

ANÁLISE CRÍTICA DA PROTEÇÃO DE DADOS PESSOAIS DURANTE O PERÍODO DE CONTINGÊNCIA DA COVID-19

CRITICAL ANALYSIS OF BRAZILIAN PERSONAL DATA PROTECTION DURING COVID-19 CONTINGENCY PERIOD

Victor Auilo Haikal ¹

RESUMO: Este artigo discute algumas medidas tomadas pelos entes públicos no Brasil durante o período de contingência sanitária da COVID-19 sobre o tratamento de dados pessoais e proteção à privacidade, levando-se em consideração que a Lei Geral de Proteção de Dados Pessoais ainda não estava em vigor, mas, nem por isso já não havia normas vigentes suficientemente estabelecidas para que os direitos dos titulares fosse adequadamente respeitado. Para chegar às conclusões almejadas utilizar-se-aram os métodos de dedução estrutural e dialético a partir de fontes confiáveis de pesquisa, relevando-se a própria interdependência que os temas da proteção de dados pessoais e segurança da informação possuem com os demais institutos a seu redor. As conclusões tiradas vertem para já conhecida deficiência do entendimento da cultura da privacidade e proteção de dados pessoais, pois os esforços não são direcionados para que os direitos do titular sejam garantidos ou que exista coesão no desenvolvimento da mencionada cultura, mas, e tão somente o atingimento de certos objetivos governamentais e institucionais.

Palavras-chaves: direito digital; direito à privacidade; proteção de dados pessoais; lei geral de proteção de dados pessoais; MP 954/2020; MP 959/2020; convênio Estado de São Paulo; dados anonimizados.

ABSTRACT: This paper assesses some actions performed by government entities about personal data treatment and privacy protection during the COVID-19 contingency period, considering that the Brazilian General Data Protection Law was not in force, but, besides that, there was sufficient norms in effect that predicted the adequate protection of the subjects right to privacy. To achieve the conclusions, the structural and dialectical deduction methods were used with trustworthy research sources, ensuring that the interdependency of the personal data protection and information security have with other related areas of knowledge. All conclusions point to the well-known privacy and personal data protection culture deficiency, because the efforts are not channeled to the protection of the subjects rights would be granted nor that would be cohesion during the development of such culture, but, and solely, the execution of government and institutional goals.

Keywords: digital law; right to privacy; personal data protection; brazilian general data protection law; MP 954/2020; MP 959/2020; State of São Paulo agreements; anonymous data

¹ Mestre e Doutorando em Direito Civil pela Universidade de São Paulo. Master of Science em Cybersecurity pela University of Maryland University College. Professor de Direito Digital da Rede LFG e CEDIN-BH. Professor convidado da Escola Superior de Advocacia de São Paulo (ESA/SP), da Fundação Instituto de Administração (FIA) e Unicuritiba. Advogado.

1 INTRODUÇÃO – CRISE NO CONTEXTO SOCIAL IMPLANTADA PELA OCORRÊNCIA DA PANDEMIA E MEDIDAS PARA CONTINGÊNCIA

Talvez o mais pessimista dos videntes e analistas não anteciparia o encerramento prático do ano de 2020 em 11 de março², quando a doença causada pelo SARS-COV2, a COVID-19, foi registrada como ameaça sanitária global, posto que presente em todos os continentes.

Isso porque tal medida tomada pela Organização Mundial da Saúde teria o condão de evitar tragédias acumuladas em países onde a doença ainda não teria sido transmitida de forma intensa, uma vez que os focos de infecção e mortes naquela data ainda eram discretos se comparados com o final do mês de março na Itália, com o falecimento acumulado de 12.428 pessoas³, ou abril, na Espanha, cujo número alcançou 24.543⁴, o que veio a se agravar nos meses subsequentes.

A partir da referida declaração, para se tentar prevenir tamanho grau de infecção e mortes na população, alguns governantes brasileiros passaram a tomar medidas de contingência, impedindo o funcionamento de serviços ou eventos tidos como não essenciais ou que pusessem a vida das pessoas que fossem utilizar de facilidades em evidente risco, sem mencionar da possibilidade de contaminação generalizada.

Nesse sentido, cabe mencionar os esforços federais na Lei nº 13.979 de 2020 que previu as diretrizes para o contorno da pandemia e, apenas a título de ilustração, o Decreto Municipal de São Paulo nº 59.283 de 16 de março de 2020 e o Decreto Estadual nº 64.881 de 22 de março de 2020, fixando, respectivamente:

- a) A utilização do teletrabalho na Administração Pública Direta e Indireta como forma de se evitar o contágio preservando a estrutura de atendimento à população⁵;
- b) Suspensão de todas as atividades de atendimento presenciais, exceto atividades de saúde, alimentação, logística e segurança nas modalidades de entrega (delivery) e retirada no local, pessoalmente (takeout) ou via automóvel (drive-thru)⁶ e os previstos

2 World Health Organization. *WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020*. 11 mar. 2020. Disponível em: <<https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020>>. Acesso em: 10 set. 2020.

3 Ministero della Salute. *Covid-19, i casi in Italia alle ore 18 del 31 marzo*. 31 mar. 2020. Disponível em: <<http://www.salute.gov.it/portale/nuovocoronavirus/dettaglioNotizieNuovoCoronavirus.jsp?lingua=italiano&menu=notizie&p=dalministero&id=4370>>. Acesso em: 10 set. 2020.

4 Departamento de Seguridad Nacional. *Coronavirus (COVID-19) - 30 de abril 2020*. 30 abr. 2020. Disponível em: <<https://www.dsn.gob.es/es/actualidad/sala-prensa/coronavirus-covid-19-30-abril-2020>>. Acesso em: 10 set. 2020.

5 Art. 7º Poderá ainda ser instituído regime de teletrabalho, no curso do período de emergência, a critério e nas condições definidas pelo titular do órgão da Administração Direta, Autarquias e Fundações, para servidores cujas atribuições, por sua natureza e meios de produção, permitam a realização do trabalho remoto, sem prejuízo ao serviço público.

Art. 8º A instituição do regime de teletrabalho, de que tratam os arts. 6º e 7º, no período de emergência está condicionada:

I – à manutenção diária na unidade de servidores suficientes para garantir o atendimento;

II – à inexistência de prejuízo ao serviço.

6 Artigo 2º - Para o fim de que cuida o artigo 1º deste decreto, fica suspenso:

I - o atendimento presencial ao público em estabelecimentos comerciais e prestadores de serviços, especialmente em casas noturnas, "shopping centers", galerias e estabelecimentos congêneres, academias e centros de ginástica, ressalvadas as atividades internas;

II - o consumo local em bares, restaurantes, padarias e supermercados, sem prejuízo dos serviços de entrega ("delivery") e "drive thru".

§ 1º - O disposto no "caput" deste artigo não se aplica a estabelecimentos que tenham por objeto atividades essenciais, na seguinte conformidade:

1. saúde: hospitais, clínicas, farmácias, lavanderias e serviços de limpeza e hotéis;

2. alimentação: supermercados e congêneres, bem como os serviços de entrega ("delivery") e "drive thru" de bares, restaurantes e padarias;

3. abastecimento: transportadoras, postos de combustíveis e derivados, armazéns, oficinas de veículos automotores e bancas de jornal;

4. segurança: serviços de segurança privada;

5. comunicação social: meios de comunicação social, inclusive eletrônica, executada por empresas jornalísticas e de radiodifusão sonora e de sons e imagens;

6. demais atividades relacionadas no § 1º do artigo 3º do Decreto federal nº 10.282, de 20 de março de 2020."

no Decreto Federal nº 10.282 de 20 de março de 2020, que regulamentam a lei nº 13.979 de 2020 e contribuem à lista anterior, mas não se limitam nos serviços de telecomunicações e internet, call center, geração, transmissão e distribuição de energia elétrica, serviços de pagamento, crédito e saque de valores sob a supervisão do Banco Central do Brasil, e serviços de tecnologia da informação e processamento de dados que sustentam todas as outras⁷.

Tais esforços foram as medidas iniciais para restringir o número de pessoas circulando nas cidades, de modo que o contato social entre elas fosse diminuto, na medida do estritamente necessário, seguindo as orientações da Organização Mundial da Saúde⁸ que foram também adotadas pelos governos mencionados⁹, cuja menção é puramente pedagógica, vez que outros Estados e cidades também adotaram medidas muito similares, se não idênticas.

Assim, estabeleceu-se o '*novo normal*', em que as pessoas deveriam somente se dirigir a estabelecimentos comerciais para aquisição dos produtos e serviços que foram taxados como essenciais e, para agravar o cenário socioeconômico, o cenário da organização do trabalho sofreu sensível abalo, posto que as atividades de varejo e serviço que dependiam do trabalho presencial humano ou em estações de labor em escritórios não poderiam funcionar em virtude da restrição governamental imposta.

Com isso, se impôs a diminuição do tráfego comercial varejista que atingiu os setores produtivos correspondentes, acarretando o aumento no desemprego¹⁰ e até mesmo fechamento de empresas¹¹ pela paralisação do consumo que outrora estava acomodado no '*antigo normal*', isto é, antes da declaração da pandemia.

Assim, se percebe crise social pela mudança abrupta na forma com que as pessoas estariam aptas a gerar riqueza e, assim, estando em xeque a capacidade de custear a própria subsistência, além de a preocupação constante em realizar as atividades necessárias para evitar a contaminação pela doença.

Com vistas a enfrentar tal cenário, discutir-se-ão algumas iniciativas governamentais adotadas que dizem respeito à proteção de dados pessoais e os impactos jurídicos e de segurança da informação decorrentes destas medidas perante a situação catastrófica

7 Art. 3º As medidas previstas na Lei nº 13.979, de 2020, deverão resguardar o exercício e o funcionamento dos serviços públicos e atividades essenciais a que se refere o § 1º.

§ 1º São serviços públicos e atividades essenciais aqueles indispensáveis ao atendimento das necessidades inadiáveis da comunidade, assim considerados aqueles que, se não atendidos, colocam em perigo a sobrevivência, a saúde ou a segurança da população, tais como: (...)

VI - telecomunicações e internet;

VII - serviço de call center;

X - geração, transmissão e distribuição de energia elétrica, incluídos: (...)

XX - serviços de pagamento, de crédito e de saque e aporte prestados pelas instituições supervisionadas pelo Banco Central do Brasil;

XXIII - serviço relacionados à tecnologia da informação e de processamento de dados (data center) para suporte de outras atividades previstas neste Decreto;

8 World Health Organization, Coronavirus disease (COVID-19) advice for the public. 4 jun. 2020. Disponível em: <<https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public>>. Acesso em: 10 set. 2020.

9 Prefeitura do Município de São Paulo. Coronavírus. Disponível em: <https://www.prefeitura.sp.gov.br/cidade/secretarias/saude/vigilancia_em_saude/doencas_e_agrivos/coronavirus/index.php?p=291730>. Acesso em: 10 set. 2020 e Governo do Estado de São Paulo. Nova campanha do Governo destaca necessidade de ficar em casa para combater coronavírus. 13 abr. 2020. Disponível em: <<https://www.saopaulo.sp.gov.br/noticias-coronavirus/nova-campanha-do-governo-destaca-necessidade-de-ficar-em-casa-para-combater-coronavirus/>>. Acesso em: 10 set. 2020.

10 LEMOS, Vinicius. Demitidos por causa do coronavírus: os brasileiros que já ficaram desempregados com a pandemia. UOL Economia. 26 mar. 2020. Disponível em: <<https://economia.uol.com.br/noticias/bbc/2020/03/26/demitidos-por-causa-do-coronavirus-brasileiros-que-ja-ficaram-desempregados-com-a-pandemia.htm>>. Acesso em: 10 set. 2020.

11 OLIVEIRA, Joana. 716.000 empresas fecharam as portas desde o início da pandemia no Brasil, segundo o IBGE. EL PAÍS. 19 jul. 2020. Disponível em: <<https://brasil.elpais.com/brasil/2020-07-19/716000-empresas-fecharam-as-portas-desde-o-inicio-da-pandemia-no-brasil-segundo-o-ibge.html>>. Acesso em: 10 set. 2020.

posta, cujo objetivo é identificar iniciativas positivas, negativas e lições aprendidas para que situação similar futura não seja contornada de maneira mais eficiente.

2 CONSIDERAÇÕES ESSENCIAIS SOBRE O DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS

Informação é *poder* sempre que potencialmente útil¹², haja vista proporcionar decisões melhores e, a partir delas, resultados melhores em todos os campos de atuação de vida da pessoa.

Poder é a capacidade de influenciar e conduzir a tomada de decisões de outros¹³, quanto mais se sabe a respeito de uma pessoa, maiores as chances de compreender seus padrões de ação e pensamento para lhe convencer de algo.

Bem a par dessas premissas, Stephen Baker explica o cenário de tratamento de dados pessoais na obra *The Numerati* e pontua a relevância do conhecimento do titular dos dados a partir de suas preferências, gostos, opiniões e, a com base nessas adotar melhor estratégia e abordagem para que a pessoa aja de determinada maneira ou que ofereça exatamente o que ela deseja comprar, ler, consumir, fazer, etc. a partir da formação e estudo de seu perfil de escolhas constantes em determinado banco de dados, atividade que é conhecida como *profiling*¹⁴.

Nesse sentido, Daniel J. Solove disserta sobre o fenômeno da “*ascensão dos dossiês digitais*”, em que tanto as instituições governamentais quanto as empresas privadas passaram a reunir quantidades massivas de dados que formam os perfis das pessoas e que permitem estudo detido de suas características e padrões¹⁵, fenômeno que passou a ocorrer a partir da década de 1960 pela evolução da computação.

A partir dessas práticas, advertiu José Afonso da Silva que o processamento de dados, sobretudo pessoais, realizado a partir do intenso e complexo desenvolvimento de

12 Consoante apontado por Susanna Davies in *Introduction: information, knowledge and power*. IDS Bulletin 25.2, 1994. Disponível em: < <https://www.ids.ac.uk/files/dmfile/davies252.pdf> >. Acesso em: 10 set. 2020, p.19, citando Emanuel de Kadt, in *Making health policy management intersectoral: Issues of information analysis and use in less developed countries*. *Social Science & Medicine*. v.29 n.4, 1989, p.503-514. Disponível em [https://doi.org/10.1016/0277-9536\(89\)90196-2](https://doi.org/10.1016/0277-9536(89)90196-2), Acesso em: 10 set. 2020, p. 507, há referências sobre ‘informação é poder’ já em textos bíblicos no Livro dos Provérbios (24:5), cuja tradução para o português é: “Um varão sábio é forte, e o varão de conhecimento consolida a força.” Existem inscrições árabes do Imam Ali, em *O Método da Eloquência*, dito 146 de que “conhecimento é poder e pode comandar a obediência. (...) Lembre que o conhecimento é o comandante e a riqueza é sua comandada.”, cuja tradução do árabe para o inglês em *Peak of Eloquence* é: “Knowledge is power and it can command obedience. (...) Remember that knowledge is a ruler and wealth is its subject.” Há referências a esta assertiva também no texto de *De corporis* de Thomas Hobbes, cuja tradução para o inglês *Concerning body* indica que: “the end of knowledge is power.”, ou seja, que o objetivo do conhecimento é o poder, p. 7. In *The English Works of Thomas Hobbes of Malmesbury*. Now first collected and edited by Sir. Bart William Molesworth. v. 1. Londres: John Bohn, 1839. Versão em e-book do Google Play. Disponível em: < https://play.google.com/books/reader?id=Gr8LAAAIAAJ&hl=pt_BR&pg=GBS.PA1 >. Acesso em: 10 set. 2020. O conceito trazido por Francis Bacon de que “knowledge of God than of his power, or rather of that part of God’s power, (for knowledge itself is a power whereby he knoweth)” foi traduzido a partir da expressão cunhada em latim de “*scientia potestas est*”, em português: “o conhecimento propriamente dito é poder”, in *Meditationes sacrae*, 1597, traduzido para o inglês como *Religious meditations*. Londres: John Iaggard, 1613. Versão em e-book Disponível em: < <https://archive.org/stream/essaiesofsfranc00baco#page/180/mode/2up> >. Acesso em: 10 set. 2020, p.180.

13 Cf. Manuel Castells. *Communication power*. 2ed. Oxford: Oxford University Press, 2013. Edição do Kindle, p.10: “Power is the relational capacity that enables a social actor to influence asymmetrically the decisions of other social actor(s) in ways that favor the empowered actor’s will, interests, and values. Power is exercised by means of coercion (or the possibility of it) and/ or by the construction of meaning on the basis of the discourses through which social actors guide their action.”, em tradução livre do autor: “O poder é a capacidade relacional que permite um participante da sociedade influenciar assimetricamente as decisões de outros conforme o desejo, interesse e veor de quem o detém. O poder é exercido por meios de coerção (ou a possibilidade de tal) e/ou pela construção de determinado significado com base nos discursos pelos quais os participantes da sociedade guiam suas ações.”

14 Cf. Stephen Baker. *The Numerati*. Nova Iorque: Houghton Mifflin Harcourt, 2008. Edição Kindle: O autor reconhece a atividade de profiling ao longo dos sete capítulos para avaliar como as escolhas e comportamentos vinculados à pessoa apontam para previsões de prováveis atos a serem praticados pelo titular ou como reagiria perante fatos a ele relacionados, com grau acurado de acerto, chegando a ponto de se identificar qual atividade profissional e qual cultura organizacional mais lhe agradaria, quais produtos desejaria comprar, em qual candidato provavelmente votaria, em qual bairro moraria e finalmente qual seria o par perfeito.

15 Cf. SOLOVE, Daniel J.. *The digital person: technology and privacy in the information age*. Nova York: New York University Press, 2004, p. 13-14.

rede de fichários eletrônicos (arquivos de computador) poderia revelar ameaça à privacidade das pessoas, em razão do esquadramento destas, devassando a individualidade e, com perigo acentuado, à medida que a interconexão possibilita formar extensos bancos de dados que desvendam a vida das pessoas, até mesmo sem seu consentimento¹⁶.

Em tempo, pertinente esclarecer que o direito à privacidade visa, dentre seus incontáveis predicados, limitar o acesso ao indivíduo, interromper a bisbilhotagem e perturbação por terceiros, conforme as lições de Samuel Warren e Louis Brandeis¹⁷, que, interpretado no contexto da Sociedade da Informação em razão de sua definição funcional significa “o *direito de manter o controle sobre as próprias informações*”¹⁸.

Tais informações, consistem na integralidade dos dados coletados do indivíduo, conquanto já exposto, a exemplo do conjunto de ações, comportamentos, opiniões, preferências, informações pessoais que forem registrados¹⁹, o que exige garantia de segurança e transparência durante seu tratamento, atributos que estão diretamente ligados com o uso da informática, de modo a não comprometer o controle do acesso aos dados por parte de seu titular²⁰, pois este autoriza o manejo de dados de forma limitada ao tratador.

Os mencionados critérios de segurança e transparência são fixados a partir da chamada *proteção de dados pessoais*²¹, que teve a Alemanha como expoente na promulgação de lei a esse respeito ante a atividade de tratamento desses dados.

Em 1970 o Estado de Hesse estabeleceu as primeiras regras para o desempenho da referida atividade pelo Poder Público com 17 artigos e que foi seguida pelo Estado da Bavária no mesmo ano e, posteriormente, pelos demais²², culminando na promulgação da lei federal de proteção de dados pessoais alemã, a *Bundesdatenschutzgesetz*, em 1977²³, que daria início a estudo mais acurado do tema no contexto europeu e nos países de tradição romano-germânica.

A importância do Estado Alemão para a proteção de dados pessoais é ressaltada pela formulação do direito à autodeterminação informativa pelas razões da Corte Constitucional Alemã ao julgar a licitude de lei federal promulgada em 1982 que obrigava cada cidadão a preencher questionário contendo 160 perguntas que seriam postas para tratamento

16 SILVA, José Afonso da. *Curso de direito constitucional positivo*. 37 ed. São Paulo: Malheiros, 2014, p. 211-212.

17 WARREN, Samuel. D.; BRANDEIS, Louis D. The right of privacy. *Harvard Law Review*, 193, 1890. Disponível em: <<http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C>>. Acesso em: 10 set. 2020. “4. The right to privacy ceases upon the publication of the facts by the individual, or with his consent. This is but another application of the rule which has become familiar in the law of literary and artistic property. The cases there decided establish also what should be deemed a publication, -- the important principle in this connection being that a private communication of circulation for a restricted purpose is not a publication within the meaning of the law.” Em tradução livre do autor: “4. O direito à privacidade cessa a partir da publicação de fatos pelo indivíduo ou com seu consentimento. Essa é mais uma aplicação da regra que já se tornou familiar na legislação de propriedade literária e artística. Os casos nos quais se decidiu em estabelecer o que foi considerado como publicação, -- a ideia norteadora nesse raciocínio é que uma comunicação privada de circulação por um propósito específico não é considerada como publicação, de acordo com os termos da lei.”

18 Cf. Alan Westin. *Privacy and freedom*. Nova Iorque: Atheneum, 1967, p. 133-158 *apud* DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006, p.206, NR 435 e RODOTÁ, Stefano. *A vida na sociedade da vigilância*. A privacidade hoje. Trad. por Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 92, indicando que o titular dos dados teria direito a conhecer, controlar, endereçar e interromper o fluxo das informações a ele relacionadas.

19 Cf. DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006, p. 92.

20 Cf. FROSINI, Vittorio. Diritto alla riservatezza e calcolatori elettronici. In: ALPA, Guido; BESSONE, Mario (Orgs.) *Banche dati telematica e diritti della persona*. Padova: Cedam, 1984, p. 37.

21 Cf. Danilo Doneda, *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006, p. 204.

22 Cf. Danilo Doneda, *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006, p. 228, citando Spiros Simits, *Crisi dell'informazioni giuridica ed elaborazione elettronica dei dati*. Milão: Giuffrè, 1977, p. VIII.

23 Muito embora não fosse a primeira lei nacional aprovada sobre o tratamento de dados pessoais, tendo sido a Suécia a pioneira em 1973, cf. DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006, p. 228.

informatizado, com vistas a retificar eventual registro desatualizado e podendo ser enviados de modo anonimizado às autoridades federais e aos Estados alemães, sob pena de multa sensível àqueles que não assim procedessem²⁴.

O *decisum* da Corte entendeu como abusivo não somente pela amplitude de abordagem das questões acerca da personalidade individual, além da dúvida de capacidade de anonimização efetiva desses dados que, caso negativa, comprometeria a '*Identifizierung*' e, por conseguinte, os direitos de personalidade e dignidade da pessoa humana²⁵.

Se por um lado o direito à privacidade vai regular a forma com que o tratamento de dados pessoais é realizado, por meio das normas específicas, o bem jurídico tutelado é, sem dúvida, a *identidade* da pessoa, dado que o manejo das informações armazenadas visam a destrinchar a formação das qualidades particularizadas e irrepetíveis desta, ou seja, dos aspectos que a individualizam perante as demais, ainda que a partir deste conhecimento haja sua associação com determinado grupo de outras pessoas²⁶.

Em termos gerais, considerando que o conjunto de dados pessoais se vincula diretamente com os atributos da *identidade pessoal* e da *imagem social* do titular, pois a partir do conhecimento destes quem os acessa passa a fazer juízo de valor sobre a pessoa e seus costumes ou características particulares, o tratamento deve se ater às condições que o titular permitiu, sendo ilícita a ação que não tiver sido expressamente autorizada ou que, embora consentida, tenha extrapolado, excedido ou se voltado para finalidade diversa da inicial, como se fosse uma espécie do prolongamento do próprio corpo do indivíduo²⁷, similar à forma que o direito à imagem deve ser respeitado²⁸.

Vale dizer, que a proteção de dados pessoais no Brasil teve como ponto de partida a Cláusula Geral de Privacidade estabelecida no artigo 5º, incisos X, XI e XII da Constituição Federal²⁹, em seguida aprimorada pelo Código de Defesa do Consumidor, artigo 43, que impunha a ciência do titular dos dados sempre que fosse aberto um cadastro com seus dados sem sua solicitação, dentre outras disposições e Código Civil pelos artigos 20, 21 e 12, protegendo a imagem, vida privada e os direitos de personalidade, respectivamente.

Não obstante, a Lei de Acesso à Informação nº 12.527 de 2011, em seu artigo 31, previu algumas linhas para o tratamento de dados pessoais por instituições de Direito Público ou de natureza privada que exerçam função pública e que mereceu regulamentação específica pelo

24 Cf. DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006, p. 193-196, a decisão considerou como abusiva a lei, em insuperável violação aos artigos 1º (1) e 2º (1) da Lei Fundamental, cf. BVerfG, 15.12.1983-1 BvR 209/83. Disponível em: <<https://research.wolterskluwer-online.de/#/document/f1bace50-1d75-40d2-8e17-789fa46e85ce?searchId=3406284>>. Acesso em: 10 set. 2020.

25 Cf. DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006, p. 193-196.

26 Cf. FLORIDI, Luciano. The ontological interpretation of informational privacy. *Ethics and information technology*, v. 185, n.7, 2005 citado por SOLOVE, Daniel J. *Understanding privacy*. Cambridge: Harvard University Press, 2009, p. 86, complementando na p.87, que a violação da privacidade pelo acesso indesejado de certos dados que o titular não queria que fossem expostos para que terceiros formassem opinião acerca deste, o que compromete sua identidade social ou honra objetiva e CHOERI, Raul Cleber da Silva. *O direito à identidade na perspectiva Civil-Constitucional*. Rio de Janeiro: Renovar, 2010, p.204.

27 FROSINI, Vittorio. La protezione della riservatezza nella società informatica. *Informatica e Diritto*. fascículo 1, jan.-abr., 1981, p.9-10 *apud* DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006, p.331.

28 Nesse sentido, BITTAR, Carlos Alberto. *Os direitos da personalidade*. 7 ed. atual. por Eduardo Carlos Bianca Bittar. Rio de Janeiro: Forense Universitária, 2008, p. 94-102.

29 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Decreto nº 7.724 de 2012 no âmbito do Poder Executivo Federal.

Cuidando de modo específico da matéria, o Marco Civil da Internet inaugurou o tratamento de dados pessoais por particulares no direito brasileiro, ainda que com tímidas disposições, mas nem por isso ineficientes, que estabeleceu princípios e obrigações ao tratador de dados que os obtiver a partir de aplicação de internet e reafirmou princípios e garantias constitucionais, artigos 3º, incisos II e III, 7º incisos I a III e VI a XI, e 16, tendo sido também regulamentado pelo Decreto nº 8.771 de 2016.

Depois de oito anos de discussão e debates, o Brasil aprovou a lei nacional que cuida do tratamento de dados pessoais, nº 13.709 de 2018, seguindo as principais disposições da Regulação Europeia 2016/679, merecendo destaque a introdução do legítimo interesse do tratador como dispensa do consentimento do titular para que trate seus dados no Direito Brasileiro, no artigo 10º, por exemplo.

Com vistas a garantir o cumprimento da lei, há previsão de sanções severas para quem violar os termos ou princípios estabelecidos durante o tratamento de dados pessoais em seu artigo 52, que compreende desde a advertência, multa de até cinquenta milhões de reais, proibição do tratamento até segunda ordem e deleção dos dados que estiverem sob poder do titular faltoso.

Feitas essas indispensáveis considerações sobre o tratamento de dados pessoais e privacidade, passar-se-á à análise de algumas medidas tomadas pelos entes de governo durante o período de contingência sanitária para prevenção da COVID-19 que colidiram diretamente com a matéria em comento.

3 MEDIDAS GOVERNAMENTAIS QUE AFETARAM A PROTEÇÃO DE DADOS PESSOAIS

3.1 Medida Provisória nº 954/2020

O primeiro ato de governo que afetou a proteção de dados pessoais que merece avaliação foi a edição da Medida Provisória nº 954 de 17 de abril de 2020, em que havia a disposição expressa para envio de dados cadastrais dos titulares pelos serviços de telefonia fixa ou móvel ao Instituto Brasileiro de Geografia e Estatística³⁰, cuja finalidade indicada era viabilizar o contato para entrevistas não presenciais pelo órgão³¹.

O édito presidencial também previu que tais dados teriam caráter sigiloso, que seriam utilizados exclusivamente para a realização das mencionadas entrevistas e que não poderiam ser aproveitados em processos administrativos, fiscais ou judiciais, ou ainda, que havia proibição de compartilhamento com quaisquer terceiros, além de indicar a obrigação de o órgão informar como os dados foram utilizados e de publicar relatório de impacto à proteção de dados pessoais nos termos da LGPD³².

30 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.

31 Art. 2º (...) § 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.

32 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.

Complementarmente, conforme descrito na exposição dos motivos pelo Ministro da Economia, indicou-se a necessidade de tais dados para que a Pesquisa Nacional por Amostra de Domicílios (PNAD) continue suas operações e para que fosse gerada massa de dados útil ao enfrentamento da pandemia, genericamente mencionado³³.

Sob intensas críticas, a vigência desta medida foi suspensa pelo Supremo Tribunal Federal em 26 de abril de 2020 por decisão liminar da Exma. Min. Rosa Weber na Medida Cautelar acostada à Ação Direta de Inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil, vez que entendeu não haver interesse público efetivo na medida, além de não estarem satisfeitos os requisitos de adequação e necessidade e ausentes os requisitos mínimos de segurança para o tratamento dos dados pessoais previsto³⁴.

Assim, entendeu que não estariam preservadas as garantias fundamentais dos brasileiros, uma vez que não havia razões suficientes para que se mitigasse o direito à privacidade e sigilo dos dados dos cidadãos em benefício da realização de estatísticas e outros propósitos não detalhados amiúde, pois vige a regra forte do *privacy by default/por padrão*³⁵.

Também foi observado pela Exma. Min. Rosa Weber que houve mau procedimento do próprio IBGE, pois submeteu ofícios em 22 de abril de 2020 para as empresas controladoras dos dados mencionados na aludida Medida Provisória exigindo o envio destes em imediato, contrariando os prazos os previstos em seu no texto³⁶, revelando-se inegável risco à privacidade

33 MINISTÉRIO DA ECONOMIA. EM nº00151/2020 ME. 15 abr. 2020. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Exm/Exm-MP-954-20.pdf>. Acesso em: 10 set. 2020: “3. Não se pode olvidar da relevância dessas atividades de produção estatística, inclusive para o enfrentamento da pandemia, o que urge a adoção de medidas que viabilizem, por outros meios, a produção desse relevante insumo para o implemento de políticas públicas. No caso da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua), que consiste na maior operação estatística domiciliar empreendida regularmente pelo IBGE, com mais de 200 mil domicílios pesquisados a cada trimestre, vislumbra-se como alternativa imediata a substituição temporária da coleta presencial pela coleta através de telefone, de modo que sejam garantidas as entrevistas e mantidas as séries históricas da pesquisa.

4. *Para que seja viável uma adaptação metodológica dessa natureza, o IBGE necessita ter acesso a informações sobre o número de telefone e respectivo endereço residencial dos consumidores de serviços de telecomunicações, de pessoas naturais ou jurídicas. (...)*

5. A garantia de realização da PNAD Contínua reveste-se de especial relevância no presente momento, já que a pesquisa deverá ser veículo para a inclusão de quesitos relacionados ao monitoramento da pandemia de COVID-19 em todo o território nacional, orientando políticas públicas e o processo decisório nas mais distintas esferas. A capilaridade da pesquisa possibilitará o levantamento de dados representativos para diferentes níveis geográficos e de segmentos socioeconômicos. (grifos no original)

34 STF. Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387 - DF, Rel. Exma. Min. Rosa Weber, j. em 27.4.2020. Disponível em: <<http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>>. Acesso em: 10 set. 2020: “17. Observo que o único dispositivo da MP n. 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o §1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados. (...) Nessa ordem de ideias, não emerge da Medida Provisória n.954/2020, nos moldes em que posta, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade da medida. E tal dever compete ao Poder Executivo ao editá-la. Nessa linha, ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva. De outra parte, o art. 3º, I e II, da MP n. 954/2020 dispõe que os dados compartilhados “terão caráter sigiloso” e “serão utilizados exclusivamente para a finalidade prevista no § 1º do art. 2º”, e o art. 3º, § 1º, veda ao IBGE compartilhar os dados disponibilizados com outros entes, públicos ou privados. Nada obstante, a MP n. 954/2020 não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, seja no seu tratamento. Limita-se a delegar a ato do Presidente da Fundação IBGE o procedimento para compartilhamento dos dados, sem oferecer proteção suficiente aos relevantes direitos fundamentais em jogo. Ênfase: ao não prever exigência alguma quanto a mecanismos e procedimentos para assegurar o sigilo, a higidez e, quando o caso, o anonimato dos dados compartilhados, a MP n. 954/2020 não satisfaz as exigências que exsurgem do texto constitucional no tocante à efetiva proteção de direitos fundamentais dos brasileiros.” (grifos no original)

35 Esse princípio contém as restrições que proíbem o controlador de realizar o tratamento incompatível de dados do titular considerando suas legítimas expectativas pelos propósitos que justificam o tratamento, assim descrito pela General Data Protection Regulation (GDPR): “2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.” Em tradução livre do autor: “O controlador deverá implementar medidas técnicas e organizacionais para assegurar que, por padrão, somente serão tratados os dados pessoais que forem necessários para cada propósito determinado.” A norma técnica NBR ISO/IEC 27701:2019, p. 51, assim descreve tal ideia: “Assegurar que processos e sistemas sejam projetados de forma que a coleta e o tratamento de DP (...) estejam limitados ao que é necessário para o propósito identificado.”

36 Art. 2º (...)

§ 3º Os dados deverão ser disponibilizados no prazo de:

I – sete dias, contado da data de publicação do ato de que trata o § 2º;

das pessoas físicas e jurídicas do país³⁷.

Em razão de o plenário corroborar com as razões apresentadas, apenas o Exmo. Min. Marco Aurélio foi contrário à suspensão da eficácia da referida Medida Provisória em 7 de maio de 2020³⁸.

De fato, não há como sustentar a legalidade na imposição da maior remessa de dados pessoais na história do Brasil com as justificativas apresentadas para a utilidade, necessidade ou adequação do referido Édito Presidencial, sobretudo no período de contingência que foi instaurado no país.

Imediatamente se identifica violação do princípio do *privacy by design/desde a concepção*, pois a medida foi imposta pelo governo exatamente com a intenção de se quebrar a privacidade ao revés de preservá-la, contrariando a ideia expressamente inserida no §2º do artigo 46 da LGPD³⁹, que as medidas de proteção do tratamento devem ser aplicadas desde a concepção da atividade para se evitar incidentes.

Também, é percebida falta de razoabilidade em se determinar que a continuidade da Pesquisa Nacional por Amostra de Domicílios (PNAD) durante o período de pandemia fosse prioridade, uma vez que a preservação das vidas deveria ser a premissa para o direcionamento das políticas públicas, considerando que seria a aplicação prática imediata para a preservação do bem jurídico mais valioso para ao antropocentrismo jurídico⁴⁰.

Noutras palavras: não é possível conceber em que medida tal tratamento de dados efetivamente contribuiria para a maior preservação da vida de quem estivesse sob a tutela do estado brasileiro, ou ainda, não se encontrou razão que justificasse a atuação da Fundação IBGE para a continuidade de suas atividades de censo durante a contingência da severa pandemia.

Convém ressaltar que a *vacatio legis* da Lei Geral de Proteção de Dados Pessoais (LGPD) provoca hiato no Ordenamento Jurídico nas hipóteses de tratamento de dados pessoais sem o consentimento do titular, que seria uma das situações hipóteses do artigo 7º, III⁴¹, portanto, sendo impossível a realização do pretendido sem a autorização expressa do titular dos dados, pela aplicação direta do princípio *privacy by default/por padrão*, salvo melhor juízo.

Além disso, se percebe contrassenso imediato pela exigência do endereço dos titulares quando vai se pretender realizar atividade de censo e pesquisa de forma remota, isto é, o dado se mostra irrelevante⁴², pois as informações sociais que merecem ser assinaladas

37 “20. Verifico, ainda, que na mesma data da publicação da MP n.954/2020 foi editada a Instrução Normativa n. 2, de 17 de abril de 2020, que estabelece procedimentos para disponibilização de dados de empresas de telecomunicações prestadoras de serviço telefônico fixo ou móvel ao Instituto Brasileiro Geográfico e Estatístico -IBGE, para fins de suporte à produção de estatística oficial, durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus. A referida Instrução Normativa teria embasado o envio, em 22.4.2020, segundo noticiado nos autos, de ofícios da Fundação IBGE às empresas de telefonia fixa comutada ou móvel pessoal, solicitando, com urgência, o compartilhamento imediato de dados, não obstante o prazo de sete fixados pela Medida Provisória 954/2020 e a determinação deste Supremo Tribunal Federal para a prestação de informações acerca do conteúdo deste ato normativo (doc. 24 do processo eletrônico).”

38 Na ausência de publicação do referido acórdão, essas foram as informações institucionais a partir da sessão realizada por videoconferência. STF. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. 7 maio 2020. Disponível em: <<http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902>>. Acesso em: 10 set. 2020.

39 Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (...)

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

40 Cf. TOBEÑAS, José Castán. *Los derechos de la personalidad*. Madrid: Reus, 1952, p. 6: “La persona individual tiene una esfera de poder jurídico. Precisamente el Derecho existe por causa del hombre y es éste el sujeto primario e indefectible del Derecho privado, al igual que del Derecho público”.

41 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

(...) III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

42 Seguindo o previsto na LGPD: Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...)

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; (...)

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; (...)

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

para fins de censo ou de emergência sanitária não necessariamente demandam saber qual o endereço físico do titular.

É evidente que a quantidade de dados envolvida nas operações não seria manejada a contento, especialmente pela dificuldade em não apenas armazenar, mas indexar e organizar tais informações em tempo diminuto para que a Fundação IBGE cumprisse com os objetivos declarados, sobretudo porque o número de telefones celulares já supera a quantidade de brasileiros desde 2018⁴³.

Não obstante, a ausência de um documento asseverando como o tratamento desses dados pessoais seria feito já no momento da publicação da Medida Provisória é suficiente para provocar insegurança jurídica intensa, sobretudo na realidade em que o uso das ferramentas tecnológicas tem servido a fins político-partidários e, conseqüentemente, vem prejudicando o espírito da democracia ao revés de incrementá-lo.

Por isso, diante da ausência da previsão de controles de segurança e medidas de resposta a incidentes mínimos indispensáveis, a exemplo do detalhamento da proteção da informação em todos os estados dos dados (uso, transmissão e repouso) e como se daria o descarte desses depois que se exaurisse a utilidade insuficientemente informada, somada às outras deficiências anteriores é que se formou justificada contrariedade ao mencionado Édito Presidencial⁴⁴.

Não é plausível haver pressa ou urgência na reunião de banco de dados da magnitude pretendida sem o atendimento básico de critérios de segurança jurídica e de segurança de informação, pois, ao revés de se solucionar um problema posto, dá-se azo a criar tantos outros, o que apenas dificulta ainda mais o cenário revelado de crise.

De todo modo, poder-se-ia obter resultado mais proveitoso para o combate da pandemia com os esforços voltados para a pasta governamental adequada aos assuntos de saúde pública, preterindo-se momentaneamente as atividades de censo e estatística geral da população, sobretudo no cenário de insegurança social que foi instaurado.

O uso pontual de dados pessoais orientado pelo princípio da minimização⁴⁵ também serviria para preservar a privacidade dos titulares ao revés da imposição indiscriminada de remessa de informações sobre as pessoas da forma realizada, o que se assemelhou à arbitrariedade legislativa na execução do censo na Alemanha anteriormente mencionada, uma vez que reconhecido o abuso à privacidade pela quantidade de perguntas que deveriam ser respondidas (160) e risco no comprometimento do sigilo dos dados pessoais envolvidos pela massa de informações que ficariam sob tutela do Estado.

3.2 Medida Provisória nº 959/2020

Como se não fosse suficiente o cenário posto, havia legítima preocupação dos controladores do tratamento de dados pessoais a despeito LGPD, pois sua entrada em vigor se

43 Cf. pesquisa da Fundação Getúlio Vargas divulgada por Daniel Junqueira in Brasil já tem mais smartphones do que habitantes. *Olhar Digital*. 20 abr. 2018. Disponível em: <<https://olhardigital.com.br/noticia/brasil-ja-tem-mais-smartphones-do-que-habitantes/75627>>. Acesso em: 10 set. 2020.

44 Esses foram apenas alguns dos critérios não observados pela legislação que, aparentemente, ignorou também a orientação técnica vigente no país sobre a matéria, a NBR ISO/IEC 27701:2019, que indica as recomendações para adoção de medidas que atendam às ideias de privacy by design/desde a concepção, por exemplo. Ou ainda, pelo não atendimento aos controles basilares previstos pela NBR ISO/IEC 27002:2013 que visa à formação de sistemas de informação confiáveis, pois inexistente qualquer disposição sobre controles de acesso, segregação de funções e segurança física necessária para que incidentes fossem evitados.

45 Incorporado na descrição do princípio da necessidade na Lei Geral de Proteção de Dados Pessoais (LGPD), artigo 6º, III já mencionado na NR 40, sendo definido pela utilização da mínima quantidade de dados pessoais e no menor tempo possível para se alcançar o resultado pretendido.

daria no dia 16 de agosto de 2020⁴⁶ e, seguindo pesquisas de mercado e cultura empresarial, em fevereiro de 2020 a monta de 25% das pequenas e médias empresas não conheciam a referida lei e apenas 40% dos empresários das brasileiras entrevistadas disseram estar totalmente preparados em uma enquete⁴⁷, sendo que resultado similar também foi alcançado, em que 58% das pequenas empresas brasileiras ainda não tinham se adaptado à lei⁴⁸.

De tal sorte, é razoável tomar como premissa que a reta final da *vacatio legis* se prestaria à maioria dos pequenos e médios empresários concluir os processos de conformidade com a LGPD em curso ou que ainda se iniciariam, o que foi brutalmente comprometido pela contingência da COVID-19, pois a rotina do comércio foi alterada sobremodo com o a restrição de circulação das pessoas.

Noutras palavras, se havia dedicação e preocupação dos controladores nas atividades de tratamento de dados pessoais já em execução para readequar seus fluxos e operações, de repente se viram compelidos a redirecionar seus recursos para tentar normalizar as atividades produtivas durante o período de contingência, pois, conforme já se adiantou, toda a estrutura do negócio foi abalada.

Tal se deve desde a mudança de como a atividade produtiva continuaria, levando-se em consideração os ajustes necessários para que continuasse em atenção à impossibilidade de frequência presencial do estabelecimento, ou ainda que seria alterado o modo que os funcionários executariam suas atividades de labor fora das instalações físicas da empresa, tendo impacto direto na necessidade de aquisição de equipamentos e outras tecnologias para que a adaptação fosse possível.

De tal sorte, se em um momento a preocupação era estar conforme com a LGPD antes de sua entrada em vigor, de repente se transformou em como manter o negócio em atividade com a disseminação do vírus e as medidas de contingência sanitária, o que se apresenta como situação sensivelmente severa.

Então, o governo tomou acertada decisão em editar a Medida Provisória nº 959 de 2020 que previa a entrada em vigor da LGPD somente no dia 3 de maio de 2021, estendendo a vacância da lei de modo que houvesse tempo suficiente para que se alcançasse a maior conformidade legal possível, sobretudo porque a própria Autoridade Nacional de Proteção de Dados ainda não tinha recebido regulamentação de sua estruturação básica quando as medidas de contingência sanitária foram impostas.

Todavia, já se sabia que a vigência de tal Medida Provisória duraria por 120 dias no máximo, ficando a tarefa de cuidar definitivamente do tema direcionada ao Parlamento⁴⁹, que

46 Cf. Art. 8º da Lei Complementar nº 95 de 1998: Art. 8º A vigência da lei será indicada de forma expressa e de modo a contemplar prazo razoável para que dela se tenha amplo conhecimento, reservada a cláusula “entra em vigor na data de sua publicação” para as leis de pequena repercussão.

§ 1º A contagem do prazo para entrada em vigor das leis que estabeleçam período de vacância far-se-á com a inclusão da data da publicação e do último dia do prazo, entrando em vigor no dia subsequente à sua consumação integral.

Dado que a lei foi publicada no dia 15 de agosto de 2020 e a *vacatio* se encerraria no dia 15 de agosto de 2020, seguindo o prazo firmado no artigo 65, II: Art. 65. Esta Lei entra em vigor: (...)

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

47 Cf. ROSSI, Lucca. Um quarto das PMEs desconhece a nova lei de proteção de dados. CAPTERRA. 13 mar. 2020. Disponível em: <<https://www.capterra.com.br/blog/1357/nova-lei-de-protecao-de-dados/>>. Acesso em: 10 set. 2020.

48 Cf. IT FORUM 365. 58% das pequenas empresas não estão preparadas para a LGPD. 21 jan. 2020. Disponível em: <<https://itforum365.com.br/58-das-pequenas-empresas-nao-estao-preparadas-para-a-lgpd/>>. Acesso em: 10 set. 2020.

49 Da Constituição Federal: 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. (...)

§ 3º As medidas provisórias, ressalvado o disposto nos §§ 11 e 12 perderão eficácia, desde a edição, se não forem convertidas em lei no prazo de sessenta dias, prorrogável, nos termos do § 7º, uma vez por igual período, devendo o Congresso Nacional disciplinar, por decreto legislativo, as relações jurídicas delas decorrentes. (...)

§ 7º Prorrogar-se-á uma única vez por igual período a vigência de medida provisória que, no prazo de sessenta dias, contado de sua publicação, não tiver a sua votação encerrada nas duas Casas do Congresso Nacional.

efetivamente decidiria se o referido Édito se converteria em lei ou perderia a eficácia.

Às vésperas da perda de sua eficácia, 26 de agosto de 2020, em entendimento contrário à da Câmara dos Deputados, o Senado Federal optou por retirar o texto de extensão da vacância que entraria em vigor, fazendo com que o prazo de 16 de agosto fosse restaurado para a entrada em vigor definitiva da parte dispositiva da LGPD.

Entretanto, a eficácia da LGPD não seria imediata, pois ainda dependia de rito formal do Presidente da República para sanção ou veto da MP 959 convertida em lei, ainda sendo válidas as disposições nela contidas até que ocorra um dos dois atos⁵⁰.

Portanto, a LGPD poderá entrar em vigor até o dia 19 de setembro de 2020, considerando a hipótese que a firma presidencial ocorra no último dia de prazo e a publicação ocorra somente no dia subsequente, como é trivial.

Ato contínuo, houve a edição do Decreto nº 10.474 também no dia 26 de agosto de 2020, estabelecendo a estrutura organizacional da Autoridade Nacional de Proteção de Dados (ANPD) em complementação do já disposto na LGPD, de modo a contribuir para o mais rápido estabelecimento de suas atividades, já que a entrada em vigor da parte dispositiva exigirá deveres de orientação, dirigismo e fiscalização do tratamento de dados pessoais no Brasil, tarefas indispensáveis para que se mantenha o nível de competitividade esperado na incubação de novos negócios e reestruturação tecnológica dos já existentes.

Pela proximidade das datas indicadas no momento de conclusão deste artigo, não é esperado que em futuro próximo a ANPD esteja em pleno funcionamento, seja pelo contexto político conturbado e escassez de recursos para contornar as consequências trazidas pelas medidas de contingência, o que vai prejudicar a aplicação das providências dispositivas que até outubro de 2020 já estarão em pleno vigor e efeito.

Com isso, se aventa a possibilidade de a lei estar vigente e haver dificuldades para a operacionalização das garantias e direitos previstos, sobretudo pelo hiato que a ausência de completa operação da ANPD pode causar, podendo até perder a credibilidade de sua efetividade, pois, qual é o exemplo que se quer passar quando há descumprimento escancarado de previsão que deveria ser realizada até a entrada em vigor da LGPD a despeito da adequação progressiva das bases de dados formadas antes de sua existência⁵¹?

Nesse sentido, o Parlamento teve chance de evitar que a lei entrasse em vigor com dispositivos já desatendidos pela própria desorganização do governo, mas, preferiu-se pela euforia e ímpeto de se evitar nova postergação, o que não foi acertado.

Assim, a resposta para o questionamento feito dificilmente será satisfatória com tamanho descompasso entre o que está previsto na LGPD e as medidas tomadas de cunho político que deveriam buscar a harmonia jurídica e guiada pela maior proteção possível dos interesses dos titulares dos dados, mas que apenas aumentam o tumulto acerca do tema que já é suficientemente complexo.

50 Da Constituição Federal: Art. 62 (...)

§ 12. Aprovado projeto de lei de conversão alterando o texto original da medida provisória, esta manter-se-á integralmente em vigor até que seja sancionado ou vetado o projeto.

51 A título de exemplo, segue o disposto no artigo 63 da LGPD que, praticamente virou letra morta, pois o prazo dado não comportará o tempo necessário para que a ANPD dê as orientações estipuladas: Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

4 DOS ACORDOS DE COOPERAÇÃO TÉCNICA OCORRIDOS NO ESTADO DE SÃO PAULO – DADOS ANONIMIZADOS DE DESLOCAMENTO COLETADOS A PARTIR DOS TELEFONES CELULARES

Assim que anunciadas na coletiva de imprensa do dia 9 de abril de 2020, as medidas tomadas pelo Governo do Estado de São Paulo também causaram desconforto pelo tipo de monitoramento que havia sido declarado: a partir do deslocamento detectado a partir do sinal do telefone celular denominado SIMI: Sistema de Monitoramento Inteligente⁵².

Tal desconforto se intensifica à medida que exatamente 1 dia antes houve reportagem que antecipou as tecnologias utilizadas com os dados da operadora de telefonia Vivo a despeito dos índices de isolamento social atingidos pela população do Estado em questão⁵³ e que, eventualmente, estavam sendo realizadas à revelia dos próprios clientes da referida empresa.

Sob esse contexto, houve medidas judiciais que visaram restringir a execução de tal medida estatal, justamente pela sensação de controle individual que fere o direito à privacidade dos cidadãos, cuja ligação com a expressão do *'Big Brother'* da obra distópica 1984 de George Orwell é praticamente imediata e assombra os usuários de *smartphones* e outros *gadgets* que permitem a funcionalidade de localização por sinal de antenas ou posicionamento global via satélite (*Global Positioning System*)⁵⁴.

Ainda que inicialmente tivesse logrado êxito o mandado de segurança coletivo impetrado no Tribunal de Justiça do Estado de São Paulo em sede liminar, julgou-se pela legalidade da medida governamental, cujo cerne da decisão do Colegiado foi a existência do tratamento de dados anonimizados⁵⁵, que sequer deveriam ser considerados como *'dados pessoais'* para fins de tratamento nos termos da LGPD⁵⁶, servindo como referência, ainda que não vigente.

No Superior Tribunal de Justiça, entretanto, houve-se por bem o indeferimento liminar do Habeas Corpus impetrado, pois não seria o remédio jurídico adequado para lidar com arbitrariedades que limitem os direitos de personalidade e não comprometam o direito de ir

52 Cf. G1. SP usa sistema de monitoramento com sinais de celulares para localizar aglomeração de pessoas no estado. 9 abr. 2020. Disponível em: <<https://g1.globo.com/sp/sao-paulo/noticia/2020/04/09/sp-usa-sistema-de-monitoramento-com-sinais-de-celulares-para-localizar-aglomeracao-de-pessoas-no-estado.ghtml>>. Acesso em: 10 set. 2020.

53 Cf. G1. Coronavírus: Governo paulista usa sinal de celular para monitorar quarentena. 8 abr. 2020. Disponível em: <<http://g1.globo.com/sao-paulo/videos/v/coronavirus-governo-paulista-usa-sinal-de-celular-para-monitorar-quarentena/8466867/>>. Acesso em: 10 set. 2020.

54 A título de exemplo foram o Mandado de Segurança Coletivo nº 2069736-76.2020.8.26.0000, impetrado no Tribunal de Justiça do Estado de São Paulo e o Habeas Corpus nº 572.996 – SP no Superior Tribunal de Justiça.

55 “Diante das elucidações técnicas trazidas pela autoridade impetrada (fls.313/325), pela FESP (fls. 106/128) e pela operadora Tim (fls. 192/208) razoável concluir que não se utilizam dados pessoais, mas apenas os anonimizados, de quantidade de conexões às Estações de Rádio Base das operadoras, e tão só para apurar as regiões com maior movimentação de pessoas. Ressalte-se ainda o lapso temporal de 24 horas para a transferência dessas informações. (...) Em resumo: assegurado o anonimato, preservado o sigilo dos dados apurados pelas empresas de telefonia móvel antes da transferência ao IPT, não há afronta a direito individual, inviabilizando o acolhimento da demanda” (TJSP, Mandado de Segurança Coletivo nº 2073723-23.2020.8.26.0000, Rel. Des. Evaristo dos Santos, j. em 4.6.2020)

56 Art. 5º (...)

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

e vir⁵⁷, por não ser esse o objetivo da natureza de tal *mandamus*.

Para avaliar juridicamente a situação posta, é indispensável que alguns recortes sejam realizados para que se compreenda a dimensão do problema posto na perspectiva do titular de dados pessoais, o que não deveria ser tão difícil por quem adota tais medidas.

O primeiro deles diz respeito à reportagem realizada no dia 8 de abril de 2020, um dia antes da divulgação da existência do SIMI, em que os dados de determinada empresa de telefonia eram expostos, haja vista já haver pacto firmado entre o Instituto de Pesquisas Tecnológicas de São Paulo, IPT e a Telefonica Brasil S.A. para o fornecimento de dados de deslocamento de usuários agregados anonimizados, firmado no dia 27 de março de 2020.

Ainda neste recorte para estudo, identifica-se o documento firmado pela Associação Brasileira de Recursos em Telecomunicações – ABR e as quatro maiores operadoras de telefonia celular do país, Claro, Vivo, TIM e Oi com o IPT-SP, datado de 16 de abril de 2020, que daria sustentação técnica ao SIMI, instituído pelo Decreto nº 64.963, de 5 de maio de 2020.

Para fins de condução do SIMI, se instituiu o ‘Comitê Gestor’, coordenado por 1 representante da Secretaria de Governo, 1 representante da Secretaria de Desenvolvimento Econômico, 2 representantes da Secretaria de Saúde e 1 representante do IPTelo Secretário de Governo.

Então, sob a perspectiva governamental, é possível concluir que a medida escolhida pelo Governo do Estado de São Paulo contou com representantes (dos interesses) das empresas e (dos interesses) do governo, mas, nenhum ente efetivamente fiscalizador ou controlador que estivesse apto a proteger (os interesses) das pessoas que teriam seus dados pessoais anonimizados coletados para uso do mencionado Governo.

Noutro recorte, na perspectiva dos clientes, se não fosse por intervenção da imprensa, dificilmente se chegaria ao conhecimento destes que haveria o uso de informações desta natureza para medição do isolamento social, sobretudo pela falta de transparência nas quais as mencionadas medidas foram divulgadas à população.

Tais descompassos poderiam ser mitigados e evitados com a inclusão de representantes não apenas das secretarias de governo, mas da própria sociedade civil que estivessem profissionalmente preparados e dedicados à preservação da privacidade, funcionando como os esperados freios e contrapesos aos comportamentos de quem está executando as ordens do Governo do Estado, mecanismo de balanceamento indispensável para que os conflitos de interesses⁵⁸ pudessem ser adequadamente harmonizados.

Diante desse quadro, caso não existissem as pretensões judiciais para interrupção das medidas tomadas, é difícil crer que haveria a divulgação dos contratos firmados espontaneamente pelas empresas de telecomunicações, a ABR ou até mesmo o IPT-SP, já que a divulgação das medidas veio desacompanhada do esclarecimento que deveria ser

57 “(...) Ou seja, não foram apontados quaisquer atos objetivos que possam causar, direta ou indiretamente, perigo ou restrição à liberdade de locomoção no caso – o que inviabiliza, por si só, o manejo do remédio heróico. Ora, “[o] risco de cumprimento, ante tempus, é meramente hipotético, sabendo-se que não cabe ação de habeas corpus contra o chamado, por alguns, ‘ato de hipótese’; portanto, não há constrangimento ilegal a ser evitado ou sanado pelo presente habeas corpus, o qual se mostra manifestamente incabível” (HC n.º 82.319/SP, Rel. Ministro Arnaldo Esteves Lima, Quinta Turma, DJ 12/09/2007). Entenda-se: a ameaça de constrangimento ao jus libertatis a que se refere a garantia prevista no rol dos direitos fundamentais (art. 5.º, inciso LXVIII, da Constituição da República) há de se constituir objetivamente, de forma iminente e plausível, e não hipoteticamente, como é a hipótese dos autos.” (STJ, HC nº 572.996 – SP, Rel. Min. Laurita Vaz, j. em 16.4.2020)

58 Conforme descrito por MICELI, Alexandre da Silveira de. *Governança Corporativa no Brasil e no Mundo*. Rio de Janeiro: Elsevier, 2010, p.53-54, o conflito de interesse não é cenário inovador ou inédito, principalmente, porque se assume que cada indivíduo busca maximizar sua sensação de bem-estar, também chamado de utilidade pessoal, que, por vezes, pode colidir ou ir em desencontro às decisões de outras pessoas, vez que essas também tomam decisões visando seu bem-estar, o que pode ser também aplicado para as decisões governamentais ou empresariais daquilo que se imagina como o melhor ou mais adequado a ser feito.

realizado proativamente, sobretudo pela maturidade da discussão do tratamento de dados pessoais na sociedade em virtude da LGPD.

Nesse sentido, as medidas indicadas não atenderam aos deveres de transparência e boa-fé que o Código de Defesa do Consumidor⁵⁹ e o Código Civil⁶⁰ exigem, pois, salvo melhor juízo, não está no aparato contratual das referidas prestadoras a autorização para tratamento de dados de seus clientes nos termos mencionados, o que dependeria de justo consentimento, pois a funcionalidade de localização do cliente pela operadora sem sua requisição fere os direitos de privacidade quando não expressamente por ele autorizados, em virtude de o serviço de telecomunicação contratado propriamente dito não depender de tal mecânica e essa funcionalidade espião não ser por ele razoavelmente esperada quando contrata tal serviço.

Tal conclusão é tirada a partir da já invocada Cláusula Geral de Privacidade, cujo entendimento implica em a regra ser a proteção da privacidade e a mitigação desta a exceção, modernamente abreviado por *privacy by default/por padrão*, que deve ter a leitura conjunta com o artigo 21 do Código Civil⁶¹ nesta situação concreta.

Assim, a conduta jurídica esperada pelo fornecedor do Serviço Móvel Pessoal (SMP) era atender ao requisito de autorização expressa para a coleta desses dados, que vai além de eventual autorização para compartilhamento desses com parceiros comerciais da empresa de telecomunicações⁶² ou quaisquer terceiros, pois o cerne do contrato celebrado visa ao fornecimento do SMP para o cliente, o que não subentende que haverá a coleta de dados de localização do titular durante sua utilização, pois não é pré-requisito para sua execução e fere, por óbvio, sua privacidade.

Isto é, o cliente paga a operadora de telefonia celular para realizar tráfego de dados utilizando a rede 2G/3G/4G, seja ele na forma de voz, internet, SMS, MMS etc. e não para ser ativamente monitorado, ainda que seja de forma anonimizada, posto que a repetição do padrão de movimentação pode individualizar determinado cliente ou facilitar o cruzamento dessas informações com outros dados que o irá individualizar e, com isso, descaracterizar a impessoalidade do dado.

Tal hipótese ocorreu no estado do Espírito Santo, em que a reportagem do *'The Intercept'* foi capaz de identificar com sucesso duas pessoas residentes em cidades com baixa população a partir do cruzamento de informações agregadas de deslocamento de clientes até então 'anonimizadas' com marcações de eventos e outras postagens em mídias sociais⁶³.

De tal sorte, seria excesso de inocência crer que tal recurso foi ativado durante o período de contingência sanitária, somente, sobretudo porque dever-se-ia ter certeza de seus resultados positivos para que o centro de inteligência do Governo do Estado de São Paulo (IPT-SP) fosse contar para alimentar as diversas secretarias e órgãos de governo com o fito de se vencer a pandemia.

59 Art. 6º São direitos básicos do consumidor: (...)

III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;

60 Art. 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé.

61 Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

62 Nesse sentido, o contrato do SMP ofertado pela Vivo prevê: "Quer receber da Vivo e parceiros ofertas e benefícios adequados ao seu perfil em seu celular? Para isso precisamos utilizar seus dados pessoais e de localização e uso na rede, que ficarão seguros em nosso banco de dados. Você ainda ajuda no desenvolvimento e melhoria de produtos. () Sim () Não."

63 Cf. DIAS, Tatiana. Vigiar e Lucrar. *The Intercept*. 13 abr. 2020. Disponível em: <<https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/>>. Acesso em: 10 set. 2020.

Esse recurso já é utilizado pela empresa Vivo desde 2013, chamado de *smart steps*, e permite que a partir dos dados de localização do cliente anonimizado sejam agregadas outras informações e, assim, gerar massa crítica com valor para fins mercantis, literalmente, às custas do próprio cliente.

Vale dizer, também, que mesmo sem a vigência da LGPD, a legislação em vigor permite às prestadoras do SMP que divulguem informações agregadas sobre o uso de seus serviços desde que seja impossível individualizar seus clientes⁶⁴, o que não se deve confundir com informações agregadas sobre a localização e trajetos realizados por seus clientes, posto que são dados inequivocamente distintos.

O uso do serviço compreende tanto a conduta ativa do cliente ao se valer da estrutura informacional com o fim de se comunicar com terceiros, seja via voz ou dados pelos mais diversos protocolos (TCP/IP, SMS, MMS etc.) quanto pela possibilidade de ser alcançado por outros usuários dos mesmos recursos, o que não depende do conhecimento da localização ou posição global do cliente para tanto, exatamente porque a ideia é permitir o serviço durante mobilidade, não importando a posição do usuário, mas, se existe a estrutura de sinal para que este consiga se comunicar.

Com isso, se percebe que o sentimento de vigilância e rastreamento antecede a própria calamidade pública, o que pode gerar ainda mais ansiedade por parte do cliente, já que nunca recebeu informações claras desta natureza ou conferiu qualquer autorização informada para a coleta dos dados de deslocamento nos moldes executados por quem provê o serviço de telefonia móvel.

O choque de realidade acontece quando o usuário se dá conta que é monitorado e acompanhado desde sempre por sabe-se lá quem e que dificilmente conseguirá se defender.

Ainda que sejam dados anonimizados, por fugirem do escopo principal do SMP contratado pelo cliente, o mínimo que deveria ser feito para homenagear a boa-fé objetiva e princípio da transparência, como já argumentado anteriormente, seria a empresa prestadora informar ao usuário que está apta a coletar dados de deslocamento e localização e perguntar expressamente se o titular autoriza a coleta desse tipo de dados com os fins já declarados, de modo que ele esteja apto a impedir que tais práticas fossem feitas consigo ou que este tome decisões já considerando a existência desse tipo de coleta de dados.

Isso para se respeitar o corolário da autodeterminação informativa, que já está incorporado na legislação brasileira consoante a Cláusula Geral de Privacidade e previsão expressa do *'habeas data'* na Constituição⁶⁵, além do disposto no Código de Defesa do Consumidor sobre os direitos daquele que estiver inserido em banco de dados⁶⁶.

Aparentemente, com a tomada dessas medidas, os melhores interesses do Governo se voltam para sua própria proteção e não para a defesa dos direitos de seus cidadãos, pois, sob o argumento de monitorar a eficácia das medidas de quarentena impostas para

64 Da Lei Geral de Telecomunicações, nº 9.472 de 1996:

Art. 72. Apenas na execução de sua atividade, a prestadora poderá valer-se de informações relativas à utilização individual do serviço pelo usuário. (...)

§ 2º A prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade.

65 Art. 5º (...) LXXII - conceder-se-á habeas data:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

66 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. (...)

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

proteção da vida se faz uso dos relatórios provenientes da coleta de dados massificados não expressamente autorizada aos clientes-titulares e divulga tais atos como sendo algo bom.

Pior que isso, não foram implementadas medidas e ordens de controle para que se verificasse se realmente haveria a anonimização dos dados antes da remessa, da qualidade dos dados produzidos para que não houvesse distorção ou falta de adequação das medidas tomadas pelos órgãos de governo que tivessem como base os resultados obtidos pelo IPT-SP.

Desta sorte, o racional de legalidade do uso de tais informações está calcado na ação dos terceiros controladores do tratamento de dados pessoais, ou seja, caso os dados não sejam efetivamente anonimizados ou que são passíveis de reversão contrariando o que foi assentado na LGPD, se permitiu uma barbaridade.

Nesse sentido, é absurdo não haver qualquer prática de fiscalização externa para que fosse assegurada a proteção da privacidade das pessoas, sobretudo em tempos de extrema adversidade, em que a qualidade de vida já fica comprometida pelo próprio contexto de pandemia e que não deveria ser agravada ao se transparecer que existe monitoramento ativo das pessoas e que ocorre à revelia destas.

5 CONCLUSÕES

Por todo o avaliado no presente artigo, tem-se que a cultura de proteção de dados pessoais e privacidade ainda dependerá de maturação por parte dos agentes públicos e entidades privadas, pois a não compreensão da condição do titular dos dados como sendo soberano em atenção às informações que lhe dizem respeito, em razão da autodeterminação informativa, gera distorções e insegurança jurídica para todo o contexto social.

É preocupante atestar tentame de obtenção compulsória de dados pessoais a partir de edição de lei ou ato governamental equivalente, ignorando a necessidade de consentimento do titular quando inexistente qualquer abertura legal para esse tipo de requisição, a exemplo do que houve com a MP 954/2020.

Não obstante, beira à irresponsabilidade exigir a remessa desmedida de dados pessoais para órgão que possui fins estatísticos para continuidade de atividade de censo durante período de contingência e sem a devida cautela com a segurança dos dados, expondo dados da população inteira a inúmeros incidentes, o que leva a crer que todo do processo de aprendizado para a promulgação da LGPD não foi suficiente.

Também se constatou a falta de cuidado do legislador que decidiu pela entrada em vigor da LGPD durante delicado período de contingência sanitária e permitiu o descumprimento de seu artigo 63, prejudicando todos os controladores de dados que já possuíam bases de dados antes de sua entrada em vigor e aguardavam orientações da ANPD para que o fizessem da melhor forma.

Ao se optar por não adiar da vigência da LGPD mesmo com a ANPD ainda em vias de constituição e organização se constrói cenário de desamparo à mencionada lei, pois a Autoridade é peça fundamental para que haja o desenvolvimento da cultura de proteção de dados e privacidade de modo transversal nas atividades praticadas no Brasil, auxiliando na fiscalização e cumprimento das regras da forma mais orgânica possível.

Além disso, se constatou situações revestidas de ilegalidade praticadas sem qualquer pudor sob o manto da 'anonimização', mesmo quando a legislação que vige sequer recepcionou tal hipótese como exceção à regra de obtenção de consentimento ou autorização do titular dos dados para que houvesse sua coleta e compartilhamento.

Com base nesses atos à margem da lei, se percebe a necessidade de os controladores

de tratamento de dados pessoais melhor compreenderem o significado das ideias de *privacy by default/por padrão*, devendo se evitar a coleta indiscriminada de dados pessoais do titular que não são pré-requisitos para a prestação do serviço ou entrega do produto efetivamente contratado, pois o abuso de direito ocorrerá independentemente se os dados forem anonimizados, ou não, já que o racional determinante está vinculado com a justa expectativa de o titular ter aqueles dados tratados quando houver confronto com a necessidade e utilidade ao que realmente por ele se pretendeu receber.

Por fim, ainda que o recurso da anonimização de dados pessoais seja reconhecido como seguro, cuidados adicionais devem ser empregados para que se evite a recombinação de tais informações com outras provenientes de bases amplamente acessíveis, pois há fundada chance de ocorrer associação dos dados com seu titular.

REFERÊNCIAS

ABNT. *ISO/IEC 27701:2019 Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes*. Brasil: ABNT, 2019.

ALI, Imam Ibn Abi Talib. *Peak of eloquence*. Imam Al Khoei Islamic Center, 1983.

ALEMANHA. BVerfG, 15.12.1983 - 1 BvR 209/83 < <https://research.wolterskluwer-online.de/#/document/f1bace50-1d75-40d2-8e17-789fa46e85ce?searchId=3406284> > Acesso em: 10 set. 2020.

BACON, Francis. *Religious meditations*. Londres: John Laggard, 1613. Versão em e-book Disponível em: < <https://archive.org/stream/essaiesofsrfranc00baco#page/180/mode/2up> > Acesso em: 10 set. 2020.

BAKER, Stephen. *The Numerati*. Nova Iorque: Houghton Mifflin Harcourt, 2008. Edição Kindle

BÍBLIA. Português. Bíblia sagrada. Antigo Testamento. Tradução de João Ferreira de Almeida. 2 ed. Rio de Janeiro: Sociedade Bíblica do Brasil.

BITTAR, Carlos Alberto. *Os direitos da personalidade*. 7 ed. atual. por Eduardo Carlos Bianca Bittar. Rio de Janeiro: Forense Universitária, 2008.

BRASIL, Constituição, 1988.

BRASIL, Decreto nº 8.771, de 11 de maio de 2016.

BRASIL, Decreto nº 10.282, de 20 de março de 2020.

BRASIL, Lei nº 9.472, de 16 de julho de 1996.

BRASIL, Lei nº 10.406, de 10 de janeiro de 2002.

BRASIL, Lei nº 12.965, de 23 de abril de 2014.

BRASIL, Lei nº 12.965, de 23 de abril de 2014.

BRASIL, Lei nº 13.709, de 14 de agosto de 2018.

BRASIL, Lei nº 13.979, de 6 de fevereiro de 2020.

BRASIL, Medida Provisória nº 954, de 17 de abril de 2020.

BRASIL, Medida Provisória nº 959, de 29 de abril de 2020.

BRASIL. MINISTÉRIO DA ECONOMIA. *EM nº00151/2020 ME*. 15 abr. 2020. Disponível em: < http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Exm/Exm-MP-954-20.pdf > Acesso em: 10 set. 2020.

BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 572.996. Impetrante: André Gustavo Zanoni Braga De Castro. Paciente: Todos os moradores do Estado de São Paulo. Autoridade Coatora: Governador do Estado de São Paulo. Relatora: Ministra Laurita Vaz. Brasília, 16 de abril de 2020.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Relatora: Exma. Min. Rosa Weber, 27 de abril de 2020. Disponível em: < <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf> > Acesso em: 10 set. 2020.

BRASIL. Tribunal Regional Federal da 4ª Região. Apelação nº 0000651-41.2005.404.7103/RS. Apelante: Marcio Adriano Dornelles Martins e outros. Apelada: União Federal. Relator: Des. Federal Carlos Eduardo Thompson Flores Lenz. Porto Alegre, 13 de julho de 2010.

CASTELLS, Manuel. *Communication power*. 2. ed. Oxford: Oxford University Press, 2013. Edição do Kindle

CHOERI, Raul Cleber da Silva. *O direito à identidade na perspectiva Civil-Constitucional*. Rio de Janeiro: Renovar, 2010.

DAVIES, Susanna. Introduction: information, knowledge and power. *IDS Bulletin* 25.2, 1994. Disponível em: < <https://www.ids.ac.uk/files/dmfile/davies252.pdf> >

DEPARTAMENTO DE SEGURIDAD NACIONAL. *Coronavirus (COVID-19) - 30 de abril 2020*. 30 abr. 2020. Disponível em: < <https://www.dsn.gob.es/es/actualidad/sala-prensa/coronavirus-covid-19-30-abril-2020> > Acesso em: 10 set 2020.

DIAS, Tatiana. Vigiar e Lucrar. *The Intercept*. 13 abr. 2020. Disponível em: < <https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/> > Acesso em: 10 set 2020.

DONEDA, Danilo. *Da Privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006

FROSINI, Vittorio. Diritto alla riservatezza e calcolatori elettronici. In ALPA, Guido; BESSONE, Mario (Orgs.) *Banche dati telematica e diritti della persona*. Padova: Cedam, 1984.

G1. *Coronavírus: Governo paulista usa sinal de celular para monitorar quarentena*. 8 abr. 2020. Disponível em: < <http://g1.globo.com/sao-paulo/videos/v/coronavirus-governo-paulista-usa-sinal-de-celular-para-monitorar-quarentena/8466867/> > Acesso em: 10 set 2020.

G1. *SP usa sistema de monitoramento com sinais de celulares para localizar aglomeração de pessoas no estado*. 9 abr. 2020. Disponível em: < <https://g1.globo.com/sp/sao-paulo/noticia/2020/04/09/sp-usa-sistema-de-monitoramento-com-sinais-de-celulares-para-localizar-aglomeracao-de-pessoas-no-estado.ghtml> > Acesso em: 10 set 2020.

HOBBS, Thomas. *Concerning body*. 1655. In *The English Works of Thomas Hobbes of Malmesbury*. Now first collected and edited by Sir. Bart William Molesworth. v. 1. Londres: John Bohn, 1839. Versão em e-book do Google Play. Disponível em: < https://play.google.com/books/reader?id=Gr8LAAAIAAJ&hl=pt_BR&pg=GBS.PA1 > Acesso em: 10 set 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27002:2013 Information technology -- Security techniques – Code of practice for information security controls*. 2. ed. Suíça: International Organization for Standardization, 2013.

IT FORUM 365. *58% das pequenas empresas não estão preparadas para a LGPD*. 21 jan. 2020. Disponível em: < <https://itforum365.com.br/58-das-pequenas-empresas-nao-estao-preparadas-para-a-lgpd/> > Acesso em: 10 set. 2020.

3E2.0.CO%3B2-C > Acesso em: 10 set. 2020.

WORLD HEALTH ORGANIZATION. *Coronavirus disease (COVID-19) advice for the public*. 4 jun. 2020. Disponível em: < <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public> > Acesso em: 10 set. 2020.

WORLD HEALTH ORGANIZATION. *WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020*. 11 mar. 2020. Disponível em: < <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> > Acesso em: 10 set. 2020.

Recebido em: 28.10.2020

Aprovado em: 20.12.2020

Como citar este artigo (ABNT):

HAIKAL, Victor Auido. Análise crítica da proteção de dados pessoais durante o período de contingência da covid-19. *Revista Eletrônica de Direito do Centro Universitário Newton Paiva*, Belo Horizonte, n.43, p.293-313, jan./abr. 2021. Disponível em: <<https://revistas.newtonpaiva.br/redcunp/wp-content/uploads/2021/06/DIR43-17.pdf>>. Acesso em: dia mês. ano.