACULDADE DE DIREITO DA ULISBOA

Revista Jurídica NELB

Jus Scriptum

REVISTA JURÍDICA
NÚCLEO DE ESTUDO LUSO-BRASILEIRO
FACULDADE DE DIREITO DA ULISBOA
ANO 16 | VOLUME 6 | NÚMERO 1 | 2021

NELB
Núcleo de Estudo Luso-Brasileiro

Revista Jurídica
NELB

Jus Scriptum






NELB
Núcleo de Estudo
Luso-Brasileiro

jusscriptum.pt

REVISTA JURÍDICA
NÚCLEO DE ESTUDO LUSO-BRASILEIRO
FACULDADE DE DIREITO DA ULISBOA
Ano 16 • Volume 6 • Número 1
Abr/Jun 2021 • Lisboa – Portugal
Periodicidade Trimestral
ISSN 1645-9024

REVISTA JURÍDICA
NÚCLEO DE ESTUDO LUSO-BRASILEIRO
FACULDADE DE DIREITO DA ULISBOA
Ano 16 • Volume 6 • Número 1
Abr/Jun 2021 • Lisboa – Portugal
Periodicidade Trimestral
ISSN 1645-9024

A PROTEÇÃO DE DADOS PESSOAIS NA PANDEMIA DE COVID-19: BREVES NOTAS SOBRE CONTACT TRACING APPS E O DIREITO À PRIVACIDADE NA ERA DA VIGILÂNCIA.

THE PERSONAL DATA PROTECTION IN COVID-19 PANDEMIC: SHORT NOTES ABOUT CONTACT TRACING APPS AND THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE

Felipe Müller Dornelas[1]

SUBMISSÃO: 24 DE MARÇO DE 2020
APROVAÇÃO: 25 DE JUNHO DE 2021

Vivenciamos atualmente a escalada da vigilância massiva sobre quase todos os aspectos da vida corriqueira. Os dados pessoais são fontes inesgotáveis de informações e, portanto, almejado pelos governos e empresas de tecnologia. Em adição, enfrentamos tempos de pandemia de COVID-19 onde se enxerga a tecnologia como ferramenta de combate ao vírus, sendo os aplicativos de rastreio de contágio fundamental aliado. Porém, estes apps lidam com inúmeros dados pessoais sensíveis, altamente cobiçados, e o direito à privacidade tende a ficar em segundo plano. Assim, o presente artigo pretende traçar breves notas para desvendar o estado atual de coisas envolvendo a proteção de dados sensíveis em meio ao cenário pandêmico - e massivamente monitorado-, a partir do estudo dos Contact Tracing Apps e as principais tecnologias empregadas nestes, bem como se há proporcionalidade entre o uso e a finalidade de combate ao COVID-19. Palavras-Chave: Contact Tracing Apps; Vigilância; Privacidade; Proteção de Dados Pessoais; COVID-19.

We are currently experiencing the escalation of massive surveillance about almost every single aspect of our lives. The personal data are inexhaustible sources of informations and, therefore, desired by governments and tech companies. In addition, we are living COVID-19 pandemic times where the technology is seen as a tool to fight the virus, and the contact tracing apps are important allies. However, theses apps stores a huge amount of sensitive personal data, highly desired, and the right to privacy tends to take low priority. Thus, this article intends to draw brief notes in order to unveil the status quo about sensitive data protection into a pandemic scenario – with mass surveillance- from the study of Contact Tracing Apps and the tech-

1 Bacharel em Direito pelo Instituto Vianna Júnior. Advogado inscrito na OAB/MG sob o número 130.265. Mestrando em Ciências Político-Jurídicas pela Universidade de Lisboa, Portugal; Pós-Graduado em Direito Processual Lato Sensu pela Universidade Federal de Juiz de Fora-UFJF; Pós-graduado em Direito Médico pelo Centro de Ensino Renato Saraiva-CERS; MBA em Gestão da Saúde pela Universidade São Camilo.

nologies assembled into the them, as well if there is a proportionality between the use and the purpose of facing COVID-19. Keywords: Contact Tracing Apps; Surveillance; Right to Privacy; Personal Data Protection; COVID-19.

1. Introdução

Os dados pessoais e a privacidade ganharam particular relevância no debate jurídico contemporâneo, pois constituem verdadeira matéria-prima para o capitalismo de vigilância e a sociedade da informação, uma vez que, através dos dados pessoais, há o fomento da indústria de tecnologia, possibilitando o desenvolvimento e a criação de produtos e serviços cada vez mais inteligentes, modernos e personalizados.

Na paradigmática obra "A Era do Capitalismo de Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder", a Socióloga Soshana Zuboff[2] revela o estado de coisas da vigilância massiva exercida sobre as pessoas nos tempos atuais -nomeadamente realizada por particulares - por meio das grandes empresas de tecnologia, funcionando os dados pessoais como verdadeiros *comodities* dos "novos tempos", cunhando tal movimento de Capitalismo da Vigilância.

Acrescenta-se a isto o fato de sermos solapados, em março de 2020, por uma crise epidemiológica de COVID-19, diante da qual as nações unem esforços para encontrar mecanismos de contenção e eliminação do vírus, valendo-se da tecnologia disponível para otimizar esses objetivos.

Por consequência, a ciência epidemiológica atrelada à tecnologia dos *smartphones*, especialmente via aplicações de rastreio de contágio - apesar de já utilizados anteriormente no combate a outros vírus, como para rastreio da *influenza*[3]

2 ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder. Traduzido por Luis Filipe Silva e Miguel Serras Pereira, Lisboa: Relógio D'Água, 2020.

3 "Smartphone science didn't start with COVID-19. But the pandemic has spurred researchers to fast-track citizen-science efforts that use smartphones to gather information about the disease. Volunteers can regularly log details about their symptoms, testing status and location through apps or websites For instance, data from 5 million users of Brownstein's crowdsourced tracker for influenza and COVID-19 — called Outbreaks Near Me — provided early evidence of the benefits of masking". Disponível em <https://www.nature.com/articles/d41586-021-01253-y>. Acesso em: 16, jun. 2.021

e o Zika virus[4]-, despontou como eficaz instrumento no combate ao COVID-19.

Nesta toada, as referidas aplicações fornecem subsídios fáticos aos governantes e autoridades sanitárias para que estas possam concretizar políticas de saúde pública na contenção à pandemia, especialmente pela facilidade e velocidade em coletar, armazenar e sistematizar uma quantidade enorme de dados pessoais que serão tratados e transformados em inteligência. Entretanto, várias questões jurídicas são levantadas pelo uso destes aplicativos, estando a temática da privacidade e da proteção aos dados pessoais no centro deste debate.

Assim, esta pesquisa busca traçar linhas gerais sobre a relação existente entre os dados pessoais e o emprego da tecnologia de *contact tracing apps*, tais como conceito e tecnologias empregadas, bem como correlacioná-los com o direito à privacidade, à proteção de dados pessoais e a máxima da Proporcionalidade, para compreender a viabilidade jurídico-constitucional do uso destas aplicações de rastreio de contágio no combate ao COVID-19 dentro de um contexto de vigilância.

2. A vigilância em massa e no contexto pandêmico de COVID-19

Os Estados Unidos da América, sobretudo após os eventos terroristas ocorridos em 11 de setembro de 2001, passaram a intensificar e aprimorar estratégias de vigilância e espionagem - em uma forma até então sem precedentes - a pretexto de combater o terrorismo e prevenir novos atentados. Porém, conforme trazido à tona pelo ex-analista da *National Security Agency (NSA)*, Edward Snowden[5], essa vigilância massiva extrapolou os limites da razoabilidade e acabou por violar direitos dos cidadãos comuns, que nada tinham relação com terrorismo e estavam sob vigilância em todos os

4 Chen, H., Yang, B. O., PEI, H., & LIU, J. (2019). Next Generation Technology for Epidemic Prevention and Control: Data-Driven Contact Tracking. IEEE, p. 2633–264 apud JUNQUILHO, Tainá Aguiar. Prós e contras do contact tracing, ou monitoramento epidêmico. In: Revista do Consultor Jurídico, 15 de julho de 2020. Disponível em <https://www.conjur.com.br/2020-jun-15/taina-junquilho-pros-contras-contact-tracing#_ftn3>. Acessado em 17, de jun. 2.021.

5 GREENWALD, Glenn. Sem lugar para se esconder Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante Tradução de Fernanda Abreu, 2014. p.5.

aspectos.

A partir desse novo cenário social e tecnológico, houve um crescimento e desenvolvimento de novas formas e tecnologias de monitoramento e vigilância em massa de pessoas, o que despertou interesse igualmente pelo setor privado.

Atentas ao potencial de oportunidades, portanto, as grandes empresas privadas de tecnologia prontamente perceberam o quão valioso consistia a coleta, análise e sistematização de informações obtidas da vigilância, ou seja, o tratamento de dados pessoais e suas utilizações potencialmente mercadológicas, tais como, *v.g* melhorias nas campanhas de marketing com personalização e *profiling*, acesso a novos possíveis clientes, personalização de produtos e serviços e, consequentemente, a nova perspectiva de lucratividade.

Assim, a rede de vigilância que incialmente era utilizada pelo Estado para o suposto combate ao terrorismo acabou por se desvirtuar ao longo do tempo e encontrou seu *locus* também no setor privado, alavancando uma indústria que chega a valer trilhões de dólares no mercado[6]. Portanto, surgiu, especialmente no Vale do Silício na Califórnia - nascedouro das *Big Techs* -, uma nova forma de capitalismo, com fulcro na vigilância, coleta e tratamento dos dados de pessoas, inicialmente à mercê de qualquer regulação, consentimento e observância do direito fundamental à privacidade e proteção de dados.

Explica-nos Zuboff (2020) que o *Capitalismo da Vigilância*[7] partiu da mera coleta de dados pessoais de usuários - que ocorria principalmente por meio de redes sociais - e posterior negociação para empresas interessadas, especialmente para fins de marketing direcionado, para uma sistematização preditiva dos referidos dados, com inteligência artificial, capaz de antever comportamentos humanos e, dessa forma, induzir os usuários a consumos personalizados. Por isso, tal prática antiética, *ipsis litteris* "reivindica unilateralmente a experiência humana como matéria-prima gratuita que

6 Em 16 de janeiro de 2.020 as 5 big techs Apple, Facebook, Microsoft, Amazon e Alphabet chegaram a valer US$ 4,795 trilhões. Neste sentido, conferir >https://www.poder360.com.br/economia/a-evolucao-do-valor-de-mercado-das-big-techs/>. Acessado em 18. Jun, 2021.

7 ZUBOFF. Op cit., p.1 "A Definição" 1. Uma nova ordem econômica que se apropria da experiência humana e a usa de forma encoberta como matéria-prima em práticas comerciais de extração, previsão e venda.

transforma em dados comportamentais".[8]

Em síntese, o *modus operandi* do Capitalismo de Vigilância consiste fundamentalmente na coleta, utilização e venda de dados pessoais, sem consentimento, com objetivo de lucro não autorizado pelos usuários/clientes via marketing direcionado e indução ao consumo.

Como bem assevera (BIONI, 2021, p.5). esta nova forma de organização da sociedade, baseada na tecnologia, tem a sua centralidade consubstanciada na coleta para tratamento de dados pessoais visando a transformação destes em informação que, por conseguinte, impulsiona todo um sistema econômico: "no estágio atual, a sociedade está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da econômica, substituindo os recursos que outrora estruturavam as sociedades agrícola, industrial e pós-industrial"[9]

Assim, a evolução tecnológica proporcionou o tratamento de uma gama infindável de dados, em velocidade jamais vista, modificando a estrutura das relações sociais para uma nova era, onde encurtam-se as distâncias de tempo e espaço e, consequentemente, as relações políticas, econômicas e culturais tomam nova forma. No entendimento de Paesani (2010) houve um "encolhimento" do mundo, por meio da compreensão do espaço-tempo[10].

À evidência, é inimaginável a quantidade de dados pessoais que as *big techs* têm sobre os seus clientes, bem como é quase impossível dizer o que elas não sabem sobre nós, como nosso e-mail, SMS, chamadas telefônicas, hábitos de navegação, histórico de compras e pesquisas etc. Neste cenário, soma-se o ambiente de vigilância pandêmica de COVID-19, uma doença respiratória aguda causada pelo SARS-CoV-2.[11]

8 Ibidem, p. 22.

9 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento – e. ed. – [3. Reimpr.] – Rio de Janeiro: Forense, 2021. p.5.

10 PAESANI, Liliana Minardi. A publicidade móvel e a vulnerabilidade do consumidor. In: MORATO, Antonio Carlos; NERI, Paulo de Tarso (org). 20 anos do Código de Defesa do Consumidor: estudos em homenagem ao professor José Geraldo Brito. São Paulo: Atlas, 2010. p. 183-188 apud BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento – e. ed. – [3. Reimpr.] – Rio de Janeiro: Forense, 2021. p.6.

11 O vírus foi identificado pela primeira vez em Wuhan, na província de Hubei, República Popular da China, em 1 de dezembro de 2019, mas o primeiro caso foi reportado em 31 de dezembro do mesmo ano. Disponível em: <https://pt.wikipedia.org/wiki/Pandemia_de_COVID-19>. Acesso em: 18, jan. 2.021

Obviamente, ao juntar essas situações, surgiram questionamentos acerca das medidas de vigilância sanitária no combate ao COVID-19 e a proteção de dados pessoais ligados à saúde. De início, na China, primeiro epicentro de disseminação, o governo se utilizou de dados pessoais da população para conter aglomerações[12] e, nessa toada, Rússia[13] e Israel[14] igualmente tiveram debates sobre o tema após tomarem medidas que envolviam o monitoramento de seus cidadãos.

Evidentemente, a tecnologia passou a assumir papel central na instrumentalização dos esforços para maximizar e viabilizar novas soluções para crise pandêmica, dentre as quais perpassam desde a criação das vacinas e fármacos altamente modernos, *v.g.*com utilização de terapias de RNA, bem como o monitoramento eletrônico de aglomerações, a utilização de *drones* para acelerar atendimentos e providencias, impressões 3D para peças em hospitais, o pagamento via cartões *contactless*, as aplicações de rastreio de contágio, dentre outras.

Vaishya *et al* (2020)[15], elencam sete possíveis usos e consequências da inteligência artificial na ajuda à pandemia, quais sejam: *i)* Detecção e diagnóstico precoce da infecção; *ii*) Projeção de número de casos e de mortalidade; *iii)* Desenvolvimento de medicamentos e vacina; *iv)* Redução da carga horária dos profissionais da saúde com a utilização, por exemplo, de robôs para limpeza e esterilização de quartos de hospital; *v)* Análise preditiva; *vi)* Monitoramento do tratamento; e *vii)* Rastreamento de contato dos indivíduos.

Neste espectro, as iniciativas tecnológicas desenvolvidas a fim de aprimorar os rastreamentos de sintomas, contatos e deslocamentos de pessoas, considerados componentes importantes para subsidiar estratégias de saúde pública,

12 Disponível em: <https://policyreview.info/articles/news/data-protection-times-covid-19-risks-surveillance-brazil/1462>. Acesso em: 17, jan. 2.021.

13 Disponível em: <https://www.themoscowtimes.com/2020/03/25/coronavirus-outbreak-is-major-test-for-russias-facial-recognition-network-a69736>. Acesso em: 17, jan. 2.021.

14 Disponível em: <https://edition.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html>. Acesso em: 17, jan., 2.021.

15 Vaishya, R., Javaid, M., Haleem, I., & Haleem, A. (2020). Diabetes & Metabolic Syndrome: Clinical Research & Reviews Arti fi cial Intelligence (AI) applications for Covid-19 pandemic. 14, 337–339. https://www.sciencedirect.com/science/article/pii/S1871402120300771?via%3Dihub apud JUNQUILHO, Tainá Aguiar. Prós e contras do contact tracing, ou monitoramento epidêmico. In: Revista do Consultor Jurídico, 15 de julho de 2020. Disponível em <https://www.conjur.com.br/2020-jun-15/taina-junquilho-pros-contras-contact-tracing#_ftn3>. Acessado em 17, de jun. 2.021.

monitoramento e vigilância de contágios pelos governos, despontaram com grande vigor, levando o assunto sobre a privacidade, proteção de dados e as consequentes vantagens e desvantagens do *Contact Tracing Apps* ao centro do debate público.

Os aplicativos supramencionados, para terem eficácia, dependem de grande adesão da população e, consequentemente, de um enorme volume de tratamento de dados pessoais sensíveis, questões que suscitam debate acerca da privacidade e proteção de dados pessoais do utilizador, tais como a quantidade de dados necessários para atingir a finalidade almejada, a possibilidade de identificação dos usuários, o tratamento vinculado ao objetivo finalístico, bem como a sua eficácia no enfrentamento à pandemia de COVID-19.

Para ilustrar o tipo de problema que estamos a enfrentar acerca da privacidade e uso de alternativas para combate à pandemia de COVID-19, recentemente o Supremo Tribunal Federal brasileiro foi instado a manifestar-se sobre a compatibilidade da Medida Provisória nº 954 de 2020 que dispunha sobre o compartilhamento de dados por empresas de telecomunicações com o Instituo Brasileiro de Geografia e Estatística-IBGE.

Ocorre que, em abril de 2020 o poder executivo, dispondo da prerrogativa que a Constituição brasileira de 1988 lhe faculta, de legislar através de Medida Provisória[16], em casos de matéria de relevância e que exija urgência, editou a MP nº 954 de 2020 autorizando o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística-IBGE, para fins de suporte à *produção estatística oficial* durante a situação de emergência de saúde pública de importância internacional decorrente do novo coronavírus.

A MP 954/2020 determinava que, durante a emergência de saúde decorrente do COVID-19, as empresas de telefonia fixa e móvel deveriam fornecer ao IBGE os dados pessoais dos seus clientes, tais como a relação dos nomes, números de telefone e endereços, e estas informações seriam utilizadas para a *produção das estatísticas de cunho oficial*.

16 CRFB - Art. 62. Em caso de relevância e urgência, o Presidente da República poderá adotar medidas provisórias, com força de lei, devendo submetê-las de imediato ao Congresso Nacional

Atentos para vigilância desproporcional sobre os dados pessoais que a referida legislação poderia impor aos brasileiros, foram ajuizadas as ações diretas de inconstitucionalidade nºs. 6.387, 6.388, 6.389, 6.390 e 6.393, cujo pedido resume-se na inconstitucionalidade dos arts. 2º, *caput* e §§ 1º a 3º e 3º[17].

Nos termos das ações diretas de inconstitucionalidade, o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), visando a produção de estatística oficial durante a pandemia de COVID-19, violaria a dignidade da pessoa humana, a intimidade, a vida privada, a honra e a imagem das pessoas bem como o sigilo dos dados, a privacidade e autodeterminação informacional, ao submeter o cidadão brasileiro à uma recolha e tratamento de dados pessoais sem delimitar precisamente o objeto da estatística a ser produzida, a finalidade específica ou a sua amplitude, ensejando uma vigilância indesejada e desproporcional.

Em sede de cognição sumária, a Relatora do caso, Ministra Rosa Weber, concedeu medida liminar *ad referendum*, que depois fora corroborada pelo Plenário do STF, para suspender a eficácia da referida MP 954/2020, entendendo que esta exorbitou dos limites traçados pela Constituição, pois a lei diz que os dados serão utilizados exclusivamente para a *produção estatística oficial* sem delimitar o objeto da estatística a ser produzida, a finalidade específica ou a sua amplitude, padecendo de desproporcionalidade. Outrossim, a MP não trouxe mecanismos técnico ou administrativo para proteger os dados pessoais de acessos não autorizados, vazamentos

17 MPV 954/2020 - Art. 2º As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas. § 1º Os dados de que trata o **caput** serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. § 2º Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o **caput.** Art. 3º Os dados compartilhados: I - terão caráter sigiloso; II - serão usados exclusivamente para a finalidade prevista no § 1º do art. 2º; e III - não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial, nos termos do disposto na Lei nº 5.534, de 14 de novembro de 1968. § 1º É vedado à Fundação IBGE disponibilizar os dados a que se refere o **caput** do art. 2º a quaisquer empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos. § 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no **caput** do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.

acidentais ou utilização indevida.[18]

> Em importante trecho de seu voto, a Min. Weber, parafraseando Clarissa Long, em estudo publicado pela Columbia Law School Books, assim alerta sobre a importância de coibir a vigilância indevida sobre o cidadão: A história nos ensina que uma vez estabelecidos, é improvável que poderes governamentais de vigilância e coleta de dados de seus cidadãos e residentes retrocedam voluntariamente. E a história também tem nos ensinado que uma vez que dados são coletados para um propósito, é muito difícil evitar que sejam usados para fins outros não relacionados. (...) Sempre haverá a próxima pandemia em algum momento no futuro, se não de COVID-19, de algum outro agente infeccioso. Os desafios que as pandemias apresentam para a privacidade da informação não irão embora nem se atenuarão com brevidade.[19]

Portanto, este caso emblemático e recente corrobora o constante embate entre a vigilância exercida pelos governos e *big techs* e o direito à privacidade e a proteção de dados pessoais, configurando-se de vital importância lançar luz sobre este tema.

3. Contact Tracing Apps

O rastreamento de contágio por aplicativos mostrou-se instrumento relevante no combate ao COVID-19, notabilizando-se como política de saúde pública face a necessidade de obter, sistematizar e compilar dados sobre como o vírus se espalha, quando isso acontece, quem são os vetores e quem está em risco, onde o vírus tem mais incidência, para então testar e isolar indivíduos infectados, a fim de diminuir a propagação e controlar a pandemia.

Logo, na sociedade hiperconectada em que vivemos, a grande quantidade de informação e o tempo recorde que ela circula nestes aplicativos é essencial para encurtar o tempo de reação das autoridades e da população no combate ao COVID[20], o que resulta numa maior perspectiva de preser-

18 STF. Plenário. ADI 6387, ADI 6388, ADI 6389, ADI 6390 e ADI 6393 MC-Ref/DF, Rel. Min. Rosa Weber, julgados em 6 e 7/5/2020 (Info 976).

19 LONG, Clarissa; Privacy and Pandemics In PISTOR, Katharina. Law in the time of COVID-19. Columbia Law School Books, 2020. p.112. Disponível em: <https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1239&context=books>. Acesso em 19, de jun. 2021.

20 Disponível em: < https://www.ecdc.europa.eu/sites/default/files/documents/Public-health-management-people-in-contact-with-COVID19-cases_PT.pdf>. Acesso

vação de vidas. Contudo, este fato também pode significar uma grande exposição ao controle e vigilância de governos e grandes industrias da tecnologia, como já explicado no capítulo anterior.

Grosso modo, estes *Apps* funcionam a partir do *download* ou da própria atualização do sistema operacional utilizado no smartphone, de modo que o usuário que testa positivo informa tal condição ao sistema este, ao seu turno, emite notificações aos demais utilizadores que mantiveram contato com a pessoa infectada, seja com base em geolocalização (GPS), seja através de troca de "chaves" por tecnologia *Bluetooth*.

Consoante a Organização Mundial de Saúde (OMS), o rastreamento de contatos é instrumento essencial de política pública de saúde e, quando corretamente implementado e utilizado sistematicamente, pode reduzir o número de novos casos, mas tal utilização deve guardar estrita observância aos direitos fundamentais dos usuários, notadamente à privacidade[21].

Todavia, para que o rastreio de contágio via aplicativos tenha eficácia, faz-se necessário que haja acesso à internet disponível e voluntariedade das pessoas em informar eventual contaminação. Portanto, tendo em vista esse cenário, podem surgir questões jurídico-constitucionais relevantes acerca da privacidade e do tratamento dos dados sensíveis e que podem variar de acordo com o tipo de tecnologia utilizada.

Como o presente estudo não pretende esgotar todas as tecnologias disponíveis de rastreio, faremos referência ao sistema de i*)* geolocalização (GPS); *ii)* proximidade via *Bluethooth* (BT); *iii)* proximidade via *Bluetooth Low Energy* (BLE).[22]

O sistema de rastreamento via geolocalização (GPS) funciona a partir do momento em que um usuário informa estar infectado ao sistema e este realiza uma comparação entre o histórico de localização do contaminado nos últimos 14 dias com o banco de dados que abrange os históricos de

em 22, jan., 2.021.

21 World Health Organization. Contact Tracing in the context of COVID-19 (Interim Guidance) 2020. Disponível em: <https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19>. Acesso em: 17, jan., 2.021.

22 Disponível em: <https://24.sapo.pt/tecnologia/artigos/sera-a-privacidade-a-ultima-vitima-da-covid-19>. Acesso em 25, jan., de 2021.

todos os outros usuários do aplicativo, emitindo alertas para aqueles em que haja coincidência de local e horário com o infectado, noticiando o possível contato com a pessoa com infectada e a necessidade de iniciar quarentena e tomar as medidas necessárias..[23]

Porém, duas são as maiores preocupações deste tipo de tecnologia, pois submete o usuário ao constante monitoramento de itinerário, bem como o armazenamento de dados pessoais sensíveis na memória. Ou seja, em tese, há possibilidade de vigilância total através pela monitoração contínua e falta de segurança no armazenamento dos dados.

Isso ocorre pois a cada instante os movimentos de centenas de milhões de pessoas são identificados pelo sistema de geolocalização embutido em seus smartphones e permanecem armazenados na memória, tornando-se suscetíveis de serem usurpados por outros aplicativos, *hackeados* ou tratados de forma ilegal, como ocorreu em Singapura, onde mais de 80% da população aderiu ao aplicativo de rastreio "Trace-Together"- que utiliza tecnologia via GPS-, mas o tratamento desses dados não se limitou ao combate ao COVID-19, sendo utilizados pelo governo também para investigações criminais[24].

À evidência, a tecnologia em comento traz graves problemas relacionados à privacidade do usuário, por utilizarem dados em excesso e armazenados de forma não muito segura, sujeitos à serem usurpados e, portanto, demonstra padecer de proporcionalidade entre o fim almejado e o meio utilizado.

Ao seu turno, na tecnologia *Bluetooth* (BT), o rastreamento é feito por proximidade e permite que as pessoas que tiveram próximas troquem "chaves" de identificação - com as informações e dados pessoais- que são códigos efêmeros criados pelos smartphones e renovados em um determinado período que gira em torno de dez a vinte minutos.

Entrementes, através do cruzamento desses identificadores anônimos será possível observar se o utilizador esteve próximo de alguém infectado e alertá-lo sobre o fato, desde

23 Ibidem.
24 Disponível em: < https://wwwl.folha.uol.com.br/tec/2021/01/relatorio-alerta-para-violacao-de-privacidade-e-potencial-vigilancia-em-medidas-do-governo.shtml>. Acesso em: 26, jan. 2.021.

que exista voluntariedade pelo próprio utilizador em inserir no sistema a informação. Neste método os dados são descontextualizados ou pseudoanonimizados[25] e torna-se praticamente impossível identificar o usuário[26], o que dá primazia à privacidade.

Outrossim, as gigantes da tecnologia *Apple* e *Google*, em uma parceria inédita, desenvolveram e aprimoraram a tecnologia de *Bluetooth Low Energy* (BLE), de participação anônima e voluntária, que tem por característica a *aleatorização* de endereço e derivação de chave entre transportes, ou seja, consiste na troca de códigos de identificação e chaves de rastreamento únicas, visando criar um sistema de rastreio de contágio mais seguro e protetivo da privacidade dos usuários[27].

Nessa tecnologia o *smartphone* também receberá códigos de outros dispositivos com notificação de exposição ativado e os salvará de forma criptografada. Ademais, estes códigos de identificação mudam regularmente para dificultar a localização. Para além, o sistema utiliza a transmissão via criptografia AES[28] para proteger as informações, cujo grau de segurança é dos mais elevados.

A chave de rastreamento, ao seu turno, é vinculada aos vários códigos de identificação transmitidos pelo aparelho, e a ligação entre a chave de rastreio e os códigos de identificação é armazenada em um servidor central, protegido para impedir a descoberta da relação por pessoas não autorizadas. Assim, apenas quem informou ter testado positivo para o vírus da COVID-19 terá essa chave de rastreamento enviada

25 Conforme conceito trazido no art. 13, §4° da LGPD a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

26 Conferir nesse sentido: <https://www.reuters.com/article/health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idINKCN22329X?edition-redirect=in>. Acesso em 28, jan., 2.021.

27 Disponível em: <https://support.apple.com/pt-br/guide/security/sec82597d97e/web>. Acesso em 28, jan., 2021.

28 AES é um subconjunto de cifra de bloco da família Rijndael desenvolvida por dois criptógrafos, Vincent Rijmen e Joan Daemen, que submeteram a proposta ao NIST durante o processo de seleção AES. Rijndael é uma família de cifras com diferentes chaves e tamanhos de bloco. ES tornou-se eficaz como um padrão do governo federal em 26 de maio de 2002, após a aprovação do Secretário de Comércio. Ela está incluída na norma ISO/IEC 18033-3. Também está disponível em muitos pacotes de criptografia diferentes e é a primeira (e única) cifra acessível publicamente aprovada pela Agência de Segurança Nacional (NSA) para informações altamente secretas quando usado em um módulo criptográfico aprovado pela NSA. Fonte: <https://pt.wikipedia.org/wiki/Advanced_Encryption_Standard>. Acesso em: 17 jan., 2.021.

para a nuvem, não sendo transmitida por *Bluetooth*[29].

Por consequência, ao menos uma vez por dia o celular fará o download de uma lista de códigos de identificação de pessoas que testaram positivo. Se houver uma correspondência entre os códigos dessas pessoas e os códigos armazenados no seu celular, isso significa que você teve contato com alguém infectado e será alertado sobre como proceder.

De mais, aduz a *Apple* que seus aplicativos possuem recursos de criptografia adicionais para resguardar os dados do usuário, mesmo que outras partes da infraestrutura de segurança tenham sido comprometidas e que todos esses recursos beneficiam tanto usuários quanto administradores de TI, protegendo informações e fornecendo métodos para o apagamento remoto completo e imediato no caso de roubo ou perda do dispositivo[30].

Em resumo, pode-se afirmar que os *apps* de rastreio de contágio trazem realmente benefícios ao combate à pandemia ao possibilitar a transformação rápida de uma imensidão de dados pessoais em inteligência, voltada ao subsídio de políticas públicas de saúde e preservar muitas vidas, notadamente diante da possibilidade de diagnóstico precoce. Também pode-se utilizar a inteligência artificial, *big data*, dentre outros, para identificar quais cidadãos tem menor ou maior propensão em se contaminar e informá-los para que haja uma atenção maior.

Todavia, não se pode esquecer que os dados, ainda que (pseudo)anonimizados informados à *Apple* e ao *Google,* via tecnologia BLE, como em caso de contaminação, farão parte de um servidor central, *cloud* ou banco de dados gigantesco e sem precedentes. Apesar destas *big techs* informarem que protegem a privacidade do usuário com o que existe de melhor, fato é que a hipossuficiência deste frente àquelas, somado à legislação lacunosa e vacilante no Brasil, não permite averiguar e atestar por vias independentes a total lisura do tratamento.

29 Conferir para maiores esclarecimentos: <https://tecnoblog.net/335748/como-funciona-a-tecnologia-feita-por-apple-e-google-para-monitorar-covid-19/>. Acesso em: 18, jan, 2021.

30 Disponível em: < https://support.apple.com/pt-br/guide/security/sece3bee0835/1/web/1>. Acesso em 28, jan., 2021.

4. Direito à privacidade e à proteção de dados sensíveis na utilização de "Contact Tracing Apps"

Segundo o abrangente estudo "A First Look at Contact Tracing Apps", que analisou diversos "Contact Tracing Apps" utilizados em vários países, notou-se que a maioria dos aplicativos coletavam dados pessoais que não guardam finalidade ao objetivo, tais como informações de localização, nome, número de telefone, data de nascimento e identificador de chamadas.[31] Por isso uma proteção ampla da privacidade e proteção de dados é imperiosa e urgente.

Noutro giro, a *densificação* do direito à proteção de dados pessoais ainda não é expressamente previsto na Constituição da República Federativa do Brasil de 1988 (CF/88) como um direito fundamental autônomo[32], mas não é prudente presumir que a proteção não tem assento constitucional, vez que, consoante escólio sempre preciso da Schertel (2014, p.172) pode-se extrair a proteção de dados pessoais através da cláusula geral de proteção à intimidade da vida privada, insculpida no inc. X, do art. 5º da CRFB. Observemos: "Entretanto, a proteção aos dados decorre da inviolabilidade da intimidade e da vida privada (art. 5º, X). Mesmo sem uma previsão expressa, é possível extrair-se da Constituição Federal um verdadeiro direito fundamental à proteção de dados pessoais". [33]

Neste sentido, os direitos da personalidade, como expressão da dignidade da pessoa humana, são verdadeiros *numerus apertus* que comportam e dão guarida à novel proteção de dados pessoais, conforme preconiza Bioni (2021):

> "Os direitos da personalidade são uma *noção inacabada* que deve ser cultivada especialmente frente ao abordado manancial de dados produzidos pelas pessoas na sociedade da informação. [...]Os direitos da personalidade não se limitam àquelas situações previstas no CC, sendo o seu rol *numerus apertus* (rol aberto). Eles não

31 Azad, Muhammad & Arshad, Junaid & Akmal, Ali & Abdullah, Sidrah & Ahmad, Farhan & Imran, Muhammad & Riaz, Farhan. (2020). A First Look at Contact Tracing Apps, disponível em: <https://www.researchgate.net/publication/342436014_A_First_Look_at_Contact_Tracing_Apps>. Acesso em: 25. jan., 2021.

32 Conferir Projeto de Emenda à Constituição Brasileira nº17 de 2019, que propõe a inclusão da proteção de dados pessoais como um direito fundamental do cidadão. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 21, jan., 2021.

33 MENDES, Laura Schertel. Privacidade, Proteção de Dados e Defesa do Consumidor, São Paulo: Saraiva, 2014. p. 172.

> exaurem naquelas espécies enumeradas nos arts. 11 a 21 do CC, o que abre caminho para o reconhecimento da proteção de dados pessoais como um *novo direito da personalidade"*[34].

Por sua vez, no âmbito da União Europeia já existe a regulamentação da matéria através do regime europeu de proteção de dados (RGPD), bem como do art.8º[35] da Carta dos Direitos Fundamentais da União Europeia.

Já no Brasil, a Lei Geral de Proteção de Dados (LGPD) n.º 13.709/2018, que entrou em vigor em 18/09/2020 – no curso da pandemia-, representou um marco na regulamentação da matéria ao dispor sobre todas as operações de tratamento de dados pessoais[36], inclusive através de meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

Por consequência, a LGPD - na esteira do Regulamento Geral de Proteção de Dados da União Europeia (RGPD)[37] -, regulamenta por meio da norma trazida pelo inc. II do art.5º a proteção de dados relacionados à saúde, como sendo de natureza sensível. Nesse diapasão, há evidente correlação entre os problemas mais encontrados nas tecnologias de *contact tracing apps*, supramecionados, e a proteção da esfera da privacidade e de dados pessoais sensíveis.

Para Doneda (2019), uma característica intrínseca da sensibilidade dos dados, como merecedora de uma tutela mais robusta, é a possibilidade potencial de utilização discriminatória e, portanto, violadora de direitos fundamentais. Senão vejamos:

> "O regime adotado em relação aos dados sensíveis varia de acordo com as concepções a este respeito em cada ordenamento. Na verdade, deve-se ter em con-

34 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento – e. ed. – [3. Reimpr.] – Rio de Janeiro: Forense, 2021. p. 52

35 RGPD - 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente

36 Segundo o art. 5º,X da LGPD o tratamento consiste em toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

37 Regulamento (UE) nº2016/679, disponível em: <https://eur-lex.europa.eu/legal content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 19, jan,, 2021.

> ta que a diferenciação conceitual dos dados sensíveis atende à uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior [...]"[38].

Entrementes, a União Europeia, atenta às possíveis violações de direitos por estes aplicativos de rastreio de contágio expediu recomendações[39] para o uso adequado da tecnologia, nas quais, em linhas gerais, interpretando o conteúdo principiológico já inserido na RGPD, indicou atenção especial ao papel das autoridades nacionais de proteção de dados, a possibilidade de controle total do usuário sobre seus dados, a utilização limitada dos dados, limites estritos na conservação destes e garantia da exatidão e segurança.

Em relação ao Brasil, imperioso destacar o "Relatório privacidade e pandemia: recomendações para o uso legítimo de dados no combate à COVID-19", confeccionado pela *DataPrivacyBR Research*, por meio do qual apresentou princípios e recomendações para a formulação de políticas de compartilhamento de dados pessoais entre entidades da Administração Pública e/ou destas com entidades do setor privado no contexto da pandemia. Senão vejamos:

> i) Motivação Fundamentada; ii) Amparo em Autorização Legal; iii) Formalização em Instrumento Jurídico; iv) Definição de Finalidade Específica: iv.1) Vedação do uso com finalidades lucrativas e discriminatórias abusivas; v) Limitação ao mínimo necessário; vi) Definição do ciclo de vida dos dados: vi.1) Limitação temporal, vi.2) Exclusão posterior ao uso adequado, vi.3) Qualidade dos dados; vii) (Pseudo)anonimização de forma a garantir baixos riscos de reidentificação de pessoas: vii.1) Compromisso de não reidentificação pelo recipiente, vii.2) Priorização da informação ('output') e não repasse de dados ('input'), vii.3) Inclusão de recipientes terceiros confiáveis caso seja preciso agregar a base de dados e vii.4) Não divulgação de identidade de recuperados, infectados ou suspeitos; viii) Garantia da Segurança da Informação: ix) Transparência Ativa e x) Preferência por aplicativos e tecnologias por código aberto. [40]

38 DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados – São Paulo: Thomson Reuters Brasil, 2019. p. 144.

39 COMMISSION RECOMMENDATION of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/1e8b1520-7e-0c-11ea-aea8-01aa75ed71a1/language-en>. Acesso em: 18.jan., 2021.

40 Disponível o conteúdo em: <https://www.dataprivacybr.org/relatorio_privaci-

À evidência, de forma aplicada à proteção de dados pessoais num contexto pandêmico, o indigitado relatório, bem como as recomendações da EU, acabam por dar primazia aos princípios insculpidos no art. 6º da própria LGPD[41], bem como aos direitos dos titulares de dados pessoais, desta feita com previsão no art. 9 da legislação supra.[42]

Por conseguinte, é imperioso que as empresas que desenvolvam as tecnologias de rastreio tenham, desde o início, a preocupação de conceber aplicativos projetados para preservar a privacidade dos dados pessoais em todos os aspectos, o que se conceitua como *privacy by design,* com especial atenção às leis - tais como LGPD/RGPD -, recomendações de órgãos representativos, devendo-se observar a compatibilidade das aplicações, desde o início, com o quadro legal e constitucional vigente.

Deve-se exigir daqueles que tratam e operam dados pessoais o compromisso, notadamente externado nas políticas de uso, quanto a adesão às boas práticas de governança, norteando-se pelos princípios elencados adrede, mormente quando relacionados à aplicativos de rastreio de contágio.

Em especial, a observância da (*pseudo)anonimização*, que assegura, em tese, maior privacidade do usuário; a *definição da finalidade específica*, que permite o controle de proporcionalidade e gestão na utilização dos dados, bem como se a modelagem de dados considerada minimiza e maximiza, respectivamente, os riscos à privacidade e a eficiência no combate à pandemia; a *limitação temporal e ao mínimo de dados possível*, que possibilita uma menor intrusão à privacidade do utilizador, que não precisa fornecer dados além daquilo que seja necessário, sendo estes tratados por tempo suficiente à busca do objetivo; a *não divulgação de identidade de recuperados*

dade/>. Acesso em 18, jan., 2021.

41 A LGPD elenca como princípios para a atividades de tratamento de dados pessoais, além da boa-fé, os seguintes: I – finalidade; II – adequação; III – necessidade; IV - livre acesso; V - qualidade dos dados; VI – transparência; VII – segurança; VIII – prevenção; IX - não discriminação e X - responsabilização e prestação de contas.

42 Consoante o Art. 9º da LGPD O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

e infectados ou suspeitos, pois trata-se de dados pessoais sensíveis e devem ser colocados no topo da privacidade e, por fim, *a preferência por aplicativos e tecnologias com código aberto*, para permitir maior, acesso, participação democrática, escrutínio público e, em última instância, eficiência.

No mesmo sentido, no âmbito da União Europeia, houve a divulgação do documento *Joint European Roadmap towards lifiting COVID -19 containment measures (2020/C 126/01 , da Comissão)*[43], onde expressamente diz que o uso de *contact tracing apps* deve ser feito com respeito ao *legal framework* atinente à proteção de dados pessoais europeu, bem como de adesão voluntária e consentida pelo usuário[44].

Corroborando o que se defende neste estudo, a supracitada orientação estabelece que é essencial que a tecnologia empregada nestes aplicativos de rastreio deva-se basear na anonimização dos dados dos utilizadores, sem qualquer forma de monitoramento nem de abertura dos nomes dos infectados para outros usuários, sendo que ao fim da pandemia os dados deverão ser apagados[45].

Em Portugal, como nos revela Egídio (2020), em se adotando o sistema de rastreio e contágio por aplicações, estas deverão ser de utilização voluntária e consentida, com uso de tecnologia Bluetooth necessariamente. Vejamos:

> "Depois de alguma discussão na comunicação social, ficou esclarecido que a aplicação a ser implementada em Portugal, integrada na iniciativa Monitorcovid19.pt e desenvolvida pelo INESCTEC, será uma plataforma de uso voluntário (ou seja, o utilizador terá de dar seu consentimento, ao fazer voluntariamente do *down-*

43 Disponível em <https://ec.europa.eu/jrc/communities/sites/default/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf>.

44 Em igual sentido conferir Diretrizes sobre utilização de dados de localização e ferramentas de contact tracing no contexto do surto de COVID-19, disponível em <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>.

45 [...]The use of such mobile applications should be voluntary for individuals, based on users' consent and fully respecting European privacy and personal data protection rules. When using tracing apps, users should remain in control of their data. National health authorities should be involved in the design of the system. Tracing close proximity between mobile devices should be allowed only on an anonymous and aggregated basis, without any tracking of citizens, and names of possibly infected persons should not be disclosed to other users. Mobile tracing and warning applications should be subject to demanding transparency requirements, be deactivated as soon as the COVID-19 crisis is over and any remaining data erased. Disponível em <https://ec.europa.eu/jrc/communities/sites/default/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf>.

> *load* da *app*), a qual pemite aos utilizadores interessados descobrir casos de contacto próximo com infectados por COVID-19 e que utilizará apenas a tecnologia Bluetooth [...]."[46]

Dessarte, Morley et al. (2020) enumeram quatro os princípios mínimos para o rastreamento ético: *i)* necessário; *ii)* proporcional; *iii)* cientificamente válido e *iv)* prazo determinado. Nesse sentido, complementa Junquilho (2020) que é de suma importância a utilização de tecnologias que garantam não identificação (anonimização) dos usuários, como um perfil com ID (identificação) randômica, que mude constantemente para garantir a privacidade, bem como que os dados pessoais tratados cumpram apenas a finalidade de combate à Covid-19 no período pandêmico[47].

Nesse contexto é forçoso reconhecer que a tecnologia de rastreio de contágio por *Bluetooth Low Energy* (BLE) demonstra-se mais consentânea com o quadro principiológico e regulatório europeu e brasileiro, haja vista que: *i)* o uso da tecnologia BLE permite maior (pseudo)anonimização, vez que não há troca de nomes, números ou identidade do usuário, apenas das "chaves" aleatórias; *ii)* o uso é cunho voluntário e consentido; *iii)* a precisão do Bluetooth é maior que a do GPS, bem como não há o monitoramento do itinerário do usuário e *iv)* a utilização de criptografia AES garante maior segurança e privacidade no conteúdo dos dados que estão armazenados.

Entretanto, como já apontado anteriormente, o sistema não é imune ao acúmulo inigualável de dados pessoais sensíveis dos usuários- potencialmente utilizáveis com grande cunho discriminatório- pelas duas das maiores empresas de tecnologias do mundo, que podem ser objeto de *hackeamento,* vigilância ou tratamento fora dos limites do consentimento.

Lado outro, no que tange à relação entre usuários e Poderes Públicos, que podem ser eventualmente realizadas para o uso de *contact trancing*, aponte-se que deve existir re-

46 EGÍDIO, Mariana Melo. Protecção de dados em tempos de COVID-19 – breves reflexões. e-Pública. Lisboa, Vol. 7, nº1 (Abr. 2020), 2020. p.247.

47 Morley, J., Cowls, J., TaddUeo, M., & Floridi, L. (2020). Ethical guidelines for Covid-19 tracing apps. Nature Machine Intelligence, 582, 29–31apud JUNQUILHO, Tainá Aguiar. Prós e contras do contac tracing, ou monitoramento epidêmico. In: Revista do Consultor Jurídico, 15 de julho de 2020. Disponível em <https://www.conjur.com.br/2020-jun-15/taina-junquilho-pros-contras-contact-tracing#_ftn3>. Acessado em 17, de jun. 2.021.

forçada incidência dos princípios da *Transparência Ativa* e da *Preferência por Códigos Abertos*, que impõem, respectivamente, a necessidade de que o tratamento seja feito com a máxima transparência, assim como seja facultado acesso a detalhes técnicos e processos decisórios.

Ao respeitar os princípios em voga, a indevida ingerência aos direitos da privacidade de dados é bastante reduzida, o que não exclui, obviamente, a possibilidade de haver situações violadoras, haja vista que perante o estado da técnica atual nenhuma informação é 100% segura na internet.

À evidência, trata-se de situação onde não se escapa à temática de restrição aos direitos fundamentais e à ponderação de valores, especialmente através do princípio da proporcionalidade, pois exercem função primordial na verificação de conformidade destas novas tecnologias ao ordenamento jurídico-constitucional.

Ensina-nos Mendes (2017) que para se efetuar restrições aos direitos fundamentais é pressuposto lógico identificar o âmbito de proteção do direito: "[...] o exame das restrições aos direitos fundamentais pressupõe a identificação do *âmbito de proteção* do direito, vez que esse processo não pode ser fixado em regras gerais, exigindo, para cada direito específico, determinado procedimento"[48].

Por conseguinte, é cediço que existe *a priori* uma colisão entre o direito à saúde pública em contraposição à liberdade e à privacidade do cidadão. Porém, através da aferição de proporcionalidade podemos identificar se existe razoabilidade nas restrições impingidas de um direito ao outro.

Quanto a proporcionalidade, ensina-nos Novais (2019, p.250) que a o princípio em voga deve verificar os sacrifícios e benefícios quando do choque entre dois direitos: "Neste controle de proporcionalidade, aquilo que se avalia, que se compara ou que se põe em relação, são os sacrifícios (custos) impostos ao direito fundamental contraposto aos benefícios (vantagens) produzidos na obtenção do fim visando com a restrição".[49]

48 MENDES, Gilmar Ferreira Curso de direito constitucional / Gilmar Ferreira Mendes, Paulo Gustavo Gonet Branco. – 12. ed. rev. e atual. – São Paulo : Saraiva, 2017. p. 174

49 NOVAIS, Jorge Reis. Direitos Fundamentais e Justiça Constitucional. AAFDL: Lisboa, 2017 reimpressão 2019, p. 250.

Desta forma, num teste de proporcionalidade aplicado ao uso de "Contact Tracing Apps" com tecnologia *Bluetooth*, notadamente *Low Energy* (BLE), percebe-se que existe adequação do meio utilizado ao o fim perseguido, ou seja, a utilização de rastreio de contágio para contenção de pandemias é prática já consagrada, conforme adrede exposto, e sua "versão 4.0" traduz-se no uso de aplicativos para esse fim.

Destarte, utilizando-se as tecnologias que são concebidas com foco na privacidade do usuário, desde a criação (*Privacy by Design*), o que nos parece ser o caso da tecnologia Bluetooth *Low Energy* (BLE) e, por ser o rastreio de contágio instrumento de combate a pandemias, podemos concluir que o meio é necessário é menos restritivo à privacidade do que outras tecnologias aqui analisadas, consagrando o binômio necessidade/exigibilidade, sem olvidar que existe espaço para evoluções no sentido de garantir a privacidade do utilizador.

Por fim, a proporcionalidade *stricto sensu* impõe que o grau de restrição a um direito fundamental deve ser justificado pelo grau de promoção a um direito contraposto (NOVAIS, 2019), razão pela qual, havendo comprometimento na privacidade do usuário, através da observância das diretrizes, recomendações e legislações apontadas, consequentemente haverá a proporcionalidade estrita no uso da ferramenta de *contact tracing apps* ao objetivo de conter o avanço da pandemia de COVID-19 pois, ainda que haja algum sacrifício do direito à privacidade, dentre todas as possibilidades tecnológicas examinadas, a BLE é a que menos se mostrou restritiva.

Entretanto, todos devem ficar atentos e vigilantes, exigindo a observância e conformidade – por parte do Estado e das demais empresas de Tecnologia que lidam com dados pessoais, como accountability e compliance - pilares das boas práticas de governança -, pois a sociedade e economia de vigilância deve ser conformada pelo Estado de Direito e não o contrário.

5. Conclusão

Conforme explicitado pelo texto, vivemos a era da Sociedade da Informação e do *Capitalismo da Vigilância*, iniciado pelos Estados e depois encampado pelas *big techs*, os quais têm fixação pela obtenção de dados pessoais, para ser-

vir como insumo aos seus objetivos de oferta de produtos e serviços mais preditivos e personalizados, ainda que para isso haja violação de direitos fundamentais das pessoas, notadamente os ligados à privacidade.

Neste contexto, a pandemia de COVID-19 que solapa o mundo desde 2020, deve valer-se da tecnologia como aliada ao combate do vírus, encontrando nos aplicativos de rastreio de contágio uma das ferramentas mais promissoras e eficazes. Porém, tais aplicações necessitam de dados pessoais sensíveis para funcionar e, assentados em um Estado de Direito, deve haver estrita observância e respeito aos direitos dos usuários, no que tange ao tratamento dos dados pessoais e a privacidade.

Exemplo emblemático de vigilância exercida pelo governo brasileiro foi a edição MP 954/2020, declarada inconstitucional liminarmente, onde se pretendia o compartilhamento de dados pessoais do cidadão entre empresas de telefonia e o IBGE, visando a *produção de estatística oficial* durante a pandemia de COVID-19, submetendo o brasileiro à uma recolha e tratamento de dados pessoais sem delimitar precisamente o objeto da estatística a ser produzida, a finalidade específica ou a sua amplitude.

Já em relação aos *apps*, algumas tecnologias foram analisadas neste trabalho, especificamente as de GPS, *Bluetooth* e *Bluetooth Low Energy* (BLE), sendo estas últimas as que mais têm mecanismos protetores contra a violação dos direitos à proteção de dados pessoais do usuário e privacidade, sendo menos invasiva ao direito protegido e alcançando o objetivo de combater o COVID-19, representando, portanto, uma opção proporcional como política de saúde. Porém, ainda não se pode falar que garante na totalidade a privacidade do usuário.

Outrossim, advoga-se neste estudo o recurso ao princípio da proporcionalidade para dirimir eventuais embates entre direito à saúde pública de um lado e privacidade e proteção de dados de outro, verificando-se os sacrifícios impostos e os benefícios gerados na obtenção do fim desejado, atestando-se ou não a compatibilidade jurídico-constitucional dos aplicativos de rastreio de contágio como medida de combate à pandemia.

6. Referência:

AZAD, Muhammad. Et al., *A First Look at Contact Tracing Apps*. 2020. Disponível em:<https://www.researchgate.net/publication/342436014_A_First_Look_at_Contact_Tracing_Apps>. Acessado em: 25, jan. de 2021.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento* – e. ed. – [3. Reimpr.] – Rio de Janeiro: Forense, 2021.

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.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, 2021. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 25, jan., 2021.

BRASIL. Lei n. 13.079, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União,* 15, ago. 2018.

CHEN, H., Yang, B. O., PEI, H., & LIU, J. (2019). Next Generation Technology for Epidemic Prevention and Control: Data-Driven Contact Tracking. IEEE.

DONEDA, Danilo. Da Privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de proteção de dados – São Paulo: Thomson Reuters Brasil, 2019.

EGÍDIO, Mariana Melo. *Protecção de dados em tempos de COVID-19 – breves reflexões.* e-Pública. Lisboa, Vol. 7, nº1 (Abr. 2020), 2020.

GREENWALD, Glenn. *Sem lugar para se esconder Edward Snowden, a NSA e a espionagem do governo americano.* Rio de Janeiro: Sextante Tradução de Fernanda Abreu, 2014

JUNQUILHO, Tainá Aguiar. *Prós e contras do contact tracing, ou monitoramento epidêmico.* In*:* Revista do Consultor Jurídico, 15 de julho de 2020.

KELLER, Clara Iglesias; PEREIRA, Jane Reis Gonçalves. *Data protection in times of Covid-19: the risks for surveillance in Brazil, Internet Policy Review*, 01 abr. 2020. Disponível em: <https://policyreview.info/articles/news/data-protection-times-covid-19-risks-surveillance brazil/1462>. Acesso em 17, jan., 2021.

LONG, Clarissa; *Privacy and Pandemics* In PISTOR, Katharina. Law in the time of COVID-19. Columbia Law School Books, 2020.

MENDES, Gilmar Ferreira Curso de direito constitucional / Gilmar Ferreira Mendes, Paulo Gustavo Gonet Branco. – 12. ed. rev. e atual. – São Paulo: Saraiva, 2017.

MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor*. São Paulo: Saraiva, 2014.

NOVAIS, Jorge Reis. *Direitos Fundamentais e Justiça Constitucional.* AAFDL: Lisboa, 2017 reimpressão 2019.

PARLAMENTO EUROPEU. Regulamento (UE) 2016/679 de 27 abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>.Acesso em: 22, jan., 2021.

WORLD HEALTH ORGANIZATION (WHO). *World Health Organization. Contact Tracing in the context of COVID-19 (Interim Guidance) 2020: WHO*; 2020. Disponível em: <https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19>. Acesso em: 17, jan., 2021.

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância – A disputa por Um Futuro Humano na Nova Fronteira do Poder*. Traduzido por Luís Filipe Silva e Miguel Serras Pereira, Lisboa: Relógio D'Água, 2020.