INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA – IDP
ESCOLA DE DIREITO DE BRASÍLIA – EDB
CURSO DE GRADUAÇÃO EM DIREITO

CAMILA AGUIAR DO MONTE DE MAGALHÃES

DIREITO À PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL: UMA ANÁLISE DO SISTEMA PROTETIVO BRASILEIRO, EM FACE DO TRATAMENTO DE DADOS NO CONTEXTO DO COVID-19

BRASÍLIA
DEZEMBRO, 2020

CAMILA AGUIAR DO MONTE DE MAGALHÃES

DIREITO À PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL: UMA ANÁLISE DO SISTEMA PROTETIVO BRASILEIRO, EM FACE DO TRATAMENTO DE DADOS NO CONTEXTO DO COVID-19

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação como requisito parcial para obtenção do título de Bacharel em Direito pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP

Orientador: Prof. Alexandre Sankievicz

BRASÍLIA
DEZEMBRO 2020

CAMILA AGUIAR DO MONTE DE MAGALHÃES

DIREITO À PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL: UMA ANÁLISE DO SISTEMA PROTETIVO BRASILEIRO, EM FACE DO TRATAMENTO DE DADOS NO CONTEXTO DO COVID-19

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação como requisito parcial para obtenção do título de Bacharel em Direito pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP

Orientador: Prof. Alexandre Sankievicz

_____

Professor Alexandre Sankievicz
Professor Orientador

_____

Professor Guilherme Pereira Pinheiro

_____

Professor Sérgio Antônio Garcia Alves Junior

DIREITO À PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL: UMA ANÁLISE DO SISTEMA PROTETIVO BRASILEIRO, EM FACE DO TRATAMENTO DE DADOS NO CONTEXTO DO COVID-19

RIGHT TO PROTECT PERSONAL DATA IN BRAZIL: AN ANALYSIS OF THE BRAZILIAN PROTECTIVE SYSTEM, IN FACE OF THE DATA TREATMENT IN THE COVID-19 CONTEXT

Camila Aguiar do Monte de Magalhães

SUMÁRIO. Introdução: 1 Direito à privacidade; 1.1 Evolução histórica: Direito à proteção de dados pessoais; 1.2 Evolução da Jurisprudência brasileira a respeito do direito fundamental à proteção de dados pessoais; 2 Como diferentes governos no mundo estão usando dados pessoais no enfrentamento da Covid-19 e quais os problemas surgidos a partir desse tratamento; 3 Quais são os mecanismos específicos que tem o ordenamento jurídico brasileiro para garantir a proteção de dados pessoais sem obstar a atuação das autoridades em uma situação de pandemia.

RESUMO

O presente estudo busca investigar se o sistema normativo brasileiro tem ferramentas para proteger os dados pessoais de seus titulares, no contexto da pandemia do Covid-19, em especial, com relação ao uso mais intenso de dados pessoais no enfrentamento da pandemia. Para tanto, foi utilizada a revisão bibliográfica sobre como o direito à privacidade evoluiu para o surgimento de um direito fundamental autônomo, qual seja, o direito à proteção de dados pessoais. Verificou-se que a Lei Geral de Proteção de Dados tem atributos qualitativos capazes de salvaguardar o direito em questão, não obstante algumas questões expostas neste artigo.

PALAVRAS-CHAVE: LGPD. Privacidade. Proteção de Dados Pessoais. Covid-19.

ABSTRACT:

This study investigates whether the Brazilian law has tools to protect the personal data of its data subjects, in the context of the Covid-19 pandemic, especially, related to more intense use of personal data to deal with the pandemic. For that purpose, a bibliographic review on how the right to privacy evolved to the emergence of an autonomous fundamental right, namely the right to protection of personal data, was used. It was found that the General Data Protection Law has qualitative attributes capable of safeguarding the right in question, despite some issues exposed in this article.

KEYWORDS: LGPD. Privacy. Personal Data Protection. Covid-19.

INTRODUÇÃO

O desenvolvimento tecnológico trouxe como consequência uma sociedade cada vez mais "monitorada". Observamos que algumas nações do mundo se utilizam de monitoramento remoto de cidades e cidadãos para fins de vigilância, segurança pública, controle de tráfego dentre outros.

A despeito dos benefícios pretendidos, o monitoramento remoto, por ser indissociável da necessidade de coleta, tratamento e armazenamento de dados pessoais, traz à baila discussões a respeito da privacidade e da proteção aos dados pessoais de seus usuários.

Na atual conjuntura, em que foi declarado pela Organização Mundial de Saúde estado de emergência em saúde pública de importância internacional decorrente do surto do Covid-19, governos estão se utilizando de aplicativos de monitoramento instalados em *smartphones* para, por exemplo, detectar o nível de isolamento social e evitar que ocorram aglomerações.

No Brasil, por exemplo, foi editada a Medida Provisória nº 954/2020[1], que trata da obrigatoriedade das empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado - STFC e do Serviço Móvel Pessoal - SMP de disponibilizarem à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979/2020.

A MP teve sua eficácia suspensa pelo Supremo Tribunal Federal em 24 de abril deste ano. Segundo a Relatora, min. Rosa Weber, além da ausência de garantias de tratamento adequado e seguro dos dados compartilhados, ainda não estava em vigor a Lei Geral de Proteção de dados (Lei nº 13.709/2018), que define critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais.

O tema é relevante e atual, não somente sob o ponto de vista social, conforme descrito alhures, mas também sob o aspecto jurídico e acadêmico, uma vez que

[1] BRASIL. Medida Provisória n° 954, de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de serviço telefônico comutado e de serviço móvel pessoal com o IBGE. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619>. Acesso em 20 de jun. de 2020.

foi editada a LGPD, cuja finalidade é fornecer instrumentos para a salvaguardar o direito à privacidade e à proteção dos dados pessoais.

Por sua vez, também foi editada a Lei nº 13.979/2020[2], que dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019, e que prevê, em seu art. 6º[3], a obrigatoriedade de compartilhamento de dados essenciais à identificação de pessoas infectadas ou com suspeita de infeção pelo coronavírus.

Cabe destacar ainda a tramitação do Projeto de Emenda à Constituição nº 17 de 2019[4], que busca incluir o direito à proteção de dados pessoais como direito fundamental, acrescentando o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

Verifica-se nas citadas normas que não se busca evitar a circulação dos dados pessoais, mas, sim, criar ferramentas para disciplinar a coleta, o tratamento e o armazenamento dos dados pessoais de forma responsável. Não é de hoje que estamos imersos na era digital e fornecemos, cada vez mais, ora por vontade própria, ora sem sequer termos conhecimento, nossos dados pessoais, os quais são coletados, armazenados e transmitidos para terceiros.

Assim, o objeto do presente estudo é verificar se o arcabouço legal brasileiro detém normas suficientes e adequadas para assegurar o direito à proteção dos dados pessoais dos brasileiros, ante a possibilidade de o governo se utilizar desses dados de maneira mais intensa e ampla durante a evolução da Covid-19 no Brasil. Isto é, em que medida o sistema normativo brasileiro tem ferramentas de proteção ao direito à privacidade e à proteção dos dados pessoais da sociedade, para lidar com os problemas advindos da atual pandemia, em especial, a coleta, o armazenamento e o tratamento de dados pessoais obtidos para fins de monitoramento remoto no combate ao Covid-19?

---

[2] BRASIL. Lei nº 13.979, de 6 de fevereiro de 2020. Institui a Lei do Corona vírus. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13979.htm>. Acesso em 6 de junho de 2020.

[3] "Art. 6º É obrigatório o compartilhamento entre órgãos e entidades da administração pública federal, estadual, distrital e municipal de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo coronavírus, com a finalidade exclusiva de evitar a sua propagação."

[4] BRASIL. **Proposta de Emenda à Constituição n° 17, de 2019**. Dispõe sobre a inclusão do direito à proteção de dados pessoais entre os direitos fundamentais do cidadão e sobra a fixação da competência privativa da União sobre a matéria. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em 6 junho de 2020.

A hipótese desse trabalho é de que a Lei Geral de Proteção de Dados surgiu para preencher as lacunas normativas relacionadas ao direito à privacidade e à proteção dos dados pessoais. A premissa inicial, portanto, é no sentido de que o arcabouço normativo é adequado, tendo em vista que a LGPD fornece os parâmetros materiais e processuais adequados para resguardar o direito fundamental à proteção de dados pessoais.

Na prática, observamos que a LGPD já vinha sendo adotada como parâmetro tanto em decisões judiciais como em normas infralegais. A exemplo, o Decreto que criou o cadastro-base do cidadão e algumas decisões do Supremo, já mencionavam os princípios e os conceitos presentes nos artigos iniciais da LGPD. Nesse contexto, observamos que o fenômeno social se antecipou ao início da vigência da lei de proteção de dados, surgindo mais um fenômeno a indicar a aproximação do direito brasileiro da *Common Law*[5].

Todavia, cabe salientar que, mesmo a Autoridade Nacional de Proteção de Dados[6] já tendo sido implementada, a aplicação das sanções previstas na Lei ainda não está em vigor.

1 DIREITO À PRIVACIDADE

1.1 Evolução histórica: Direito à proteção de dados pessoais

O marco inicial no estudo do direito à privacidade na contemporaneidade foi a publicação, na revista *Harvard Law Review*, do artigo *The Right to Privacy*, pelos autores Samuel Warren e Louis Brandeis, em 1890.

[5] No *Common Law* "as decisões judiciais são a principal fonte do direito e produzem efeitos vinculantes e gerais. A norma de direito corresponde ao comando extraído de uma decisão concreta, que será aplicado, por indução, para solucionar conflitos idênticos no futuro. Ela é determinada a partir do problema e deve ser compreendida à luz dos seus fatos relevantes. É mais fragmentada, ligada às particularidades da demanda e à justiça do caso concreto; é menos voltada a produzir soluções abrangentes e sistemáticas. O uso da lei como fonte do direito no common law é menos usual do que no direito romano-germânico." MELO, Patrícia Perrone Campos; BARROSO, Luís Roberto. **Trabalhando com uma nova lógica: A ascensão dos precedentes do direito brasileiro.** Brasília, 2016. Disponível em: <https://www.conjur.com.br/dl/artigo-trabalhando-logica-ascensao.pdf.>. Acesso em 19 de nov. de 2020.

[6] Art. 5º, XIX, da Lei Geral de Proteção de Dados Pessoais: "autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Institui a Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. >. Acesso em 19 de nov. de 2020.

Naquele escrito, os autores defenderam que, embora a Constituição Americana não mencionasse, expressamente, o termo *privacy*, seus princípios já faziam parte da *common law*, sobretudo, ao se garantir à proteção constitucional ao domicílio.[7]

Assim, ante o desenvolvimento tecnológico experienciado já naquela época, Warren e Brandeis pugnavam pela expressa garantia no texto da Constituição do direito à privacidade.[8]

Para Doneda,

> em seus primórdios, marcada por um individualismo exacerbado e até egoísta, portava a feição do direito a ser deixado só. A esse período remonta o paradigma da privacidade como uma zero-relationship, pelo qual representaria, no limite, a ausência de comunicação entre uma pessoa e as demais. Essa concepção foi o marco inicial posteriormente temperado por uma crescente consciência de que a privacidade seria um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade.[9]

Com o surgimento da Rede Mundial de Computadores, a velocidade de coleta e transmissão de dados se intensificou, ensejando novas discussões a respeito do tema privacidade. A partir de década de 1960, a proteção de dados passou a ser objeto de legislações em vários países. Em um primeiro momento, buscou-se garantir a privacidade do indivíduo em relação ao Estado, posteriormente, a proteção foi ampliada para as relações com terceiros. Nesse momento, houve também o reconhecimento da pessoa como objeto da proteção à privacidade, independente da tutela da propriedade, como outrora.[10]

Na União Europeia, a proteção de dados pessoais teve seu primeiro marco regulatório por meio da Diretiva 95/46/CE, de 24/11/1995, seguida da Diretiva 2002/58/CE, de 12/6/2002, e, recentemente, do Regulamento UE 2016/679, de 27/4/2016. Isto é, com a edição do Regulamento, a norma passou a ser vinculativa para todos os Estados-membros.

Nos EUA, a legislação sobre privacidade e proteção de dados é fragmentada, não havendo uma estrutura jurídica unificada, mas, sim, proteção paralela

---

[7] ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right to privacy nos Estados Unidos. Revista **Jus Navigandi**, ISSN 1518-4862, Teresina, ano 22, n. 5130, 18 jul. 2017. Disponível em: <https://jus.com.br/artigos/57228>. Acesso em: 22 ago. 2020.

[8] *Ibidem*

[9] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais [livroeletrônico]: elementos da formação da Lei geral de proteção de dados**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. Rb-1.1.

[10] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de dados Pessoais no Direito Brasileiro.** Ed 2019. São Paulo, SP. Thomson Reuters Brasil, 2019.

pela Constituição Americana (ainda que até hoje não haja menção expressa à proteção de dados pessoais ou à privacidade) e pelas Constituições Estaduais, o que pode provocar algumas disparidades normativas entre os estados.

Além disso, as leis são setorizadas, de modo que há leis aplicáveis ao setor bancário, ao setor médico etc., sendo que alguns setores são autorregulados pelas próprias empresas.

Como exemplos de normas americanas, podemos citar a *Health Insurance Portability and Accountability Act (HIPAA),* lei federal que visa proteger informações sensíveis de saúde de pacientes e a *Children's Online Pivacy Protection Act (COPPA)*, que regula a coleta e utilização de informações de crianças menores de 13 anos sem o consentimento dos pais, dentre outras.

Acontecimentos recentes nos Estados Unidos, envolvendo vazamento de dados, motivaram a proposição de um projeto de lei de proteção de dados, em 13/2/2020, pela senadora Kirsten Gillibrand (*Data protection Act of 2020*)[11]. O projeto encontra-se na Comissão de Comércio, Ciência e Transporte.

No sistema jurídico brasileiro, o tema privacidade é tratado: na Constituição de 1988, que consagra, em seu art. 5º, como direito fundamental, a proteção aos direitos à privacidade e à intimidade[12], ao sigilo de dados/informações/comunicações[13], à inviolabilidade do domicílio[14]; no Código Civil de 2002, que também prevê inviolabilidade ao direito à privacidade[15], sendo classificado como direito da personalidade; no Código Penal (Decreto-Lei No 2.848, de 7/12/1940), que traz a proteção ao sigilo das correspondências[16], bem como em outras leis a serem vistas no decorrer deste artigo.

Não há consenso na doutrina sobre a conceituação e a diferenciação dos institutos tratados, sobretudo, por serem trazidos nas citadas normas indistintamente. Há

---

[11] ESTADOS UNIDOS. **Data Protection Act of 2020**. Disponível em: <https://www.congress.gov/bill/116th-congress/senate-bill/3300/text>. Acesso em 20 de jun. de 2020

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

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

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

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

[16] Art. 151: "Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena – detenção, de 1 a 6 meses, ou multa."

quem diga que o direito ao sigilo é uma faceta do direito à intimidade, há que diferencie direito à intimidade do direito à privacidade. Outros optam pela unificação dos conceitos.

Segundo Gilmar ferreira Mendes e Paulo Gustavo Gonet Branco, o direito à intimidade refere-se a uma esfera de proteção ainda mais restrita que o direito à privacidade. Para os professores,

> o direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas. O direito à privacidade é proclamado como resultado da sentida exigência de o indivíduo "encontrar na solidão aquela paz e aquele equilibrio, continuamente comprometido pelo ritmo da vida moderna". A reclusão periódica à vida privada é uma necessidade de todo homem, para a sua própria saúde mental. Além disso, sem privacidade, não há condições propícias para o desenvolvimento livre da personalidade. Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracassos à critica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muito menos como o indivíduo se autoavaliar, medir perspectivas e traçar metas. A privacidade é componente ainda de maior relevo de certas relações humanas, como o casamento, por exemplo. A divulgação de dificuldades de relacionamento de um casal pode contribuir para a destruição da parceria amorosa. E mesmo um núcleo de privacidade de cada cônjuge em relação ao outro se mostra útil à higidez da vida em comum. [17]

Ainda segundo, os Autores a privacidade pode ser conceituada da seguinte forma,

> a pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral. Como acontece com relação a qualquer direito fundamental, o direito à privacidade também encontra limitações, que resultam do próprio fato de se viver em comunidade e de outros valores de ordem constitucional. [18]

Laura Schertel Mendes também trata da discussão sobre a terminologia do direito à privacidade. Segundo a Autora,

> a própria Constituição Federal propicia o debate terminológico sobre o direito à privacidade, ao determinar em seu artigo 5º, X, que são invioláveis a vida privada e a intimidade. Nesse sentido, a norma suprema

[17] MENDES, Gilmar ferreira e BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 1. ed. rev. e atual. – São Paulo: Saraiva, 2015. p. 280-286.
[18] *Ibidem*.

> suscita a discussão acerca do sentido de cada uma das expressões: designariam "vida privada" e "intimidade" bens jurídicos distintos?[19]

A Autora traz a definição da privacidade de Alan Westin (1970, p. 7), para quem,

> privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar, quando, como e em que extensão, informações sobre si próprios devem ser comunicadas a outros.[20]

Conforme dito anteriormente, na doutrina civilista, o direito à privacidade se insere nos direitos da personalidade. Para os autores Pablo Stolze Gagliano e Rodolfo Pamplona Filho, o instituto manifesta-se, sobretudo, por meio do direito à intimidade, cujo elemento fundamental é o respeito ao isolamento de cada ser humano que não deseja que terceiros tenham conhecimento sobre certos aspectos de sua vida.[21]

Os mesmos Autores citam o enunciado nº 400 da V Jornada de Direito Civil, por meio do qual, defendem que a tutela da privacidade compreende o controle dos próprios dados, sendo necessário expresso consentimento para o tratamento de informações sobre estado de saude, condição sexual, etc.[22]

Nesse sentido, Danilo Doneda[23] menciona a definição proposta por Stefano Rodotà para a privacidade, segundo a qual esse instituto é "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada".

Para Doneda, devido à crescente complexidade das situações, não faz sentido a frase a "transparência de quem não tem nada a temer", uma vez que uma esfera privada, dentro da qual o indivíduo possa desenvolver sua personalidade é pressuposto para que ele não seja submetido aos controles sociais, que "anulariam sua individualidade, cercearíam sua autonomia privada (para tocar em um conceito caro ao direito privado) e, em última análise, inviabilizariam o livre desenvolvimento de sua personalidade."[24]

---

[19] MENDES, Laura Schertel. **TRANSPARÊNCIA E PRIVACIDADE: VIOLAÇÃO E PROTEÇÃO DA INFORMAÇÃO PESSOAL NA SOCIEDADE DE CONSUMO**. Disponível em [http://dominiopublico.mec.gov.br/download/teste/arqs/cp149028.pdf] Acesso em 25 de jun. de 2020.
[20] *Ibidem*.
[21] GAGLIANO, Pablo Stolze e PAMPLONA FILHO, Rodolfo. **Manual de direito civil**. volume único. – São Paulo: Saraiva, 2017. p. 72.
[22] *Ibidem*.
[23] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais [Livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados**. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. RB-.1.10.
[24] *Ibidem*.

Assim, se antes a violação aos direitos à privacidade, ao sigilo e à intimidade eram uma "questão física", "palpável", como a divulgação de imagens em jornais impressos, violação de domicílio e violação de correspondência, demandando uma postura absenteísta do Estado, hoje, com o intenso fluxo de informações, podemos falar em uma evolução dos direitos evocados para o direito à proteção de dados, exigindo do Estado, uma concreta e efetiva atuação para garanti-lo.

A respeito da evolução do direito à privacidade, em face da revolução tecnológica, Laura Schertel Mendes comenta que,

> a partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais. Nesse contexto, percebe-se, uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominado privacidade informacional, "proteção de dados pessoais", "autodeterminação informativa", entre outros[25]

Doneda ressalta que, na Carta dos Direitos Fundamentais da União Europeia, a privacidade e a proteção de dados pessoais são tratados em artigos diferentes, sendo a primeira abordada no art. 7º, que trata do respeito pela vida familiar e privada e o segundo no art. 8º, que dispõe especificamente sobre proteção dos dados pessoais. [26] Assim, segundo o Autor,

> a Carta, dessa forma, reconhece a complexidade dos interesses ligados à privacidade e a disciplina em dois artigos diferentes: um destinado a tutelar o indivíduo de intromissões exteriores; e outro destinado à tutela dinâmica dos dados pessoais nas suas várias modalidades – sem fracionar sua fundamentação, que é a dignidade do ser humano, matéria do capítulo I da Carta.[27]

Ainda conforme preceitua o mesmo Autor, o direito à proteção de dados:

> É uma garantia de caráter instrumental, derivada da tutela da privacidade, porém, não limitada por esta; ainda, faz referência a um leque de garantias fundamentais que se encontram no ordenamento brasileiro.[28]

Para o Ministro Gilmar Mendes, o marco da evolução do direito à privacidade foi o desenvolvimento jurisprudencial do conceito de autodeterminação

---

[25] MENDES, Laura Schertel. TRANSPARÊNCIA E PRIVACIDADE: VIOLAÇÃO E PROTEÇÃO DA INFORMAÇÃO PESSOAL NA SOCIEDADE DE CONSUMO. Disponível em <http://dominiopublico.mec.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em 25 de jun. de 2020.
[26] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais [Livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados**. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. RB-1.1.
[27] *Ibidem.*
[28] *Ibidem.*

informacional pelo Tribunal Constitucional Alemão em 1983, trazido na discussão a respeito da Lei do Censo alemã[29],

> No paradigmático Volkszählungsurteil (BVerfGE 65, 1), de 1983, o Tribunal declarou a inconstitucionalidade da chamada Lei do Censo alemã (Volkszählunsgesetz), que possibilitava que o Estado realizasse o cruzamento de informações sobre os cidadãos para mensuração estatística da distribuição especial e geográfica da população.
> (...)
> No caso concreto, o Tribunal entendeu que o processamento automatizado dos dados, possibilitado pela Lei do Censo, de 1983, colocaria em risco o poder do indivíduo de decidir por si mesmo sobre se e como ele desejaria fornecer seus dados pessoais a terceiros. A situação de risco identificada pelo Tribunal referia-se à possibilidade concreta de, por meio de sistemas automatizados, as informações fornecidas sobre profissões, residências e locais de trabalho dos cidadãos serem processadas de modo a se formar um "perfil completo da personalidade".
> Essa nova abordagem revelou-se paradigmática, por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso.[30]

Já no Brasil, a evolução do conceito de privacidade pode ser primeiro observada com a edição de normas setoriais assecuratórias da proteção de dados pessoais, tais como: o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet – que inclusive assegura aos usuários da internet, entre outros direitos, a inviolabilidade e o sigilo do fluxo de comunicações e dos dados armazenados (art. 7º, II e III) – e, mais recentemente, a Lei Geral de Proteção de Dados (Lei 13.709/2018).[31]

1.2 Evolução da Jurisprudência brasileira a respeito do direito fundamental à proteção de dados pessoais

Recentemente, pode-se mencionar três momentos importantes para o reconhecimento da autonomia do direito fundamental à proteção de dados pessoais na jurisprudência brasileira.

Primeiramente, na apreciação do Recurso Extraordinário 673.707, da Relatoria do Min. Luiz Fux, o Pleno do STF entendeu cabível *habeas data* para acessar

[29] BRASIL. Supremo Tribunal Federal. Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal. Partido Socialista Brasileiro – PSB e União. Relator: Ministro Gilmar Mendes. Decisão, 24 jun. 2020. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753108946&prcID=5938693&ad=s#>. Acesso em 15 de out. de 2020.
[30] *Ibidem*.
[31] *Ibidem*.

informações incluídas no banco de dados Sistema de Conta-Corrente de Pessoa Jurídica – SINCOR, da Receita Federal (julgado em 17.6.2015, DJe 30.9.2015).[32]

Para Min. Gilmar Mendes, ao comentar o citado RE, foi nesse momento que houve a abertura constitucional ao reconhecimento da autonomia do direito fundamental à proteção de dados pessoais[33]. Segundo o Ministro,

> essa orientação se justificou ante o fato de os dados serem entendidos em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto, causando-lhe dano ao seu direito de privacidade. Assim, aos contribuintes foi assegurado constitucionalmente o direito de conhecer as informações que lhes digam respeito em bancos de dados públicos ou de caráter público, em razão da necessidade de preservar o status de seu nome, planejamento empresarial, estratégia de investimento e, em especial, a recuperação de tributos pagos indevidamente. [34]

Posteriormente, o STF, ao deliberar sobre as Ações Diretas de Inconstitucionalidade nºs 6387, 6388, 6389, 6390 e 6393, referendou a medida cautelar que suspendeu a eficácia da Medida Provisória nº 954 de 17/4/2020, a qual estabelecia:

> 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 (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

Quando da suspensão da Medida Provisória, a Relatora do feito, Min. Rosa Weber, destacou em sua decisão monocrática que a Constituição "confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade".[35]

---

[32] BRASIL. Supremo Tribunal Federal. **DIREITO CONSTITUCIONAL. DIREITO TRIBUTÁRIO. HABEAS DATA. ARTIGO 5º, LXXII, CRFB/88. LEI Nº 9.507/97. ACESSO ÀS INFORMAÇÕES CONSTANTES DE SISTEMAS INFORMATIZADOS DE CONTROLE DE PAGAMENTOS DE TRIBUTOS. SISTEMA DE CONTA CORRENTE DA SECRETARIA DA RECEITA FEDERAL DO BRASIL-SINCOR. DIREITO SUBJETIVO DO CONTRIBUINTE. RECURSO A QUE SE DÁ PROVIMENTO.** RE 673707/MG – Minas Gerais. Rigliminas Distribuidora LTDA e União. Relator: Ministro Luiz Fux. Acordão, 30 set. 2015. Disponível em: < https://jurisprudencia.stf.jus.br/pages/search/sjur322444/false>. Acesso em 26 de jun. de 2020.

[33] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal**. Partido Socialista Brasileiro – PSB e União. Relator: Ministro Gilmar Mendes. Decisão, 24 jun. 2020. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753108946&prcID=5938693&ad=s#>. Acesso em 15 de out. de 2020.

[34] *Ibidem*.

[35] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Conselho Federal da Ordem dos Advogados do Brasil e Presidente da República. Relator: Ministra Rosa Weber. Decisão, 24 abr. 2020. Disponível em: < http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em 6 de jun. de 2020.

Ressaltou ainda que "o direito à privacidade (*right to privacy)* e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações", e que a inviolabilidade do sigilo, sobretudo, de dados, é prevista constitucionalmente como forma de instrumentalizar os citados direitos.[36] Destacou também que à proteção à privacidade e à autodeterminação informativa receberam tratamento no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), "como fundamentos específicos da disciplina da proteção de dados pessoais".[37]

Ainda que, à época da Decisão, a LGPD não estivesse em vigor, seus princípios foram utilizados como parâmetros para o pronunciamento. Outrossim, é importante perceber a preocupação da Relatora com vazamento de dados e/ou sua utilização indevida, no seguinte trecho,

> Nada obstante, a MP n. 954/2020 não apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, seja no seu tratamento. [38]

Por fim, em um terceiro momento da evolução do direito fundamental à proteção de dados pessoais, o STF, na ADPF nº 695/DF, se deparou com a potencial cessão dos dados constantes nas carteiras de motorista de mais de 70 milhões de brasileiros pelo Serviço Federal de processamento de Dados (SERPRO) à Agência Brasileira de Inteligência (ABIN).

Na ADPF, ainda em trâmite, o Relator, min. Gilmar Mendes defendeu que a autonomia do direito fundamental à proteção de dados exorbita o conteúdo normativo da cláusula de proteção ao sigilo, asseverando que[39]

> a afirmação de um direito fundamental à privacidade e à *proteção de dados pessoais* deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do

[36] *Ibidem*.
[37] *Ibidem*.
[38] *Ibidem*.
[39] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal**. Partido Socialista Brasileiro – PSB e União. Relator: Ministro Gilmar Mendes. Decisão, 24 jun. 2020. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753108946&prcID=5938693&ad=s#>. Acesso em 15 de out. de 2020.

Em seguida, o Ministro ressaltou que a proteção do direito fundamental à proteção de dados tem dupla dimensão: subjetiva e objetiva. Na dimensão subjetiva, refere-se à proteção do indivíduo contra ameaça a sua personalidade decorrente da coleta, tratamento e transmissão de seus dados pessoais. Já na dimensão objetiva, relaciona-se a proteção da sua autodeterminação informacional, ou seja, poder de controle e consentimento a respeito da utilização de seus dados pessoais.[40]

Cabe ainda mencionar que a proteção de dados no contexto público possui peculiaridades que a diferenciam do âmbito das relações particulares. Isso porque os dados para a Administração Pública são estratégicos para a prestação de serviços públicos, sobretudo os essenciais, segurança pública, educação, saúde, assistência, etc.

Assim, o fato é que com o avanço tecnológico, os dados pessoais são indispensáveis para a melhoria dos serviços públicos e sua necessidade e utilidade justificam, por si só, sua coleta e tratamento.

Para Gilmar Mendes, a modernização da Administração Pública de um modelo de *Data Driven Public Sector* (tomada de decisões públicas com base em dados) constitui importante passo na direção da concretização de direitos sociais.[41]

Assevera ainda o Ministro que países podem melhorar os resultados da gestão utilizando novas tecnologias de forma responsiva, protetiva e transparente e o tratamento de dados é instrumento essencial para o desenho, a implementação e o monitoramento de políticas e serviços públicos essenciais.[42]

Destaca o Cadastro Base do Cidadão[43], que tem por objetivo unificar as informações dos cidadãos dentro do governo, como parte da iniciativa de digitalização da Administração Pública brasileira.[44]

---

[40] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal**. Partido Socialista Brasileiro – PSB e União. Relator: Ministro Gilmar Mendes. Decisão, 24 jun. 2020. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753108946&prcID=5938693&ad=s#>. Acesso em 15 de outubro de 2020.

[41] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Conselho Federal da Ordem dos Advogados do Brasil e Presidente da República. Relator: Ministra Rosa Weber. Decisão, 24 abr. 2020. Disponível em: < http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em 6 de jun. de 2020.

[42] *Ibidem*.

[43] BRASIL. **Decreto nº 10.046 de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em 15 de out. de 2020.

[44] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Conselho Federal da Ordem dos Advogados do Brasil e Presidente da República. Relator: Ministra Rosa

Todavia, é preciso ponderar que um grande banco de dados centralizado e contendo dados pessoais de milhões de brasileiros exige um sistema de segurança cibernética robusto para evitar vazamentos.

Por fim, outra questão importante é que a proteção de dados envolve principalmente o contexto em que ocorre o tratamentos de dados e a sua finalidade, pois não existem mais dados neutros e, mesmo o tratamento de dados cadastrais, que são considerados públicos, pode oferecer sérios riscos ao desenvolvimento da personalidade, a depender da finalidade com a qual esse tratamento ocorre.

No capítulo seguinte serão mais bem explorados os riscos envolvidos na coleta, tratamento e armazenamento de dados pessoais.

2 COMO DIFERENTES GOVERNOS NO MUNDO ESTÃO USANDO DADOS PESSOAIS NO ENFRENTAMENTO DA COVID-19 E QUAIS OS PROBLEMAS SURGIDOS A PARTIR DESSE TRATAMENTO

A situação de emergência internacional que experienciamos em 2020, decorrente da pandemia do Covid-19, trouxe desafios à saúde pública e à economia, que demandaram atuações de empresas e governos.

Se antes já se observava significativa dependência tecnológica para o regular funcionamento de empresas e governos, hoje, com a pandemia, e o isolamento social dela advindo, é impensável o funcionamento dos mais diversos setores da economia mundial sem o uso das tecnologias da informação.

Com o objetivo de conter a crise global experimentada, autoridades sanitárias têm se utilizado de ferramentas digitais para o monitoramento de contágios, o que implica na coleta, tratamento, armazenamento e transmissão de uma grande quantidade de dados.

Não obstante a relevância estratégica dos dados pessoais no combate à pandemia, surgem questionamentos relacionados à proteção desses dados, quanto aos aspectos ético, legal e técnico, tais como: qual o destino desses dados; é possível assegurar que os dados não serão alvo de ataques cibernéticos; é possível garantir a privacidade dos titulares; dentre outros.

Weber. Decisão, 24 abr. 2020. Disponível em: < http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em 6 de jun. de 2020.

Importante salientar que os dados pessoais para o setor público têm peculiaridades em relação ao setor privado. Segundo Gilmar Mendes, "para além da questão meramente econômica, os dados constituem ativos estratégicos para a gestão pública nas sociedades contemporâneas e, além disso, constituem verdadeiramente pré-condições para o exercício da democracia."[45]

Desse modo, o compartilhamento de dados entre entidades/órgãos da Administração pública é muitas vezes uma necessidade, em face do princípio do interesse público. Contudo, a proteção aos dados pessoais da coletividade, como um direito fundamental autônomo, também deve ser perseguida.

Uma importante reflexão que deve ser feita é: quais serão os critérios adotados para que o princípio do interesse público prepondere e permita o tratamento de dados? Caso não haja parâmetros, corre se o risco de a proteção de dados pessoais sempre ser suplantada pelo princípio do interesse público.

Voltando ao contexto da pandemia do Covid-19, exemplos de monitoramento de indivíduos por governos não faltam.

Na Rússia, o sistema de câmeras de vigilância foi utilizado para monitorar, via reconhecimento facial, pessoas que violem as medidas de quarentena[46].

O governo chinês está utilizando um aplicativo (*Alipay Health Code)* que restringe a circulação de pessoas a depender do risco que apresentem para o contágio do Covid-19, com base em uma classificação de cores.

> De acordo com o aplicativo, pessoas que recebem o código verde podem se locomover livremente. Para aquelas que recebem o código amarelo, o aplicativo solicita que se isolem em suas residências pelo período de sete dias e, por fim, para quem recebe o código vermelho, a permanência em quarentena de duas semanas é obrigatória.[47]

Também na China, a população é vigiada por uma câmera desenvolvida pela *Hanwang Technology* que, por meio do reconhecimento facial, identifica quais

---

[45] BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal**. Partido Socialista Brasileiro – PSB e União. Relator: Ministro Gilmar Mendes. Decisão, 24 jun. 2020. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753108946&prcID=5938693&ad=s#>. Acesso em 15 de outubro de 2020.

[46] MAGALHÃES, Guilherme. Russos resistem a mudanças de rotina enquanto governo aperta cerco contra coronavírus. **Folha de São Paulo**. São Paulo, 13 de março de 2020. Disponível em: <https://www1.folha.uol.com.br/equilibrioesaude/2020/03/russos-resistem-a-mudancas-de-rotina-enquanto-governo-aperta-cerco-contra-coronavirus.shtml>. Acesso em 14 de outubro de 2020.

[47] DE ARAÚJO, Priscila Maria Menezes, BANDEIRA, Natália Ferreira. Na pandemia, é possível flexibilizar as balizas da proteção de dados pessoais? **Jota**, 1 de abr. de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/na-pandemia-e-possivel-flexibilizar-as-balizas-da-protecao-de-dados-pessoais-01042020>. Acesso em 14/10/2020.

chineses têm usado máscaras de proteção nas ruas e detecta o nome e a temperatura corporal das pessoas.[48]

A Coreia do Sul se utilizou de registros do GPS do celular ou uso do cartão de crédito para rastrear onde pessoas contaminadas estiveram, emitindo alertas para outros potenciais contaminados se testarem e se isolarem.[49]

O governo de Israel desenvolveu um sistema de rastreamento de pessoas próximas a quem testou positivo para o Covid-19 para que fiquem em quarentena, obrigatória, ainda que não apresentem sintomas[50].

Em Singapura, o governo lançou o aplicativo *TraceTogether*, que monitora as ações da população, o app não é obrigatório, mas teve grande adesão da população, apesar da falta de normas de privacidade com seus usuários.[51]

> O aplicativo funciona da seguinte forma: o usuário permite o uso constante do bluetooth e de sua localização, que vão para a rede central de dados do TraceTogether. Assim, a ferramenta sabe com quem essa pessoa interagiu, por quanto tempo e até mesmo a qual distância elas estavam. Quando alguém é diagnosticado com o vírus, médicos podem olhar o histórico de interações da vítima e notificar todas as pessoas que podem ter sido expostas à doença. Do mesmo jeito, é possível ter uma ideia de quem passou o vírus para essa pessoa.[52]

No Brasil, em âmbito federal, dados de geolocalização foram usados para monitorar qual o percentual de pessoas em determinada região está cumprindo a quarentena, apontando aglomeração por mapa de calor[53]. Contudo, as tratativas entre o governo federal e as empresas telefônicas foram suspensas, o que não impediu os estados firmarem suas próprias parceiras com o mesmo fim.[54]

---

[48] DE ARAÚJO, Priscila Maria Menezes, BANDEIRA, Natália Ferreira. Na pandemia, é possível flexibilizar as balizas da proteção de dados pessoais? **Jota**, 1 de abr. de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/na-pandemia-e-possivel-flexibilizar-as-balizas-da-protecao-de-dados-pessoais-01042020>. Acesso em 14 de out. de 2020.

[49] SCHREIBER, Mariana. Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade? **BBC**, 21 de abr. de 2020. Disponível em: <https://www.bbc.com/portuguese/brasil-52357879>. Acesso em: 14 de out. de 2020.

[50] BATEMAN, Tom. Coronavirus: Israel turns surveillance tools on itself. **BBC**, 11 de maio de 2020. Disponível em: <https://www.bbc.com/news/world-middle-east-52579475>. Acesso em 15 de out. de 2020.

[51] LABBATE, Mariana. Conheça o TraceTogether, app de monitoramento do coronavírus criado por Singapura. **Forbes**, 25 de março de 2020. Disponível em: <https://forbes.com.br/negocios/2020/03/conheca-o-tracetogether-app-de-monitoramento-do-coronavirus-criado-por-singapura/>. Acesso em 14 de out. de 2020..

[52] LABBATE, Mariana. Conheça o TraceTogether, app de monitoramento do coronavírus criado por Singapura. **Forbes**, 25 de março de 2020. Disponível em: <https://forbes.com.br/negocios/2020/03/conheca-o-tracetogether-app-de-monitoramento-do-coronavirus-criado-por-singapura/>. Acesso em 14 de out. de 2020.

[53] SCHREIBER, Mariana. Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade? **BBC**, 21 de abr. de 2020. Disponível em: <https://www.bbc.com/portuguese/brasil-52357879>. Acesso em 14 de out. de 2020.

[54] SCHREIBER, Mariana. Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade? **UOL**, 21 de abr. de 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/bbc/2020/04/21/coronavirus-uso-de-dados-de-geolocalizacao-contra-a-pandemia-poe-em-risco-sua-privacidade.htm>. Acesso em 15 de out. de 2020.

O Estado de São Paulo – SP, por exemplo, implementou o "Sistema de Monitoramento Inteligente" dos cidadãos, SIMI-SP, que, por meio de acordo com as operadoras de telefonia Vivo, Claro, Oi e TIM, possibilita que o Estado consulte informações agregadas sobre deslocamento de pessoas nos municípios paulistas.

Segundo o governador de SP, João Dória,

> com 100% dos usuários de telefonia celular em São Paulo, nós podemos identificar os locais onde as pessoas estarão e onde houver concentração para analisar o percentual de isolamento e também ações de orientação e advertência, se necessário.[55]

Ademais, a Apple e a Google firmaram uma parceria para criar uma plataforma de rastreamento de contato por meio de Bluetooth, por meio da qual será possível indicar se um usuário esteve perto de alguém contaminado[56].

No Reino Unido, o governo contratou empresas de tecnologia para construir um banco de dados com dados de pacientes com Covid-19. O governo declarou que os dados são anônimos e confidenciais e que estão protegidos peça legislação de proteção de dados pessoais.[57]

Essas ferramentas de vigilância têm um propósito específico de combate ao coronavírus, e é razoável a utilização de algumas delas, desde que garantidos os princípios concernentes ao tratamento desses dados

É importante observar, que o monitoramento da localização de indivíduos por meio do celular é uma intrusão de grande porte em sua vida pessoal, pois é possível saber exatamente todos os lugares que o monitorado frequentou, quanto tempo permaneceu e, cruzando dados com outros celulares, com quem estava e com qual proximidade.

Por outro lado, uma vez instalada a infraestrutura necessária para monitoramento dos cidadãos, há um risco de que o monitoramento seja normalizado no futuro, tornando-se permanente, por motivos diversos, a serem justificados pelo governo, caso a caso.

---

[55] VALENTE, Jonas. Covid-19: iniciativas usam monitoramento e geram preocupações. **Agência Brasil**, 12 de abr de 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/covid-19-iniciativas-usam-monitoramento-e-geram-preocupacoes>. Acesso em 20 de jun. de 2020.

[56] Apple e Google se unem para rastrear e tentar conter coronavirus. **Veja**, 10 de abr. de 2020. Disponível em: <https://veja.abril.com.br/tecnologia/apple-e-google-se-unem-para-rastrear-e-tentar-conter-coronavirus/>. Acesso em 12 de nov. de 2020.

[57] LEWIS, Paul; CONN, David; PEGG, David. UK Government using confidential patiente data in coronavirus response. **The Guardian**, 12 de abril de 2020. Disponível em: < https://amp.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response?CMP=share_btn_tw&__twitter_impression=true>. Acesso em 12 de nov. de 2020.

> Não pode essa grave crise mundial servir como justificativa para montar um sistema de vigilância e monitoramento, por parte de empresas e governos, ainda mais severo sobre os cidadãos. A preocupação sobre como se dará o uso desses dados e dos seus sistemas de tratamento no futuro se agrava, principalmente, quando se pensa em governos que tendam ao autoritarismo. Esta excepcional capacidade de monitoramento, somada a poderes especiais que têm sido dados a governantes em alguns países, podem, inclusive, trazer prejuízo à própria democracia.[58]

Há também o risco de os dados coletados não serem excluídos após o período de pandemia ou de serem transmitidos para outros órgãos que não as autoridades sanitárias, sendo utilizados para outros fins não previstos inicialmente.

Conforme, mencionado no Capítulo 1, o Decreto nº 10.046, de 9 de outubro de 2019[59]**,** criou o Cadastro Base do Cidadão, que embora seja uma iniciativa condizente com a agenda de digitalização da Administração Pública brasileira, pode oferecer riscos à proteção de dados pessoais, caso não haja parâmetros para seu tratamento e compartilhamento com outros órgãos/entidades, não seja respeitada a finalidade para a qual o tratamento foi motivado, e não conte com um robusto sistema de segurança cibernética.

Nesse sentido, cabe trazer o conceito de divisão informacional de poderes, segundo o qual "a finalidade de coleta e tratamento de dados pessoais por cada órgão público circunscreve-se à estrita definição de sua competência legal, sendo vedado o uso para outra finalidade dentro da Administração."[60]

Por outro lado, caso haja vazamento na base de dados do Cadastro Base do Cidadão, por exemplo, que abrange vários dados relacionados à saúde das pessoas, inclusive dados do Sistema Único de Saúde, pode ocorrer tratamento discriminatório, como no caso de um Plano de Saúde que tenha acesso previamente ao fato de que uma pessoa tenha alguma doença ou que, eventualmente, saiba que os pais dessas pessoas têm alguma doença de caráter hereditário, como a diabetes ou pressão alta. Esse plano de saúde poderá cobrar mais caro dessa pessoa ou simplesmente negar-se a celebrar contrato

---

[58] REQUIÃO, Maurício. Covid-19 e proteção de dados pessoais: o antes, o agora e o depois. **Conjur**, 5 de abril de 2020. Disponível em: <https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protecao-dados-pessoais-antes-agora-depois#sdfootnote9anc>. Acesso em 15 de out. de 2020.

[59] BRASIL. **Decreto nº 10.046 de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em 15 de out. de 2020.

[60] CAMPOS, Ricardo, MARANHÃO, Juliano. A divisão informacional de Poderes e o Cadastro Base do Cidadão. **JOTA**, 18 de nov. de 2019. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019>. Acesso em 16 de out. de 2020.

com ela. O mesmo tipo de discriminação poderia ocorrer no mercado de trabalho, na hipótese de uma empresa se recusar a contratar uma pessoa com alguma doença.

Ressalta-se, ainda, o risco de a coleta de dados extrapolar a estrita necessidade e utilidade que a justificou, quanto aos aspectos quantitativos e qualitativos. Pode se questionar ainda a quem será atribuída a responsabilidade caso ocorram vazamentos de dados.

Nessa toada, noticiou-se o compartilhamento indevido de dados com terceiros, sem o consentimento de seus titulares, pelo Facebook[61], o que ressalta a reponsabilidade das empresas gestoras de dados pessoais.

É preciso deixar claro que, se não houver gestão do intenso fluxo de informações que circula na sociedade, corre-se o risco de se expor dados pessoais, tais como de saúde, genéticos ou mesmo de localização, capazes de submeter seus titulares a discriminação racial, étnica, política, religiosa, e relacionada à orientação sexual.

Ademais, a circulação dessa quantidade de dados pessoais, de valor inestimável, pode ser objeto de ataques cibernéticos.

Foi notícia na mídia internacional que há vulnerabilidades à ataques cibernéticos em 83% de organizações de saúde, e que muitos computadores estão com sistemas desatualizados. Devido à pandemia, essas organizações estão se utilizando mais do que nunca do monitoramento dos pacientes, o que leva especialistas no assunto a crerem que os cyber criminosos irão focar no setor de saúde em 2020[62].

Divulgou-se ainda que os sistemas do *Department of Health and Human Services* (HHS) dos Estados Unidos foram afetados por ataques com o objetivo de causar lentidão em seu funcionamento[63]. Casos de vazamento de dados por empresas tais como

[61] ROSSI, Marina. Brasil multa Facebook em 6,6 milhões de reais pelo vazamento de dados no caso Cambridge Analytica. **El País**, São Paulo, 30 de dez. de 2019. Disponível em: <https://brasil.elpais.com/tecnologia/2019-12-30/brasil-multa-facebook-em-66-milhoes-de-reais-pelo-vazamento-de-dados-no-caso-cambridge-analytica.html>. Acesso em 16 de out. de 2020.

[62] CISOMAG. 83% of Healthcare Devices at Security Risk Due to COVID-19 Outbreak. **Cisomag**, 20 de mar. de 2020. Disponível em: <https://cisomag.eccouncil.org/83-of-healthcare-devices-at-security-risk-due-to-covid-19-outbreak/>. acesso em 12 de nov. de 2020.

[63] ALI, Javed. Cyber operations already impacting coronavirus response. **The Hill**, 16 de mar. de 2020. Disponível em: <https://thehill.com/opinion/cybersecurity/487814-cyber-operations-already-impacting-coronavirus-response>. Acesso em 12 de nov. de 2020.

da rede de hotéis Marriot[64], do Banco Inter[65] e da British Airways[66] não são incomuns e mostram a fragilidade dos sistemas de segurança de dados.

Por outro lado, verifica-se ainda que, no caso de monitoramento remoto por meio de geolocalização, se está diante de uma situação em que não há contato direto entre quem fornece os dados dos celulares (empresa telefônica ou empresa gestora de aplicativo) e quem faz o tratamento (autoridade sanitária), o que torna ainda mais difusa a garantia de que os titulares terão controle da utilização de seus dados.

A despeito dos mencionados riscos, o Conselho Europeu de Proteção de dados (European Data Protection Board) admitiu o monitoramento de indivíduos por meio de celulares com vistas a minimizar a disseminação do Covid-19, acolhendo a possibilidade de se enviar mensagens relacionadas à saúde pública para pessoas em área específica, desde que observadas algumas questões tais como: priorizar o tratamento anonimizado; propiciar adequadas salvaguardas, tais como o direito à ação judicial; dar preferência às soluções menos intrusivas, considerando o propósito a ser alcançado; o respeito aos princípios dos dados pessoais (proporcionalidade da medida, em termos de escopo e duração, retenção limitada dos dados e propósito limitado).[67]

Para a LGPD, dado anonimizado é aquele não permite a identificação do titular, "considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento"[68]. Assim, a preferência pelo tratamento de dados de forma anonimizada é positiva, contudo, não há garantia de que de fato seus titulares não serão identificados futuramente. Há estudos que comprovaram que é relativamente fácil reverter a anonimização.[69]

> Um segundo estudo, este mais recente, de 2019, denominado "Estimating the success of re-identifications in incomplete datasets using generative models", realizado mais uma vez pela Universidade de Louvain, em

[64] G1. Vazamento de dados dos hotéis Marriott pode ter afetado 500 milhões de clientes. **G1**, 31 de nov. de 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2018/11/30/vazamento-de-dados-dos-hoteis-marriott-pode-ter-afetado-500-milhoes-de-clientes-diz-a-rede.ghtml>. Acesso em 16 de out. de 2020.

[65] LUIZ, Gabriel. Banco Inter fecha acordo para pagar R$ 1,5 milhão após vazamento de dados de clientes. **G1**, 19 de dez. de 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2018/12/19/banco-inter-fecha-acordo-para-pagar-r-15-milhao-de-indenizacao-apos-vazamento-de-dados-de-clientes.ghtml>. Acesso em 16 de out. de 2020.

[66] PRESSE, France. British Airways é multada em US$ 230 milhões por caso de roubo de dados de passageiros. **G1**, 8 de jul. de 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/07/08/british-airways-e-multada-em-us-230-milhoes-por-caso-de-roubo-de-dados-de-passageiros.ghtml>. Acesso em: 16 de out. de 2020.

[67] JELINEK, Andrea. Statement on the processing of personal data in the context of the COVID-19 outbreack. **European Data Protection Board**, 2020. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>. Acesso em 15 de out. de 2020.

[68] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Institui a Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 12 de abril 2020.

[69] Migalhas. A efetividade da anonimização de dados pessoais. **Migalhas**, 31 de jan. de 2020. Disponível em: <https://migalhas.uol.com.br/coluna/impressoes-digitais/319519/a-efetividade-da-anonimizacao-de-dados-pessoais>. Acesso em 15 de nov. de 2020.

> conjunto com a Imperial College of Science, Technology and Medicine, em Londres, publicado na Nature Communications, estimou, com a ajuda de machine learning, a probabilidade de um indivíduo específico ser reidentificado a partir de bancos de dados anonimizados, ainda que incompletos.
> Nesta pesquisa, chegou-se à conclusão de que 99,98% dos americanos podem ser corretamente reidentificados a partir de qualquer banco de dados, utilizando 15 atributos demográficos - idade, gênero, estado civil etc. - sugerindo que técnicas tradicionais de anonimização como adding noise e sampling podem não ser suficientes para manter-se aderente às regras de privacidade de dados de normas como a General Data Protection Regulation - a Lei Geral de Proteção de Dados da Comunidade Europeia ("GDPR") ou a Consumer Privacy Act - o Ato de Privacidade do Consumidor da Califórnia ("CCPA").
> A preocupação certamente se estende ao Brasil, já que a LGPD, amplamente inspirada na GDPR, traz dispositivos semelhantes de tutela da anonimização.[70]

Desse modo, é inegável que o uso dos dados pessoais para acompanhamento da disseminação do covid-19, por meio do monitoramento da localização de usuários de *smartphones* é de grande utilidade. Contudo, não se pode olvidar os riscos envolvidos na coleta, tratamento e armazenamento desses dados, tais como: vazamento de dados, coleta de dados além da necessidade, transferência indevida de dados e normalização do monitoramento.

Nessa toada, faz se necessário examinar quais os mecanismos que o sistema jurídico brasileiro oferece para, de um lado, possibilitar a melhoria da eficiência da gestão pública, e, de outro, garantir a proteção dos dados pessoais dos cidadãos

3 QUAIS SÃO OS MECANISMOS ESPECÍFICOS QUE TEM O ORDENAMENTO JURÍDICO BRASILEIRO PARA GARANTIR A PROTEÇÃO DE DADOS PESSOAIS SEM OBSTAR A ATUAÇÃO DAS AUTORIDADES EM UMA SITUAÇÃO DE PANDEMIA

Conforme trazido neste artigo, o direito à privacidade evoluiu para o direito à proteção de dados pessoais, motivado, dentre outros fatores, pelo aumento exponencial da circulação de dados em nossa sociedade.

Assim, se por um lado devemos garantir a proteção de dados pessoais, como direito fundamental autônomo, por outro, há situações nas quais o Estado tem a

[70] Migalhas. A efetividade da anonimização de dados pessoais. **Migalhas**, 31 de jan. de 2020. Disponível em: <https://migalhas.uol.com.br/coluna/impressoes-digitais/319519/a-efetividade-da-anonimizacao-de-dados-pessoais>. Acesso em 15 de out. de 2020.

possibilidade de se utilizar desses dados para fins de interesse público, como, no caso em estudo, para controle da pandemia sanitária advinda do Covid-19.

Diante dessa conjuntura, verifica-se que o sistema jurídico brasileiro possui como balizas para a proteção do direito à proteção de dados pessoais: a Constituição de 1988, o Marco Civil da Internet, e, recentemente a Lei Geral de Proteção de dados Pessoais – LGPD, o qual é objeto deste artigo.

O cerne da questão, quando se aborda o tema proteção de dados pessoais no contexto da pandemia do Covid-19, é se a Lei Geral de Proteção de dados é completa a ponto de garantir direito à proteção de dados pessoais contra os riscos citados no capítulo 2, quais sejam, risco de normalização do monitoramento; risco de os dados coletados não serem excluídos após o período de pandemia e serem transmitidos para outros órgãos, sendo utilizados para outros fins não previstos inicialmente; o risco de a coleta de dados extrapolar a estrita necessidade e utilidade que a justificou; risco de vazamento de dados; e risco de não ser possível responsabilizar quem deu causa ao vazamento de dados.

Adentrando no estudo da LGPD[71], seu art. 2º prevê como fundamento da proteção de dados pessoais, o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Dentre os fundamentos citados, cabe destacar a autodeterminação informativa, a qual consiste no conhecimento preciso, pelo titular, de quais dados pessoais serão coletados, e como serão coletados, tratados e armazenados.

É cediço que as informações hoje trafegam de forma instantânea e que empresas se utilizam de banco de dados pessoais para identificar indivíduos mais propensos a comprar seus produtos. Assim, a LGPD não busca impedir o fluxo de dados e as atividades dele decorrentes, mas sim, tornar visível ao titular o que está sendo feito com seus dados.[72]

---

[71] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Institui a Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 31 de out. de 2020.

[72] FEIGELSON, Bruno et al (Coord.). **Comentários à Lei Geral de Proteção de Dados – Ed. 2020**. RB-.1.3 São Paulo : Thomson Reuters Brasil, 2020.

Nesse contexto, segundo Wilson Zaury Filho, autodeterminação informativa é,

> [...] o direito de o indivíduo poder dispor dos atos de informação pessoais próprios e, portanto, permitir ou recusar seu uso por parte das agências de informação que manejam os bancos de dados; direito de controlar a veracidade dos dados, o acesso a seu conhecimento por parte de terceiros e o uso que deles se faça com finalidades sociais econômicas ou políticas.[73]

Ademais, a LGPD[74] dispõe também que o tratamento de dados pessoais deverá observar a boa-fé e os princípios: da finalidade; da adequação; necessidade; do livre acesso; da qualidade dos dados; da transparência; da segurança; da prevenção; da não discriminação; e da responsabilização e prestação de contas (art. 6º).

O princípio da finalidade traduz a coerência do tratamento de dados com a finalidade declarada. Assim, se evita que dados pessoais sejam colhidos com o objetivo de combater a pandemia do Covid-19, e, posteriormente, sejam utilizados para outros fins, como por exemplo, a autoridade sanitária informa que utilizará os dados pessoais para mapeamento de aglomerações e, posteriormente, os compartilha com órgão da receita fazendária, que os utiliza para traçar um perfil de gastos daquele titular.

Nesse ponto, por exemplo, o tratamento dos dados pessoais no multicitado Cadastro Base do Cidadão deve observar, de um lado, o art. 25 da LGPD, o qual dispõe que:

> Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

E de outro, o art. 26 da Lei, que prevê que:

> O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

Ademais, deve ser observado o princípio da divisão informacional de poderes, segundo o qual os dados pessoais devem ser utilizados para finalidades atinentes à competência do órgão/agente de tratamento, de modo a evitar um compartilhamento indiscriminado por diferentes órgãos da Administração Pública, com o argumento de

---

[73] Ibidem.

[74] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Institui a Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 31 de out. de 2020.

ganhos de eficiência, ao ponto de transformar o Estado numa unidade informacional, sob pena de se esvair a proteção ao direito fundamental à privacidade[75].

Outro princípio que merece destaque é o da necessidade, que visa impedir o risco de que sejam coletados dados além dos necessários à finalidade pretendida, como por exemplo, coletar dados de localização de um indivíduo em determinado lugar, mas efetivamente utilizar a sua localização coletada em outro lugar.

O art. 7º, por sua vez, traz as hipóteses em que o tratamento de dados pode ser realizado:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.[76]

Destaca-se o contido no inciso VIII, que permite o tratamento de dados, independentemente do consentimento de seus titulares para tutela da saúde, exclusivamente por profissionais de saúde, serviços de saúde ou autoridade sanitária.

---

[75] CAMPOS, Ricardo, MARANHÃO, Juliano. A divisão informacional de Poderes e o Cadastro Base do Cidadão. **JOTA**, 18 de nov. de 2019. Disponível em: < https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019>. Acesso em 16 de out. de 2020.

[76] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Institui a Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 31 de out. de 2020.

Nesse inciso, busca-se preservar o bem jurídico "vida", não só a vida do próprio titular dos dados coletados, mas também da de terceiros.

O art. 9º da Lei trata do direito de o titular ter acesso facilitado às informações sobre o tratamento de seus dados, mas não define os meios pelos quais o acesso ocorrerá, se será *on line* ou não, por exemplo. Todavia, impõe que as informações "deverão ser disponibilizadas de forma clara, adequada e ostensiva".

O dispositivo traz também um rol, exemplificativo, da informações a serem fornecidas, quais sejam: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e direitos do titular, com menção explícita aos direitos contidos no art. 18 da Lei.

Em relação aos dados pessoais sensíveis[77], o art. 11 da LGPD admite o seu tratamento sem consentimento de seu titular, nas hipóteses em que for indispensável para:

> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Destaca-se que, no rol, taxativo, previsto no artigo em questão, na alínea "f", tal como no art. 7º, inciso VIII, há a possibilidade de tratamento de dados pessoais sem consentimento de seu titular quando forem indispensáveis à tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (alínea "f").

[77] "dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, inciso II da LGPD).

Isto é, nas citadas hipóteses, tanto os dados pessoais como os dados pessoais sensíveis podem ser tratados independentemente do consentimento de seus titulares.

O art. 12 aborda a anonimização dos dados pessoais, prevendo que

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

Conforme o art. 5º, inciso I da LGPD, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Assim, se o dado for, por exemplo, de natureza estatística, utilizado para saber o gênero das pessoas que contraíram Covid-19 no ano de 2020, não será considerado dado pessoal.

A anonimização significa tornar os dados independentes de seus titulares, contudo, como já comentado no capítulo 2, o processo de anonimizar pode ser revertido por quem o realizou.

Contudo, a previsão contida no parágrafo 3º do art. 12 da LGPD, a seguir transcrita, confere mais segurança à questão.

> § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Como mencionado anteriormente, por meio do SIMI-SP, o Governo buscou monitorar aglomerações sem se utilizar de dados pessoais, pois não era possível identificar as pessoas, mas somente verificar os locais de concentração populacional.[78]

Assim, não haveria afronta aos dispositivos da LGPD, ainda que a Lei estivesse em vigor, à época, uma vez que os dados não são considerados dados pessoais, segundo o conceito legal, posto que se tratava de dados anonimizados[79], os quais,

> não identificam qualquer cidadão, nem o perfil dos titulares de celulares observados na aglomeração, mas é utilizado e aplica-se apenas a estudos de medidas de concentração de pessoas em áreas públicas, que descumprem o isolamento social determinado pelo Governo, conforme orientação da OMS - Organização Mundial de Saúde, para evitar a disseminação mais rápida da doença causada pelo vírus covid-19.[80]

---

[78] ARRUDA, maria Clara Villasbôas. O Governo do Estado de São Paulo não utiliza dados pessoais para medir aglomerações: A privacidade dos titulares de aparelhos de celular está preservada. **Migalhas**, 28 de maio de 2020. Disponível em: <https://migalhas.uol.com.br/depeso/327796/o-governo-do-estado-de-sao-paulo-nao-utiliza-dados-pessoais-para-medir-aglomeracoes--a-privacidade-dos-titulares-de-aparelhos-de-celular-esta-preservada>. Acesso em 19 de nov. de 2020.

[79] Art. 5º, I, da LGPD: "dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

[80] ARRUDA, maria Clara Villasbôas. O Governo do Estado de São Paulo não utiliza dados pessoais para medir aglomerações: A privacidade dos titulares de aparelhos de celular está preservada. **Migalhas**, 28 de maio de 2020.

O que é diferente do que foi feito na Coreia do Sul, em que eram emitidos alertas pessoais para potenciais contaminados se testarem e se isolarem.

Após o término do tratamento, que ocorrerá nas hipóteses previstas no art. 15 da LGPD, quais sejam: verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; fim do período de tratamento; comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º da Lei, resguardado o interesse público; ou determinação da autoridade nacional, quando houver violação ao disposto na Lei, os dados devem ser excluídos, conforme art. 16 da LGPD. Assim, o dispositivos busca evitar o risco de os dados não serem excluídos após o tratamento.

Nessa toada, cabe trazer à baila ainda que o art. 16 da LGPD admite, excepcionalmente, a conservação dos dados para as seguintes finalidades: cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

A respeito das regras para o tratamento dos dados pessoais pelo poder público, a LGPD, em seu art. 23, prevê que determinadas pessoas jurídicas de direito público deverão realizá-lo respeitando ao interesse à finalidade públicos e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

As pessoas jurídicas de direito público em questão são, conforme parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação):

> I – os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II – as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Ademais, foi prevista no art. 26 da LGD, a possibilidade de compartilhamento de dados pessoais entre as citadas pessoas jurídicas para execução de

Disponível em: <https://migalhas.uol.com.br/depeso/327796/o-governo-do-estado-de-sao-paulo-nao-utiliza-dados-pessoais-para-medir-aglomeracoes--a-privacidade-dos-titulares-de-aparelhos-de-celular-esta-preservada>. Acesso em: 19 de nov. de 2020.

políticas públicas, respeitados os princípios de proteção de dados pessoais. Por outro lado, vedou-se a transferência de dados pessoais pelo Poder Público às entidades privadas (parágrafo único), com as exceções a seguir e mediante, em regra, consentimento do titular:

> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou
> V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Assim, o dispositivo visa coibir o risco de ocorrência da livre transmissão de dados entre vários órgãos/entidades públicas, como regra, sendo admitida somente em hipóteses excepcionais devidamente justificadas ao abrigo da Lei.

Nesse sentido, a exclusão dos dados pessoais após o tratamento e a não transmissão entre órgãos/entidades está alinhada com a minimização do risco da normalização do monitoramento.

No que concerne a eventuais violações à LGPD pelo Poder Público, o tema foi tratado em dois artigos (arts. 31 e 32), nos quais foi previsto que a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação; solicitar relatórios de impacto à proteção de dados pessoais; e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Em relação aos relatórios de impacto à proteção de dados pessoais, o art. 38 da Lei dispõe que a autoridade nacional poderá exigir a sua elaboração pelo controlador, inclusive quanto aos dados sensíveis. Isto é, o relatório pode ser exigido independente de ocorrer violação à LGPD.

O capítulo VI, arts. 37 a 45, versa sobre os agentes de tratamento de dados pessoais, que são o controlador e o operador, cuja definição foi trazida no art. 5º, incisos VI e VII:

> VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

O art. 37 dispõe que os agentes devem manter registro de todas as fases do tratamento de dados que realizarem, especialmente quando baseado no legítimo interesse.

No que se refere à responsabilidade do controlador ou operador por dano patrimonial, moral, individual ou coletivo, os agentes de tratamento de dados pessoais são obrigados a promover a devida reparação, conforme art. 42 da LGPD.

Nesse sentido, tem-se a previsão para responsabilização de eventuais violações decorrentes de ataques cibernéticos, por exemplo, em que os agentes de tratamento não tomaram as devidas cautelas visando a efetiva proteção dos dados pessoais.

Todavia, a Lei traz em seu art. 43 hipóteses em que não serão responsabilizados, quais sejam, quando provarem:

> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

A respeito da segurança e do sigilo de dados, o art. 46 prevê que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas capazes de proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Ademais, qualquer pessoa que participe de alguma das fases do tratamento de dados pessoais obriga-se a garantir a segurança da informação, mesmo após o seu término (art. 47).

Por fim, o art. 49 traz a necessidade de se estruturar sistemas coerentes com requisitos de segurança, padrões de boas práticas e de governança e com os princípios gerais previstos na LGPD.

Verifica-se, a partir dos citados dispositivos, a preocupação da LGPD com o risco de ataques cibernéticos, uma realidade cujos exemplos foram mencionados no capítulo anterior.

O art. 52 prevê que as sanções administrativas, que serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa (conforme parágrafo primeiro), previstas pela LGPD, ante as infrações às normas previstas na Lei são:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A par de uma lei de proteção de dados, algumas iniciativas internacionais merecem ser estudadas por autoridades brasileiras, inclusive a fim de verificar uma possível regulamentação do tema pela Autoridade Nacional de Proteção de Dados.

No Estado da Califórnia, por exemplo, tramitam dois projetos de lei que tratam do tema. O Projeto de Lei nº 660, proíbe que os dados coletados para fins de rastreamento de contato sejam utilizados ou divulgados para qualquer propósito que não o rastreamento propriamente dito. Também exige que os dados coletados sejam excluídos em 60 dias, salvo se os dados estiverem em posse de um departamento de saúde estadual ou local.

O segundo Projeto de lei, o e nº 1782, exige que os dados coletados e mantidos durante o cumprimento das obrigações de um contrato TACT (technology-assisted contact tracing) sejam criptografados na medida do possível. Também requer seja oportunizado ao titular dos dados um mecanismo simples para revogar o consentimento para a coleta, uso, manutenção ou divulgação de dados[81].

Nessa toada, cabe trazer à baila que, conforme consignado em Declaração Conjunta sobre o direito à proteção de dados no contexto da pandemia do Covid-19, por Alessandra Pierucci e Jean-Philippe Walter, não obstante a situação de emergência de saúde internacional, os direitos humanos, externados em diversos instrumentos

[81] KAGAN, Odia. California Moves Two COVID Privacy Bills Forward. **Data Privacy**, Califórnia, 25 de ago. de 2020. Disponível em: <https://dataprivacy.foxrothschild.com/2020/08/articles/california-consumer-privacy-act/coronavirus-and-data-protection-series-part-88-california-covid-privacy-bills/>. Acesso em: 12 de nov. de 2020.

internacionais (como o Pacto Internacional de Direitos Civis e Políticos e a Convenção Europeia dos Direitos do Homem) e as normas nacionais são aplicáveis e não podem ser suspensos, podendo ser restringidos por lei, na estrita medida exigida pelas circunstâncias.[82]

Segundo Alessandra Pierucci e Jean-Philippe Walter, devem ser garantidos aos titulares dos dados: informação sobre tratamento de dados que lhes digam respeito; que os dados tratados sejam apenas os necessários e proporcionais ao objetivo pretendido; que seja realizada uma verificação de impacto antes do tratamento; e *privacy by design*, em que o tratamento de dados deve ser realizado com foco na proteção à privacidade.[83]

Os autores ainda enfatizam que o direito à proteção de dados pessoais não pode ser impedimento para o monitoramento epidemiológico, nem para o uso de informações de localização para sinalizar movimentos das pessoas que estão infringindo o confinamento ou que estão se deslocando de uma área com muitos casos do Covid-19.[84]

Por outro lado, mencionam que, segundo a Convenção 108+ (Art. 11), as restrições aos direitos e princípios relacionados à proteção de dados pessoais devem ser "previstas por lei, respeitar a essência dos direitos e liberdades fundamentais e constituir uma medida necessária e proporcional em uma sociedade democrática". [85]

Sugerem ainda que o processamento de dados pessoais em grande escala somente pode ser realizado com base em evidências científicas, de modo a trazer benefícios potenciais à saúde pública superiores à adoção de alternativas menos invasivas, sendo estas sempre preferíveis às que envolvam tratamentos de dados pessoais[86].

Nesse contexto, O *Information Commissioner's Office* publicou seis etapas que organizações devem considerar ao realizar tratamento de dados pessoais: (i) somente coletar e tratar dados necessários; coletar e tratar o mínimo de dados possível; ser transparente com os titulares sobre seus dados pessoais; ter uma abordagem justa e não

[82] PIERUCCI, Alessandra, WALTER, Jean Philippe. The Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe recall the principles of data protection in these times of fight against the COVID-19 pandemic. **COE.INT**, Estrasburgo, 30 de mar. de 2020. Disponível em: <https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter>. Acesso em 12 de nov. de 2020.
[83] *Ibidem*.
[84] *Ibidem*.
[85] *Ibidem*.
[86] *Ibidem*.

discriminatória; manter os dados seguros; propiciar o exercício do direito à proteção de dados a seus titulares[87].

Muitas dessas recomendações e sugestões são abordadas na LGPD. A situação de calamidade, de fato, demanda excepcionalmente uma atuação mais intrusiva na vida dos cidadãos, a qual deve ser responsável, e primar pela segurança das informações e transparência durante todo o processo de coleta, tratamento, armazenamento e exclusão dos dados pessoais.

Todavia, diante das ameaças de ataques aos sistema informatizados, é indispensável que os agentes de tratamento atuem em ambientes dotados de infraestrutura tecnológica para combatê-las, antes mesmo que haja a coleta de dados pessoais, o que pode implicar em parcerias com universidades ou contratação de empresas especializadas em segurança da informação. E esses contratos/parcerias devem estabeleces quais os papeis de cada uma das partes[88].

Assim, verifica-se que os riscos mencionados no parágrafo 4º deste Capítulo, quais sejam, risco de os dados coletados não serem excluídos após o período de pandemia e serem transmitidos para outros órgãos, sendo utilizados para outros fins não previstos inicialmente; o risco de a coleta de dados extrapolar a estrita necessidade e utilidade que a justificou; risco de vazamento de dados; e risco de não ser possível responsabilizar quem deu causa ao vazamento de dados, são passíveis de serem evitados por meio da LGPD.

Contudo, o tratamento de dados pessoais pelo poder público, inclusive no contexto do Covid-19, demanda tecnologia, pessoal capacitado e infraestrutura, com vistas a proteger, em última instância, os titulares dos dados pessoais contra vazamentos, o que, eventualmente, compromete a própria democracia.

Nesse ponto, cabe salientar que ANPD revelar-se-á essencial no estabelecimento de balizas mais concretas para dirimir eventuais dúvidas a respeito da aplicação da LGPD. Isto é, a atuação da ANPD tem o papel de conferir concretude aos parâmetros trazidos pela LGPD.

---

[87] ICO. Data protection and coronavirus - six data protection steps for organisations. **ICO**. Disponível em: <https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-six-data-protection-steps-for-organisations/>. Acesso em 12 de nov. de 2020.

[88] ALMEIDA, Bethania de Araujo et al. Personal data usage and privacy considerations in the COVID-19 global pandemic. **Ciênc. saúde coletiva**. vol.25 supl. 1, Rio de Janeiro, 5/5/2020. Disponível em: <https://www.scielo.br/scielo.php?pid=S1413-81232020006702487&script=sci_arttext&tlng=en#B11>. Acesso em 12 de nov. de 2020.

A ANPD é uma autoridade independente, ou seja, sua atuação deve ser isolada da influência do Estado.

> A independência dessas autoridades é um atributo fundamental para que sua missão seja exitosa. Essa independência é importante não somente para a tutela do cidadão, como também para a estruturação de todo o sistema normativo de proteção de dados, que compreende aspectos da regulação do próprio fluxo de dados. Também para o setor privado uma Autoridade afigura-se como útil por diversos motivos, como manter padrões persistentes de aplicação da lei – diferentemente de tribunais, que são em geral chamados a decidir sobre situações particulares. Essa consistência, aliás, também é importante para impedir que empresas que eventualmente não cumpram com uma legislação de proteção de dados tenham vantagens competitivas em relação às demais, com prejuízo para os cidadãos.[89]

Segundo Doneda, a existência de uma autoridade administrativa para proteção de dados é uma tendência em vários ordenamentos jurídicos, pelo fato de que "os tratamentos de dados e os seus efeitos são dificilmente passíveis de serem acompanhados de forma eficaz pelo cidadão", ademais, "a necessidade de uma constante atualização em função do desenvolvimento tecnológico, entre vários outros, justificaram o recurso a esses órgãos"[90]

Ademais, como a LGPD é uma norma principiológica, a qual estabelece parâmetros gerais para o tratamento de dados pessoais, sem uma autoridade de proteção de dados incorrer-se-ia em fragmentação da interpretação da lei entre tribunais. Desse modo, centralizar a matéria em um só órgão/entidade, "garante a uniformidade dos direitos do cidadão e a segurança jurídica na aplicação da legislação de proteção de dados"[91].

Nesse sentido, a atuação da ANPD, evita uma judicialização em massa em relação à proteção de dados pessoais. Isto porque as demandas podem ser solucionadas extrajudicialmente, uma vez que a ANPD tem competência para:

> Apreciar petições de titular contra controlador após comprovação de não solução de reclamação no prazo estabelecido em regulamentação;
> Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a lei;
> Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
> Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais; e

[89] *Ibidem*. Rb-4.13.
[90] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais [livroeletrônico]: elementos da formação da Lei geral de proteção de dados**. 1. ed. -- São Paulo: Thomson Reuters Brasil, 2019. Rb-4.11.
[91] *Ibidem*. Rb-4.13.

> Editar orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à lei.[92]

Conforme trazido neste artigo, o tratamento de dados pessoais é importante para o planejamento e implementação de políticas públicas de saúde e combate à disseminação do Covid-19. Porém, sem a ANPD regulamentando procedimentos sobre esse tratamento, poderão surgir dúvidas sobre quem terá acesso a esses dados, e a quais dados, para quais finalidades e durante quanto tempo.

Se já tivesse sinto instalada, antes da pandemia, a ANPD estaria exercendo um papel fundamental, orientando gestores de órgãos/entidades públicas e empresas privadas, protegendo os dados pessoais do usuários contra utilização indevida, diminuindo a insegurança jurídica e emitindo relatórios com orientações pertinentes ao contexto do Covid-19, como as autoridades europeias e inglesas vem realizando.

Todavia, só recentemente ocorreu a nomeação dos diretores da ANPD[93]. Desse modo, se formos indicar falhas no sistema de proteção de dados, seriam o fato de os diretores terem sido indicados tardiamente e o fato de a ANPD ainda não ter tido tempo hábil de orientar pessoas jurídicas públicas e privadas, no que se refere aos conflitos advindos da pandemia.

CONSIDERAÇÕES FINAIS

O presente estudo buscou analisar o direito à proteção de dados pessoais no contexto da pandemia do Covid-19, à luz do sistema normativo brasileiro, com enfoque na Lei Geral de Proteção de dados Pessoais.

Já inicialmente foi possível verificar que garantir somente o direito à privacidade não mais satisfaz as novas demandas sociais, em face do desenvolvimento tecnológico e do consequente aumento do fluxo de dados.

Nesse sentido, antes o papel do Estado em relação ao direito à privacidade era absenteísta. Porém, na sociedade em que os dados trafegam em instantes, se exige do Estado atuação efetiva no sentido de garantir à proteção de dados pessoais.

---

[92] VAINZOF, Rony. A prorrogação das sanções da LGPD e a relevância da ANPD. **Conjur**, 12 de jun. de 2021. Disponível em: <https://www.conjur.com.br/2020-jun-12/rony-vainzof-lgpd-relevancia-anpd>. Acesso em: 19/11/2020.

[93] BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Disponível em: <https://www.in.gov.br/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226>. Acesso em: 19 de nov. de 2020.

Por outro lado, há situações excepcionais que exigem o tratamento de dados pelo poder público visando ao interesse da coletividade. Nessas circunstâncias, é preciso que o processo atenda o princípio da finalidade, dentre outros. Ou seja, a Administração Pública, ao processar dados pessoais, deve fazê-lo somente para atingir o fim público declarado e não aproveitar os dados coletados para outras finalidades, ainda que públicas, caso contrário, incorrer-se-á no risco da normalização do controle da população do Estado. Ademais, devem ser garantidas a segurança da coleta contra ataques virtuais, o que exige do Estado e que o faça as vezes, um aparato tecnológico robusto.

Quando começou a pandemia do Covid-19, a LGPD ainda não estava em vigor, embora já fosse adotada como parâmetro em decisões judiciais. Além disso, só recentemente foram nomeados os diretores da ANPD e as sanções previstas na LGPD ainda não estão em vigor. Tais fatos impedem a concretude da Lei.

Apesar disso, verificou-se que, com a sua integral vigência, diante dos riscos relacionados ao tratamento de dados pelo poder público, a LGPD é uma importante ferramenta para salvaguardar o direito em questão.

REFERÊNCIAS

ALI, Javed. **Cyber operations already impacting coronavirus response**. The Hill, 16 de março de 2020. Disponível em: <https://thehill.com/opinion/cybersecurity/487814-cyber-operations-already-impacting-coronavirus-response>. Acesso em 12 de novembro de 2020.

ALMEIDA, Bethania de Araujo et al. Personal data usage and privacy considerations in the COVID-19 global pandemic. **Ciênc. saúde coletiva**. vol.25 supl. 1, Rio de Janeiro, 5/5/2020. Disponível em: <https://www.scielo.br/scielo.php?pid=S1413-81232020006702487&script=sci_arttext&tlng=en#B11>. Acesso em 12 de nov. de 2020.

ARRUDA, maria Clara Villasbôas. O Governo do Estado de São Paulo não utiliza dados pessoais para medir aglomerações: A privacidade dos titulares de aparelhos de celular está preservada. **Migalhas**, 28 de maio de 2020. Disponível em: <https://migalhas.uol.com.br/depeso/327796/o-governo-do-estado-de-sao-paulo-nao-utiliza-dados-pessoais-para-medir-aglomeracoes--a-privacidade-dos-titulares-de-aparelhos-de-celular-esta-preservada>. Acesso em 19 nov. 2020.

BATEMAN, Tom. **Coronavirus: Israel turns surveillance tools on itself.** BBC, 11 de maio de 2020. Disponível em: <https://www.bbc.com/news/world-middle-east-52579475>. Acesso em 15 de outubro de 2020.

BRASIL. **Decreto-Lei nº 2.848 de 7/12/1940**. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 19 de novembro de 2020.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal**. Partido Socialista Brasileiro – PSB e União. Relator: Ministro Gilmar Mendes. Decisão, 24 jun. 2020. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753108946&prcID=5938693&ad=s#>. Acesso em 15 de outubro de 2020.

BRASIL. Supremo Tribunal Federal. **DIREITO CONSTITUCIONAL. DIREITO TRIBUTÁRIO. HABEAS DATA. ARTIGO 5º, LXXII, CRFB/88. LEI Nº 9.507/97. ACESSO ÀS INFORMAÇÕES CONSTANTES DE SISTEMAS INFORMATIZADOS DE CONTROLE DE PAGAMENTOS DE TRIBUTOS. SISTEMA DE CONTA CORRENTE DA SECRETARIA DA RECEITA FEDERAL DO BRASIL-SINCOR. DIREITO SUBJETIVO DO CONTRIBUINTE. RECURSO A QUE SE DÁ PROVIMENTO**. RE 673707/MG – Minas Gerais. Rigliminas Distribuidora LTDA e União. Relator: Ministro Luiz Fux. Acordão, 30 set. 2015. Disponível em: < https://jurisprudencia.stf.jus.br/pages/search/sjur322444/false>. Acesso em 26 de junho de 2020.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Conselho Federal da Ordem dos Advogados do Brasil e Presidente da República. Relator: Ministra Rosa Weber. Decisão, 24 abr. 2020. Disponível em: < http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em 6 de junho de 2020.

BRASIL. **Decreto nº 10.046 de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em 15 de outubro de 2020.

BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança., Disponível em: <https://www.in.gov.br/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226>. Acesso em: 19 nov. 2020.

BRASIL. **Medida Provisória n° 954, de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de serviço telefônico comutado e de serviço móvel pessoal com o IBGE. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619>. Acesso em 20 de junho de 2020.

BRASIL. **Proposta de Emenda à Constituição n° 17, de 2019**. Dispõe sobre a inclusão do direito à proteção de dados pessoais entre os direitos fundamentais do cidadão e sobra a fixação da competência privativa da União sobre a matéria. Disponível em:

<https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em 6 junho de 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Institui a Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 12 de abril 2020.

BRASIL. **Lei nº 13.979, de 6 de fevereiro de 2020**. Institui a Lei do Corona vírus. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Lei/L13979.htm>. Acesso em 6 junho 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 12 abril 2020.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014.** Institui o Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 12 abril 2020.

BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002.** Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em 21 abril 2020.

CAMPOS, Ricardo, MARANHÃO, Juliano. **A divisão informacional de Poderes e o Cadastro Base do Cidadão.** JOTA, 18 de novembro de 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019>. Acesso e 16 de outubro de 2020.

CISOMAG. **83% of healthcare devices at security risk due to COVID-19 outbreak**. CISOMAG. 20 de março de 2020. Disponível em: < https://cisomag.eccouncil.org/83-of-healthcare-devices-at-security-risk-due-to-covid-19-outbreak/>. Acesso em 12 de novembro de 2020.

DA REDAÇÃO. **Apple e Google se unem para rastrear e tentar conter coronavírus**. Veja, 10 de abril de 2020. Disponível em: <https://veja.abril.com.br/tecnologia/apple-e-google-se-unem-para-rastrear-e-tentar-conter-coronavirus/>. Acesso em 12 de novembro de 2020.

Data protection and coronavirus - six data protection steps for organisations. **ICO**. Disponível em: <https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-six-data-protection-steps-for-organisations/>. Acesso em 12/11/2020.

DE ARAÚJO, Priscila Maria Menezes; BANDEIRA, Natália Ferreira Freitas. **Na pandemia, é possível flexibilizar as balizas da proteção de dados pessoais?** Jota, 1 de abril de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/na-pandemia-e-possivel-flexibilizar-as-balizas-da-protecao-de-dados-pessoais-01042020>. Acesso em 14 de outubro de 2020.

DONEDA, Danilo**. Da privacidade à proteção de dados pessoais [Livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados**. 1ª ed. São Paulo, SP. Thomson Reuters Brasil, 2019.

ESTADOS UNIDOS**. Data Protection Act of 2020**. Disponível em: <https://www.congress.gov/bill/116th-congress/senate-bill/3300/text>. Acesso em 20 de junho de 2020.

FEIGELSON, Bruno et al (Coord.). **Comentários à Lei Geral de Proteção de Dados – Ed. 2020**. RB-.1.3 São Paulo: Thomson Reuters Brasil, 2020.

GAGLIANO, Pablo Stolze e PAMPLONA FILHO, Rodolfo. **Manual de direito civil**. volume único. – São Paulo, SP. Saraiva, 2017. G1. **Vazamento de dados dos hotéis Marriott pode ter afetado 500 milhões de clientes.**

G1, 31 de novembro de 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2018/11/30/vazamento-de-dados-dos-hoteis-marriott-pode-ter-afetado-500-milhoes-de-clientes-diz-a-rede.ghtml>. Acesso em 16 de outubro de 2020.

JELINEK, Andrea. **Statement on the processing of personal data in the context of the COVID-19 outbreack**. European Data Protection Board, 2020. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>. Acesso em 15 de outubro de 2020.

KAGAN, Odia. California Moves Two COVID Privacy Bills Forward. **Data Privacy**, Califórnia, 25 de ago. de 2020. Disponível em: <https://dataprivacy.foxrothschild.com/2020/08/articles/california-consumer-privacy-act/coronavirus-and-data-protection-series-part-88-california-covid-privacy-bills/>. Acesso em 12 nov. 2020.

LABBATE, Mariana. **Conheça o TraceTogether, app de monitoramento do coronavírus criado por Singapura**. Forbes, 25 de março de 2020. Disponível em: <https://forbes.com.br/negocios/2020/03/conheca-o-tracetogether-app-de-monitoramento-do-coronavirus-criado-por-singapura/>. Acesso em 14 de outubro de 2020.

LEWIS, Paul; CONN, David; PEGG, David. **UK Government using confidential patiente data in coronavirus response**. The Guardian, 12 de abril de 2020. Disponível em: < https://amp.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response?CMP=share_btn_tw&__twitter_impression=true>. Acesso em 12 de novembro de 2020.

LUIZ, Gabriel. **Banco Inter fecha acordo para pagar R$ 1,5 milhão após vazamento de dados de clientes.** G1, 19 de dezembro de 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/2018/12/19/banco-inter-fecha-acordo-para-pagar-r-15-milhao-de-indenizacao-apos-vazamento-de-dados-de-clientes.ghtml>. Acesso em 16 de outubro de 2020.

MAGALHÃES, Guilherme. **Russos resistem a mudanças de rotina enquanto governo aperta cerco contra coronavírus**. Folha de São Paulo. São Paulo, 13 de março de 2020. Disponível em: <https://www1.folha.uol.com.br/equilibrioesaude/2020/03/russos-

resistem-a-mudancas-de-rotina-enquanto-governo-aperta-cerco-contra-coronavirus.shtml>. Acesso em 14 de outubro de 2020.

MELLO, Patrícia Perrone Campos; BARROSO, Luís Roberto. **Trabalhando com uma nova lógica: A ascensão dos precedentes do direito brasileiro.** Brasília, 2016. Disponível em: <https://www.conjur.com.br/dl/artigo-trabalhando-logica-ascensao.pdf.>. Acesso em 19 de novembro de 2020.

MENDES, Laura Schertel. **TRANSPARÊNCIA E PRIVACIDADE: VIOLAÇÃO E PROTEÇÃO DA INFORMAÇÃO PESSOAL NA SOCIEDADE DE CONSUMO.** Disponível em <http://dominiopublico.mec.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em 25 de junho de 2020.

MENDES, Gilmar ferreira e BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 1. ed. rev. e atual. – São Paulo, SP. Saraiva, 2015.

MIGALHAS. A efetividade da anonimização de dados pessoais. **Migalhas**, 31 de janeiro de 2020. Disponível em: <https://migalhas.uol.com.br/coluna/impressoes-digitais/319519/a-efetividade-da-anonimizacao-de-dados-pessoais>. Acesso em 15 de outubro de 2020.

PIERUCCI, Alessandra, WALTER, Jean Philippe. The Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe recall the principles of data protection in these times of fight against the COVID-19 pandemic. **COE.INT**, Estrasburgo, 30 de mar. de 2020. Disponível em: <https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter>. Acesso em 12/11/2020.

PRESSE, France. **British Airways é multada em US$ 230 milhões por caso de roubo de dados de passageiros**. G1, 8 de julho de 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/07/08/british-airways-e-multada-em-us-230-milhoes-por-caso-de-roubo-de-dados-de-passageiros.ghtml>. Acesso em 16 de outubro 2020.

REQUIÃO, Maurício. **Covid-19 e proteção de dados pessoais: o antes, o agora e o depois**. Conjur, 5 de abril de 2020. Disponível em: <https://www.conjur.com.br/2020-abr-05/direito-civil-atual-covid-19-protecao-dados-pessoais-antes-agora-depois#sdfootnote9anc>. Acesso em 15 de outubro de 2020.

ROSSI, Marina. **Brasil multa Facebook em 6,6 milhões de reais pelo vazamento de dados no caso Cambridge Analytica**. El País. São Paulo, 30 de dezembro de 2019. Disponível em: <https://brasil.elpais.com/tecnologia/2019-12-30/brasil-multa-facebook-em-66-milhoes-de-reais-pelo-vazamento-de-dados-no-caso-cambridge-analytica.html>. Acesso em 16 de outubro de 2020.

SCHREIBER, Mariana. **Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua privacidade?** BBC, 21 de abr. de 2020. Disponível em: <https://www.bbc.com/portuguese/brasil-52357879>. Acesso em 14 de outubro de 2020.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de dados Pessoais no Direito Brasileiro.** Ed 2019. São Paulo, SP. Thomson Reuters Brasil, 2019.

VAINZOF, Rony. A prorrogação das sanções da LGPD e a relevância da ANPD. **Conjur**, 12 de jun. de 2021. Disponível em: <https://www.conjur.com.br/2020-jun-12/rony-vainzof-lgpd-relevancia-anpd>. Acesso em: 19/11/2020.

VALENTE, Jonas. **Covid-19: iniciativas usam monitoramento e geram preocupações.** Agência Brasil, 12 de abril de 2020. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/covid-19-iniciativas-usam-monitoramento-e-geram-preocupacoes>. Acesso em 20 de junho de 2020.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right to privacy nos Estados Unidos. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 22, n. 5130, 18 jul. 2017. Disponível em: <https://jus.com.br/artigos/57228>. Acesso em: 22 de agosto de 2020.