Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 15.12.2020
Aprovado em: 26.12.2020

Revista de Direito, Governança e Novas Tecnologias

AUTODETERMINAÇÃO INFORMATIVA E COVID-19: A PONDERAÇÃO DE MEDIDAS NO USO DE DADOS PESSOAIS

INFORMATIVE SELF-DETERMINATION AND COVID-19: THE PONDERING OF MEASURES IN THE USE OF PERSONAL DATA

Rhaissa Souza Proto[1]
Arthur Pinheiro Basan[2]
Laiza Silva Aleixo[3]

Resumo: A utilização de dados ganha cada vez mais importância na busca de respostas para enfrentar a pandemia causada pelo COVID-19, diante a urgência do atual cenário e da necessidade de utilização de medidas ágeis. As mazelas já demonstravam as consequências jurídicas variadas e que fizeram despertar a premência da vigência da LGPD, com o objetivo de contenção da insegurança jurídica. Porém, mesmo diante da possibilidade de utilização dos dados anonimizados dos usuários, sem seu prévio consentimento, as inseguranças permeiam, o que motiva a necessidade de levantar as variáveis advindas dessa exceção e buscar as melhores estratégias.

Palavras-chave: COVID-19. LGPD. Segurança. Dados. Anonimizados.

Abstract: The use of data is increasingly important in the search for answers to face the pandemic caused by COVID-19, given the urgency of the current scenario and the need for agile measures. The ailments had already demonstrated the varying legal consequences that have given rise to the urgency for the LGPD to remain valid,

[1] Mestranda profissional em Direito da Empresa e dos Negócios pela UNISINOS. Especialista em direito do Trabalho pela EDH. Graduada em Direito pela UniRV. Atualmente é advogada. Contato eletrônico: rhaissaproto@hotmail.com
[2] Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Mestre em Direito pela Universidade Federal de Uberlândia – UFU. Professor adjunto na UniRV. Contato eletrônico: arthurbasan@hotmail.com
[3] Mestranda profissional em Direito da Empresa e dos Negócios pela UNISINOS. Especialista em Direito Empresarial pela UniRV. Graduada em Direito pela UniRV. É servidora pública e advogada. Contato eletrônico: laizaaleixo@hotmail.com

with the goal of barring legal uncertainty. However, even in the face of the possibility of using users' anonymized data, without their prior consent, insecurities permeate, which motivates the need to raise the variables resulting from this exception and seek for the best strategies.

Keywords: COVID-19. LGPD. Safety. Data. Anonymous.

1 INTRODUÇÃO

Com a declaração de emergência em saúde pública de importância internacional pela Organização Mundial de Saúde (OMS) em decorrência da infecção humana pelo coronavírus (Sars-Cov-2), popularmente designado como novo coronavírus, passou-se a viver um marco na história do ano de 2020, trazendo reflexos transversais para a ciência do direito. Momento desafiador em que se poderia utilizar qualquer argumento para exceção de aplicação de direitos mas que instigou-se debates acerca da efetividade de deveres fundamentais, bem como a possibilidade de extrapolação de seus limites.

Dentre vários setores que se englobam pela transformação digital, o da área de saúde está se tornando cada vez mais dependente de dados para se alcançar resultados mais eficazes, principalmente na atualidade para contenção do COVID-19. Esse mecanismo tem sido amplamente utilizado por diversos países, sendo uma grande aliada na exploração de questões científicas, beneficiando em informações a partir de características da população de uma posição geral, tendo em vista a necessidade premente de resposta ágil às adversidades provocadas pela pandemia. Em virtude disso, iniciativas apoiadas em tecnologias digitais vêm sendo desenvolvidas tanto por empresas privadas quanto pelos governos para que as lacunas do conhecimento sobre a pandemia sejam respondidas rapidamente, maximizando atitudes eficientes.

De forma concomitante com a busca por soluções eficazes para controlar o Sars-Cov2, a Lei Geral de Proteção e Dados Pessoais brasileira (Lei nº 13.709, de 14 de agosto de 2018, ou simplesmente LGPD) que entrou em vigor no dia 18 de setembro de 2020 (BRASIL, 2018), nesse período pandêmico, se tornou um assunto de grande relevância social e de interesse de toda sociedade, haja vista que com o aumento da utilização da internet os dados

pessoais passaram a ficar expostos. Desde seu advento, mesmo antes da sanção do governo, emergiu questionamentos acerca da quantidade e tipos de dados pessoais coletados, bem como a sua destinação posterior, já que seu uso deve seguir uma série de restrições legais.

A LGPD dispõe que em casos para fins exclusivos de segurança pública, a lei não será aplicável para o tratamento de dados pessoais em cujos cenários deverão utilizar medidas proporcionais e especificamente necessárias ao atendimento do interesse público, implementando salvaguardas para proteção dos dados do usuário.

Pois bem, frente à relevância do tema para a sociedade, parte-se das seguintes problemáticas: o interesse coletivo pode sempre justificar e sobrepor toda e qualquer limitação ao direito da autodeterminação informativa (que será posteriormente explicada) ou há limites ao tratamento e divulgação desses dados em situações como a vivenciada atualmente? O indivíduo pode sofrer danos colaterais futuros decorrentes do tratamento de dados pessoais utilizados na tentativa de combate o COVID-19? Esses dados foram mesmo necessários para utilização de uma medida efetiva?

No afã de que o presente estudo alcance sua finalidade, será apresentada a estrutura jurídica básica acerca da LGPD e a efetivação do direito de proteção de dados como direito fundamental, bem como contextualizar a utilização dessas informações no combate à pandemia causada pelo coronavírus. Nessa senda, serão expostos assuntos sobre o imbróglio do tema levado a efeito neste trabalho.

Almeja-se com o presente estudo demonstrar que com a utilização de algoritmos através dos dados pessoais no combate à pandemia, mesmo se tratando da exceção legal ao cumprimento da regulamentação de proteção de dados, se o emprego destes se der de forma demasiada será contraproducente em face ao usuário. Isso porque, o uso dessas informações ultrapassa os limites geográficos, especialmente por se tratar de um setor ligado por uma grande cadeia de segmentos que se interligam e que lidam com a segurança física e emocional dos cidadãos.

2 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

Com o surgimento de uma nova fronteira da hipercomunicação, que nas palavras de Manuel Castells (2001), trata-se de uma nova 'galáxia da Internet', com a internet das coisas (*Internet of Things*, ou IoT) propiciada pelo 5G, o *blockchain*, os contratos inteligentes e os indivíduos estarão cada vez mais ameaçados de invasão da privacidade, de suas autodeterminações informativas.

Os direitos da personalidade no ordenamento pátrio são regulados pelo Código Civil (em seus artigos 11 a 21) e são decorrentes dos direitos fundamentais da pessoa humana, (art. 1º, III, da Constituição Federal) que dentre eles destaca-se os direitos à intimidade e vida privada (expressos no art. 5º, X). Os aludidos dispositivos estabelecem, ainda, o dever de reparação de quaisquer danos causados a estes direitos. Nesse diapasão (anterior à vigência da LGPD), os direitos da personalidade que eram resguardados apenas por esses preceitos, assim definia os direitos anteriormente evidenciados como conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter o controle exclusivo (RODOTÁ, 2008).

Há a necessidade de um reposicionamento da ordem, diante desse surgimento de um novo direito fundamental, encaixando aqui a grande dificuldade da LGPD, já que se trata de uma lei muito extensa diante do seu impacto e inúmeros aspectos a serem atendidos. Essa divisão revela, por se tratar então de uma segmentação técnica, a necessidade de se adaptar, em um primeiro momento, toda a estrutura organizacional, processual e sistemática (principalmente dos sistemas de informação e da sua comunicação entre as repercussões que podem ser geradas). Nessa linha, defende Bruno Bioni (2019) que o enquadramento da proteção de dados como categoria autônoma dos direitos da personalidade é relacionada à uma visão de liberdade positiva, ao contrário do direito à privacidade, que é relacionado como liberdade negativa.

A transversalidade da LGPD abrange toda a sociedade, não ficando apenas destinada a um grupo, como quando aconteceu com a revolução do código de defesa do consumidor que aplicava-se meramente nas relações de consumo, o que motiva a exigência de uma readequação, a fim de atender a necessidade de quando dentro de um sistema de informação o usuário precisa descobrir, de forma clara, o que pode ser e o que não pode ser feito.

Nesse sentido, importante frisar que a recente decisão do Supremo Tribunal Federal (STF) em foram referendadas medidas cautelares deferidas pela ministra Rosa Weber em cinco Ações Diretas de Inconstitucionalidade (ADIs) ajuizadas contra a Medida Provisória (MP) 954/2020 que trata sobre compartilhamento de dados pessoais entre operadoras de telefonia e o IBGE, para firmar o entendimento de que o compartilhamento previsto na referida MP viola o direito constitucional à intimidade, à vida privada e ao sigilo de dados. Os ministros do STF enalteceram a higidez do IBGE e seu caráter de instituição pública de pesquisa, porém não esconderam sua desconfiança em relação aos objetivos da coleta do nome, endereço e número de telefone de milhões de brasileiros (artigo 2º da MP 954/20) (BRASIL, 2020).

A LGPD positivou e deu caráter geral à essa proteção, e agora, o STF por ocasião da suspensão dos efeitos da MP 954/2020 que mandava que as telefônicas fixas e móveis mandassem todos os dados de sua base de informação para o IBGE sem cuidados de segurança, sem cuidados de identificação dos dados relevantes, pela primeira vez, demonstrou a visão do Judiciário quanto a necessidade de aplicação dos princípios de transparência (quanto à finalidade da coleta dos dados), minimização, bem como assegurem o seu tratamento de modo necessário e adequado ao fim declarado, reconhecendo, assim, a existência de um direito fundamental: a proteção de dados pessoais. O tema é de tamanha relevância que há em tramitação no Congresso Nacional a Proposta de Emenda à Constituição 17/2019 cujo objetivo é a inclusão da proteção de dados pessoais entre os direitos e garantias fundamentais do cidadão, inserindo o inciso XII-A ao rol do artigo 5º da Constituição (BRASIL, 2019).

Essa decisão acolheu uma angústia generalizada em relação a iniciativas de monitoramento no período da quarentena e a ameaça de um Estado vigilante, já que não havia até o momento a entrada em vigor da LGPD, não existindo a figura de um fiscalizador. A decisão reconheceu que a Constituição Federal sedia elementos basilares da proteção de dados (direito à intimidade, honra, imagem, dignidade e vida privada) e pronunciou explicitamente o princípio de autodeterminação informacional.

Esse conceito de autodeterminação informativa nasceu na República Federal da Alemanha, reconhecido pela primeira vez como direito fundamental numa decisão histórica

em 1983 de um caso paradigmático da autodeterminação informativa emitida pelo Tribunal Constitucional Federal Alemão (TCFA) sobre a Lei do Censo (MARTÍNEZ, 2007). A partir daí houve vários refinamentos nesse direito fundamental e no Brasil sempre se colocou a questão se teria ou não um direito fundamental a proteção de dados.

Autodeterminação informativa significa dizer que a cada um dos titulares de dados, aos cidadãos, é dado o direito de determinar o que sobre si deve e quer ser divulgado à terceiros (CUEVA, 2011). Seria então dizer que o primeiro pilar dessa geração de proteção de dados é o consentimento, distinguindo do direito à privacidade que é de caráter mais privatista voltado à exclusão de terceiro sobre uma informação, a confiabilidade, a proteção de sigilo.

Já esse direito da autodeterminação informativa possui um caráter mais público, no sentindo de permitir que o indivíduo possa transitar com o mínimo de opacidade, ou seja, usufruir do seu direito à livre formação de personalidade, a fim de que ele não seja permanentemente discriminado, invadido, ter a sua dignidade humana ameaçada. Quando do uso de dados pessoais é um aspecto substancial a ser levado em apreço, sincronicamente com as garantias de segurança, minimização e transparência no uso de dados.

Entretanto, utilizando de preceitos da LGPD, existem situações em que o uso de dados pessoais é permitido mesmo sem o consentimento do seu titular, que ocorre em casos de emergência e de interesse público, como a saúde pública, nas hipóteses em que for indispensável para a realização de estudos por órgão de pesquisa para a proteção da vida, desde que haja salvaguardas, proporcionalidade no destes para alcance das finalidades e especificidades dos órgãos autorizados a processar esses dados, conforme estabelecido na Lei Geral de Proteção de Dados brasileira.

3. O USO DE DADOS PESSOAIS PARA O COMBATE À PANDEMIA ATRAVÉS DA UTILIZAÇÃO DE ALGORITMOS

Para auxílio ao combate do coronavírus, na busca de providências para volta à normalidade e para proteção dos cidadãos, surgiram iniciativas de desenvolvimento de medidas no segmento tecnológico que tornaram possível a rastreabilidade de deslocamentos importantes de indivíduos para o monitoramento e vigilância pelos governos, dos contatos

interligados à essa pessoa e até a viabilidade de identificar sintomas. Com a dificuldade de realizar diagnóstico em toda a população as apostas estão se dando no desenvolvimento de aplicativo, de softwares, que podem coletar a geolocalização, dados pessoais, rastreamento a fim de controlar a propagação através do controle da circulação de pessoas.

Esses dados integram-se os tão chamados *big datas*, que no entendimento de Gonzáles (2016, p. 17) por referir-se a "[...] grandes quantidades e informação digital controlada por companhias, autoridades e outras organizações, sujeitas a uma análise extensa baseada em algoritmos". Se utilizados por si só não conseguem causar danos, com exceção de utilizados por terceiros se, os consentimentos das personalidades a eles interligados. Faleiros Júnior (2020, p. 289) traz a conceituação de *big data* como sendo:

> "[...] nada mais é que um enorme banco de dados no qual se armazena todo tipo de informação para que, posteriormente, se trabalhe com esses bancos de dados, cruzando as informações coletadas através de algoritmos, oferecendo possibilidades variadas de previsão de eventos futuros e, ainda, condições de se identificar correlação de dados a partir de causalidades complexas, oferece possibilidades de análises estatísticas infindáveis, normalmente se valendo de amostragens. Quanto maior o banco de dados, maior é a sua confiabilidade e, consequentemente, mais precisa será a aferição obtida pelo algoritmo utilizado na testagem proposta."

Alguns desenvolvedores de software estão contribuindo com essa ação, que é o caso por exemplo do Google e Apple que, em apoio a essa causa, através de um trabalho em cooperação, utilizando a tecnologia Bluetooth, visaram uma solução que inclui interfaces de programação de aplicações (APIs) e tecnologia de sistema operacional para auxiliar nesse rastreamento de pessoas na tentativa de coadjuvar as autoridades governamentais a frear o avanço do vírus (NEWSROOM, 2020).

A União também de mobilizou, através do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), se unindo às operadoras Vivo, Claro, Oi, TIM e Algar Telecom, para que, a partir das informações de suas torres de transmissão monitorasse os dados de 220 milhões de aparelhos móveis, sendo possível através deles identificar a movimentação dos indivíduos, porém afirmando que se tratam de dados acima dos pessoais, se caracterizando, portanto, conforme definição pelo art. 5º, III da LGPD, como anonimizados (MAGENTA, 2020).

Em São Paulo foi implementado o Sistema de Informações e Monitoramento Inteligente (SIMPA-SP) que se trata de um ambiente computacional para vigilância de dados e controle de aglomerações pelo Governo do Estado de São Paulo através do uso de implementos algorítmicos. Quando iniciado a sua execução começou a apontar questionamentos pelos cidadãos paulistas acerca do fato de que o referido sistema não apresenta confiabilidade de técnicas aplicadas sobre os dados coletados, nem qualquer confirmação sobre a efetiva anonimização, acarretando insegurança pelos indivíduos.

Isadora Maria Roseiro Ruiz e Cristina Godoy Bernardo de Oliveira (2020) apontaram quatro grandes problemas dessa iniciativa pelo sistema SIMI-SP, se destacando: a) violação ao artigo 7º da LGPD por haver a ausência de concordância do usuário, através de expressar o seu consentimento sobre a disponibilidade das informações acerca da sua localização; b) observância do artigo 22 da LGPD em que os titulares de dados devem ter assegurados seus interesses para defesa em juízo, porém na prática, quando vários destes pleitearam a remoção de seus telefones celulares do monitoramento feito pelas operadoras e repassadas ao Instituto de Pesquisas Tecnológicas – IPT, tiveram suas solicitações denegados sob o argumento de que não há tratamento de dados pessoais; c) desrespeito à inversão do ônus da prova prevista no artigo 42, §2º, da LGPD quando nessas ações movidas anteriormente citadas foram entendido que ao autor da ação deve provar que os dados não foram anonimizados; d) as datas de disponibilização dos dados ao IPT pelas operadoras de telefonia antecederam a celebração prévia do ato normativo de criação do próprio sistema, sendo os dados dos usuários indevidamente utilizados.

De fato, a LGPD traz hipóteses legítimas de tratamento, independente de consentimento, para formulação e execução de políticas públicas, porém essa escusa da obtenção do consentimento não exclui a observação aos demais princípios da LGPD, bem como se trata de utilização exagerada. Posto isso, mesmo em meio a uma pandemia como a COVID-19, quando da utilização de dados pessoais no enfrentamento ao combate à transmissão do coronavírus sem o consentimento do usuário, deve haver uma avaliação de atendimento às exigências da LGPD, bem como ser realizado um juízo de ponderação.

O governo, bem como a iniciativa privada, tem tomado um conjunto de medidas para garantir um combate mais eficaz diante das incertezas provocadas pelo coronavírus, porém,

em contrapartida, o direito fundamental à proteção de dados não pode ser prejudicado mediante compartilhamento sem fundamentação ou quando exagerado na necessidade de informações para se alcançar a eficiência pretendida. Nesse contexto, a LGPD assume um papel norteador, mas que deve ser fiscalizada frente aos desafios impostos no momento de crise estampado.

4. A PROTEÇÃO DE DADOS E O COMBATE À PANDEMIA: UM JUÍZO DE PONDERAÇÃO NECESSÁRIO

A pandemia apresenta uma série de desafios, não se podendo ainda dizer em pós-pandemia, mas sem dúvidas nenhuma os dados pessoais podem ser um excelente instrumento para se pensar em inúmeras formas de contenção da disseminação dessa doença. Por se tratar de um momento delicado e que, em alguns casos, os indivíduos empolgados com as necessidades e urgências que o caso demanda podem abrir mão de um dado, prestar algum tipo de consentimento, porém, apesar de se tratar de motivos muito nobres estes apresentam riscos, ainda mais sem uma proteção adequada. Nesse sentido, expressam Marcos Ehrhardt Júnior e Gabriela Buarque Pereira Silva (2020, p. 305) "O cenário caótico criado pela propagação do vírus tem acarretado cada vez mais a adoção de escolhas trágicas, que sacrificam interesses relativos à privacidade em prol da salvaguarda da saúde pública".

Importante mencionar, como bem explicado por van Dijk (2006), que a informação constitui a essência da sociedade contemporânea, que adquire formato a partir das estruturas organizacionais, podendo difundir efeitos e gerar danos na esfera jurídica. Para melhor contextualização, reporta-se à confidencialidade, que conforme definição do dicionário da Academia de Letras (2008), o confidencial é aquilo revelado em segredo por dizer respeito a assunto íntimo de alguém. No imbróglio aqui tratado, é o dever de sigilo sobre todas as informações obtidas no exercício da tutela da confiança do paciente, que implica no dever de segredo a qual é intrínseca. Nessa realidade, os efeitos da confidencialidade são impostos tanto em relação aos médicos – efeito relativo ou interno da confidencialidade –, como também contra terceiros (SCHAEFER, 2010).

É cada vez mais importante pensar sobre essa confidencialidade e o uso de algoritmos para combate ao coronavírus. Isso porque embora muitos desses mecanismos e tecnologias estejam sendo desenvolvidas sempre com base no consentimento do usuário, questiona-se o fato de em que medida essa permissão é informada e se atende a todos os requisitos previstos pela LGPD.

Harari (2018) já citava, em *21 lições para o século 21*, que a questão da governança dos dados é o maior problema da atualidade, do qual depende o futuro da humanidade e das democracias. Já no cenário da pandemia traz que as questões a serem enfrentas será além de optar pelo que se chama de um 'nacionalismo isolacionista' ou uma 'cooperação global', também se esses dados serão utilizados numa perspectiva de empoderamento dos cidadãos, ou numa perspectiva um totalitarismo estatal, ou seja, diversas iniciativas ou de estados ou do mercado ou combinando iniciativas estatais e de mercado que possam utilizar os nossos dados sem as devidas seguranças (HARARI, 2020). E essa reflexão traz uma perplexidade que grande maioria dos indivíduos detém, no sentido de que qual o tamanho dessa autoridade, questionamento acerca da ideia de transparência saber quem utiliza, para qual finalidade, a necessidade, quando e porque empregou aquele dado. Essas exigências precisam ser atendidas mormente pelos agentes que estão realizando os tratamentos disposto a atender a preocupação com os dados para se evitar vazamento.

O crescimento do volume e da diversificação dos dados que podem ser combinados teve uma evolução rápida especialmente pelo uso intensivo da Internet, ilimitado no tempo e no espaço, elevando o risco de re-identificação mesmo após a anonimização ou desidentificação de bases isoladas (MOONEY e PEJAVER, 2018). Destaca-se ainda o fato de que os mercados que são ricos em dados são cercados por segredos quanto a aplicação de seus algoritmos, os quais são utilizados para propiciar uma vantagem concorrencial e os danos decorrentes dessa obscuridade são variados (FALEIROS JÚNIOR, 2020). Frank Pasquale (2015) define esse quesito como caixas-pretas (*black boxes*).

Dentre os riscos propensos a ocorrer, pode-se citar os seguintes: 1. Quais são as garantias dadas de que os dados dos usuários serão utilizados para as finalidades específicas que justificaram a sua coleta?; 2. Qual é a garantia que se tem de que se trata de um meio que

será adequado, seguro, de que haverá transparência, *accountability*[4], devidos controles, o que será feito com esses dados após a pandemia, após a extinção da finalidade que justificou o tratamento desses dados, se em caso de ocorrência de vazamento de dados quem será penalizado? Há uma série de questões que precisam ser respondidas, principalmente em um cenário em que se vivencia uma série de iniciativas governamentais e também do meio privado, no sentido de desenvolvimento de tecnologias que se utilizam desses dados, como o caso da Apple e Google anteriormente citada.

Outro aspecto envolto de discussões refere-se ainda a questão relativa aos direitos de propriedade intelectual, pois a disposição de informações em um banco de dados configura-se em direito autoral (GUANES, 2018). Mesmo quando os temas são tratados pela legislação, que é o caso do uso dos dados pessoais que antes da LGPD o assunto possuía um vácuo jurídico, o são insuficientemente, como ocorre, por exemplo, na proteção dos bancos de dados por direitos autorais, com destaque quanto aos "extratos de base de dados que se tornam adaptações, as quais, por sua vez, precisam de autorização para reuso e decisão sobre sua titularidade". (GUANAES, 2018, p. 9).

A título de exemplo, para lançar outro questionamento, importante mencionar o fato ocorrido em Amazonas que, naquela oportunidade, o governo estadual decretou regime de quarentena para os passageiros que desembarcaram no Aeroporto Internacional Eduardo Gomes. Não somente isso, o governo do Estado do Amazonas desenvolveu um aplicativo para smartphones que todos esses mencionados passageiros tiveram que instalar para que sua localização fosse monitorada, em tempo real, nos 14 (quatorze) dias submetidas à quarentena (AMAZONAS, 2020). Esse fato gera a seguinte indagação: Além do fato que o Estado pode coletar e tratar dados pessoais sem o consentimento do indivíduo, no atual cenário poderia também obrigar o indivíduo a fornecer tais dados, independentemente do meio empregado?

Outro importante ponto a se destacar é que o causador do dano ainda pode sofrer multas administrativas e/ou sanções penais, previstas no próprio ordenamento jurídico.

[4] Na definição de Faleiros Júnior (2020, p. 131), *accountability é o* "Processo pelo qual as entidades e os gestores públicos são responsabilizados pelas próprias decisões e ações, contemplando o trato com recursos públicos e todos os aspectos de desempenho".

Havendo também a incerteza quanto as ocorrências de imposição de danos e multas no meio jurídico, o qual, como se sabe, ainda carece de insegurança[5].

Destaca-se ainda, nesse contexto, se a coleta e a divulgação de tantos dados pessoais são a medida realmente necessária para o combate à pandemia, ou se posteriormente, pode gerar algum proveito econômico diante dessa situação. Na decisão do Supremo Tribunal Federal anteriormente mencionada, percebe-se que uma das questões centrais foi exatamente a falta de finalidade da transferência desmesurada de dados das empresas telefônica.

É essencial que para um controle posterior da possibilidade ou não de desvio de finalidade, deve-se dar um tratamento adequado e equilibrado. Pondera Bioni (2020) que não seria suficiente apenas apontar a forma genérica que o uso de dados será apontado, como por exemplo evitar a propagação da pandemia, mas deve ser claro sobre qual é a medida de combate específico cogitada a partir dos tratamentos dos dados pessoais coletados.

Esses nortes já estão previstos de uma maneira muito clara como princípios na lei geral, ou seja, especificamente precisa-se ter uma finalidade que não tenha somente a geral por ser legítima, necessita ser específica, de ter adequação do meio, ter proporcionalidade, transparências, segurança, *accountability*, precisa ter regras que assegurem a não utilização indevida desses dados (como fins discriminatórios, etc.), quais as medidas de segurança e as políticas de segurança e informação utilizada, bem como, essencialmente em saber qual o prazo de conservação e o que será feito após o fim do tratamento, já que seu armazenamento não se dará infinitamente.

Há várias pesquisas que demonstram a existência de tecnologias que possibilitam a utilização em respeito aos direitos dos titulares dos dados, a questão é como vamos fazer com que essas tecnologias possam ser utilizadas adequadamente, já que a celeuma gira em torno da

[5] A título apenas de menção, como curiosidade, na primeira Ação Civil Pública ajuizada para aplicação da LGPD, movida pelo Ministério Público do Distrito Federal protocolada sob o nº 0730600-90.2020.8.07.0001 na segunda-feira (21), foi movida contra dois empresários de Minas Gerais em que foi identificado a comercialização maciça de dados pessoais de milhares de brasileiros. A sentença proferida no mesmo dia, indeferiu a petição inicial pelo fato de que ao consultar o sítio eletrônico do caso em questão o mesmo se encontra em manutenção. Aqui cumpre fazer o seguinte comentário quanto a insegurança jurídica que ainda nos cerca. Mesmo acionando o judiciário para aplicação da LGPD já em vigor, o juiz *a quo*, *data máxima vênia*, indeferiu o pedido por entender, de oficio, que estar em manutenção já significava estar se adaptando à nova legislação, quando na realidade poderia se ter inúmeros outros motivos. Essa decisão ainda leva a crer a necessidade de ata notarial para se ingressar com ações para cumprimento da referida Lei, que também poderá ser objeto de discussão quanto à sua segurança de informações.

imprudência e da falta de controles e filtros de quem deles se utiliza, que pode gerar danos irreparáveis. Além das questões que podem ser respondidas em como minimizar os dados, como verificar os padrões de segurança, destaca-se o fato de que a utilidade dos dados não é autoevidente, é muito menos que isso. Mesmo que se levante o argumento referente ao fato de que dados anonimizados não são considerados dados pessoais pelas leis de proteção de dados, tendo em vista que são caracterizados por proteger a identificação dos indivíduos, há ainda a possibilidade de prejudicar grupo de pessoas de forma geral em virtude de informações sobre etnicidade, locais, situações de saúde e condições socioeconômicas. O Webinar nomeado *Beyound the exit strategy: ethical uses of data-driven technology in the fight against COVID-19* enfatiza que não há proteção contra o uso de tecnologias irresponsáveis, já que as leis de proteção de dados não abrangem as liberdades e os direitos do grupo, mas voltam-se exclusivamente à proteção de dados pessoais (NUFFIELD COUNCIL ON BIOETHICS e ADA LOVELACE INSTITUTE, 2020).

Importante ainda ponderar que na realidade brasileira a tecnologia ainda é muito falha e propícia a ocorrência de vícios e fraudes perante o cidadão. Destacando-se o fato de que golpes estão sendo aplicados, em que os indivíduos se utilizam do período pandêmico solicitando informações de pesquisa sobre a pandemia do COVID-19 ou envolvendo galezias sobre o auxílio cidadão, em que culminou em cerca de 2 milhões de pessoas já atingidas por essa ação maliciosa (FRANCO, 2020). Destaca Ehrhardt Júnior e Modesto (2020, p. 147) que "[...] a divulgação de dados pessoais no intento de auxiliar o combate ao coronavírus é capaz de gerar danos outros às pessoas,cuja gravidade individual, efeitos e duração no tempo podem ser muito mais lesivos que os causados pela própria COVID-19."

Nesse sentido, demonstra-se a importância de uma empresa que lida com dados pessoais aplicar um programa de *compliance*.[6] A LGPD é trabalhada em todo um estímulo de autorregulação, o que se reflete na verdade numa co-regulação, auxiliada pela tecnologia.

[6] No Brasil, o compliance chega com maior efetividade por meio da Lei nº 12.846/2013, conhecida como Lei Anticorrupção ou Lei da Empresa Limpa. Ela foi a responsável por instituir, no Brasil, a responsabilização objetiva (tanto a administrativa, quanto a civil) das pessoas jurídicas pela prática de atos lesivos que sejam cometidos contra a Administração Pública nacional ou estrangeira. Com a Lei aprovada, surgiu um grande interesse e atenção sobre o tema do combate à corrupção, com ênfase nas sanções severas por responsabilização. Além deste caráter punitivo, a Lei supracitada também atribuiu relevância às medidas anticorrupção adotadas por empresas, as quais constituem o chamado Programa de Integridade (CGU, 2015).

Importante entender que a tecnologia pode ser um importantíssimo vetor ou mecanismo regulatório que no caso da proteção de dados tem um grande potencial para ser utilizado e que quanto mais se atentar para as probabilidades de risco, menor a chances de vazamento de dados. O que se observa é a necessidade de verdadeiro diálogo de fontes, isso porque nesse novo paradigma tecnológico, o conceito do direito ou de fontes jurídicas precisam ressignificar-se frente aos novos direitos advindos com a sociedade digital.

Fatores relacionados ao direito à privacidade, direito à autodeterminação informativa não inviabilizam a possibilidade do uso de dados pessoais para responder ao combate da pandemia, porém, diante de todo o contexto exposto, há possíveis lados nefastos da hiperconectividade e os seus impactos obterão maior ênfase no cenário pandêmico e pós-pandêmico. Trata-se de um caso de urgência discussão, em que há uma importante necessidade de se aprofundar o debate, já que seus efeitos de grande impacto tem um importante papel na sociedade. O que repisa ainda mais o teor aqui discutido diante da necessidade de transparência quanto a segurança jurídica na utilização dos dados, com ênfase na peculiaridade do período pandêmico.

Por mais que se tenha as melhoras normas implementadas à segurança das informações estas nunca serão suficientes, estando propício à ocorrência de vazamento de dados, já que faz parte do próprio sistema em si, mas que, em caso de sua ocorrência pode afetar negativamente (não podendo falar em mensuração) um indivíduo em um caso avulso, uma organização, uma instituição, ou até mesmo toda uma sociedade. Porém, um questionamento trago à baila é a extensão desse novo direito, já que por ser nupérrimo no ordenamento jurídico brasileiro, necessitará de muitas interpretações para que se possa cingir entre o que realmente está ligado à sua esfera privada de proteção.

3 CONCLUSÃO

Ainda não é possível falar em pós-pandemia, mas não há dúvidas de que o ano de 2020 marcará a história da humanidade em razão das mazelas provocadas pelo Covid-19, desencadeando consequências jurídicas e que fizeram desencadear a premência da vigência da

Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), na tentativa da contenção da insegurança jurídica.

Essa insegurança se originou através da busca de soluções ágeis e eficientes para o combate à pandemia, em que o governo e as empresas privadas passaram a utilizar dados pessoais, sem o consentimento dos usuários para obter informações úteis nas medidas tomadas. Ocorre que, apesar da previsão legal de exceção a essa necessidade de consentimento do cidadão, continua a pairar dúvidas no respeito aos outros aspectos legais.

O desafio nesse momento é detectar quais seriam as melhores estratégias para se ter resultados mais eficazes visando o bem da coletividade, vislumbrando a viabilidade tecnológica e a legalidade da aplicação. Para isso, é preciso pensar cada vez mais na prevenção e na construção de projetos e sistemas que enfatizam a prevenção, uma vez que, após a ocorrência de incidentes pelo uso de dados ocorrer de forma equivocada ou indesejada, os eventuais danos financeiros, as penalidades e os danos reputacionais podem gerar incalculáveis impactos para a Empresa/Administração Pública ou indivíduo.

Em síntese, não é difícil antever que as violações originárias desse fato podem causar danos que perdurarão por muito mais tempo que a pandemia. Inicialmente deveria haver um estágio de implementação da infraestrutura tecnológica para posteriormente se estabelecer as estratégias, porém, diante do contexto atual, lançou-se aqui a necessidade de ponderar que a utilização de dados pessoais deve ser feito de maneira proporcional ao almejado, não se admitindo que a coleta se dê de forma excessiva e exposta.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE LETRAS. **Dicionário escolar da língua portuguesa**. São Paulo: Cia. Editora Nacional, 2008.

AMAZONAS. Governo do Estado**. Wilson Lima anuncia monitoramento remoto de pessoas que chegam pelo aeroporto e aquisição de testes rápidos.** 2020. Disponível em: <http://www.amazonas.am.gov.br/2020/03/wilson-lima-anunciamonitoramento-remoto-de-pessoas-que-chegam-pelo-aeroporto-e-aquisicao-de-testes-rapidos/>. Acesso em: 22 set. 2020.

BRASIL. **Lei nº. 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/Lei/L13709.htm>. Acesso em: 18 set.L 2020.

BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17, de 2019.** 2019. https://www25.senado.leg.br/web/atividade/materias/-/materia/135594Acesso em: 20 set. 2020.

BRASIL. **Supremo Tribunal Federal. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE.** 2020. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902>. Acesso em: 27 set. 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 92-93.

CASTELLS, Manuel. ***The Internet galaxy: reflections on the Internet, business, adn society***. Oxford: Oxford University Press, 2001.

CONTROLADORIA GERAL DA UNIÃO (CGU). **Programa de Integridade - Diretrizes para empresas privadas**. Setembro, 2015. Disponível em: <https://www.legiscompliance.com.br/images/pdf/programa_integridade_diretrizes_para_empresas_privadas_cgu.pdf>. Acesso em: 21 de agosto de 2020.

CUEVA, Pablo. Informática y Protección de Datos Personales. **Revista Chilena de Derecho Informático**. 2011. Disponível em <https://www.researchgate.net/publication/314947621_Informatica_y_Proteccion_de_Datos_Personales>. Acesso em: 20 set. 2020.

EHRHARDT JÚNIOR, Marcos; SILVA, Gabriela Buarque Pereira. Breves notas sobre a privacidade e proteção de dados pessoais durante a pandemia. *In:* MONTEIRO FILHO, Carlos Edison do Rêgo; ROSENVALD, Nelson; DENSA, Roberta (Coords.). **Coronavírus e responsabilidade civil:** impactos contratuais e extracontratuais. Indaiatuba: Foco, 2020.

FALEIROS JÚNIOR, José Luiz de Moura. **Administração pública digital:** proposições para o aperfeiçoamento do Regime Jurídico Administrativo na sociedade da informação. São Paulo: Editora Foco, 2020.

FRANCO, Marcela. **'Auxílio coronavírus' e outros golpes no WhatsApp atingem 2 milhões**. TechTudo, 23 MAR. 2020.Disponível em: <https://www.techtudo.com.br/noticias/2020/03/auxilio-coronavirus-e-outros-golpes-no-whatsapp-atingem-2-milhoes.ghtml>. Acesso em: 6 set. 2020.

GONZÁLEZ, Elena Gil. ***Big data, privacidade y protección de dados***. Madris: Agencia Española de Protección de Datos. 2016. Disponível em: <

https://www.researchgate.net/publication/324831404_Big_data_privacidad_y_proteccion_de_datos>. Acesso em: 27 set. 2020.

GUANAES, Paulo Cezar Vieira; SOUZA Allan Rocha;r DONEDA, Daniello; NASCIMENTO, Francisco José Tavares do. **Marcos legais nacionais em face da abertura de dados para pesquisa em saúde:** dados pessoais, sensíveis ou sigilosos e propriedade intelectual. Rio de Janeiro: Fiocruz; 2018.

HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.

_____ **Against Coronavirus, Humanity Lacks Leadership**. 2020. Disponível em: <https://time.com/5803225/yuval-noah-harari-coronavirus-humanity-leadership/>. Acesso em: 17 set. 2020.

MARTÍNEZ MARTÍNEZ, Ricard. El derecho fundamental a la protección de datos: perspectivas**. Revista Internet, Derecho y Política**, nº 5, 2007. Disponível em <https://www.researchgate.net/publication/28178556_El_derecho_fundamental_a_la_proteccion_de_datos_perspectivas>. Acesso em: 19 set. 2020.

MAGENTA, Matheus. **Coronavírus:** governo brasileiro vai monitorar celulares para conter pandemia. BBC News Brasil, 3 abr. 2020. Disponível em: <https://www.bbc.com/portuguese/brasil-52154128>. Acesso em: 17 set. 2020.

MODESTO, Jéssica Andrade. EHRHARDT JÚNIOR. Marcos. Danos Colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. **Revista Eletrônica de Direito e Sociedade**. Canoas, v. 8, n. 2. 2020. Editora UnilaSalle. Disponível em < https://revistas.unilasalle.edu.br/index.php/redes/article/view/6770>. Acesso em 12 set 2020.

MOONEY, S. J.; PEJAVER V. Big data in public health: terminology, machine learning, and privacy. **Annu Rev. Public Health,** 2018, nª 39, p.95-112.

NEWSROOM. **Apple e Google formam parceria para tecnologia de rastreamento de contato com COVID-19.** 2020. Disponível em: <https://www.apple.com/br/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>. Acesso em 19 de setembro de 2020.

NUFFIELD COUNCIL ON BIOETHICS; ADA LOVELACE INSTITUTE. **Webinar - Beyound the exit strategy:** ethical uses of data-driven technology in the fight against COVID-19. 2020. Disponível em: <https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19>. Acesso em: 20 set. 2020.

PASQUALE, Frank. **The black box society:** Cambridge: Harvard University Press, 2015. Disponível em **<**https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf>. Acesso em 11 set 2020.

RODOTÁ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008. Disponível em <https://openaccess.blucher.com.br/download-pdf/404/21235>. Acesso em 10 set 2020.

RUIZ, Isadora Maria Roseiro; OLIVEIRA, Cristina Godoy Bernardo de. Os 4 problemas do sistema de informações e monitoramento inteligente do governo de SP. **Migalhas de Proteção de Dados**. 2020. Disponível em: <http://s.migalhas.com.br/S/65D4C>. Acesso em: 17 set. 2020.

SCHAEFER, Fernanda. Proteção de dados de saúde na sociedade de informação. **A busca pelo equilíbrio entre privacidade e interesse social**. Curitiba: Juruá, 2010.

VAN DIJK, Jan. **The network society**. 2. ed. Londres: Sage Publications, 2006. Disponível em < http://www.forschungsnetzwerk.at/downloadpub/The_Network_Society-Jan_van_Dijk.pdf>. Acesso em 26 ago 2020.