O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19

Victória FÉLIX*

Juliano Ralo MONTEIRO**

RESUMO: O objetivo desse trabalho foi o de analisar o uso legítimo de dados pessoais, mediante tecnologias digitais, para a propositura de políticas públicas de saúde no contexto da pandemia de COVID-19. O método utilizado nessa pesquisa foi o dedutivo; quanto aos meios, a pesquisa foi bibliográfica e quanto aos fins, qualitativa. A conclusão a que se chegou foi a de que a coleta de dados pessoais e circulação de informações, no setor da saúde, são salutares para o combate de pandemias como a do SARS-COV-2, e com a atual entrada em vigor da Lei Geral de Proteção de Dados, a segurança jurídica no planejamento de políticas públicas nesse setor será maior desde que observados princípios norteadores para o tratamento de dados, e que o órgão fiscalizador instituído estabeleça outras diretrizes e um diálogo para efetiva proteção de dados pessoais.

PALAVRAS-CHAVE: Dados pessoais; saúde pública; tecnologias digitais.

TITLE: The Use of Technologies and Personal Data in Public Health Policies in the COVID-19 Context

ABSTRACT: The objective of this work was to analyze the legitimate use of personal data, through digital technologies, for proposing public health policies in the context of the COVID-19 pandemic. The method used in this research was deductive; as for the means, the research was bibliographic and for the ends, qualitative. The conclusion reached was that the collection of personal data and the circulation of information in the health sector are satisfactory for combating pandemics, such as SARS-COV-2, and with the current entry into force of the General Data Protection Law, legal certainty in the planning of public policies in this sector will be greater provided that the guiding principles for the treatment of data are observed, and a supervisory body is established other guidelines and a dialogue for the effective protection of personal data.

KEYWORDS: Personal data; public health; digital technologies.

* Mestranda em Direito pela Universidade Federal do Amazonas (UFAM), pelo Programa de Pós-Graduação em Constitucionalismo e Direitos na Amazônia, Especialista em Direito e Processo do Trabalho pela Universidade do Estado do Amazonas (UEA) em parceria com a Associação dos Magistrados da Justiça do Trabalho da 11ª Região (AMATRA XI). Bacharel em Direito pela Universidade do Estado do Amazonas. Advogada.

** Doutor em Direito Civil pela Pontifícia Universidade Católica de São Paulo. Mestre em Direito pelo Centro Universitário FIEO. Especialista em Gestão Educacional pelo Instituto Damásio de Direito – IBMEC. Especialista em Docência do Ensino Superior pela Universidade Nilton Lins. Graduado em Direito pelo Centro Universitário FIEO. Vice-coordenador e Professor Permanente do Programa de Mestrado em Constitucionalismo e Direitos da Amazônia da Universidade Federal do Amazonas (UFAM). Professor Adjunto da Graduação da Faculdade de Direito da UFAM. Advogado.

1. Introdução

A pandemia da COVID-19, que assolou o mundo ao longo de 2020, por ser uma doença desconhecida, de rápido contágio e elevada mortalidade, provocou a atuação de diversos países, e seus respectivos governantes, em prol de elaboração de estratégias proativas para o controle da contaminação. É nesse cenário que o uso de tecnologias e dados pessoais para a formulação de políticas públicas de saúde alcança especial relevo, sobretudo porque além de evitar implicações na saúde pública, o completo isolamento social, medida adotada pelo Brasil, por exemplo, poderia estagnar o crescimento econômico e agravar outras mazelas sociais.

A pesquisa é relevante porque os dados pessoais tornaram-se um dos recursos mais valiosos na sociedade da informação, no âmbito da saúde podem ser citados inúmeros benefícios quando empregados em conjunto com inovações tecnológicas, como a otimização de recursos e melhor qualidade do serviço. Além disso, a atuação brasileira no combate à pandemia foi inócua, a Lei Geral de Proteção de Dados entrou recentemente em vigor, e o país não tem um legado de vigilância. Para tanto é preciso dialogar as normas de proteção de dados nacionais com experiências estrangeiras, de modo que o país esteja preparado para situações futuras.

Nesse sentido, a problemática centra-se no seguinte questionamento: de que forma os dados pessoais devem ser utilizados como fontes de informação para o planejamento de políticas públicas de saúde? O principal objetivo é analisar o uso legítimo de dados pessoais, mediante tecnologias digitais, para a propositura de políticas públicas de saúde no contexto da pandemia de COVID-19.

Para tal, será demonstrado como os dados pessoais e as inovações tecnológicas atuam como mecanismos estratégicos no combate à pandemia, serão apresentados os modelos internacionais de dados pessoais em saúde, como estão estruturados os direitos à saúde e à tutela da privacidade e proteção no ordenamento nacional e, por fim, os princípios e fundamentos legais para uso legítimo de dados.

A metodologia da pesquisa utilizada é dedutiva, de natureza exploratória e abordagem qualitativa, com predominância de bases teóricas de revisão bibliográfica. A primeira seção apresentará o uso estratégico do *big data*, inteligência artificial e internet das coisas no combate à COVID-19. A segunda abordará sobre os modelos internacionais de dados pessoais em saúde e regulamentação correspondente. Posteriormente, a terceira seção buscará delinear o conflito aparente no caso da pandemia, bem como conceitos e previsão no ordenamento nacional sobre saúde pública, tutela da privacidade e proteção de dados. Por fim, quarta seção será desenvolvida com base nas recomendações do Relatório de Privacidade e Pandemia do *Data Privacy* Brasil, com destaque à mitigação do risco, dever de transparência e consentimento informado.

2. *Big data*, inteligência artificial (AI) e internet das coisas (IOT) como mecanismos estratégicos no combate à COVID-19

Aos dados pessoais tem sido atribuído, de forma crescente, o valor de mercadoria pelas preciosas informações, sejam de natureza política, econômica e social que deles se extraem. Na era da internet das coisas, em que os diversos dispositivos tecnológicos encontram-se interconectados, ao ponto de serem indispensáveis para o desenho atual da sociedade, os grandes volumes de dados oriundos da revolução digital também se mostram de enorme valia para o setor da saúde.

Com a pandemia da COVID-19, e a necessidade de mecanismos para o controle da contaminação, o uso da Inteligência Artificial (AI), do *Big Data* e da Internet das Coisas (IoT) tornaram-se mais evidentes em escala mundial, de modo que vários países utilizaram de tecnologias digitais como estratégia de saúde pública, a qual possivelmente será aplicada em emergências futuras.

É nesse sentido, que o presente tópico busca analisar como o *Big Data*, a Inteligência Artificial e a Internet das Coisas podem contribuir no combate à Síndrome Respiratória Aguda Grave Coronavírus 2 (SARS-CoV-2),[1] formulando possíveis modelos de tecnologias digitais no setor de saúde e de políticas públicas.

À luz do *Article 29 Data Protection Working Party*,[2] o termo *big data* pode ser definido como:

---

[1] SWAPNAREKHA *et al.* Role of inteliggente computing in Covid-19 prognosis*:* a state-of-the-art review. *Chaos, Solitons and Fractals*, vol. 138, 2020, p. 3. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0960077920303465>. Acesso em: 15.09.2020.

[2] Nos termos do art. 29 da Diretiva 95/46/CE do Parlamento Europeu, foi criado o Grupo de Proteção das pessoas no que diz respeito ao tratamento de dados pessoais, de caráter consultivo e independente, com regimento interno, composto por um representante da autoridade ou autoridades de controle designadas por cada Estado-membro, por um representante da autoridade ou autoridades criadas para as instituições

> *Big data* se refere ao crescimento exponencial tanto na disponibilidade quanto no uso automatizado de informações: referem-se a gigantescos conjuntos de dados digitais mantidos por empresas, governos e outras grandes organizações, que são amplamente analisadas (daí o nome: analytics100) usando algoritmos de computador. *Big data* pode ser usado para identificar tendências e correlações mais gerais, mas também pode ser processado para afetar diretamente os indivíduos (tradução nossa).[3]

É uma expressão reconhecida pela sua imprecisão e amplitude. Sem o intuito de esgotar o tema, Rodrigo Gomes entende que o mencionado termo concerne à análise de grande volume de dados, realizada de forma automatizada por algoritmos, cujo objetivo principal é a extração de resultados e benefícios.[4] Nesse mesmo sentido, complementa António Jácomo, que o *big data* aumenta com a utilização de novos meios digitais a fim de gerar dados a cada minuto e incentivar, de forma estruturada, o cruzamento de informações para alcançar a tomada de decisões estratégicas.[5]

Conclui-se que, embora seja um termo dotado de variada interpretação, em síntese, trata-se de enorme quantidade de dados, sendo adquiridos e administrados por diferentes pessoas sociais, analisados por algoritmos e utilizados para finalidades positivas em diversos setores. Consequentemente, à medida que os avanços tecnológicos são aperfeiçoados, busca-se um aprimoramento no armazenamento desses bancos de dados e na extração dos valores contidos nas informações obtidas.

Dentre os benefícios para os quais os dados podem ser utilizados, no campo da saúde, há diversos exemplos, como o e-saúde, modalidade de atendimento *online* que é apresentado por telefonia móvel para a captura de dados, considerados sensíveis,[6]

---

e organismos comunitários, e por um representante da Comissão. Dentre suas atribuições, conforme art. 30, está o de dar parecer à Comissão sobre o nível de proteção na Comunidade e nos países terceiros. (EUROPEAN COMMISSION. *Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995*. Disponível em: <https://eur-lex.europa.eu/lega-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 13 jul. 2020).

[3] "*Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics100) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals.*" (EUROPEAN COMMISSION. *Opinion 03/2013 in ourpose limitation*. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 13.07.2020).

[4] GOMES, Rodrigo Dias Pinho. *Big data:* desafios à tutela da pessoa humana na sociedade da informação. Rio de Janeiro: Lumen Juris, 2019, p. 29.

[5] JÁCOMO, António. Saúde e inteligência artificial: uma perspectiva bioética. *Lex Medicine Revista Portuguesa de Direito da Saúde*, ano 16, n.31-31, 2019, p.3.

[6] Conforme disposição normativa, art. 5º, II, da Lei n.º 13.709/2018, os dados de saúde são considerados dados sensíveis. BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. art. 5º, II. [*Para os fins desta Lei, considera-se: II- dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa*

relacionados à saúde pessoal. Por intermédio de um aplicativo, esses dados são armazenados, analisados, e até diagnósticos são elaborados. Nesse cenário são conjugados as tecnologias de *softwares* e o armazenamento de informações em nuvem.[7]

Há também a coleta e administração de dados para a concessão de planos de saúde, no contexto da saúde suplementar, que aborda o sigilo médico quanto às informações concedidas pelo paciente. Dentre as finalidades para as quais os dados são destinados está a de definir os serviços fornecidos pela seguradora, como a Cobertura Parcial Temporária (CPT) com a disponibilização de leitos de alta tecnologia e procedimentos cirúrgicos especificados na enfermidade acometida pelo beneficiário.[8]

Outro exemplo, a Telemedicina, tecnologia que tem sido bastante utilizada e repensada em meio à pandemia de COVID-19, que proporciona remotamente a realização de diagnóstico, além da interpretação de exames médicos e emissão de laudos mediante o emprego de tecnologias de informação e comunicação,[9] ferramenta necessária para atender localidades mais distantes, como os interiores do Brasil. A relação entre dados, tecnologias e telemedicina, neste caso, está na tutela física e virtual das informações pessoais norteadas pela veracidade dos dados, acessibilidade controlada e o uso finalístico para os quais são direcionados.[10]

A compilação do *big data* e o manuseio da inteligência artificial, como visto, proporcionam uma gama de benefícios no setor da saúde, que podem ser divididos em

---

natural]. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 17.07.2020.

[7] MARTINS, Guilherme Magalhães; SOARES, Flaviana Rampazzo. Proteção de dados pessoais em e-saúde: seu confronto com a utilidade do fornecimento e uso de dados, em aplicativos para dispositivos móveis. *Revista do Consumidor*, vol. 130/2020, jul./ago. 2020, p.11. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9a0000017455aefa0ae3f0c19c&docguid=Ic07f7d90b56011ea91b89e1cb972d876&hitguid=Ic07f7d90b56011ea91b89e1cb972d876&spos=1&epos=1&td=515&context=8&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1>. Acesso em: 17.07.2020.

[8] SILVA, Luciana Vasco da; PICORELLI, Luiz Fernando. A Lei Geral de Proteção de Dados e suas implicações a seguradoras e operadoras de planos de saúde. *Revista de Direito e Medicina*, vol. 5/2020; jan./abr. 2020.

[9] MAIA, Maurilio Casas. Telemedicina, prontuário eletrônico e atualização do Código de Defesa do Consumidor – a tutela da hipervulnerabilidade eletrônica do paciente e de sua personalidade virtual. *Revista de Direito do Consumidor*, vol. 89/2013, pp. 303-319, set./out. 2013. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b000001745777af97bc84b11a&docguid=I517536602b2411e39b0e010000000000&hitguid=I517536602b2411e39b0e010000000000&spos=2&epos=2&td=13&context=31&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1>. Acesso em: 21.07.2020.

[10] FALEIROS JUNIOR, José Luiz de Moura; NOGAROLI, Rafaella; CAVET, Caroline Amadori. Telemedicina e proteção de dados: reflexões sobre a pandemia da covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. *Revista dos Tribunais*, vol. 1016/2020, pp. 327-362, jun. 2020. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b000001745777af97bc84b11a&docguid=I43c00410895e11ea8842f4a47af1044e&hitguid=I43c00410895e11ea8842f4a47af1044e&spos=1&epos=1&td=13&context=23&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1>. Acesso em: 21.07.2020.

três abordagens: 1) agilidade na descoberta de diagnósticos; 2) prevenção, detecção de doenças e identificação de tratamentos; 3) aperfeiçoamentos no processo de gerenciamento, operacionalidade e racionalização dos atos médicos.[11]

Quanto ao gerenciamento de dados, Doug Laney, em 2001, elencou três princípios fundamentais para reger esse cenário empresarial dos dados, sintetizado no denominado "3V": velocidade, variedade e volume.[12] Ampliando essa perspectiva, António Jácomo traçou as cinco áreas essenciais, na qual, a mais-valia dos dados pode ser vista, quais sejam: 1) volume; 2) velocidade; 3) variedade; 4) veracidade; 5) valor.[13] Adiante, os "5V" serão mais bem abordados.

A tendência do volume de dados é crescer, portanto, o primeiro desafio do *big data* é gerenciar esse volume disponível, e converter esses dados em informação útil e segura. Ao mesmo tempo, a velocidade com que são produzidos e tornam-se desatualizados é instantâneo. O desafio, neste caso, é utilizar os dados antes que fiquem defasados. Além disso, há diversas fontes das quais são provenientes, para tanto, é importante desenvolver ferramentas que deem conta do seu processamento e de sua diversidade. Outra questão é a veracidade dos dados coletados, e para isso é preciso estabelecer o que é verídico e atual, e determinar a relevância dos dados, que possa dar segurança quanto à utilização da informação. Por fim, no âmbito do valor, deve-se definir qual a abordagem que será feita com esses dados para serem convertidos em informação útil e utilizável.[14]

Com a crise emergencial de saúde pública global, COVID-19, e a imprescindibilidade de uma resposta ágil para a contenção da propagação e o controle da doença, a fim de evitar o congestionamento em hospitais e da saúde pública, e consequentemente, a morte de muitos cidadãos pela ausência de aparelho respiratório disponível, a utilização de dados pessoais e aplicativos tecnológicos destacaram-se como principais táticas para diagnóstico, manejo clínico, reabilitação dos casos e estratégias de prevenção.[15]

---

[11] JÁCOMO, António. Saúde e inteligência artificial: uma perspectiva bioética, cit., p.3.

[12] LANEY, Doug. *3D Data Management:* Controlling Data Volume, Velocity, and Variety. Feb. 2001. Disponível em: <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Acesso em: 21.07.2020.

[13] JÁCOMO, António. Saúde e inteligência artificial: uma perspectiva bioética, cit., p. 6.

[14] JÁCOMO, António. Saúde e inteligência artificial: uma perspectiva bioética, cit., pp. 6-7.

[15] ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e pandemia global. *Ciênc. saúde coletiva*, Rio de Janeiro, vol. 25, supl. 1, jun. 2020, p. 2488. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=pt&nrm=iso&tlng=pt>. Acesso em: 24 jul. 2020.

Segundo Swapnarekha *et al*, podem ser classificados em três os dados usados na pesquisa da COVID-19: 1) dados clínicos convertidos em informações acerca do número registrados de casos de pessoas contaminadas acrescidos de suas respectivas localizações geográficas; 2) dados *online* baseados no crescimento, natureza e disseminação da COVID-19 ao longo dos níveis local, regional, (inter)nacional, além dos dados de autoridades médicas que possam distinguir mortes causadas pelo coronavírus e mortes decorrentes de causa diversa; 3) dados biomédicos coletados de imagens médicas, como as de tórax ou radiografias que ajudam na verificação da pneumonia.[16]

Tendo em vista que os dados são fontes de conhecimento em estado bruto, é necessária, especialmente no mundo atual, a potencialização do seu valor pela aplicação, em conjunto, das modernas tecnologias, que não somente automatizam a qualidade das informações, como também aperfeiçoam a formulação de bancos de dados sobre determinada matéria, tal como tem sido empregado na pandemia.

É nesse liame, que a Inteligência Artificial (AI) surge como importante instrumento de sistematização do *Big Data*, definida, nas palavras de Jácomo, como "área das Ciências da Computação capaz de elaborar dispositivos que simulam a capacidade humana de raciocinar, perceber, tomar decisões e resolver problemas".[17]

Segundo Vaishya *et al*, a inteligência artificial contribui de sete maneiras no monitoramento e controle da disseminação da COVID-19: 1) detecção e diagnóstico precoce da infecção, que pode utilizar algoritmos úteis, como imagens de tomografia computadorizada e ressonância magnética para uma tomada de decisão rápida que contribua com o diagnóstico e a gestão dos casos; 2) acompanhamento do tratamento, em que a AI tem potencial para auxiliar com o monitoramento automático e previsão da propagação do vírus, ao fornecer atualizações dos pacientes e soluções a serem seguidas para a redução da pandemia; 3) rastreamento do contato dos indivíduos, que pode ajudar a analisar o nível e o lastro de infecção, e realizar a previsão dos possíveis locais de contaminação; 4) Projeção de casos e mortalidade de modo a rastrear e prever o vírus com base em dados disponíveis em mídias sociais que veiculem as consequências da infecção e sua disseminação, corrobora na verificação de casos positivos e número de óbitos, identificando as regiões mais vulneráveis; 5) desenvolvimento de medicamentos e vacinas, que podem advir da análise de informações e da inteligência artificial na pesquisa de drogas acelerando, assim, o

[16] SWAPNAREKHA *et al*. *Role of intelligent computing in Covid-19 prognosis:* a state-of-the-art review, cit., p. 11.
[17] JÁCOMO, António. Saúde e inteligência artificial: uma perspectiva bioética, cit., p.3.

processo; 6) redução da carga de trabalho dos profissionais da saúde, ao realizarem diagnósticos precoces e tratamentos mais perspicazes; 7) prevenção da doença a ser obtida com a análise de dados em tempo real, ao prever possíveis locais de infecção, e com isso, ajudar na administração de leitos e disponibilização de profissionais de saúde.[18]

Desta maneira, a inteligência artificial combinada com a utilização de dados pessoais apresenta um leque de soluções que contribuem com uma resposta satisfatória face ao coronavírus, doença de rápida propagação. Além disso, há as tecnologias na forma da Internet das Coisas (IoT), a qual, conforme Rahman *et al*, significa rede interconectada de dispositivos inteligentes, sensores e indivíduos, que pode coletar os dados em sua forma bruta e transmiti-los para servidores de monitoramento em tempo real dos casos positivos da doença, em uma espécie de sistema de vigilância global. Para o mencionado autor, a IoT é instrumento crucial para o combate da COVID-19.[19] E de fato, é um dos caminhos pelos quais países das diversas regiões têm seguido, seja por *IoT-Enabled Health Monitoring* (Monitoramento de saúde habilitado pela Internet das Coisas) ou *contact tracing* (rastreamento de contato).

3. A regulamentação e os modelos internacionais de dados pessoais em saúde

Há muito, os dados pessoais são apresentados como o novo petróleo devido aos valores extraídos das informações analisadas. Entretanto, é válido ressaltar o caráter personalíssimo, e de dignidade humana, que tais dados apresentam, aqui abarcados também os dados em saúde, motivos pelos quais se exige adequada proteção mediante disposições normativas.

Como visto em tópico precedente, os dados pessoais em saúde e as tecnologias digitais são mecanismos indispensáveis para o efetivo controle da pandemia. Desta feita, a presente seção verificará os principais modelos de dados pessoais no combate à COVID-19, assim como as regulamentações dos referidos países que permeiam a instituição de tecnologias de dados pessoais em saúde, para ao final, em um estudo comparado, averiguar, entre os modelos apresentados, qual(is) pode(m) ser utilizado(s) como inspiração para o Brasil.

---

[18] VAISHYA *et al*. Artificial Intelligente (AI) applications for COVID-19 pandemic. *Diabetes & Metabolic Syndrome*: *Clinical Research & Reviews*, vol. 14, 2020, pp. 337-339. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1871402120300771>. Acesso em: 15.09.2020.
[19] RAHMAN *et al*. Defending against the Novel Coronavirus (COVID-19) outbreak*:* how can the Internet of Things (IoT) help to save the world? *Health Policy and Technology*, vol. 9, 2020, p. 136. Disponível em: <https://www.sciencedirect.com/science/article/pii/S221188372030040X>. Acesso em: 16.09.2020.

A seguir serão citados três modelos de usos de dados pessoais que optaram por soluções digitais que envolvem dados de geolocalização dos cidadãos para o monitoramento e rastreio dos focos de contaminação pelas autoridades públicas. É importante ressaltar que há outros modelos, mas os da Coreia do Sul, Singapura e Europa são os que se encontram em evidência seja pela robusta previsão normativa e/ou pela estratégia eficaz adotada para o enfrentamento da supracitada crise.

A Coreia do Sul, país que tem sido reconhecido pela resolução da crise da COVID-19 em tempo recorde, devido às medidas tomadas durante a pandemia, passou a ser vista pelos demais Estados como um modelo a ser estudado e talvez seguido, o denominado "modelo coreano" tem sido destaque no mundo todo.[20] E não é a primeira vez que o país é acometido por uma doença epidemiológica. No ano de 2015, houve o surto da Síndrome Respiratória do Oriente Médio (MERS), com 186 casos positivos e 38 confirmações de morte na região.[21]

Entre as disposições normativas para o combate a doenças infecciosas, destaca-se a Lei de Controle e Prevenção de Doenças Infecciosas (IDCPA), em vigor desde 2010, mas modificada após 2015, em face da ineficácia no enfrentamento da epidemia de MERS.[22] O IDCPA traz em seu bojo normas sobre coleta de dados pessoais pelo governo, incluindo sua distribuição por agências de telecomunicação quanto à localização de indivíduos possivelmente infectados.[23]

A partir do Capítulo 4, art. 16, o referido diploma coreano aborda o aspecto de monitoramento de doenças infecciosas, investigação epidemiológica e outros. Com alterações já realizadas no ano de 2020, o art. 18 do IDCPA dispõe sobre a investigação epidemiológica, de responsabilidade dos chefes dos centros urbanos coreanos, dos prefeitos e governadores que deverão investigar o surto, coletar as informações e fornecê-las a instituições médicas pertinentes. O mesmo artigo prevê ainda a troca de informações entre instituições médicas com o fito de evitar a propagação da doença, além de ser proibida a rejeição ou obstrução da investigação, a omissão de fatos e

[20] ORLANDO, Alberto. Il modello sudcoreano contro il Covid-19: imparare con cautela. *DPCE Online*, vol. 43, n. 2, 2020, p. 2069. Disponível em: <http://www.dpceonline.it/index.php/dpceonline/article/download/995/969>. Acesso em: 12.08.2020.
[21] ORGANIZAÇÃO MUNDIAL DA SAÚDE. *Surto de MERS na República da Coréia*, 2015. Disponível em: <https://www.who.int/westernpacific/emergencies/2015-mers-outbreak>. Acesso em: 12.08.2020.
[22] ORLANDO, Alberto. Il modello sudcoreano contro il Covid-19: imparare con cautela, cit., p. 2076.
[23] PALHARES, Gabriela Capobiano *et al.* A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. *Estud. av.*, vol. 34, n. 99. São Paulo: ago. 2020, pp. 181-182. Disponível em: <https://www.scielo.br/scielo.php?pid=S0103-40142020000200175&script=sci_arttext&tlng=pt>. Acesso em: 10.07.2020.

declarações falsas. O próprio médico que desconfie de doença infecciosa também pode solicitar investigação, nos termos do art. 18-2.[24]

Ademais, o art. 76-2 do IDCPA que trata sobre a solicitação e confirmação de fornecimento de informações, entre outros, aborda importantes pontos, dentre os quais são exemplificadas as entidades que podem solicitar dados de localização de indivíduos potencialmente infectados (tais como instituições públicas, instituições médicas, farmácias, empresas, organizações, etc. que atuem na contenção da pandemia), quais os tipos de informação (nome, número de registro de residência, endereço, número de telefone e conteúdos médicos, incluindo também localização do paciente com a doença infecciosa), e a vedação de uso dos referidos dados para finalidade diversa. A norma também evidencia que a pessoa que recebe a solicitação de fornecimento das informações deve cumpri-la.[25]

O modelo coreano de dados em saúde para o combate da COVID-19 baseia-se no chamado 3 "T": teste, rastreamento e tratamento. Em primeiro lugar, com relação à entrada de viajantes para a Coreia. Ao chegarem ao país, os indivíduos submetem-se à medição de temperatura corporal, além do fornecimento de informações pessoais. Se forem viajantes sintomáticos realizam o teste, se positivo são encaminhados para tratamento e, se negativos, verifica-se primeiramente se são visitantes de curto prazo (primeiro grupo) e sul-coreanos ou estrangeiros de longa duração (segundo grupo). Os primeiros instalam o aplicativo de autodiagnóstico, e o último grupo, o aplicativo de proteção de segurança de auto-quarentena. No caso dos assintomáticos, cidadãos sul-coreanos ou estrangeiros de longa duração, além da quarentena, devem instalar o aplicativo de segurança de auto-quarentena, e testados tão somente quando os sintomas aparecerem. Enquanto os estrangeiros que permanecerem por um curto período, devem instalar o aplicativo de autodiagnóstico.[26]

O Governo coreano utiliza, em especial, dois diferentes aplicativos a serem instalados em *smartphones*. O *aplicativo de autodiagnóstico*, utilizado apenas por estrangeiros cuja permanência é de curto prazo, existe com o objetivo de os cidadãos fornecerem seus dados pessoais: nome, nacionalidade, endereço, passaporte e demais informações essenciais para a quarentena. Além de os usuários serem obrigados a atualizar seu estado de saúde uma vez por dia, os que não instalam o aplicativo ou não atualizam

[24] COREIA DO SUL. *Lei de Prevenção e Gerenciamento de Doenças Infecciosas*. Disponível em: <http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=215387&ancYd=20200304&ancNo=17067&efYd%20=%2020200905%20&%20nwJoYnInfo%20=%20N%20&%20efGubun%20=%20Y%20&%20chrClsCd%20=%20010202%20&%20ancYnChk%20=%200%20#J76:2>. Acesso em: 16.08.2020.
[25] COREIA DO SUL. *Lei de Prevenção e Gerenciamento de Doenças Infecciosas*, cit.
[26] ORLANDO, Alberto. Il modello sudcoreano contro il Covid-19: imparare con cautela, cit., p. 2083.

suas informações, recebem nos dois primeiros dias notificações por mensagem, no terceiro dia são contatados por telefone e, no quarto, a polícia rastreia o então considerado infrator.[27]

O *aplicativo de segurança de auto-quarentena* é obrigatório tanto para sul-coreanos, como para estrangeiros de longa duração. As funções resumem-se em: a) duas vezes ao dia, o usuário realiza o autodiagnóstico que é enviado às autoridades governamentais; além disso, b) fornece informações úteis para a quarentena; c) e o aplicativo rastreia, via GPS, a localização do paciente com o intuito de averiguar o cumprimento da quarentena. Caso haja violação de alguma das regras, o indivíduo é notificado e todas as medidas cabíveis são tomadas.[28]

Além desses, há outros aplicativos governamentais disponíveis no país: a) o *Coronavirus Map* que informa aos usuários regiões em que se encontram pacientes positivos; b) O aplicativo *Now and Here* que fornece cálculo com o risco de contágio pelo caminho do usuário, oferecendo rotas alternativas; c) aplicativo *Cobaek* que sinaliza a distância de 100 metros, quando o usuário está próximo de local em que um paciente positivo se encontrava.[29]

Dessas informações, o que se pode constatar é que a Coreia do Sul empregou massivamente tecnologias de rastreio de telefones, mediante aplicativos de celulares, que cruzam dados pessoais fornecidos de forma obrigatória pelos coreanos e também por estrangeiros. Caso haja descumprimento, haverá sanções também dispostas na norma coreana. Em suma, os aplicativos identificam regiões de contaminação, além de coleta de informações de pacientes contagiados, ou não, pelo vírus.

O modelo de Singapura, também baseado no rastreamento de contato, é reconhecido pelo uso do aplicativo *Trace Together,* que foi desenvolvido pelo governo de Singapura em conjunto com o Ministério da Saúde, e cuja finalidade envolve a identificação de todos os contatos com os quais o usuário manteve em um período dos catorze últimos dias, com outras pessoas.[30] O aplicativo, ao utilizar *Bluetooth,* rastreia os indivíduos expostos ao vírus, e alerta o usuário que teve contato com algum indivíduo que testou positivo ou encontra-se em alto risco de ser portador da doença. Quando confirmado o diagnóstico ou a suspeita, a pessoa pode optar por fornecer seus dados ao hospital,

[27] ORLANDO, Alberto. Il modello sudcoreano contro il Covid-19: imparare con cautela, cit., p. 2084.
[28] ORLANDO, Alberto. Il modello sudcoreano contro il Covid-19: imparare con cautela, cit., p. 2084.
[29] ORLANDO, Alberto. Il modello sudcoreano contro il Covid-19: imparare con cautela, cit., p. 2085.
[30] INSTITUTO DE PESQUISA ECONÔMICA APLICADA. *Nota Técnica n.º 38:* o uso de tecnologia da informação para o enfrentamento à pandemia da covid-19, jun. 2020, p. 8. Disponível em: <http://repositorio.ipea.gov.br/bitstream/11058/10108/1/NT_38_Diest_O%20uso%20de%20tecnol%20inform%20enfrentamento.pdf>. Acesso em: 17 .09.2020.

Ministério de Saúde e a terceiros para identificar os contatos próximos. O país tem cogitado transformar em código aberto o protocolo de preservação da privacidade em que se baseia a troca de dados do referido aplicativo.[31]

Desde 2012, os dados pessoais em Singapura são regulamentados pela Lei de Proteção de Dados Pessoais (PDPA), que estabelece regras sobre coleta, armazenamento, uso e divulgação dos dados. A norma fundamenta-se em três pilares: o consentimento do indivíduo dado às organizações que administram os dados; o objetivo destinado para os dados, que devem ser previamente informados aos indivíduos; e a razoabilidade, conceito utilizado para que as organizações manuseiem dados apenas para fins apropriados para uma pessoa razoável.[32]

Acerca da coleta de dados pessoais para rastreamento de contato no contexto da COVID-19, a Comissão de Proteção de Dados Pessoais de Singapura (PDPC) aduz que as organizações podem coletar dados pessoais para fins de resposta contra a pandemia, e que os relevantes podem ser usados, coletados e divulgados sem consentimento durante o período atual, no caso do aplicativo *SafeEntry*, com a justificativa de que o país se encontra em emergência, situação que ameaça a vida, saúde e segurança dos indivíduos. No entanto, tais organizações devem cumprir o previsto na Lei de Proteção de Dados do país, para serem tomadas medidas de segurança que protejam os dados pessoais contra acesso e divulgação não autorizados e garantir que não sejam utilizados para outras finalidades sem o devido consentimento ou autorização conforme o permissivo legal.[33]

O modelo europeu, no que lhe concerne, é bastante incipiente. Países da região manifestaram o interesse de adotar o monitoramento tecnológico, seja por meio da localização da pessoa usando GPS ou triangulação pelas antenas telefônicas; ou rastreamento pela proximidade com o mecanismo de *Bluetooth*, que não utiliza localização, mas o emprego de códigos ou pseudônimos criptografados. De todo modo, tanto a Comissão Europeia, como a Agência Espanhola de Proteção de Dados, por

[31] ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE. *Rastreamento e monitoramento da covid*: proteção da privacidade e dos dados pessoais na utilização de aplicativos e biometria, 2020, p.3. Disponível em: <https://read.oecd-ilibrary.org/view/?ref=133_133567-f5gnsq4agh&title=Rastreamento-e-monitoramento-da-COVID-19>. Acesso em: 12.08.2020.

[32] SINGAPORE. *Personal data Protection Act 2012*. Disponível em: <https://sso.agc.gov.sg/Act/PDPA2012>. Acesso em: 14.08.2020.

[33] PERSONAL DATA PROTECTION COMISSION SINGAPORE. *Advisiores on collection of personal data for covid-19 contact tracing and use of safeentry*. Disponível em: <https://www.pdpc.gov.sg/Help-and-Resources/2020/03/Advisory-on-Collection-of-Personal-Data-for-COVID-19-Contact-Tracing>. Acesso em: 14.08.2020.

exemplo, afirmam que deve haver voluntariedade na instalação e desativação de aplicativos de rastreio, no que se destaca como consentimento.[34]

A Bélgica aprovou a utilização de dados anonimizados de empresas locais de telecomunicações, a Alemanha adequou-se ao compartilhamento de dados de deslocamentos das pessoas presentes em seu país, e a Itália assinou acordo para que operadoras de telecomunicações pudessem coletar dados de localização anonimizados.[35]

A União Europeia, desde meados de 2018, disciplina a proteção jurídica dos dados pessoais pelo Regulamento 679/2016, que revogou a Diretiva 95/46 com a justificativa de estabelecer maior uniformidade na proteção de dados entre os países da Europa, o que não era obtido com a Diretiva, que dependia de regulamentação interna conforme a liberalidade de cada país.[36] A diretriz nuclear do Regulamento 679 consiste em tratamento de dados concomitantemente com progresso econômico, estímulo ao desenvolvimento do comércio, bem como promoção do bem-estar humano.[37]

Além disso, a referida norma, embora com o intuito de proteção dos dados pessoais, não a considera direito absoluto. Logo, pode ser limitado e ponderado em análise com outros direitos, bem como limitado conforme vontade do titular do direito, desde que observado o consentimento informado.[38] Por fim, acerca das noções gerais do Regulamento 679, é importante salientar característica própria do modelo europeu com a presença de autoridade de controle, independente, com poderes de investigação, intervenção, entre outras providências de cunho fiscalizatório.[39]

Sobre o tratamento de dados de saúde, o Regulamento apresenta previsão específica, no âmbito da saúde pública, e legitimidade quanto ao tratamento de dados em situação de crise ou pandemia, conforme o considerando 46. Prevê também o processamento de dados pessoais relativos à saúde, que em regra são proibidos (art. 9, 1, GDPR), mas excepcionados no caso de proteção dos interesses vitais do titular dos dados ou de outra

---

[34] MARTÍNEZ, Mª Belén Andreu. Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la covid-19. *Actualidade Jurídica Iberoamericana*, n. 12 bis, may 2020, pp. 853-854.
[35] MOURA, Raíssa; FERRAZ, Lara. *Meios de controle à pandemia da covid-19 e a inviolabilidade da privacidade*, p. 3. Disponível em:<https://content.inloco.com.br/hubfs/Estudos%20-%20Conte%C3%BAdo/Coronavirus/Meios%20de%20controle%20a%CC%80%20pandemia%20da%20COVID-19%20e%20a%20inviolabilidade%20da%20privacidade.pdf>. Acesso em: 15.07.2020.
[36] BESSA, Leonardo Roscoe. *Nova lei do cadastro positivo:* comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD. São Paulo: Thomson Reuters Brasil, 2019, p.57.
[37] BESSA, Leonardo Roscoe. *Nova Lei do Cadastro Positivo:* comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD, cit., p. 58.
[38] BESSA, Leonardo Roscoe. *Nova Lei do Cadastro Positivo:* comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD, cit., p. 59.
[39] BESSA, Leonardo Roscoe. *Nova Lei do Cadastro Positivo:* comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD, cit., p. 60.

pessoa singular (art. 9, 2.c, GDPR); quando o tratamento é necessário por motivos de interesse público substancial, desde que proporcional ao objetivo requerido, e que em respeito à proteção dos dados, preveja medidas apropriadas e especiais (art. 9, 2.g, GDPR); casos em que o processamento é necessário, dentre outros motivos, devido ao diagnóstico médico (art. 9, 2.h, GDPR); quando o motivo envolva interesse público no domínio da saúde pública, a exemplo de proteção contra ameaças graves transfronteiriças à saúde (art. 9, 2.i, GDPR), e quando se trate de investigação científica (art. 9, 2. j, GDPR).[40]

Até o momento, foi observado como os países podem utilizar dados pessoais e tecnologias digitais para o combate da pandemia da COVID-19, e os benefícios que se extraem do somatório desses mecanismos, os quais desenham o futuro das tecnologias de dados no planejamento e execução da saúde pública. Entre os três modelos descritos, é possível constatar que o modelo coreano é mais ostensivo na administração de dados pessoais em saúde, prevendo inclusive sanções em caso de descumprimento de fornecimento de informações, na negativa da disposição de dados, ou se forem falsos. Enquanto os modelos de Singapura e da União Europeia, mesmo com aplicativos de rastreamento, convergem em uma proteção mais robusta de dados pessoais, flexibilizado pelo interesse da saúde pública, mas ainda sim, permanecendo como modelos protetivos.

O Brasil, em escala federal, não adotou nenhuma estratégia nesse sentido, até que alguns estados, como São Paulo, começaram a utilizar o sistema de monitoramento de geolocalização, cujo intuito, através de um "mapa de calor", era de verificar regiões que estavam descumprindo o isolamento social.[41]

Em abril do presente ano, porém, a Presidência da República editou a Medida Provisória n. 954/2020,[42] que determinou, para fins de estatística, o compartilhamento de informações pessoais dos cidadãos a empresas concessionárias de Serviço Telefônico Fixo Computado (STFC) e do Serviço Móvel Pessoal (SMP) com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE). É importante ressaltar que durante a pandemia, o ato normativo teve seu prazo de vigência encerrado em 14 de agosto de

[40] UNIAO EUROPEIA. *Regulamento Geral de Proteção de Dados (GDPR)*. Disponível em: <https://gdpr-info.eu/art-9-gdpr/>. Acesso em: 16.07.2020.
[41] AGÊNCIA BRASIL. *Covid-19:* iniciativas usam monitoramento e geram preocupações. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/covid-19-iniciativas-usam-monitoramento-e-geram-preocupacoes>. Acesso em: 16.07.2020.
[42] BRASIL. *Medida Provisória n.º 954, de 17 de abril de 2020*. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Congresso/adc-112-mpv954.htm>. Acesso em: 16 jul. 2020.

2020. [43] Antes disso, foi objeto, de no mínimo, cinco Ações Diretas de Inconstitucionalidade, que dentre os argumentos apresentados, fora alegado o de violação do direito à autodeterminação informacional, privacidade e intimidade dos cidadãos.[44]

Mesmo não se tratando do uso de tecnologias digitais para compartilhamento de dados, ou rastreamento de contato, em âmbito federal, a tão somente previsão de repartição dessas informações foi apontada como possível violação prática na defesa da proteção de dados pessoais, o que reforça o questionamento de quais devem ser os fundamentos legítimos que proporcionam o uso devido de dados pessoais como fonte de informação para o planejamento de políticas públicas.

4. Saúde pública v. tutela da privacidade e proteção de dados pessoais no ordenamento jurídico brasileiro

As seções anteriores dispuseram sobre os benefícios que as tecnologias digitais (inteligência artificial e internet das coisas) e o uso de dados pessoais têm trazido para o setor da saúde, em especial, no contexto da SARS-COV-2, além dos modelos de dados pessoais utilizados por alguns países. Entretanto, o uso de dados pessoais em saúde possui outra faceta, a negativa, consubstanciada em ameaça à privacidade do indivíduo e o uso indevido das informações, por exemplo, para prática de atos discriminatórios, vigilantismo preditivo, e consequentemente, violação dos direitos da personalidade.

No específico caso do coronavírus, ainda há de se considerar a peculiar situação de anormalidade em questão. O mundo foi assolado por um vírus de grande propagação e elevada mortalidade, que implicou na paralisação de boa parte das atividades econômicas, gerou desemprego em massa, tal como abalo para o sistema financeiro de inúmeros países, um cenário caótico, e de grave ameaça à saúde pública.

Dessa forma, o caso da COVID-19 coloca em aparente colisão dois direitos fundamentais: a proteção de dados pessoais, face à tutela da privacidade (art. 5º, X, CF/88), e a defesa da saúde pública (art. 196, CF/88). Para prosseguir na análise proposta pelo presente artigo, faz-se imperioso descrever o escorço jurídico sobre os direitos em questão e verificar, conforme aparato doutrinário, se a persecução por

---

[43] BRASIL. *Ato declaratório do presidente da mesa do Congresso Nacional*. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Congresso/adc-112-mpv954.htm>. Acesso em: 16.07.2020

[44] PALHARES, Gabriela Capobiano *et al*. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio, cit., pp. 178-179.

soluções em prol da saúde pública atua, ou não, em desarmonia com a proteção dos dados pessoais.

A proteção de dados pessoais, no Brasil, não está corporificada em texto normativo constitucional, alteração intentada pela PEC 17/2019, ainda sujeita à apreciação, cujo objetivo é incluir a proteção de dados pessoais entre os direitos e garantias fundamentais da Constituição Federal e fixá-la como matéria de competência privativa da União.[45] Enquanto isso, a proteção de dados e seu mais recente diploma normativo têm sido apresentados como diretrizes relevantes para a tutela da privacidade e da personalidade humana à luz da interpretação constitucional.[46]

A dimensão histórico-evolutiva da constitucionalização do direito privado certamente foi um dos grandes avanços do constitucionalismo moderno para a proteção dos direitos fundamentais. A superação da perspectiva dicotômica do universo jurídico, estrita separação entre direito público e direito privado, convergiu, dentre as principais consequências, para uma publicização do direito privado e a constitucionalização de alguns de seus princípios e institutos jurídicos.[47]

Em decorrência deste último, derivou-se o fenômeno da despatrimonialização do direito civil, em que o objeto primordial desse ramo, que antes era o patrimônio, passou a ser a pessoa humana, o que colocou em voga a proteção dos direitos da personalidade e uma leitura a partir dessa valoração.[48] Conforme Eugenio Facchini Neto, a acepção moderna da constitucionalização do direito privado baseia-se em dois enfoques: a relevância constitucional das relações privadas e a força normativa de princípios interpretados em conformidade com a constituição. [49] A primeira corresponde a uma análise civil-constitucional, e a segunda à resolução de casos por princípios constitucionais com a devida normatividade jurídica.

A partir desse entendimento da constituição como fonte normativa do direito civil, vislumbra-se, segundo Danilo Doneda, a existência da cláusula geral da personalidade, com base na dignidade da pessoa humana, na cidadania, fundamentos da República, e nas garantias de igualdade material e formal. A cláusula geral é vista como norte

---

[45] CÂMARA DOSDEPUTADOS. *Proposta de Emenda à Constituição n.º 17/2019*. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 10.09.2020.
[46] REGIS, Erick da Silva. Linhas gerais sobre a Lei 13.709/2018 (LGPD): objetivos, fundamentos e axiologia da lei geral de proteção de dados brasileira e a tutela da personalidade/privacidade. *Revista de Direito Privado*, vol. 103, 2020, p. 2.
[47] FACCHINI NETO, Eugênio. A constitucionalização do direito privado. *Iurisprudentia*: *Revista da Faculdade de Direito da Ajes*, ano 2, n. 3. Juína: jan./jun., 2013, p.23.
[48] FACCHINI NETO, Eugênio. A constitucionalização do direito privado, cit., p. 26.
[49] FACCHINI NETO, Eugênio. A constitucionalização do direito privado, cit., pp. 29-30.

interpretativo a ser seguido pelas leis infraconstitucionais para a proteção da personalidade da pessoa humana.[50] Nesse sentido, também afirma Gustavo Tepedino:

> [...] em respeito ao texto constitucional, parece lícito considerar a personalidade não como um novo reduto de poder do indivíduo, no âmbito do qual seria exercido a sua titularidade, mas como valor máximo do ordenamento, modelador da autonomia privada, capaz de submeter toda a atividade econômica a novos critérios de validade.[51]

Abarcado pelos direitos da personalidade está o direito à privacidade, que nos termos do art. 21 do Código Civil aduz: "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".[52] Ao aplicar a cláusula geral, é possível compreender que não basta proibir a violação à privacidade, mas produzir normas que protejam à vida privada e sejam interpretadas nesse sentido, como núcleo irradiante no ordenamento. No âmbito do objeto de estudo em questão, pugna-se pela proteção da privacidade materializada nos dados pessoais de saúde.

Desta feita, observa Erick Regis, que o controle dos dados pessoais, senão acompanhado de devida regulamentação, pode ser analisado sob a ótica de três perspectivas de degradação: 1) a privacidade, pois os dados podem ser transformados em insumo negocial do mercado; 2) os caracteres da personalidade frequentemente invadidos ilicitamente tendo o lucro como objetivo; 3) e violação das características existenciais da pessoa devido ao vazamento em larga escala de dados.[53]

A privacidade delineia a própria individualidade da pessoa, que se materializa em um fluxo informativo, o que reclama por si tamanha proteção. Historicamente, a definição do direito à privacidade foi delineada por Warren e Brandeis, na célebre frase "o direito de ser deixado em paz", nesse liame trata-se de liberdade negativa. No entanto, conforme observa Stefano Rodotà, devido à relação com as tecnologias da informação, atualmente privacidade denota uma noção dinâmica devendo, portanto, prevalecer definições funcionais. "Assim a privacidade pode ser definida mais precisamente, em

---

[50] DONEDA, Danilo. Os direitos da personalidade no Código Civil. *Revista da Faculdade de Direito de Campos*, ano VI, n. 6, jun. 2005, p.82.
[51] TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil constitucional brasileiro. In: TEPEDINO, Gustavo. *Temas de direito civil*. Rio de Janeiro: Renovar, 2004, p. 49
[52] BRASIL. *Lei n.º 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 10.09.2020.
[53] REGIS, Erick da Silva. Linhas gerais sobre a Lei 13.709/2018 (LGPD): objetivos, fundamentos e axiologia da lei geral de proteção de dados brasileira e a tutela da personalidade/privacidade, cit., p. 5.

uma primeira aproximação, como o direito de manter o controle sobre as próprias informações", pondera o referido autor.[54]

Com esse conceito moderno e dinâmico, privacidade é conduzida a uma percepção de liberdade positiva face ao controle sobre as informações pessoais. E a redefinição de seu conceito abrange, segundo Rodotà, três paradoxos e quatro tendências:

1. do direito a ser deixado só ao direito de manter controle sobre as informações que me digam respeito;
2. da privacidade ao direito à autodeterminação informativa;
3. da privacidade à não-discriminação;
4. do sigilo ao controle.[55]

Embora a proteção de dados pessoais tenha fundamento no direito à privacidade, contudo, não deve ser reduzida à evolução da tutela da vida privada, pois requer autonomia própria como novo direito da personalidade, conforme estabelece Bruno Bioni, sob alegação de inviabilização normativa para melhor regulamentação do fluxo informacional.[56]

O direito à proteção de dados pessoais representa de forma ativa e individual a proteção da dignidade da pessoa humana nos meios informatizados, e pelo seu fundamento axiológico a tutela da privacidade. Não mais abordada como uma impossibilidade de manuseio das informações nas diversas atividades, como a econômica, mas como objeto autônomo a ser controlada pela pessoa diretamente afetada, a pessoa humana sobre a qual os dados informam.

No âmbito da proteção de dados pessoais, no Brasil, foi criada a Lei n.º 13.709/2018, que entrou em vigor em setembro de 2020. A Lei Geral de Proteção de Dados (LGPD) inaugura o "sistema protetivo de dados pessoais" no país, com princípios que norteiam a coleta, armazenamento e compartilhamento de dados pessoais, assim como as obrigações dos responsáveis por essas atividades.[57] Referida norma coexiste com outras que tratam de proteção de dados, ainda que em termos gerais, devendo ser aplicadas em conjunto com o instituto do diálogo das fontes, a exemplo do Código de Defesa do Consumidor e do Marco Civil da Internet.

---

[54] RODOTÀ, Stefano. *A vida na sociedade da vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p.92.
[55] RODOTÀ, Stefano. *A vida na sociedade da vigilância:* a privacidade hoje, cit., pp. 97-98.
[56] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, pp. 94-95.
[57] TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei geral de proteção de dados pessoais:* comentada artigo por artigo. 2. ed. rev. atual. e ampl. Salvador: Editora Juspodivm, 2020, p. 12.

Nos termos do art. 1º da LGPD, a lei regula o tratamento de dados pessoais dispostos nos meios informatizados, ou não, da pessoa natural/ jurídica de direito público ou privado, para a proteção dos direitos fundamentais de liberdade, privacidade, livre desenvolvimento da pessoa natural. Quanto ao tratamento de dados pessoais em saúde, a norma dispõe, conforme previsão do art. 7º, que poderá ser realizado pela administração pública, inclusive o compartilhamento de dados, desde que a finalidade seja a execução de políticas públicas previstas em instrumento normativo (inciso III), o tratamento está protegido para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviço de saúde e autoridade sanitária (inciso VIII).[58]

Para Tarcisio Teixeira e Ruth Armelin, o Poder Público é um dos grandes agentes de tratamento de dados, devido ao bem coletivo, o qual obriga a coletar dados para o planejamento e execução de políticas públicas, justificado para esse fim a ausência do consentimento. Além disso, afirmam que a hipótese da tutela da saúde é um complemento ao inciso VII, do art. 7º, que prevê o tratamento de dados para a proteção da vida ou incolumidade física do titular dos dados, ou de terceiros, fundamentos que desencadeiam em uma relativização da privacidade e intimidade em prol da proteção do indivíduo e da coletividade.[59] Diretrizes que se assemelham a norma europeia que flexibiliza a proteção de dados em prol de iminência degradação da saúde pública.

A saúde, no direito brasileiro, é dever do Estado e direito de todos, garantida, conforme previsão constitucional no art. 196, CF/88, pela utilização de políticas sociais e econômicas em prol da minimização do risco de doença e do amplo acesso a serviços que conduzam a promoção, proteção e recuperação desse direito. O direito à saúde como direito social, sob a ótica do Estado Democrático, tutela como base a vida, a ser perseguida não na dualidade morte/vida, mas como compromisso de uma qualidade digna.[60]

Além disso, Schwartz e Ractz ressaltam que o direito fundamental a saúde, embora de competência do poder público, não deve excluir da responsabilidade de sua efetivação, os particulares, em geral. O Estado é o principal garantidor da saúde, direito que pode

---

[58] BRASIL. *Lei n.º 13.709, de 14 agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 17.07.2020.

[59] TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei geral de proteção de dados pessoais:* comentada artigo por artigo, cit., pp. 57-58.

[60] MORAIS, Jose Luis Bolzan de; NASCIMENTO, Valéria Ribas do. O direito à saúde e os "limites" do estado social: medicamentos, políticas públicas e judicialização. *Novos Estudos Jurídicos (NEJ)*, vol. 12, n.2, jul./dez. 2007, p. 260. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/view/467>. Acesso em: 12.09.2020.

ser efetivado por prestações positivas, como o planejamento e execução de políticas públicas, ou de forma negativa, como defesa.[61]

Nessa seara, o contexto da COVID-19 representa situação complexa. Países, como os anteriormente citados, adotaram medidas de contenção da pandemia pela utilização de tecnologias de informação e compartilhamento de dados. A coleta e administração em massa de dados colocam em possível risco as informações sensíveis da pessoa humana, ao mesmo tempo em que a não utilização dessas medidas acentuaria a crise na saúde atual que traz consequências em diversos setores da sociedade.

Nesse cenário, pode-se verificar, em uma visão macro, a presença de dois direitos fundamentais, o direito à saúde e o direito à proteção de dados, pela tutela da privacidade, a princípio não colidentes, mas que podem, a depender da situação, entrar em conflito. Caso isso ocorra, será preciso ponderar os interesses conflitantes. Para Alexy, quando se trata de colisão entre princípios, um deles não será aplicado no caso em questão, não no sentido de invalidade de um em detrimento do outro, mas de precedência, o que significa que, ao analisar o caso em concreto e verificar a específica condição tratada, um princípio terá maior peso, situação a ser resolvida pela ponderação dos interesses conflitantes.[62]

Aplica-se para a resolução o princípio da proporcionalidade, mediante a verificação de três máximas parciais que o compõem: adequação, necessidade e proporcionalidade em sentido estrito. Respectivamente, a primeira analisa as possibilidades para a efetivação da finalidade desejada, posteriormente a averiguação da medida menos restritiva aos direitos envolvidos, e em último, aplica-se a otimização dos princípios colidentes ao evidenciar a finalidade pública importante ao ponto de afastar a aplicação de outro princípio.[63]

Por fim, é importante destacar que as normas de proteção de dados pessoais são, conforme Bioni, historicamente, normas de dupla função, qual seja, garantir a proteção à privacidade e outros direitos fundamentais, assim como estimular o desenvolvimento econômico.[64] Logo, a proteção aos dados e a defesa da saúde pública podem trabalhar

---

[61] SCHWARTZ, Germano; RACTZ, Juliana. O direito público subjetivo à saúde: efetividade via políticas públicas. *Revista Direito e Justiça*, Reflexões Sociojurídicas, ano VI, n. 9, nov/2006, pp. 160-161. Disponível em: <http://srvapp2s.santoangelo.uri.br/seer/index.php/direito_e_justica/article/view/300>. Acesso em: 18.06.2020.
[62] ALEXY, Robert. *Teoria dos Direitos Fundamentais*. Trad. de Vírgilio Afonso da Silva. São Paulo: Malheiros, 2008, p. 93.
[63] ÁVILA, Humberto Bergmann. *Teoria dos princípios:* da definição à aplicação dos princípios jurídicos. São Paulo: Malheiros, 2005, p.114.
[64] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento, cit., p. 103.

em conjunto para buscar soluções não somente no caso da SARS-COV-2, como em outras áreas da saúde.

5. Mitigação do risco, dever de transparência e consentimento informado: breves considerações sobre o Relatório de Privacidade e Pandemia do *Data Privacy* Brasil

No Brasil, não houve, ao longo do ano de 2020, formulação de políticas públicas, a nível nacional, de tratamento de dados em saúde para o combate à COVID-19. Primeiramente, pela divergência governamental no controle da pandemia, e em segundo, porque à época, a Lei Geral de Proteção de Dados não se encontrava em vigor, o que causava certa insegurança normativa para os gestores de dados.

O cerne desta seção é analisar quais os meios adequados e legítimos para a formulação de políticas públicas de dados pessoais no combate à pandemia do coronavírus e de outras que possam existir. Para tanto, será utilizado como base para a análise o documento do *Data Privacy* Brasil, Relatório de Privacidade e Pandemia, que traz considerações sobre o referido assunto. Além disso, serão averiguadas, com destaque, três diretrizes importantes para a proteção e administração dos dados: a mitigação do risco, o dever de transparência e o consentimento informado.

O Relatório "Privacidade e Pandemia" esboça princípios e recomendações para a elaboração de políticas públicas de compartilhamento de dados, entre entidades da Administração pública e destas com o setor privado, à luz do Decreto 10.212/2020 (Regulamento Sanitário Internacional) e da Lei 13.979/2020 (Lei de Quarentena).[65] Em suma, as recomendações são resultados de um processo de 5 (cinco) passos que devem ser seguidos para a instituição de políticas públicas de dados, para cada passo foram identificados princípios correspondentes, totalizando 10 (dez) a serem verificados pelos gestores públicos e agentes privados.[66]

O Decreto n.º 10.212/2020 promulgou o texto do Regulamento Sanitário Internacional da Organização Mundial da Saúde, que estabeleceu normas para o enfrentamento da síndrome respiratória aguda grave. Com destaque ao artigo 45 do Regulamento que prevê o tratamento de dados pessoais em saúde, *in verbis*:

---

[65] 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, p. 6. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/04/Relatorio-Privacidade-e-Pandemi-a-Data-Privacy-Brasil-2.pdf>. Acesso em: 29.07.2020.

[66] BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. Privacidade e pandemia: recomendações para o uso legítimo de dados no combate à covid-19, cit., p. 7.

> 1. As informações de saúde coletadas ou recebidas por um Estado Parte de outro Estado Parte ou da OMS, consoante este Regulamento, referentes a pessoas identificadas ou identificáveis, deverão ser mantidas em sigilo e processadas anonimamente, conforme exigido pela legislação nacional.
> 2. Não obstante o Parágrafo 1º, os Estados Partes poderão revelar e processar dados pessoais quando isso for essencial para os fins de avaliação e manejo de um risco para a saúde pública, no entanto os Estados Partes, em conformidade com a legislação nacional, e a OMS devem garantir que os dados pessoais sejam:
> (a) processados de modo justo e legal, e sem outros processamentos desnecessários e incompatíveis com tal propósito;
> (b) adequados, relevantes e não excessivos em relação a esse propósito;
> (c) acurados e, quando necessário, mantidos atualizados; todas as medidas razoáveis deverão ser tomadas a fim de garantir que dados imprecisos ou incompletos sejam apagados ou retificados; e
> (d) conservados apenas pelo tempo necessário.
> 3. Mediante solicitação, a OMS fornecerá às pessoas, na medida do possível, os seus dados pessoais a que se refere este Artigo, em formato inteligível, sem demoras ou despesas indevidas e, quando necessário, permitirá a sua retificação.[67]

O referido artigo do Regulamento Sanitário estabelece o tratamento anônimo e em sigilo dos dados de saúde, em conformidade com a legislação nacional, além de determinar no parágrafo segundo, que nos casos de risco à saúde pública, haverá a possibilidade de processamento dessas informações pessoais desde que observados a legalidade, adequação, atualização e tempo de armazenamento.

A Lei n.º 13.979/2020, denominada como "Lei da Quarentena", também retrata em seu texto normativo a administração de dados. À luz do artigo 6º do mencionado diploma legal, foi estabelecido a obrigatoriedade do compartilhamento, entre órgãos e entidades das três esferas federativas, de dados essenciais para a identificação de pessoas infectadas ou com suspeita de infecção de modo a controlar a propagação do vírus. O §1º, do art. 6º amplia essa obrigação para as pessoas jurídicas de direito privado, quando autoridade sanitária solicitar os dados, e o §2º dispõe a necessidade de manter tais dados públicos e atualizados pelo Ministério de Saúde, reforçando a necessidade do direito ao sigilo das respectivas informações.[68]

---

[67] BRASIL. *Decreto n.º 10.212, de 30 de janeiro de 2020*. Promulga o texto revisado do Regulamento Sanitário Internacional, acordado na 58ª Assembleia Geral da Organização Mundial, em 23 de maio de 2005 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10212.htm #anexo>. Acesso em: 17.09.2020.
[68] BRASIL. *Lei n.º 13.979, de 6 de fevereiro de 2020*. Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo

Utilizando por referência essas disposições normativas, além das demais normas setoriais no território nacional, o Relatório de Privacidade e Pandemia elaborou cinco passos para a formulação de políticas públicas de saúde que utilizem os dados no combate à COVID, a seguir:

> Passo 1: Avaliação da necessidade da elaboração de política de saúde centrada em dados pessoais;
> Passo 2: Definição da finalidade e necessidade do tratamento de dados;
> Passo 3: Definição do ciclo de vida e descarte dos dados;
> Passo 4: Definição de salvaguardas específicas para direitos fundamentais;
> Passo 5: Garantia de publicidade, transparência e participação.[69]

Para avaliar a necessidade de elaboração de políticas públicas com base em dados pessoais de saúde, o Relatório propõe seguir, como primeiro passo, a observância dos princípios da motivação fundamentada, autorização legal e formalização em instrumento contratual ou congênere. Nesse caso, deve-se analisar o contexto da pandemia e verificar, com base em evidências técnicas e científicas, a necessidade de resultado pelo tratamento de dados pessoais, tudo dentro da legalidade e da formalização do procedimento por instrumento legalmente adequado.[70]

Como regra, a efetivação e defesa do direito à saúde são de responsabilidade do Estado mediante prestações positivas do Poder Público, no caso, políticas públicas de dados em saúde, tornando-se inerente para o seu planejamento a observância de previsões legais acerca da matéria, instrumento necessário para a execução, e adequada fundamentação, sobretudo porque para a implementação da medida serão utilizados a coleta e compartilhamento de dados pessoais como objeto principal para a solução do problema.

O segundo passo sobre a finalidade e necessidade do tratamento deve ser conduzido pela definição de finalidade específica e expressa, e limitação dessa coleta de dados ao mínimo necessário para o objetivo proposto. Assim, se a finalidade é coletar dados pessoais de saúde para evitar a propagação da COVID, tal coleta não pode ser utilizada

---

surto de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13979.htm>. Acesso em: 17.09.2020.

[69] BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. Privacidade e pandemia*:* recomendações para o uso legítimo de dados no combate à covid-19, cit. p. 14.

[70] BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. Privacidade e pandemia*:* recomendações para o uso legítimo de dados no combate à covid-19, cit. p. 17.

para objetivo diverso do pretendido, além de utilizar-se especificamente dos dados que ajudarão para atingir a finalidade proposta.[71]

Esse ponto é importante para evitar que os dados pessoais sejam utilizados para outros fins que não o proposto inicialmente pela política pública. É sabido que os dados são considerados insumos negociais de onde se extraem informações valiosas utilizadas em diversos setores, a exemplo da economia da informação. Portanto, limitar o uso ao fim primário é uma garantia de proteção e manutenção da privacidade.

O terceiro passo busca o estabelecimento do ciclo de vida e descarte dos dados, instruído por limite temporal e devida atualização de modo a evitar que sejam compartilhados dados desatualizados, que podem ser considerados falsos por não corresponderem à realidade. Dessa forma, o gestor da administração dos dados deve formular plano de vida e descarte, prevendo o início, meio, fim e o modo pelos quais os dados serão armazenados.[72]

O quarto passo propõe a previsão de mecanismos específicos para a proteção dos direitos fundamentais na administração desses dados. Essa etapa pode ser conduzida pelo princípio da (pseudo)anonimização, que visa a uma minimização dos riscos de reidentificação das pessoas, e também pelo princípio da garantia da segurança da informação. Essa fase ressalta os riscos à privacidade e a outros direitos fundamentais pela má utilização dos dados. Tanto na sua coleta como no seu compartilhamento existem riscos ao indivíduo a quem pertence o dado e a informação dele extraída. Para reduzir esses riscos torna-se imprescindível o planejamento dessas políticas públicas, além da diligência no manejo dos dados com a aplicação de técnicas de proteção, a exemplo da (pseudo)anonimização.[73]

No direito brasileiro, dados anonimizados não recebem proteção legal como dados pessoais, isto porque, o art. 5º, inciso I estabelece como dado pessoal aquela informação relacionada à pessoa natural identificada ou identificável, e conforme o inciso III do mesmo artigo, o dado anonimizado é dado que se refere a titular que não possa ser identificado.[74] Dessa forma, entre as técnicas disponíveis para a mitigação do risco dos dados pessoais, a (pseudo)anonimização é a mais recomendada, porque consiste em mecanismo que emprega medidas organizativas e de segurança de modo

[71] BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. Privacidade e pandemia*:* recomendações para o uso legítimo de dados no combate à covid-19, cit. p. 20.
[72] BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. *Privacidade e pandemia:* recomendações para o uso legítimo de dados no combate à covid-19, cit., p. 21.
[73] BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. *Privacidade e pandemia:* recomendações para o uso legítimo de dados no combate à covid-19, cit., p. 26.
[74] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD), cit.

que para identificar o titular específico dos dados seria necessário dispor de informações suplementares.[75] Vale ressaltar ser de responsabilidade do gestor de dados prover técnicas de diminuição do risco na reidentificação do titular dos dados.

Por fim, o quinto passo prevê a garantia da publicidade, transparência e participação, que devem ser resguardados pela aplicação do princípio da transparência ativa e da preferência por aplicativos e tecnologias de código aberto. Ou seja, mecanismos de transparência que não sejam reduzidos a um controle social, mas também atuem em colaboração com a sociedade. O código aberto trata de utilização de tecnologias que não sejam de proprietários privados, e que possam ser acessados por qualquer indivíduo, a fim de que a sociedade tenha a possibilidade de avaliar as ferramentas e contribuir com seu aprimoramento.[76]

Sobre o princípio da transparência, o art. 6º, inciso VI, da Lei n.º 13.709/2018, retrata que esse princípio é uma "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento observados os segredos comercial e industrial".[77] No âmbito do poder público, nos termos do art. 23 da LGPD, a transparência é nuclear, afinal o interesse público deve prevalecer em observância a proteção dos direitos fundamentais. Nesse sentido, preleciona Teixeira e Armelin, que as pessoas jurídicas previstas no *caput* do art. 1º da Lei n.º 12.527/2011 (Lei de Acesso à Informação) deverão possibilitar o acesso à informação do titular dos dados, em diálogo com os princípios da finalidade e da transparência, com informações adequadas e fundamento legal.[78]

A transparência é primordial para a sociedade informacional, pois proporciona ao cidadão o acesso pormenorizado de suas informações, contribuindo para que o indivíduo possa acompanhar a administração de seus dados, reforçando que mesmo para finalidade de interesse público, como a proteção à saúde pública, os dados compõem a personalidade do titular e merecem efetiva proteção.

O consentimento informado não é posto no Relatório como passo ou princípio a ser seguido, entretanto, por ser visto como vetor central para a proteção de dados pessoais, algumas considerações serão tecidas sobre sua aplicação, ou não, em políticas públicas

---

[75] MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. Caderno Especial – a regulamentação da criptografia no direito brasileiro, *Revista dos Tribunais* online, vol. 1, dez. 2018, p. 5.
[76] BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato; RIELLI, Mariana. *Privacidade e pandemia:* recomendações para o uso legítimo de dados no combate à covid-19, cit., 27.
[77] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD), cit.
[78] TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei geral de proteção de dados pessoais:* comentada artigo por artigo, cit., pp. 97-98.

de dados de saúde. Debate relevante, haja vista que a Medida Provisória n.º 954/2020, com vigência encerrada, previu, em seu art. 1º, o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoas – SMP com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, o objetivo era de realizar à distância o estudo estatístico do perfil socioeconômico da população brasileira.[79] Contudo, o texto apresentado não foi claro ao especificar a produção estatística oficial a ser produzida, deixando em dúvida se os dados coletados seriam utilizados para relacionar números de casos de contaminação pelo coronavírus.

Em oposição à Medida Provisória e questionando sua observância à Constituição foram propostas cinco Ações Diretas de Inconstitucionalidade (ADI 6387, ADI 6388, ADI 6389, ADI 6390, ADI 6393), as quais perderam o objeto pelo encerramento da vigência da medida provisória. Contudo, em sede de julgamento do plenário, foi proferida decisão que suspendeu a aplicação da MP n.º 954/2020. O Supremo Tribunal Federal firmou o entendimento de que o compartilhamento de dados pessoais violava direito constitucional à intimidade, à vida privada e ao sigilo de dados.[80]

O consentimento, nos termos da Lei Geral de Proteção de Dados, art. 5º, inciso XII, é conceituado como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". [81] Além desse artigo, outras previsões sobre a essencialidade do consentimento estão presentes no mesmo diploma, tais como art. 7º, §5º, art. 14, §1º e art.33, inciso VIII. Embora visto como núcleo principal para o tratamento de dados, não possui hierarquia superior em relação aos demais requisitos do art. 7º, que regulam a legalidade do tratamento de dados pessoais prevendo nove hipóteses além do consentimento.

Bruno Bioni afirma que uma das possíveis disputas interpretativas da referida lei de proteção de dados serão em dois pontos principais: 1) se as demais hipóteses previstas no art. 7º da LGPD, que tratam da legitimidade para tratamentos de dados pessoais,

---

[79] BRASIL. *Medida Provisória n.º 954, de 17 de abril de 2020.* Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei n.º 13.979, de 6 de fevereiro de 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm>. Acesso em: 16.07.2020

[80] *STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Supremo Tribunal Federal.* Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902>. Acesso em: 17.07.2020.

[81] BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD), cit.

são taxativas e referem-se a situações em que o tratamento ocorre sem o consentimento do titular; e, 2) no caso de aplicação dessas hipóteses com a dispensa do consentimento, como será garantida a transparência da informação para o cidadão exercer sua autodeterminação informacional mediante o consentimento ainda que posterior.[82] Levando em conta que o Relatório de Privacidade e Pandemia do *Data Privacy* é também de autoria do mencionado autor, compreende-se em vista do estudo abordado que o consentimento é dispensado para tratar da hipótese de compartilhamento de dados no âmbito de execução de políticas públicas, proteção da vida e tutela da saúde, conforme art. 7º, inciso III, VII e VIII, respectivamente.

É válido ressaltar que Tarcisio Teixeira e Ruth Armelin, com as devidas ponderações, entendem que mesmo com o estabelecimento de outras hipóteses para o tratamento legal de dados, o consentimento do titular continua a ser primordial e ter prioridade sobre os demais, sendo utilizado como norte, em especial, por facilitar a prestação de contas, conhecido como princípio da *accountability*.[83]

Embora o embate interpretativo quanto à necessidade do consentimento para a utilização de dados pessoais em políticas públicas de saúde, é uníssono quando o assunto é sobre a transparência no tratamento de dados. Princípio que se mostra como via para titular e gestor. Visto que os dados são necessários para políticas públicas, o questionamento não é mais se deve existir ou não, mas como fazê-las de forma eficiente e com menos riscos para os cidadãos. A transparência é o caminho para que a própria população ativamente desempenhe seu papel social.

6. Considerações finais

Como demonstrado, os dados pessoais são necessários para a formulação de políticas públicas em saúde, e surgem como importantes instrumentos no combate à COVID-19. Vale ressaltar, que diferente do conceito clássico da tutela da privacidade, consubstanciado no direito de estar só, o direito à proteção de dados pessoais de liberdade positiva não é contrário à circulação de dados. Essas informações devem ser coletadas, armazenadas, compartilhadas em observância às leis protetivas, para que o tratamento realizado proporcione ao titular dos dados uma atuação ativa.

Embora o Brasil seja jovem na previsão legal de proteção de dados, e ainda não possua políticas públicas que utilizem dados e tecnologias, a experiência estrangeira propicia

[82] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento, cit., p. 129.
[83] TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei geral de proteção de dados pessoais:* comentada artigo por artigo, cit., pp. 55-56.

modelos que, analisados em contexto com a estrutura nacional, são inspirações do que fazer e não fazer quanto à administração de dados. Estudo que é necessário para que o país se encontre preparado para cenários futuros. A SARS-COV-2 até então é uma doença incerta, assim como os surgimentos de outras pandemias.

De todo modo, mesmo com a LGPD e robusta proteção de direitos fundamentais que abarcam a privacidade e personalidade, a realidade da proteção de dados ainda parece distante, haja vista que a instituição da Autoridade Nacional de Proteção de Dados (ANPD), órgão de regulamentação e fiscalização responsável pelo fiel cumprimento da referida lei, é recente. É necessário que referido órgão estabeleça diretrizes, dialogue com os diferentes setores da sociedade e seja o mediador para os interesses que atuam em relação aos dados, sem isso será difícil estabelecer limites jurídicos em concreto que proporcionem o uso adequado das informações e sua efetiva proteção.

7. Referências

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. de Vírgilio Afonso da Silva. São Paulo: Malheiros, 2008.

ALMEIDA, Bethania de Araujo *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e pandemia global. *Ciênc. saúde coletiva,* Rio de Janeiro, vol. 25, supl.1, jun. 2020. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-81232020006702487&lng=pt&nrm=iso&tlng=pt>. Acesso em: 24.07.2020.

ÁVILA, Humberto Bergmann. *Teoria dos princípios*: da definição à aplicação dos princípios jurídicos. São Paulo: Malheiros, 2005.

BESSA, Leonardo Roscoe. *Nova Lei do Cadastro Positivo*: comentários à Lei 12.414, com as alterações da Lei Complementar n. 166/2019 e de acordo com a LGPD. São Paulo: Thomson Reuters Brasil, 2019.

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

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. Disponível em: <https://www.dataprivacybr.org/relatorio_privacidade/>. Acesso em: 29.07.2020.

CORÉIA DO SUL. *Lei de Prevenção e Gerenciamento de Doenças Infecciosas*. Disponível em: <http://www.law.go.kr/LSW//lsInfoP.do?lsiSeq=215387&ancYd=20200304&ancNo=17067&efYd%20=%2020200905%20&%20nwJoYnInfo%20=%20N%20&%20efGubun%20=%20Y%20&%20chrClsCd%20=%20010202%20&%20ancYnChk%20=%200%20#J76:2>. Acesso em: 16.08.2020.

DONEDA, Danilo. Os direitos da personalidade no Código Civil. *Revista da Faculdade de Direito de Campos*, Ano VI, n. 6, jun. 2005.

EUROPEAN COMMISSION. *Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em 13.07.2020.

EUROPEAN COMMISSION. *Opinion 03/2013 in ourpose limitation*. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 13 jul. 2020.

FACCHINI NETO, Eugênio. A constitucionalização do direito privado. *Iurisprudentia*: *Revista da Faculdade de Direito da Ajes*. Juína/MT, ano 2, n. 3, jan./jun., 2013.

FALEIROS JUNIOR, José Luiz de Moura; NOGAROLI, Rafaella; CAVET, Caroline Amadori. Telemedicina e proteção de dados: reflexões sobre a pandemia da covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. *Revista dos Tribunais*, vol. 1016, jun. 2020. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b000001745777af97bc84b11a&docguid=I43c00410895e11ea8842f4a47af1044e&hitguid=I43c00410895e11ea8842f4a47af1044e&spos=1&epos=1&td=13&context=23&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1>. Acesso em: 21.07.2020.

GOMES, Rodrigo Dias de Pinho. *Big data*: desafios à tutela da pessoa humana na sociedade de informação. 2. ed. Rio de Janeiro: Lumen Juris, 2019.

INSTITUTO DE PESQUISA ECONÔMICA APLICADA. *Nota Técnica n.º 38*: O uso de tecnologia da informação para o enfrentamento à pandemia da COVID-19, jun. 2020, p.8. Disponível em: <http://repositorio.ipea.gov.br/bitstream/11058/10108/1/NT_38_Diest_O%20uso%20de%20tecnol%20inform%20enfrentamento.pdf>. Acesso em: 17.08.2020.

JÁCOMO, António. Saúde e inteligência artificial: uma perspectiva bioética. *Lex Medicine Revista Portuguesa de Direito da Saúde*, ano 16, n.31-31, 2019.

LANEY, Doug. *3D Data Management*: Controlling Data Volume, Velocity, and Variety. Feb. 2001. Disponível em: <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Acesso em: 21.07.2020.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. Caderno Especial – a regulamentação da criptografia no direito brasileiro, *Revista dos Tribunais* online, vol. 1, dez. 2018.

MARTINS, Guilherme Magalhães; SOARES, Flaviana Rampazzo. Proteção de dados pessoais em e-saúde: seu confronto com a utilidade do fornecimento e uso de dados, em aplicativos para dispositivos móveis. *Revista do Consumidor*, vol. 130, jul./ago. 2020. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9a00000017455aefa0ae3f0c19c&docguid=Ic07f7d90b56011ea91b89e1cb972d876&hitguid=Ic07f7d90b56011ea91b89e1cb972d876&spos=1&epos=1&td=515&context=8&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1>. Acesso em: 17.07.2020.

MARTÍNEZ, Mª Belén Andreu. Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la COVID-19. *Actualidade Jurídica Iberoamericana*, n. 12 bis, may 2020.

MAIA, Maurilio Casas. Telemedicina, prontuário eletrônico e atualização do Código de Defesa do Consumidor: a tutela da hipervulnerabilidade eletrônica do paciente e de sua personalidade virtual. *Revista de Direito do Consumidor*, vol. 89, set./out. 2013. Disponível em: <https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0ad82d9b000001745777af97bc84b11a&docguid=I517536602b2411e39b0e010000000000&hitguid=I517536602b2411e39b0e010000000000&spos=2&epos=2&td=13&context=31&crumb-action=append&crumb-label=Documento&isDocFG=true&isFromMultiSumm=true&startChunk=1&endChunk=1>. Acesso em: 21.07.2020.

MORAIS, Jose Luis Bolzan de; NASCIMENTO, Valéria Ribas do. O direito à saúde e os "limites" do estado social: medicamentos, políticas públicas e judicialização. *Novos Estudos Jurídicos (NEJ)*, vol. 12, n. 2, jul./dez. 2007. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/view/467>. Acesso em: 12.09.2020.

MOURA, Raíssa; FERRAZ, Lara. *Meios de controle à pandemia da covid-19 e a inviolabilidade da privacidade*. Disponível em: https://content.inloco.com.br/hubfs/Estudos%20-%20Conte%C3%BAdo/Coronavirus/Meios%20de%20controle%20a%CC%80%20pandemia%20da%20COVID-19%20e%20a%20inviolabilidade%20da%20privacidade.pdf?hsCtaTracking=ad1577ba-e5bc-4ff3-afdd-54a896891088%7C07ab4d6b-53d3-4a06-9f43-fb43621df88f&hsLang=pt>. Acesso em: 15.07.2020.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. *Surto de mers na República da Coréia, 2015*. Disponível em: <https://www.who.int/westernpacific/emergencies/2015-mers-outbreak>. Acesso em: 12.08.2020.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE, 2020, p.3. *Rastreamento e monitoramento da covid*: proteção da privacidade e dos dados pessoais na utilização de aplicativos e biometria. Disponível em: https://read.oecd-ilibrary.org/view/?ref=133_133567-f5gnsq4agh&title=Rastreamento-e-monitoramento-da-COVID-19>. Acesso em: 12.08.2020.

ORLANDO, Alberto. Il modello sudcoreano contro il Covid-19: imparare con cautela. *DPCE Online*, vol. 43, n. 2, 2020. Disponível em: <http://www.dpceonline.it/index.php/dpceonline/article/download/995/969>. Acesso em: 12 ago. 2020.

PALHARES, Gabriela Capobiano *et al.* A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. *Estud. av.*, São Paulo, vol. 34, n. 99, ago. 2020. Disponível em: <https://www.scielo.br/scielo.php?pid=S0103-40142020000200175&script=sci_arttext&tlng=pt>. Acesso em: 10.07.2020.

PERSONAL DATA PROTECTION COMISSION SINGAPORE. *Advisiores on collection of personal data for covid-19 contact tracing and use of safeentry*. Disponível em: <https://www.pdpc.gov.sg/Help-and-Resources/2020/03/Advisory-on-Collection-of-Personal-Data-for-COVID-19-Contact-Tracing>. Acesso em: 14.08.2020

POMPEU, João Cláudio Basso *et al. O uso de tecnologia da informação para o enfrentamento à pandemia da covid-19*. IPEA, Nota técnica, n.º 38, jun. 2020. Disponível em: <http://repositorio.ipea.gov.br/bitstream/11058/10108/1/NT_38_Diest_O%20uso%20de%20tecnol%20inform%20enfrentamento.pdf>. Acesso em: 14.07.2020.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RAHMAN *et al. Defending against the novel coronavirus (covid-19) outbreak*: how can the internet of things (iot) help to save the world? *Health Policy and Technology*, vol. 9, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S221188372030040X>. Acesso em: 16.09.2020.

SCHWARTZ, Germano; RACTZ, Juliana. O direito público subjetivo à saúde: efetividade via políticas públicas. *Revista Direito e Justiça*, Reflexões Sociojurídicas, ano VI, n. 9, nov. 2006, Disponível em: <http://srvapp2s.santoangelo.uri.br/seer/index.php/direito_e_justica/article/view/300>. Acesso em: 18.06.2020.

SILVA, Luciana Vasco da; PICORELLI, Luiz Fernando. A lei geral de proteção de dados e suas implicações a seguradoras e operadoras de planos de saúde. *Revista de Direito e Medicina*, vol. 5, jan./abr. 2020.

SINGAPORE. *Personal data Protection Act 2012*. Disponível em: <https://sso.agc.gov.sg/Act/PDPA2012>. Acesso em: 14.08.2020.

SWAPNAREKHA *et al.* Role of inteliggente computing in Covid-19 prognosis: a state-of-the-art review. *Chaos, Solitons and Fractals*, vol. 138 2020. Disponível em: <https://reader.elsevier.com/reader/sd/pii/S0960077920303465?token=DD11C37279A3DC4EF0616AAAE1F8670E157E12F55176E13B941A939D44E15AA25FA3C09C51CECED5C6EA52E4CAE75DEF>. Acesso em: 16.09.2020.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. *Lei geral de proteção de dados pessoais*: comentada artigo por artigo. 2. ed. rev. atual. e ampl. Salvador: Juspodivm, 2020.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil constitucional brasileiro. In: TEPEDINO, Gustavo. *Temas de Direito Civil*. Rio de Janeiro: Renovar, 2004.

UNIAO EUROPEIA. *Regulamento Geral de Proteção de Dados (GDPR)*. Disponível em: <https://gdpr-info.eu/art-9-gdpr/>. Acesso em: 16.07.2020.

VAISHYA *et al.* Artificial intelligente (ai) applications for covid-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, 2020. Disponível em:

<https://reader.elsevier.com/reader/sd/pii/S1871402120300771?token=4A178EE5AF60F572316B50220FC2DA890385B6D1EDC443294C192D686D3BA6D8C47B83EE9A0589A4357D6C3CC1477006>. Acesso em: 15.09.2020

VALENTE, Jonas. Covid-19*:* iniciativas usam monitoramento e geram preocupações. *Agência Brasil*, 12 abr. 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/covid-19-iniciativas-usam-monitoramento-e-geram-preocupacoes>. Acesso em: 16.07.2020.

civilistica.com

Recebido em: 8.10.2021
Aprovado em:
2.5.2022 (1º parecer)
13.5.2022 (2º parecer)

Como citar: FÉLIX, Victória; MONTEIRO, Juliano Ralo. O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19. **Civilistica.com**. Rio de Janeiro, a. 11, n. 1, 2022. Disponível em: <http://civilistica.com/o-uso-de-tecnologias/>. Data de acesso.