COMPARTILHAMENTO DE DADOS PESSOAIS E O COMBATE À PANDEMIA DA COVID-19 NO BRASIL: ANÁLISE DA MEDIDA PROVISÓRIA 954/2020

PERSONAL DATA SHARING AND THE FIGHT AGAINST THE COVID-19 PANDEMIC IN BRAZIL: ANALYSIS OF PROVISIONAL MEASURE 954/2020

ELÍSIO AUGUSTO VELLOSO BASTOS[1]
CRISTINA PIRES TEIXEIRA DE MIRANDA[2]
VITÓRIA BARROS ESTEVES[3]

REVISTA MERITUM • v.16 • n.4 • p. 53-71 • 2021

RESUMO

Medidas de combate à pandemia causada pela COVID-19 estão sendo adotadas em diversos países. No Brasil, foi editada a Medida Provisória 954/2020, que determinava o compartilhamento de dados pessoais de brasileiros ao IBGE para a finalidade de produção estatística. O presente artigo tem como objetivo refletir criticamente acerca de tal compartilhamento em face do direito fundamental à intimidade e à autodeterminação informativa, para tanto, utiliza-se, especialmente, os conceitos desenvolvidas por Perez Luño. Investiga-se, portanto, de que forma o compartilhamento de dados pessoais, previsto pela MP, viola o direito fundamental à intimidade e autodeterminação informativa. Avalia-se também os possíveis efeitos de tal compartilhamento no campo democrático. A pesquisa tem caráter teórico-descritivo e viés qualitativo, proposto em uma perspectiva reflexiva acerca dos riscos das operações de compartilhamento de dados pessoais. Utiliza-se a técnica de pesquisa bibliográfica especializada no assunto. O artigo conclui que a MP 954/2020 não observou os limites constitucionais e legais de proteção à intimidade e ao direito à autodeterminação informativa, à medida que não indicou os mecanismos protetivos necessários ao compartilhamento, assim como não forneceu aos usuários de telefonia a opção de autorizar ou não a transferência dos dados para o IBGE. Ademais, por oferecer potenciais riscos ao próprio equilíbrio democrático, o compartilhamento de dados pessoais deve vir acompanhado de medidas legais e operacionais que assegurem a sua utilização tão somente ao propósito de pesquisas estatísticas ou sanitárias.

Palavras-chave: MP 954/2020; dados pessoais; intimidade; autodeterminação informative; democracia.

1 Doutor em Direito do Estado pela faculdade de Direito da Universidade de São Paulo (USP). Professor em Direitos Humanos e em Teoria Geral da Constituição (Graduação) e em Teoria da Constituição no Centro Universitário do Estado do Pará-CESUPA. Coordenador do Grupo de Pesquisa Inteligência Artificial, Democracia e Direitos Fundamentais. Procurador do Estado do Pará. Advogado. ORCID ID: https://orcid.org/0000-0001-8183-5920. E-mail: elisio.bastos@uol.com.br.

2 Mestranda do Programa de Pós-graduação Stricto Senso em Direito, Políticas Públicas e Direitos Humanos do Centro Universitário do Pará – CESUPA. Membro do Grupo de Pesquisa Inteligência Artificial, Democracia e Direitos Fundamentais. Advogada do Banco do Estado do Pará – BANPARÁ. ORCID ID: https://orcid.org/0000-0001-7884-2687.

3 Mestranda em Ciência Política no Programa de Pós-Graduação em Ciência Política da UFPA. Pós-Graduanda em Direito Digital pelo Complexo de Ensino Renato Saraiva. Membro do Grupo de Pesquisa em Inteligência Artificial e Direitos Fundamentais da Liga Acadêmica Brasileira de Direito do Estado. Advogada. ORCID ID: https://orcid.org/0000-0003-3914-6499.

Como citar esse artigo:/*How to cite this article*:
BASTOS, Elísio Augusto Velloso; MIRANDA, Cristina Pires Teixeira de; ESTEVES, Vitória Barros. Compartilhamento de dados pessoais e o combate à pandemia da COVID-19 no Brasil: análise da medida provisória 954/2020. **Revista Meritum**, Belo Horizonte, vol. 16, n. 4, p. 53-71, 2021. DOI: https://doi.org/ 10.46560/meritum.v16i4.8201.

ABSTRACT

Measures to fight against the pandemic caused by COVID-19 are being adopted in several countries. In Brazil, the Provisional Measure 954/2020 was edited, which determined the sharing of brazilians personal data to Brazilian Institute of Geography Statistics (IBGE) for the purpose of statistical production. This article aims to critically reflect on such sharing in view of the fundamental right to privacy and informative self-determination, for this purpose, it is used, especially, the concepts developed by Perez Luño. Therefore, it is investigated how the sharing of personal data, provided for by the Provisional Measure 954/2020, violates the fundamental right to privacy and information self-determination. The possible effects of such sharing in the democratic field are also evaluated. The research has a theoretical-descriptive character and qualitative bias, proposed in a reflective perspective about the risks of personal data sharing operations. The technique of bibliographical research specialized in the subject is used. The article concludes that Provisional Measure 954/2020 did not observe the constitutional and legal limits to protect privacy and the right to informational self-determination, as it did not indicate the necessary protective mechanisms for sharing, nor did it provide telephone users with the option of to authorize or not to transfer the data to IBGE. Furthermore, because it offers potential risks to the democratic balance itself, the sharing of personal data must be accompanied by legal and operational measures that ensure its use solely for the purpose of statistical or health researches.

Keywords: *provisional measure 954/2020; personal data; privacy. informative self-determination; democracy.*

REVISTA MERITUM • v.16 • n.4 • p. 53-71 • 2021

1. INTRODUÇÃO

O mundo encontra-se em meio a uma pandemia global que gerou uma crise de saúde pública que atinge diversos países. Neste cenário, como estratégia de combate à pandemia, surge a necessidade de maior monitoramento da população, considerando que o agente vetor de tal pandemia, popularmente conhecido como novo coronavírus (**SARS-CoV-2**), possui alto poder de transmissão e contágio.

Assim, os governos foram obrigados a adotar estratégias de combate à pandemia, dentre elas: o fechamento de fronteiras, escolas, comércio e demais locais que possibilitassem o fluxo de pessoas e/ou aglomerações. Em alguns países, como China (MOZUR; ZHONG; KROLIK, 2020) e Israel (HAMAGEN, 2020), medidas de coleta, compartilhamento e de controle de dados pessoais dos cidadãos foram adotadas. Tais medidas têm como objetivo fiscalizar e monitorar o estado de saúde dos cidadãos ou mapear o contato da pessoa infectada com os demais indivíduos.

No Brasil, por exemplo, os Estados de São Paulo, Recife e Mato Grosso do Sul têm utilizado dados de geolocalização, através da triangulação de antenas das operadoras de celular, para localizar possíveis aglomerações por toda a cidade (JORNAL NACIONAL, 2020). Tais estratégias revelam, em alguma medida, a possibilidade de violação de direitos fundamentais, como o direito à livre locomoção e à intimidade.

No contexto federal, foi editada a Medida Provisória (MP) 954/2020, que estabelecia o compartilhamento de dados pessoais dos usuários das empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE), a fim de dar suporte à produção estatística oficial durante a situação de emergência de saúde pública causada pela COVID-19.

O propósito geral deste artigo é analisar referida MP 954/2020 e a real possibilidade de que seu exercício pudesse violar desproporcionalmente direitos fundamentais dos cidadãos

brasileiros, especialmente a proteção da intimidade e o direito à autodeterminação informativa. Para tanto, utiliza-se metodologia qualitativa, proposta a partir de uma reflexão teórico-jurídico acerca dos impactos das operações de compartilhamento de dados pessoais. Utiliza-se a técnica de pesquisa bibliográfica especializada no assunto.

Inicialmente, serão analisados o teor da MP 954/2020 e os principais fundamentos materiais apontados pelos Ministros do Supremo Tribunal Federal (STF), por ocasião do julgamento das Ações Diretas de Inconstitucionalidade (ADIs) propostas em face da MP. Após, serão analisados a relevância dos dados pessoais, sua definição e o entendimento de que vivemos, atualmente, numa sociedade de dados; Em seguida, a proteção da intimidade e o direito à autodeterminação informativa como limites constitucionais ao compartilhamento de dados pessoais. Por último, serão vistos quais os riscos do compartilhamento de dados pessoais, quer em face da intimidade e autodeterminação informativa, quer em face da liberdade e autonomia em realizar escolhas, inclusive as de cunho democrático.

A relevância da pesquisa está em delinear os principais limites e riscos ao compartilhamento de dados pessoais no Brasil. Ainda que tal matéria seja considerada recente no ordenamento jurídico pátrio, o movimento é de se construir e consolidar um ambiente seguro para o tratamento de dados no Brasil, seja este realizado pelo próprio Estado, ou pelo setor privado, e até mesmo ambos atores agindo conjuntamente. Antes, porém, o trabalho analisa, como ponto de partida, os principais argumentos materiais expostos durante o julgamento da ADI 6387, proposta em face da MP 954/2020.

2. A MP 954/2020 E SUA ANÁLISE PELO SUPREMO TRIBUNAL FEDERAL

Antes de delinear o conteúdo da MP 954/2020, importa destacar que a referida medida entrou em vigor em 17 de abril de 2020, porém teve seus efeitos suspensos a partir de 24 de abril de 2020, por decisão cautelar do Supremo Tribunal Federal (STF, 2020a). A medida provisória em questão, após o prazo constitucional, não foi convertida em lei, tendo, portanto, perdido sua vigência e eficácia no ordenamento jurídico pátrio.

No entanto, embora não tenha mais eficácia, a problemática criada em torno da medida se deu por dois motivos: o primeiro relaciona-se ao apressado processo de publicação, sem discussão prévia com a sociedade civil e com atores especializados da área; o segundo, à insuficiência do seu texto acerca do detalhamento dos motivos, operações, e mecanismos de proteção do compartilhamento dos dados. O foco deste trabalho incide justamente sobre este segundo tópico.

Notadamente, a MP 954/2020 tinha como objeto o compartilhamento de dados das empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado (STFC) e do Móvel Pessoal (SM) para o IBGE, com o fim declarado de suporte à produção estatística oficial durante a emergência em saúde pública decorrente da COVID-19. Assim, ela previa que as empresas de telefonia deveriam, no prazo de sete dias, contados da data de publicação de Ato do Presidente do IBGE, disponibilizar a esse órgão, por meio eletrônico, a relação dos

nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas, para fins de realização de entrevistas em caráter não presencial, no âmbito de pesquisas domiciliares (BRASIL, 2020). Com objetivo de questionar a constitucionalidade da referida norma, foram propostas cinco ADIs (STF, 2020a), de autoria do Conselho Federal da OAB (ADI 6387) e dos partidos PSDB (ADI 6388), PSB (ADI 6389), PSOL (ADI 6390) e PCB (ADI 6393). Em 24 de abril de 2020, o STF, por larga maioria de dez votos a favor, deferiu medida cautelar requerida na ADI 6387, suspendendo a eficácia da MP 954/2020 e determinando que o IBGE se abstivesse de requerer a disponibilização dos dados ou sustasse o pedido caso já houvesse feito. No âmbito material, argumentou-se, principalmente, em favor do direito fundamental à privacidade, intimidade e proteção de dados pessoais, na concepção de um direito à autodeterminação informativa.

Em seu voto[4], a relatora do feito, Ministra Rosa Weber, afirmou que um dos desafios contemporâneos do direito à privacidade (e de seus consectários da intimidade) é precisamente a manipulação de dados pessoais por agentes públicos ou privados. Destacou, ainda, que a MP não satisfaz as exigências constitucionais de proteção à privacidade e à intimidade, e que, ao não descrever finalidades específicas, métodos de tratamento e critérios de eventuais responsabilizações, a Medida não oferece condições necessárias para sua validação (STF, 2020b).

Ressaltou também o risco proveniente da capacidade atual das tecnologias de transformar dados não estruturados em perfis extremamente individualizados dos cidadãos. Conclui que, em momento algum, subestima-se a gravidade do cenário de urgência da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O combate à pandemia, todavia, não poderia legitimar o atropelo de garantias fundamentais consagradas na Constituição Federal (STF, 2020b).

No mesmo sentido, o Ministro Alexandre de Moraes[5] destacou que a limitação do poder estatal e a observação de limites constitucionais são pilares da democracia, e que qualquer relativização de direitos fundamentais é excepcional, devendo ser feita apenas a partir de hipóteses legais ou judiciais, adequadas, proporcionais e razoáveis. Já os Ministros Celso de Melo e Luís Roberto Barroso reconheceram que os dados estatísticos são importantes para a atividade estatal moderna, inclusive para o enfrentamento da pandemia da COVID-19. Contudo, frente à ausência de elementos que indicassem a efetiva proteção da privacidade dos cidadãos brasileiros, ambos votaram com a Relatora pela suspensão da MP (STF, 2020c).

Os Ministros Luiz Fux e Cármen Lúcia ressaltaram os riscos do compartilhamento dos dados de que trata a MP, destacando, ainda, que a proteção de dados pessoais e o direito à autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia constitucional de inviolabilidade da intimidade e da vida privada (STF, 2020c).

O Ministro Ricardo Lewandowski (STF, 2020c) ratificou integralmente o voto da Relatora e destacou os riscos da vigilância sutil e da consolidação do *big data*. Veja-se:

> [...] Nos dias atuais o maior perigo para a democracia não é mais representado por golpes de estados tradicionais perpetrados com fuzis, tanques ou canhões, mas agora pelo progressivo controle da vida privada dos cidadãos

4 Voto em vídeo proferido na sessão virtual do pleno realizada no dia 07/05/2020.

5 Todos os demais Ministros, com exceção da Relatora, Ministra Rosa Weber, manifestaram-se na sessão virtual do pleno realizada no dia 08/05/2020 (STF, 2020c).

> levado a efeito por governos de distintas matizes ideológicas, mediante a coleta massiva e indiscriminada de informações pessoais, incluindo de maneira crescente o reconhecimento facial. Esses dados são submetidos a um novo instrumental da tecnologia denominado *big data* que consegue armazenar, interligar e manipular uma enorme quantidade de dados, para o bem ou para o mal. (STF, 2020c)

O Ministro Gilmar Mendes também argumentou que o quadro fático contemporâneo, apesar de excepcional em razão da pandemia da COVID-19, deve ser analisado à luz da Constituição Federal de 1988, e que nunca foi estranho à jurisdição constitucional a ideia de que os parâmetros dos direitos fundamentais devem permanecer abertos à evolução tecnológica. Remontou esse entendimento à decisão do Tribunal Constitucional Alemão de 1983, que declarou nulo dispositivos da chamada "Lei do Censo", que possibilitavam a coleta, o cruzamento e a transmissão de dados pessoais dos cidadãos alemães. Referido julgamento, segundo o Ministro, já indicava uma concepção dinâmica da privacidade, aberta às referências sociais e aos seus múltiplos contextos de usos (STF, 2020c).

No único voto dissidente, o Ministro Marco Aurélio afirmou que os riscos da MP não poderiam ser presumidos e que não deveria se assumir um mau uso dos dados por parte do IBGE. Por fim, defendeu a necessidade de se aguardar o crivo do Congresso Nacional.

Nota-se, portanto, a partir dos argumentos acima referendados, que o STF, ao analisar o caso da MP 954/2020, já indica a importância de proteção dos pessoais no Brasil, principalmente frente aos riscos para a privacidade dos cidadãos e para o próprio regime democrático, e já o faz antes mesmo da vigência da LGPD. Isso porque a proteção de dados pessoais também tem como base, como bem indicado pelos ministros, o texto constitucional, que aponta a intimidade e a concepção de um direito à autodeterminação informativa como fundamentos desta matéria. Além disso, o STF também destaca a importância coletiva de se proteger os dados pessoais, seja por, no caso concreto, estimar se tratar de dados de milhões de usuários de telefonia, seja por considerar que essa nova realidade informacional/tecnológica atinge ou tem potencial de atingir a coletividade como um todo.

Dessa forma, antes de analisarmos detalhadamente a intimidade e autodeterminação informativa como bases e limites constitucionais para o compartilhamento de dados pessoais, é necessário entender o que são esses dados, como se classificam e qual o grau de relevância destes para as sociedades atuais, denominadas de informacionais, tecnológicas, digitais, dadocêntricas, entre outras terminologias.

3. DEFINIÇÃO E RELEVÂNCIA DOS DADOS PESSOAIS: A NOVA SOCIEDADE DE DADOS

A MP 954/2020 previa que as empresas de telefonia privada deveriam compartilhar os nomes, número de telefones e endereços de todos os seus clientes cadastrados. Essa referida iniciativa do Governo Federal reacendeu importantes questionamentos sobre a relevância dos dados pessoais, principalmente sobre operações de tratamento que utilizam informações pessoais dos cidadãos no contexto atual de pandemia.

Antes da internet, a divulgação de dados pessoais ocorria predominantemente em materiais físicos, como por exemplo listas telefônicas. Com a evolução da capacidade computacional e a expansão da rede mundial de computadores, a divulgação de dados pessoais ganhou novos contornos, digitais e eletrônicos.

Quando se fala especificamente em dado pessoal, vincula-se este ao plano da informação[6] e da projeção de uma personalidade. Em outra palavras, opera no campo de identificação pessoal de uma personalidade, por isso sua necessária proteção jurídica. A Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD), apresenta o direcionamento normativo quanto ao conceito de dados pessoais, definindo-os como todas as informações relacionadas a uma pessoa natural, identificada ou identificável[7]. A LGPD (BRASIL, 2018) traz ainda os conceitos de dados pessoais sensíveis[8], como aqueles dados que revelam informações de origem racial ou étnica, religião, opinião política, saúde, genética e de ordem sexual, quando relacionados a uma pessoa natural; e dados anonimizados[9], como dados incapazes de revelar a identidade de uma pessoa.

No que diz respeito aos dados sensíveis, Bioni (2020) lembra que seu conteúdo oferece uma especial vulnerabilidade: a possibilidade de discriminação. Diante dessa condição especial, o compartilhamento dos dados sensíveis deve ser condicionado ao consentimento específico e destacado, e deverá estar vinculado a finalidades específicas.

Boa parte dos dados pessoais têm potencial de se tornarem sensíveis, o que torna a sua proteção ainda mais urgente e necessária. Isso porque, atualmente, algoritmos inteligentes têm a capacidade de identificar dados sensíveis a partir do acesso a dados pessoais não sensíveis. Assim, a partir de dados supostamente banais dos indivíduos é possível obter dados relevantes, que podem ser transformados em perfis comportamentais, que revelam opiniões políticas, dados biológicos, etnia, raças, religião etc.

Precisamente por isso é que os dados pessoais se tornaram insumo de grande importância para a sociedade, quer no aspecto econômico, político ou social. Não à toa, são responsáveis pelo surgimento da "sociedade de dados". Por sua vez, essa nova forma de organização técnico-social, que se cria em torno dos dados e das informações produzidas pelos próprios indivíduos, porém coletadas, analisadas e controladas por empresas privadas de tecnologia, traz consequências para a vida dos cidadãos, que podem afetar não apenas a sua privacidade, como também toda a coletividade.

Harari (2018) afirma que no século XXI os dados vão suplantar tanto a terra quanto a maquinaria como o ativo mais importante. Nesse cenário, o autor descreve o surgimento do "dataísmo", uma espécie de religião na qual a produção e circulação livre dos dados formariam o valor preponderante a organizar toda a sociedade e seus fenômenos. Harari (2019) adverte, ainda, que a liberdade de informação passaria a ter nova conotação, vez que sua busca agora ocorre em favor dos dados e não mais em favor do cidadão. Esse intuito de assegurar o livre fluxo de dados se dá, em geral, sob a justificativa de supostos benefícios que tal fluxo pode

6 É necessário evidenciar que, embora ainda sejam tratados como sinônimos, dados e informações não se equivalem (BIONI, 2020). Dados seriam o estado primitivo da informação, que, quando processados e organizados, convertem-se em algo inteligível, podendo ser deles ser extraído uma informação. Já a informação seria um conjunto de fatos organizados de modo a ter valor adicional ao revelar algo.

7 Art. 5º, I da LGPD (BRASIL, 2018).

8 Art. 5º, II da LGPD (BRASIL, 2018).

9 Art. 5º, III da LGPD (BRASIL, 2018).

trazer ao indivíduo e à sociedade, como por exemplo: melhoramento de pesquisas relativas à saúde, descoberta de novos medicamentos e, em especial, o controle de pandemias.

Os dados, cuja vasta coleta, estavam inicialmente ligados a fins publicitários e ao desenvolvimento de inteligência artificial, agora se tornam o ativo mais importante das sociedades modernas (MOROZOV, 2019). Nelas, as tecnologias de informação e comunicação, em especial a internet, adquirem vital importância, pois permitem a conexão de pessoas, lugares e ideias. Tais novidades relevantes autorizam e exigem, como bem demonstra Lessig (1999), a construção de um código para o ciberespaço, para que as relações lá desenvolvidas sejam permeadas pelos valores que a sociedade escolha, valores esses que, na visão dos autores do presente artigo, precisam ser democráticos, inclusivos e igualitários.

Pois bem, para Leonardi (2012), a internet pode ser definida como uma rede internacional de computadores conectados entre si, sendo um meio de comunicação que possibilita o intercâmbio de informações de toda natureza, em escala global, com nível de interatividade jamais vista anteriormente. Tal noção técnica deixa de revelar um importante ângulo do conceito, de que, em verdade, muito mais do que uma rede de computadores, trata-se de uma rede de pessoas (OLIVEIRA, 2018).

Nesse sentido, Castells (2019) afirma, acertadamente que vivemos numa sociedade em rede na qual tudo está conectado pela internet. Essa "sociedade em rede" é entrelaçada por dados pessoais e informações que possibilitam não só a identificação de qualquer cidadão, mas o conhecimento de suas características, hábitos e comportamentos. Eis o grande risco social, pois é possível, a partir da avançada capacidade computacional, transformar todos esses dados em rigorosos perfis comportamentais. Essa é uma característica atual da conjuntura do *big data*: a possibilidade de transformar dados e informações em padrões.

Autores como O'Neil (2016) indicam que, a partir desses padrões, podem ser até mesmo revelados aspectos íntimos dos indivíduos, tais como ignorância, dor, sofrimento, baixa autoestima e outros estados similares de vulnerabilidade que podem ser utilizados para realizar ofertas de produtos ou pessoas que, "coincidentemente", aparecem como uma possível ou certa solução para minorar tais estados. Procura-se o "*pain point"*(ponto da dor) das pessoas, não para curá-lo, mas para aproveitar-se dele (O'NEIL, 2016).

Observa que "em todo o lugar onde se achar a combinação de grande necessidade e ignorância, provavelmente existirá publicidade predatória" (O'Neil, 2016, p. 70). Muitas destas pessoas fragilizadas acessam mecanismos de buscas do Google, por exemplo, revelando sua fragilidade, seus desejos, seus medos, suas convicções, crenças, excitação, sua intimidade e personalidade. Portanto, não há mais dados insignificantes. Qualquer cruzamento entre dados de um indivíduo possibilita, na atual conjuntura tecnológica, a criação de metadados, que servem a diversos interesses, sejam eles o lucro, a eleição de certo candidato, a escolha de certa ideia, produto, medicamento etc.

Além disso, por meio da conexão com a rede, tornou-se mais fácil também vigiar. A sutileza da vigilância moderna está justamente na sua capacidade de ser manter oculta. As pessoas raramente têm conhecimento de que estão sendo vigiadas, quais dados estão sendo registrados e para quais fins. Marx (2005) denominou essa nova forma de vigilância como "*Soft Surveillance*" ou vigilância sutil. Nesse cenário urge refletir acerca da facilidade com que se entrega dados e informações, seja para acessar plataformas e serviços ou até mesmo para se adequar às expectativas sociais de participação da vida online.

Marx (2005) entende que essa voluntariedade é, de certa forma, uma voluntariedade obrigatória. Pois, por exemplo, como acessar o conhecimento disponível na internet sem estar sujeito ao rastreamento e à coleta? Pariser (2012) comenta, inclusive, que essa falsa voluntariedade pode gerar um fenômeno de aprisionamento dos usuários, os quais estão tão presos em determinado serviço que, mesmo que um concorrente apresente um serviço melhor, não vale a pena mudar. Assim, se determinado usuário é membro do *Facebook*, imagine o trabalho que ele teria para migrar todas suas informações para outro site de relacionamento social.

Destaca-se que boa parte dos usuários desconhece que cada atividade *online* ou *offline* deixa um rastro, e havendo poucas opções de não estar sujeito à mecanismos de vigilância sutil, a intimidade deixa de ser regra para ser exceção. A intimidade logo é convertida em uma *commodity*, na qual os dados são a principal moeda de troca. Diante dessa diversidade de fins inerentes à grande circulação de dados pela internet é que o compartilhamento de dados pessoais por empresas privadas para agências ou órgãos do governo ganha grande relevância e notoriedade, tornando-se objeto de enorme preocupação.

Isto posto, mesmo o STF já tendo suspendido os efeitos da MP 954/2020 ou mesmo devido a perda da sua eficácia, pois não foi convertida em lei no prazo legal, trouxe ao debate a real possibilidade de que o IBGE tivesse acesso à relação de milhares de nomes, números de telefone e endereços de consumidores das empresas de telefonia. Os dados de que tratava a MP 954/2020 configuram-se simultaneamente como registro eletrônico e como dados pessoais, uma vez que identificavam brasileiros por intermédio da produção de um banco de dados eletrônicos. Em 2020, a Anatel informou que existem 226,28 milhões de linhas móveis ativas no Brasil e 32,65 milhões linhas de telefone fixos (ANATEL, 2020), contabilizando uma estimativa de 258,93 milhões de possíveis cadastros telefônicos que seriam repassados para o IBGE.

O nome e telefone dos indivíduos podem ser considerados a porta de entrada a dados pessoais sensíveis. Isso porque, por meio do número de telefone é possível ter acesso a aplicativos como o *Whatsapp* e, por conseguinte, a conta de *Facebook*. No ano passado, o *Facebook* solicitou aos seus usuários que cadastrassem o número de celular. Aparentemente, a estratégia denota maior segurança e proteção ao usuário, porém o cadastro do número celular na referida rede social, na realidade, fragiliza e expõe ainda mais o indivíduo (SILVA, 2019).

Ademais, o número de celular permite o acesso aos dados de geolocalização, isto é, possibilita o conhecimento acerca de todos os locais onde o dono do aparelho celular esteve e os trajetos que fez. As conexões realizadas pelos aparelhos, por sua vez, permitem a produção do que os especialistas denominam de mapa de calor, que indica a concentração de celulares em determinada área.

Os dados de geolocalização, especificamente o mapa de calor, têm sido utilizados por diversos países como estratégia de combate ao COVID-19, inclusive por alguns estados brasileiros. Contudo, a MP 954/2020 não indica tal utilização, ou outra finalidade que pudesse resultar em um combate imediato à pandemia, como por exemplo, diminuição da taxa de contágio e transmissão. Apenas informa que necessita dos dados para produção de estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

Em relação ao endereço, o risco é notável também, principalmente considerando que há um forte nível de segregação sócio territorial no Brasil, com lógicas próprias de apropriação

e de distribuição de renda. O endereço transforma-se, pois, em informação de caráter social relevante. Além disso, é possível extrair informações secundárias do endereço, como a renda familiar. Essa metodologia já é utilizada em pesquisas de saúde pública, por exemplo (Alves; Soares, 2009). Ressalta-se, ainda, o questionamento de que, se as entrevistas anunciadas iriam ser realizadas em caráter não presencial, qual seria a necessidade de compartilhamento do endereço dos cidadãos?

Assim, diante desse cenário, torna-se extremamente preocupante o compartilhamento dos dados pessoais dos cidadãos para a realização de pesquisa por órgãos do governo, sem o devido detalhamento dos métodos, das finalidades específicas e dos mecanismos de proteção e responsabilização por eventuais vazamentos. A preocupação não deve ser entendida como desconfiança dos órgãos estatais, por considerar que eles podem desviar a finalidade para qual os dados serão compartilhados, mas sim em razão de ainda não haver um ambiente seguro para que o compartilhamento aconteça. Entende-se por ambiente seguro aquele respaldado por legislações protetivas, com instituições capazes de operacionalizar e fiscalizar o controle de dados e que possuam um cidadão devidamente educado para o ambiente digital (letramento digital, o que, infelizmente, ainda não é o caso do Brasil.

Quando a Medida estava prevista para ser aplicada, a LGPD (BRASIL, 2018) ainda nem havia entrado em vigor. Contudo, é importante destacar que mesmo com a entrada recente ainda falta ao ordenamento jurídico brasileiro um conjunto de mecanismos que, de fato, possibilitem um ambiente seguro para o compartilhamento de dados pessoais. Nesse aspecto, lembre-se que até o presente momento sequer tiveram início as atividades da Autoridade Nacional de Proteção de Dados, órgão responsável por fiscalizar as empresas e o Poder Público a quando do tratamento desses dados. Ora, se ainda sequer se possui uma Autoridade Nacional para fiscalizar e adotar as medidas necessárias para a efetiva proteção de dados dos brasileiros, o compartilhamento dos dados pessoais, como pretendia a MP 954/2020, é claramente um risco.

Assim, diante de todos os riscos que envolvem o compartilhamento de dados pessoais, pretendido pela MP 954/2020, faz-se mister uma análise crítica acerca de seu conteúdo e efeitos, especialmente em face dos direitos à intimidade e à autodeterminação informativa. Nesse sentido, o próximo tópico faz uma análise reflexiva acerca do direito à intimidade e sua evolução frente aos avanços tecnológicos e do direito à autodeterminação informativa como direitos que limitam o compartilhamento de dados pessoais de forma ampla e irrestrita. Faz, ainda, uma análise de tais direitos face à Constituição Federal e à LGPD.

4. PROTEÇÃO À INTIMIDADE E À AUTODETERMINAÇÃO INFORMATIVA COMO LIMITE CONSTITUCIONAL AO COMPARTILHAMENTO DE DADOS PESSOAIS

A vigente CR/88 assegura a inviolabilidade do sigilo de dados e comunicações telefônicas, salvo, em último caso, interferências autorizadas por ordem judicial, nas hipóteses e na forma que a lei estabelecer, para fins de investigação criminal ou instrução processual penal,

como bem aponta o artigo 5º, XII da Constituição Federal (BRASIL, 1988). Essa proteção, evidentemente, deriva do âmbito de proteção do direito à intimidade, o qual ocupa a esfera de proteção dos denominados direitos da personalidade. A construção doutrinária sobre esse conjunto de direitos enfrentou algumas controvérsias ao longo dos anos. A primeira delas refere-se à contraposição entre a tese da unidade e tese da pluralidade.

Segundo Luño (2005), alguns autores defendem a tese da unidade dos direitos de personalidade (personalidade entendida como a qualidade de ser pessoa), ou seja, o estabelecimento de um direito unitário ou geral da personalidade, concebido por intermédio de um marco de referência que englobasse a livre atuação da personalidade em todas suas direções. Tal entendimento se dá na Alemanha, por exemplo, como demonstra Vasconcelos (2019), onde o direito geral de personalidade, expressamente reconhecido pelo texto constitucional, convive com vários direitos especiais de personalidade.

Contudo, perante a CR/88, bem como à luz da Constituição portuguesa, não se verifica a necessidade, sentida na Alemanha, de construir um direito geral de personalidade (VASCONCELOS, 2019), visto que tais textos constitucionais tutelam, expressamente, direitos especiais da personalidade, tais como: vida, integridade física e moral, intimidade, vida privada, honra e imagem, e, de modo não escrito – ou seja, implícitos ou decorrentes – os direitos ao nome, à identidade pessoal, ao livre desenvolvimento da personalidade etc. Para o ordenamento jurídico constitucional brasileiro, o papel do direito geral de personalidade é cumprido pelo reconhecimento da Dignidade da Pessoa Humana.

Seja como for, aqueles que defendem a unidade do direito à personalidade se veem obrigados a reconhecer de imediato a diversidade de suas manifestações, dotadas de certo status jurídico autônomo. Ao mesmo tempo, aqueles que se inclinam pela concepção pluralista dos direitos de personalidade não podem descartar a existência de um fundamento geral para esse conjunto de direitos, qual seja, a dignidade humana, que representa tanto um fundamento, como ponto de referência para esses direitos (LUÑO, 2005). Todavia, à luz de nosso texto constitucional, como já dito, parece-se mais apropriado tratar do âmbito normativo de cada um dos direitos especiais de personalidade em detrimento da busca pela definição de um direito geral de personalidade. Ao presente estudo será importante a intimidade, razão pela qual tais direitos serão, doravante, analisados.

Nesse sentido, a Constituição de 88, em seu artigo 5º, X, garante como invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas. Parece desejar tratar, assim, intimidade e vida privada como dois direitos diferentes (BRASIL, 1988). A distinção, todavia, entre intimidade e vida privada não se revela adequada aos novos tempos e nem, muito menos, útil.

O presente trabalho, portanto, adotará as expressões privacidade e intimidade como expressões cujo âmbito normativo é equivalente, ou cuja diferença sutil não justifica tratá-los como algo diverso. Quer isso dizer que, mesmo quando a distinção é feita, ela não se conseguirá revelar materialmente relevante, sendo apenas uma questão de aprofundamento material. Na doutrina brasileira, perfilados a esse entendimento estão Gonet Branco, Luiz Avólio, José Afonso da Silva (Garcia, 2018).

Ademais, se do ponto de vista tradicional o direito à intimidade protegeria a capacidade de autodeterminação pessoal e familiar, garantindo a não interferência de terceiros nos espaços privados e no plano de vida dos indivíduos (Pérez, 2008), é indene de dúvida razoável que,

a partir do momento em que as sociedades se tornaram mais complexas, especialmente com o avanço das tecnologias, a possibilidade de exposição da intimidade a níveis e formas antes inconcebíveis fez surgir a necessidade de uma nova compreensão do que seria o íntimo. Compreensão essa que precisava ser atualizada para proteger também situações, objetos e espaços virtuais.

Luño (2005) afirma que esse era um dilema conceitual, pois manter fidelidade ao primeiro significado do direito à intimidade causaria o risco de torná-lo ineficaz aos novos tempos. Sustentar a exclusividade de uma dimensão interna e isolada da intimidade contrasta com a existência dos indivíduos em sociedade, especialmente suas formas de comunicação coletiva, que integram e socializam o que há de mais íntimo no ser.

As questões que gravitam em torno da disciplina jurídica da intimidade têm perdido seu exclusivo caráter individual e privado, para assumir progressivamente um significado público e coletivo, principalmente com o surgimento da internet e suas complexas redes de socialização. Realocar esses direitos para além do ordenamento privatista e estritamente individual aponta para o reconhecimento da importância de sua perspectiva coletiva. Assim, houve, naturalmente, uma aproximação de ambos os conceitos, pelo que, atualmente, revela-se perfeitamente adequado perceber que o novo conceito de intimidade responde de modo perfeitamente adequado às demandas que anteriormente eram respondidas por intermédio da bifurcação entre privacidade e intimidade.

Contudo, isso ocorre desde que se perceba que a intimidade não poderá mais ser entendida apenas em seu aspecto negativo, clássico, ou seja, como "direito ao isolamento, ao confinamento a si mesmo, ao poder de retirar-se virtual e provisoriamente do mundo e pôr-se dentro de si", como assevera Morente (1935 apud LUÑO, 2005, p. 355), ou mesmo a "pretensão, liberdade, poder e imunidade de dispor de um âmbito de vida pessoal subtraído de qualquer tipo de intromissão perturbadora ou, simplesmente, indesejadas", no dizer de Hohfeld (1913 apud LUÑO, 2005, p. 356).

A tal aspecto negativo, é mister que se inclua uma concepção aberta, ativa ou dinâmica, pelo que a intimidade também passa a abranger o direito de conhecer, acessar e controlar as informações que dizem respeito, que são relevantes a cada pessoa (LUÑO, 2005, p. 357). Mais que um estado de auto confinamento, trata-se de uma qualidade que deve permear a relação com os outros, no preciso dizer de Podlech (1984 apud LUÑO, 2005, p. 357), "uma condição ou qualidade social da pessoa".

Trata-se do núcleo da autodeterminação informativa, o qual já se encontra previsto como fundamento específico da disciplina de proteção de dados pessoais no Brasil, conforme art. 2º, II, da LGPD, enquanto aspecto básico da intimidade (LUÑO, 2005), reconhecido pelo Tribunal Constitucional Alemão como a Liberdade do cidadão em determinar quem, o que e em que ocasião se pode conhecer e utilizar dados que o afete.

Sampaio (1998, p. 363) afirma que a pessoa, isoladamente ou enquanto ser social, seria um "centro de referência de informações", pelo que o direito à intimidade consistiria numa gama de faculdades que permitem a seletividade de informações que penetram (*inputs*) e que partem (*outputs*) do campo perceptivo da pessoa.

Segundo Solove (2013), esse instituto surgiu em 1973, quando o Departamento de Saúde, Educação e Bem-Estar dos EUA começou a se preocupar com a crescente onda de digitaliza-

ção de dados. O conceito diz respeito à capacidade do indivíduo de gerenciar seus próprios dados e sua privacidade, como pressuposto para fornecer um consentimento livre e consciente do uso de seus dados. Ou seja, os indivíduos devem ter a capacidade de influenciar de forma efetiva e definitiva sobre como serão utilizados seus dados pessoais.

O autor (SOLOVE, 2013) cita alguns requisitos que foram colocados na época para que fosse possível essa autodeterminação, como: (I) a transparência do sistema de registro dos dados, (II) o direito de contestar os registros, (III) o direito de impedir a utilização de seus dados, (IV) o direito de corrigir os dados e (V) a responsabilização dos utilizadores dos dados, em caso de uso indevido. Dentro dessa adequada amplitude conceitual, a noção de intimidade identifica-se com a própria noção de liberdade, aparecendo, ainda, como uma condição para o convívio democrático (LUÑO, 2005).

Igualmente dentro dessa adequada amplitude conceitual, a intimidade aproxima-se da noção de *privacy* desenvolvida nos Estados Unidos (LUÑO, 2005), que, para além dessas duas dimensões (positiva e negativa), ainda engloba a garantia de respeito às opções pessoais em matéria de associação ou crenças e a liberdade de eleição sem interferências (LUÑO, 2005).

No Brasil, a proteção constitucional da intimidade adquire outro importante aspecto. A Constituição Federal incluiu a intimidade, a honra e a imagem na categoria de bens jurídicos que não foram merecedores nem de restrições imediatas, nem de restrições mediatas. Ou seja, foram garantidos sem que fosse prevista, ao contrário do que ocorre em inúmeros outros casos, a possibilidade de limitação imposta pelo próprio texto constitucional ou mediante lei infraconstitucional devidamente autorizada pelo texto constitucional. Assim, seria razoavelmente questionável o poder do Legislador em limitar um direito que o constituinte expressamente não autorizou que fosse limitado, pelo que tal limite apenas poderia advir do direito constitucional de colisão.

Desta forma, percebe-se que o STF incorporou essa necessidade de tutela eficiente da autodeterminação informativa. Nesse sentido, a decisão que cessou os efeitos da MP já indica o status fundamental das garantias relativas à proteção de dados pessoais e estabelece um novo horizonte paradigmático para casos e medidas futuras, adotadas por entidades governamentais ou privadas, antes mesmo da vigência da LGPD, num nítido reforço ao papel de protagonismo que vem exercendo em relação aos Poderes da República.

A proteção da intimidade e concepção de um direito à autodeterminação informativa são operacionalizadas através dos conceitos trazidos pela própria LGPD, como consentimento, necessidade (atendimento das finalidades específicas) e transparência. O consentimento, por exemplo, está previsto no art. 5º, XII da LGPD (BRASIL, 2018) e é definido como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Logo, operacionaliza a ideia de autodeterminação informativa, ou seja, de controle, pela pessoa, de quais dados e quais informações irão entrar ou sair do seu campo pessoal. É a ideia de que o titular dos dados deve consentir, através do autocontrole de seus dados.

Contudo, o texto da MP 954/2020 em nenhum momento trata de consentimento, de que os usuários de telefonia teriam a chance de consentir sobre o compartilhamento de seus dados cadastrais. Tal ausência se torna ainda mais grave, se for levado em consideração que os dados produzidos pelas entrevistas poderiam ser da categoria de dados sensíveis,

por exemplo, no caso de as respostas revelarem quadros sintomáticos da doença. Referida categoria exige um consentimento específico e destacado, segundo art. 11, inciso I da LGPD (BRASIL, 2018).

A LGPD (BRASIL, 2018) traz uma hipótese em que o tratamento dos dados sensíveis poderia ser realizado sem o consentimento do titular no art. 11, inciso II, alínea C: "realização de estudos por órgão de pesquisa, garantida sempre que possível, a anonimização dos dados sensíveis". Logo, a MP 954/2020, se nunca considerou inserir o consentimento naquele compartilhamento, deveria ter previsto ao menos a anonimização dos dados pessoais. Contudo, isso exigiria a mudança dos próprios dados exigidos (relação de nomes, endereços e telefone), além de uma mudança na própria operação de coleta e análise desses dados, hipótese nem levantada pelo texto da Medida.

A necessidade, por sua vez, prevista no art. 6º, inciso III da LGPD (BRASIL, 2018) refere-se à "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". É a ideia de que o tratamento deve utilizar apenas os dados estritamente necessários para a realização da finalidade proposta.

Na circunstância da MP 954/2020, seria o caso do seu texto ter indicado expressamente como todos os dados cadastrais solicitados iriam ser necessários para as entrevistas não presenciais. Inclusive, considerando que o IBGE já possui seu próprio banco de dados institucionais, então a MP deveria ter indicado qual a necessidade atual para a solicitação destes novos dados. Além disso, a necessidade está muito ligada à finalidade, no sentido de entender se aqueles dados são necessários para aquela finalidade. No contexto da pandemia, deveria ter sido indicado detalhadamente como os dados poderiam efetivamente contribuir, de forma imediata, para a vigilância epidemiológica, ou para reunir informações sobre o comportamento da doença. A necessidade visa proteger a esfera da intimidade, para que as interferências nessa esfera sejam apenas nos limites necessários para a realização da finalidade.

Por último, vale ressaltar o princípio da transparência, previsto no art. 6º, inciso VI da LGPD (BRASIL, 2018), que garante aos titulares dos dados, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento, bem como os respectivos agentes de tratamento, observados os segredos comercial e industrial. Verifica-se que a falta de transparência e a falta de indicação sobre como seria realizado o tratamento foram pontos questionados pelo STF na análise material da MP 954/2020. Isso porque não fora indicado mecanismos de proteção dos dados ou mecanismos de responsabilização para eventuais vazamentos e usos diversos.

Assim, os limites constitucionais do compartilhamento de dados pessoais se baseiam na proteção da intimidade na concepção de um direito à autodeterminação informativa, como bem delineado pelo julgamento do STF. Tais limites dialogam, são detalhados e operacionalizados com os conceitos e princípios previstos pela LGPD (BRASIL, 2018), que vem para fortalecer e disciplinar a proteção de dados pessoais no Brasil.

Ainda que de forma indireta, é possível vislumbrar na decisão do STF a preocupação da Corte de que o compartilhamento de dados pessoais, previsto na MP 954/2020, tenha impactos que ultrapassam a esfera do direito à intimidade e à autodeterminação informativa. Trata-se do risco ao regime democrático, tendo-se em conta a capacidade de transformação dos dados pessoais dos cidadãos em perfis políticos capazes de desequilibrar a tomada de deci-

sões políticas coletivas. Por este motivo, o próximo tópico trata do acesso aos dados pessoais e do risco à democracia, considerando que a posse de informações sensíveis dos cidadãos, tanto por empresas privadas quanto pelo poder estatal, produz riscos ao regime democrático.

5. O ACESSO AOS DADOS PESSOAIS E O RISCO À DEMOCRACIA

Nos últimos anos, atores políticos têm utilizado o espaço virtual como um novo meio para atingir eleitores e ganhar apoio político. Possibilidade, iniciada com a televisão, de que as lideranças políticas poderiam se comunicar com o eleitorado de forma direta, sem intermediários, na forma da expressão quase "olho no olho". Com a internet e as novas plataformas de vídeo, isso também se tornou possível, e de certa forma até potencializado. Entretanto, candidatos também começam a pensar estratégias político-virtual a partir de dados pessoais. Utiliza-se dados pessoais para coletar informações, rastrear probabilidades de apoio eleitoral e até mesmo direcionar comportamentos. Agentes políticos, conjuntamente com empresas privadas de tecnologia, têm sido notificados por essas práticas.

Foi o caso das eleições presidenciais dos EUA em 2016. Na ocasião, a empresa *Cambridge Analytica* usava, a favor o candidato eleito, Donald Trump, o chamado micro-targeting político. A empresa utilizava o máximo de dados individuais possível para criar um perfil psicológico e político dos eleitores, com o intuito de persuadi-los de forma mais eficiente aos fins da campanha de Trump (POLONSKI, 2017). Importante notar que as referidas análises e coordenações de ações políticas por parte da empresa só foram possíveis graças ao imenso volume de dados coletados dos usuários a partir de um aplicativo do Facebook, de testes supostamente informais.

O direcionamento pode ocorrer com tamanha precisão que o eleitor indeciso recebe propaganda política acerca dos temas que lhe são mais sensíveis, prevendo e ao mesmo tempo moldando as suas escolhas políticas. Nesse sentido, o acesso aos dados pessoais dos cidadãos brasileiros sem qualquer medida de proteção ou responsabilização em caso de violação dos direitos dos usuários pode se tornar uma arma poderosa no jogo democrático. Assim, Frazão afirma que:

> O conhecimento profundo das características dos usuários, inclusive no que diz respeito às suas fragilidades, pode ser utilizado para toda sorte de discriminações e abusos, além da manipulação de suas emoções, crenças e opiniões para os fins mais diversos, inclusive os políticos (FRAZÃO, 2019, p. 37).

É necessário que haja um balanceamento ético-jurídico nas práticas advindas do ciberespaço, por intermédio de uma análise centrada nos efeitos das ações dentro da esfera privada ou sensível dos indivíduos. Deve-se encarar o avanço tecnológico como uma realidade que tende a se desenvolver mais rápido, talvez, do que a capacidade do Direito em acompanhá-la. No entanto, é papel fundamental do Direito e das instituições jurídicas fiscalizar essas práticas, protegendo os indivíduos de violações que interfiram no exercício de sua autonomia.

Sendo assim:

> O Direito, (...), servirá como um canalizador do processamento de dados e demais materialidades tecnológicas evitando uma tecnorregulação nociva à humanidade. Nesse novo papel, é importante que o Direito oriente a produção e o desenvolvimento de Coisas (artefatos técnicos) de forma a serem sensíveis a valores, por exemplo, regulando privacidade, segurança e ética *by design* (MAGRANI, 2019, p. 257).

Afinal, o direito ao autodesenvolvimento individual só pode ser exercido por quem tem controle sobre sua vida, o que pressupõe a autodeterminação informacional, o que, por seu turno, exige um modelo de educação e de condutas voltado para esses novos problemas e fragilidades.

Discutindo ideias para uma melhor proteção do cidadão, em face das novas tecnologias, Helbing *et al*. (2017, tradução nossa) defendem, corretamente, a instituição dos seguintes princípios para nortear a relação com as novas tecnologias:

> (1) Descentralizar a função dos sistemas de informação; (2) Apoiar a autodeterminação e participação da informação; (3) Melhorar a transparência, a fim de obter maior confiança; (4) Reduzir a distorção e poluição da informação; (5) Habilitar filtros de informação controlados pelo usuário; (6) Apoiar a diversidade social e econômica; (7) Melhorar a interoperabilidade e as oportunidades de colaboração; (8) Criar assistentes digitais e ferramentas de coordenação; (9) Apoiar a inteligência coletiva, e (10) Promover o comportamento responsável no mundo digital por meio da alfabetização digital[10]

Para que tais princípios possam atuar, é mister a realização de uma escolha, que não é apenas do indivíduo, mas precipuamente do Estado, no exercício da arte de governar, definindo e implementando prioridades. Em outras palavras, a questão jamais poderá ser enfrentada corretamente sem a instituição e o desenvolvimento de recursos públicos e políticas públicas centrais que determinem o caminho a ser trilhado. Além disso, é fundamental que o Estado incentive e crie medidas que favoreçam a alfabetização digital, uma vez que esta é pressuposto fundamental para que os cidadãos entendam os riscos da violação de sua privacidade, assim como os riscos das dinâmicas de desinformação.

Logo, a atividade estatal deve estar voltada a proteger e não fragilizar os direitos a intimidade e autodeterminação informativa, pois tais direitos quando violados possibilitam que a própria liberdade e autonomia do indivíduo sejam ameaçadas, o que pode comprometer um dos pilares do regime democrático vigente no país, qual seja, o próprio regime eleitoral de escolhas políticas. O debate acerca da proteção desses direitos deve ser estimulado, considerando que as novas tecnologias permitem maior acesso aos dados pessoais e ainda propiciam a sua ampla e irrestrita circulação, o que gera a real necessidade de adequação dos instrumentos de proteção jurídica no ordenamento brasileiro vigente.

10 Tradução livre de: 1. to increasingly decentralize the function of information systems; 2. to support informational self-determination and participation; 3. to improve transparency in order to achieve greater trust; 4. to reduce the distortion and pollution of information; 5. to enable user-controlled information filters; 6. to support social and economic diversity; 7. to improve interoperability and collaborative opportunities; 8. to create digital assistants and coordination tools; 9. to support collective intelligence, and 10. to promote responsible behavior of citizens in the digital world through digital literacy and enlightenment (HELBING *et al.*, 2017).

6. CONSIDERAÇÕES FINAIS

Nas últimas décadas, o avanço da tecnologia transformou quase a totalidade das atividades técnicas, informacionais, científicas, e até mesmo sociais. Com o surgimento da pandemia em 2020, a tecnologia foi utilizada como aliada no "combate ao novo coronavírus", até porque a velocidade de transmissão e contágio impôs que os Estados fornecessem respostas rápidas a um agente viral, com o qual nunca se havia lidado antes. A análise de dados, nesse contexto emergencial, auxiliou na predição e, eventualmente, na própria tomada de decisão pelos governos. Dentre essas operações, o compartilhamento de dados pessoais foi muito utilizado, como o que fora proposto pela MP 954/2020.

Como delineado durante o julgamento do STF, essas iniciativas, advindas do poder público, devem observar os limites constitucionais, principalmente o respeito à intimidade e o direito à autodeterminação informativa, além dos mecanismos protetivos previsto pela Lei Geral de Proteção de Dados Pessoais. A MP 954/2020 escolheu a via da desproteção imotivada dos dados pessoais, pois colocou em risco informações da esfera pessoal dos cidadãos brasileiros, sem o devido detalhamento dos métodos, das finalidades específicas e dos mecanismos de proteção e responsabilização por eventuais vazamentos, o que viola a proteção da intimidade, compreendida agora também a partir de uma perspectiva conectiva, digital e eletrônica. Além disso, violou também o direito à autodeterminação informativa, ao não fornecer mecanismos ou opções que permitem os usuários consentirem ou não com a transferência de seus dados.

Diante de um cenário de combate a pandemia, torna-se extremamente preocupante o compartilhamento dos dados pessoais dos cidadãos desta forma desprotegida e insuficientemente motivada. Deve-se ter em mente que os dados pessoais do cidadão são ativos de grande importância e que podem revelar muito mais do que apenas nome, endereço e telefone. Ademais, o controle desses dados, quanto a sua exposição e compartilhamento, deve, necessariamente, ser do indivíduo e não das empresas e/ou do Estado.

Isso porque, para além da lesão à intimidade, o acesso aos dados pessoais pode comprometer o próprio equilíbrio democrático, razão pela qual, ainda que, em tese, possível e compatível com o ordenamento jurídico pátrio, o acesso a tais dados deve vir acompanhado de medidas legais e operacionais que assegurem a sua utilização tão somente ao propósito de pesquisa estatísticas ou sanitárias. O que tornaria a utilização dos dados pessoais legítima e compatível com o ordenamento jurídico brasileiro, já que a favor da coletividade.

Não à toa, a decisão do STF suspendeu os efeitos da MP 954/2020, por vislumbrar a possibilidade de grave lesão aos direitos fundamentais do cidadão, em especial o direito à privacidade e à autodeterminação informativa, feito que deve ser elogiado, tendo em vista que a LGPD ainda não havia entrado em vigor, e o cidadão, não fosse a suspensão, poderia ter sido gravemente prejudicado.

A pesquisa aqui desenvolvida abordou o teor da MP 954/2020 e a lesão por ela perpetrada aos limites constitucionais e legais à proteção de dados pessoais. Sua limitação refere-se justamente a este campo restrito de análise. Contudo, tais reflexões podem auxiliar na construção de outras pesquisas acadêmicas acerca do tema, seja por correlação ou afinidade, tendo em vista que a tendência é de que cada vez mais o poder público, empresas do

setor privado ou ambos em conjunto utilizem medidas de tratamento de dados pessoais. Por isso, é fundamental que se estimule a consolidação de um ambiente seguro para a proteção de dados pessoais no Brasil, seja por meio de estudos sobre o tema ou na fiscalização de medidas de tratamento de dados pessoais através das autoridades competentes, inclusive aquelas previstas na Lei Geral de Proteção de Dados Pessoais.

REFERÊNCIAS

ALVES, Maria Teresa Gonzaga; SOARES, José Francisco. Medidas de nível socioeconômico em pesquisas sociais: uma aplicação aos dados de uma pesquisa educacional. *Opinião Pública,* Campinas, v. 15, n. 1, p. 1-30, jun. 2009. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104=62762009000100001-&lng=en&nrm-iso. Acesso em: 28 jun. 2020.

AMARAL, Bruno do. Coronavírus: TIM e Prefeitura do Rio assinam acordo para coletar dados de deslocamento. *Teletime*, São Paulo, 23 mar. 2020. Disponível em: https://teletime.com.br/23/03/2020/coronavirus-tim-e-prefeitura-do-rio-assinam-acordo-para-coletar-dados-de-deslocamento/. Acesso em: 8 out. 2020.

ANATEL. Panorama Setorial de Telecomunicações. *In:* ANATEL. *Relatório anual de gestão.* Brasília, DF: ANATEL, 2020. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO59jtrWc1-S4nfX-SeHrqZ0yJ4y5VQfXUs0tAawmhcxMpvx_M5wnV-y55u7TZxpVC1wbPvX8lqe4T93KoIvcrei. Acesso em: 28 de jun. 2020.

APLICATIVO Coronavírus-SUS vai alertar contatos próximos de pacientes com Covid-19. *Gov.br.,* Brasília, jul. 2020. Disponível em: https://www.hmg.saude.gov.br/noticias/agencia-saude/47292-aplicativo-coronavirus-sus-vai-alertar-contatos-proximos-de-pacientes-com-covid-19. Acesso em: 8 out. 2020.

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

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil.* Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 13 jul. 2020.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 jul. 2020.

BRASIL. Medida provisória nº 954, de 11 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 nº 13.979, de 6 de fevereiro de 2020. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 11 abr. 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 19 ago. 2020.

CASTELLS, Manuel. *A era da informação, economia, sociedade e cultura.* 20. ed. São Paulo: Paz e Terra, 2019.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais – Noções Introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 23-49.

GARCIA, Rafael de Deus. Os Direitos à Privacidade e á Intimidade: Origem, Distinção e Dimensões. *Revista da Faculdade de Direito do Sul de Minas.* Pouso Alegre, v. 34, n. 1, p. 1-26, jan./jun. 2018. Disponível em: https://www.fdsm.edu.br/mestrado/revista_artigo.php?artigo=288&volume=34.1. Acesso em: 28 jun. 2020.

HAMAGEN. *The Nacional app to fight the spread of Covid-19.* Jerusalém: *Ministry Of Health*, 2020. Disponível em: https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/. Acesso em: 8 out. 2020.

HARARI, Yuval Noah. *21 Lições sobre o século XXI.* São Paulo: Companhia das Letras, 2018.

HARARI, Yuval Noah. *Homo Deus, uma breve história do amanhã.* São Paulo: Companhia das Letras, 2019.

HELBING, Dirk *et al*. Will Democracy Survive Big Data and Artificial Intelligence. *Scientific American*, [*S. l.*], 2017. Disponível em https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/. Acesso em: 31 jul. 2019.

JORNAL NACIONAL. Governo de SP usa dados de celulares para localizar aglomerações. *G1*, [*S. l.*], 8 abr. 2020. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2020/04/08/governo-de-sp-usa-dados-de-celulares-para-localizar-aglomeracoes.ghtml. Acesso em: 8 out. 2020.

LEONARDI, Marcel. Determinação da Responsabilidade Civil pelos ilícitos na Rede: os deveres dos provedores de serviços de internet. *In:* SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos (org.). *Responsabilidade Civil na Internet e nos demais meios de comunicação.* 2. ed. São Paulo: Saraiva, 2012. *E-book*. (Série Gvlaw). Disponível em: https://lelivros.love/book/download-responsabilidade-civil-na-internet-e-nos-demais-meios-de-comunicacao-serie-gvlaw-regina-beatriz-tavares-da-silva-em-epub-mobi-e-pdf/. Acesso em: 18 out. 2020.

LESSIG, Lawrence. *Code and Other Laws of Cyberspace.* New York: Basic Books, 1999.

LUÑO, Antonio Enrique Perez. *Derechos Humanos, Estado de Derecho y Constituicion.* Madrid: Tecnos, 2005.

MAGRANI, Eduardo. *Entre dados e robôs:* ética e privacidade na era da hiperconectividade**.** Porto Alegre: Arquipélago Editorial, 2019.

MARX, Gary T. Soft Surveillance: Mandatory Voluntarism and the Collection of Personal Data. *Dissent Magazine,* Philadelphia, v. 52, n. 4, p. 36-43, 2005. Disponível em: https://www.dissentmagazine.org/article/soft-surveillance-mandatory-voluntarism-and-the-collection-of-personal-data. Acesso em: 18 out. 2020.

MOROZOV, Evgeny. *Big Tech:* A ascensão dos dados e a morte da política**.** São Paulo: UBU Editora, 2018.

MOZUR, Paul; ZHONG, Raymond; KROLIK, Aaron. Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. *NYTimes,* Nova Iorque, 2020. Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 8 out. 2020.

O'NEIL, Cathy. *Weapons of Math Destruction:* how big data increases inequality and threatens democracy. New York: Crown Publishing Group, 2016.

OLIVEIRA, Neide M. C. Cardoso de; MORGADO, Marcia. Projeto Ministério Público pela Educação Digital nas Escolas. *In*: SILVA, Ângelo Roberto Ilha da (Org.). *Crimes Cibernéticos.* 2. ed. Porto Alegre: Livraria do Advogado, 2018

PARISER, Eli. *O filtro invisível:* O que a Internet está escondendo de você. São Paulo: Editora Zahar, 2012.

PÉREZ, Xiomara Lorena Romero. El alcance del derecho a la intimidad em la sociedade atual. *Revista Derecho del Estado,* Bogotá, v. 1, n. 21, p. 209-222, dez. 2008. Disponível em: https://revistas.uexternado.edu.co/index.php/derest/article/view/499. Acesso em: 28 jun. 2020.

POLONSKI, Vyacheslav. *Artificial Intelligence Has the Power to Destroy or Save Democracy.* Nova York: Council on Foreign Relations, 2017. Disponível em: https://on.cfr.org/2RpE1kT. Acesso em: 20 out. 2018.

SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada:* uma visão jurídica da sexualidade da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SILVA, Rafael Rodrigues da. Facebook permite busca por número de telefone de usuários na rede social. *Canaltech.* [*S. l*], 2009. Disponível em: https://canaltech.com.br/redes-sociais/facebook-permite-busca-por-numero-de-telefone-de-usuarios-na-rede-social-134075/. Acesso em: 13 jul. 2020.

SOLOVE, Daniel J. *Nothing to Hide:* The False Tradeoff Between Privacy and Security. New Heaven: Yale University Press, 2013.

STF. *Medida Cautelar na ação direta de inconstitucionalidade 6.387Distrito Federal*. Rel. Ministra Rosa Weber, 24 de maio de 2020a. Disponível em : http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf . Acesso em: 18 out. 2020.

STF. *Pleno*: dados de usuários de telefonia. [*S. l.: s. n*.], 2020b. 1 vídeo (172 min). Publicado pelo canal STF. Disponível em: https://www.youtube.com/watch?v=84M0nOQhQXo. Acesso em: 8 out 2020.

SUPREMO TRIBUNAL FEDERAL. Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE. *STF*, Brasília, 2020c. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442823. Acesso em: 18 out. 2020.

VASCONCELOS, Pedro Pais de. *Direitos de Personalidade.* Coimbra: Almedina, 2019.

Dados do processo editorial

- Recebido em: 19/08/2020

- Controle preliminar e verificação de plágio: 28/08/2020

- Avaliação 1: 28/09/2020

- Avaliação 2: 28/09/2020

- Decisão editorial preliminar: 29/09/2020

- Retorno rodada de correções: 21/10/2020

- Decisão editorial/aprovado: 25/10/2021

Equipe editorial envolvida

- Editor-chefe: 1 (SHZF)

- Editor-assistente: 1 (ASR)

- Revisores: 2