



**BREVES CONSIDERAÇÕES À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)  
E SUA CONSONÂNCIA COM O DIREITO FUNDAMENTAL À SAÚDE  
EM TEMPOS DA PANDEMIA DO NOVO CORONAVÍRUS.**

*Jarli Cardoso Alves<sup>1</sup>*

**RESUMO:**

O presente artigo acadêmico apresenta um estudo sobre a nova Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD). O objetivo é traçar um alinhamento entre o direito de proteção de dados pessoais, afinado à inviolabilidade da privacidade, e os direitos de proteção da vida e da saúde pública considerando o contexto atual da pandemia causada pelo Coronavírus/COVID-19. As considerações deste trabalho levam em conta o movimento global de estruturação de mecanismos tecnológicos de controle e combate à disseminação da doença. A reflexão converte-se, ao final, no reconhecimento de que o efetivo cumprimento da nova legislação protetiva de dados pessoais, em tempos de pandemia, contribui significativamente com o aperfeiçoamento contínuo de preservação dos direitos fundamentais inerentes à privacidade dos indivíduos.

**Palavras chaves:** Lei Geral de Proteção de Dados. Globalização e Tecnologias de Informação. Direito à Privacidade. Direito à Saúde. Pandemia.

**BRIEF CONSIDERATIONS TO THE GENERAL DATA PROTECTION LAW (LGPD)  
AND ITS INLINE WITH THE FUNDAMENTAL RIGHT TO HEALTH  
IN TIMES OF THE PANDEMIC OF THE NEW CORONAVIRUS.**

**ABSTRACT:**

This academic work presents a study on the new General Data Protection Law (Law N. 13.709/2018 – LGPD). It seeks to draw an alignment between the right of protection of personal data, in tune to the inviolability of privacy, and the rights of protection of life and public health.

---

<sup>1</sup> Bacharelada em Direito pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP/Brasília - DF. Especialista em Gestão Pública. Graduada em Letras – Português/Inglês pelo Centro de Ensino Unificado de Brasília – CEUB.



This work takes to consideration the current context of the pandemic caused by the new Coronavirus / COVID-19 and takes into account the global movement of structuring technological mechanisms to control and combat the spread of the disease. The reflection is converted, eventually, in the recognition that the effective compliance with the new legislation protecting personal data, in times of pandemic, contributes significantly to the continuous improvement of preservation of the privacy related fundamental rights of individuals.

**Keywords:** General Data Protection Act. Globalization and Information Technologies. Right to Privacy. Right to Health. Pandemic.

## 1. INTRODUÇÃO

A globalização política dos Direitos Fundamentais, relacionados à perspectiva de novas democracias, remete-se aos direitos de quarta geração, teoricamente defendidos por Bonavides (2014), e representa sua universalização no campo institucional, tendo como base a globalização na esfera da normatividade jurídica e da institucionalização do Estado Social. Representam, dessa forma, a dimensão máxima da universalidade, a concretização da sociedade do futuro, aberta a todas as relações de convivência materialmente possíveis em face dos avanços da tecnologia de comunicação, do acesso às informações e do pluralismo de sistemas – direitos paralelos e coadjuvantes da Democracia.

Nesse sentido, o Regime Jurídico de Proteção de Dados normalmente adotado em países diversos advém, em sua maioria, de proteção constitucional por tratar de direito fundamental que garante a seu titular o estabelecimento de limites no tratamento de seus dados pessoais. A cobertura constitucional justifica-se como salvaguarda à privacidade do indivíduo, direito fundamental correlato à proteção de dados.

No contexto brasileiro, a inclusão da proteção de dados pessoais como direito fundamental tramita no Senado Federal mediante a Proposta de Emenda à Constituição nº 17/2019. A PEC pretende não apenas o reconhecimento do direito no art. 5º da Magna Carta, como também sua inclusão como matéria de competência legislativa privativa da União, no art. 22<sup>2</sup>. As alterações



buscam sedimentar a importância do tema, além de garantir a unificação das regras praticadas pelos diferentes entes federativos, tornando-as únicas e harmônicas.

Quanto à padronização das regras brasileiras, foi consolidada, no ano de 2018, a Lei Geral de Proteção de Dados – LGPD<sup>3</sup>, que, no último dia 18 de setembro de 2020, depois de muitas discussões e adiamentos, passou a vigorar em todo o território nacional.

Além da unificação das normativas sobre o uso de dados pessoais, a LGPD procura ajustá-las ao contexto mundial, tornando o Brasil apto a processar dados oriundos de outros países, e atendendo, dessa forma, a normativas internacionais que exigem níveis de proteção de extremas eficácia e eficiência e, concomitantemente, oferecendo maior flexibilidade ao tratamento de dados pessoais ao dispor acerca de regras claras sobre sua adequada coleta, armazenamento, tratamento e compartilhamento por empresas, sem deixar de prover o direito constitucional à privacidade, permitindo, assim, um maior controle por meio de práticas transparentes e seguras.

Outro ângulo a ser abordado no estudo em tela atenta-se ao conteúdo do anúncio da Organização Mundial da Saúde - OMS, no dia 11 de março de 2020, relacionado à atual situação de pandemia vivenciada pela disseminação da covid-19, mais conhecida como novo coronavírus. O mundo contemporâneo acometido por escalada vertiginosa de surto originado na cidade chinesa de Wuhan, que afetou diretamente o estilo e rotina de vida de indivíduos em diversas nações e ampliou as discussões acerca do tratamento de informações pessoais.

Ressalta-se que o principal fator que caracteriza uma pandemia é o geográfico, ou seja, quando certificado que todas as pessoas do mundo possam estar sujeitas à infecção. Por essa razão, à época atual, a humanidade vivencia uma globalização do compartilhamento de dados em escala sem precedentes, protagonizada por atores políticos e agentes econômicos que atuam sob a justificativa e escopo único de oferecer resistência ao processo de disseminação da doença, em prol do bem maior.

A vigilância otimizada e exercida de forma célere passou a ser alternativa de gerenciamento de riscos que o atual cenário exige. Entretanto, com a utilização de novas

---

<sup>2</sup> “Art. 1º Inclua-se no art. 5º, da Constituição Federal, o seguinte inciso: XII-A – é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais.” e “Art. 2º Inclua-se no art. 22, da Constituição Federal, o seguinte inciso: XXX- proteção e tratamento de dados pessoais.”

<sup>3</sup> Lei nº 13.709/2018



tecnologias, a vigilância intrusiva, com foco no monitoramento da pandemia, também pode tornar-se mecanismo expandido para funções obscuras, de ética questionável quanto à real finalidade do tratamento de dados por gestores públicos e privados.

## 2. ASPECTOS RELEVANTES SOBRE A LEI n° 13.709/2018 – LGPD

No contexto brasileiro, o processo público e legislativo que resultou na criação da Lei Geral de Proteção de Dados originou-se a partir de uma consulta pública do Ministério da Justiça e teve, durante sua tramitação no Congresso Nacional, a contribuição de mais de 2.500 atores nacionais e internacionais e de vários setores envolvidos (PL 5276/2016, renumerada para PLC 53/2018<sup>4</sup>).

O novo regramento traz maior segurança jurídica à privacidade e ao uso dados pessoais nos setores privados e públicos, visando não somente a proteção do direito fundamental, bem como o fomento ao desenvolvimento econômico, tecnológico e de inovação, com foco no uso de regras claras, amplas e transparentes sobre o levantamento, compartilhamento, tratamento e armazenamento de dados.

Vários fatores compeliram o governo brasileiro a se adaptar ao contexto de unificação das regras sobre o uso de dados pessoais, devido à contemporaneidade e extraterritorialidade em tempos de “*big data*”<sup>5</sup>, flexibilizando seu tratamento e procurando contribuir significativamente no setor de tecnologia da informação (MONTEIRO, 2020).

Dentre muitos, vale destacar a Regulação Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR) que cria obstáculos para a transferência de dados pessoais a países que não possuem sistema de proteção de dados considerado adequado. Normativa que, apesar de ser uma lei da União Europeia, interfere consideravelmente no âmbito comercial e

---

<sup>4</sup> Projeto de Lei Complementar que tem o propósito de atender as orientações acerca da proteção de dados contidas na General Data Protection Regulation (GDPR), Lei de Proteção de Dados da União Europeia, instituída em 25.05.2018.

<sup>5</sup> Armazenamento de dados significativos em grande volume, estruturados ou não estruturados e disponibilizados a uma velocidade incrível, que podem ser utilizados para os mais variados fins, em conformidade com o interesse e área de mercado a que se destinam de forma que o empreendedor/interessado consiga identificar os melhores investimentos. Fundamentos norteadores: volume, variedade, velocidade, veracidade e valor.



econômico, tendo sua eficácia para além dos limites geográficos do velho continente, afetando, portanto o cenário brasileiro (MONTEIRO, 2020).

Outro fator importante a ser considerado trata-se da necessidade de o Brasil adequar-se às regras estabelecidas pela Organização para a Cooperação e o Desenvolvimento Econômico – OCDE, organismo internacional que busca possibilidades de gestão pública com foco na promoção do desenvolvimento econômico voltado para a sustentabilidade e estabilidade financeira dos governos participantes, a partir de informações contidas em sua base de dados, com a finalidade de pleitear sua entrada no organismo internacional (idem).

## **2.1 PROTEÇÃO DE DADOS PESSOAIS E DIREITOS FUNDAMENTAIS DIRETAMENTE RELACIONADOS.**

Com o advento do desenvolvimento desmensurado das novas tecnologias de informação, a atuação do Estado tornou-se essencial para a proteção do indivíduo enquanto detentor de direitos. Assim, quando se trata de proteção de dados, o objetivo é proteger o titular dos dados e não os dados por si só.

Por dado entende-se informação em potencial, definido sobre o prisma da LGPD (art. 5º, I a III) em três dimensões: dado pessoal e dado pessoal sensível, ambos identificáveis, e dado anonimizado, não identificável (não alcançado pela normativa).

Outrossim, tendo em conta o propósito da presente reflexão, vale destacar o art. 13 da LGPD que inclui a pseudomização de dados como instrumento alternativo na realização de estudos em saúde pública. Por pseudomização de dado entende-se pela não possibilidade de associação, direta ou indiretamente, de um dado a um indivíduo, pelo uso de informação adicional/suplementar mantida pelo controlador em ambiente controlado e seguro (§ 4º), gerando redução de riscos a seus titulares.

A redução de riscos é fator primordial quando se trata de direito à proteção de dados (direito coletivo a ser fiscalizado pelo Estado), considerando que diretamente ligada à proteção do direito à privacidade (direito individual e negativo<sup>6</sup>) que diz respeito ao direito de escolha do



indivíduo em esconder ou revelar aquilo que acredita, pensa e possui, solidificado no Diploma Civil brasileiro (art. 21, CC)<sup>7</sup>.

Por outro lado, em relação complementar ou limitante ao direito à proteção de dados, a depender da situação fática, o texto constitucional brasileiro garante o direito de acesso à informação (art. 5º, XXXIII). Esse direito é essencial à democracia que impõe arcabouço de normas como dever de prestação por parte do Estado, concentrado no dever de dar transparência a seus atos, ou seja, franquia a informação ao cidadão, sendo que tudo que é produzido tem que ser publicizado. A publicidade é sempre a regra e o sigilo será sempre a exceção (Exemplo: informações imprescindíveis à segurança do Estado). Essa mudança de paradigma estabelece punição a quem não franqueia a informação<sup>8</sup>.

Nesse sentido, a Lei de Acesso à Informação – LAI (BRASIL, 2011) traz diretrizes à administração pública, dentre elas a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso (art. 6º, III) e, atendendo à temática do estudo, orientações quanto ao tratamento de “informações pessoais” (art. 31), trazendo como hipóteses de divulgação, ou acesso por terceiro, apenas mediante previsão legal ou mediante consentimento expresso (inciso II, restrição ao acesso) – consistente com limitação de natureza privada (direito de privacidade).

Acentua-se, por último, que o mesmo dispositivo, em seu Art. 31, § 3º, faz previsões de exceções à necessidade de consentimento do titular da informação pessoal, em se tratando de referências necessárias, a constar:

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. (...)  
§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

---

<sup>6</sup> Prerrogativa expressa no texto constitucional em seu art. 5º, 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; (...)

<sup>7</sup> O artigo estabelece mecanismo de proteção, obrigação de fazer ou não fazer, ao lado da responsabilidade civil. Código Civil: “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.”

<sup>8</sup> CF/88: art 5º, inciso LX; art. 37, caput; e art. 93, incisos IX e X.



- I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
- II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; (...) (BRASIL, 2011, s/p).

## 2.2 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Para fins de supervisão da adequada aplicação da lei, em caráter coletivo de proteção de dados, a LGPD cria a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República, autônomo e independente, que deverá funcionar nos moldes de uma agência reguladora, devendo ficar responsável por fiscalizar o tratamento de dados, regular matérias e aplicar sanções. Esse dispositivo estabelece, dessa forma, diretrizes para a promoção da proteção de dados pessoais no Brasil, por intermédio da implementação de uma Política de Proteção de Dados e da Privacidade.

Integrando a própria estrutura da ANPD, o Conselho Nacional de Proteção de Dados Pessoais e Privacidade consiste em órgão consultivo multissetorial (art. 58), composto por 23 representantes, que tem o propósito de propor diretrizes para a elaboração e acompanhamento da execução da política de proteção de dados, bem como promover estudos/pesquisas e audiências públicas, e propor ações, inclusive aquelas voltadas à transmissão de conhecimentos, na intenção de conscientizar a população acerca de seus direitos à proteção de dados e à privacidade.

Vale ressaltar que a ANPD, como uma das atribuições mais importantes, deverá dispor sobre padrões técnicos mínimos voltados aos de segurança estabelecidos pelos princípios do “*Privacy by Design*”<sup>9</sup> e do “*Privacy by Default*”<sup>10</sup>, de observância obrigatória aos agentes

---

<sup>9</sup> A LGPD recepciona o princípio do “*Privacy by Design*” (art. 46, § 2º) que traduz-se na incorporação de ferramentas de privacidade desde o momento da criação do código, como a finalidade de proteção durante toda sua existência, com foco não só na adoção de medidas que previnam, garantam e comuniquem todas as possibilidades de riscos ao titular dos dados, como também no desenvolvimento de sistemas conforme a necessidade e interesse do usuário.

<sup>10</sup> O princípio do “*Privacy by Default*” (art. 55-J, inciso VIII) configura como um decurso do “*Privacy by Design*”. Diz respeito ao dever de configuração de privacidade o mais restrito possível, em relação à coleta de dados pessoais a ser realizada por aplicativos (por padrão). Aplicado, por exemplo, em se tratando de oferta de produtos e serviços aos titulares que poderão autorizar a coleta de dados extra, caso julguem necessário. Ou seja, reproduz a obrigação de que



envolvidos diretamente nos tratamentos de dados pessoais (controlador, operador e encarregado)<sup>11</sup>, sejam de natureza pública ou privada, podendo os titulares flexibilizá-los a seu conteúdo ou entendimento próprio.

### **2.3 A LEI GERAL DE PROTEÇÃO DE DADOS E O TRATAMENTO DE DADOS RELATIVOS À SAÚDE.**

No Brasil, aplica-se a dimensão positiva do direito fundamental à saúde, direito subjetivo do cidadão que pode exigir de qualquer esfera da organização federativa brasileira, solidariamente ou por meio de uma ação judicial, o efetivo fornecimento de acompanhamento e/ou tratamento médico, ou de qualquer outro meio de proteção à saúde do indivíduo, impossibilitando ao poder público demonstrar-se indiferente<sup>12</sup>.

Segundo a LGPD, além das finalidades que autorizam a manipulação de dados pessoais com foco na tutela da saúde, inerentes à rigorosa manutenção dos direitos e garantias fundamentais e princípios e regras aplicáveis, a utilização dos dados só poderá ser realizada por profissionais da área de saúde ou autoridade sanitária e para serviços inerentes às áreas, não podendo ser utilizado tendo como objetivo a obtenção de vantagem econômica pela área privada<sup>13</sup>.

---

o serviço ou produto a ser ofertado se adequa a todas as coberturas e reservas que foram concebidas durante o seu desenvolvimento, de forma que informações além daquelas necessárias devam ser previamente liberadas pelo usuário do serviço.

<sup>11</sup> “Art. 5º Para os fins desta Lei, considera-se: (...) 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; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (...)” (BRASIL, 2018, s/p).

<sup>12</sup> “O caráter programático da regra inscrita no art. 196 da Carta Política - que tem por destinatários todos os entes políticos que compõem, no plano institucional, a organização federativa do Estado brasileiro - não pode converter-se em promessa constitucional inconsequente, sob pena de o Poder Público, fraudando justas expectativas nele depositadas pela coletividade, substituir, de maneira ilegítima, o cumprimento de seu impostergável dever, por um gesto irresponsável de infidelidade governamental ao que determina a própria Lei Fundamental do Estado” (BRASIL, 2000, s/p).

<sup>13</sup> Nesse sentido, o art. 11, § 5º da Lei veta, categoricamente, o emprego dos dados para seleção de riscos por operadoras de planos de saúde, a exceção de sua utilização em benefício dos interesses dos titulares (§ 4º), e para permitir a portabilidade, quando solicitada pelo titular (§ 4º, I), e para transações financeiras e administrativas resultantes do uso e da prestação de serviços de saúde, de assistência farmacêutica ou de assistência à saúde (§ 4º, II).



Preliminarmente, é essencial que se proceda à distinção entre dados relativos à saúde do indivíduo que podem, de forma prejudicial, serem usados para discriminar pessoas, e dados do indivíduo para finalidades relacionadas à saúde, havendo, portanto, que se diferenciar a natureza do dado e a finalidade de seu tratamento.

As principais preocupações de proteção de dados pessoais referentes à saúde dizem respeito a não discriminação e à manutenção das oportunidades sociais. Em atenção a esse imperativo, a LGPD confere grau de proteção especial, ao tratar as informações relativas à saúde como dados pessoais de natureza sensível, submetidos a regime limitado de tratamento, especialmente em relação ao consentimento ou não do titular dos dados. Ou seja, o regime adotado para a saúde pela LGPD depreende que os dados sejam utilizados para a consecução de sua finalidade, exigindo coerência entre a natureza do dado e o respectivo emprego, de forma que não sujeite o seu titular a práticas discriminatórias.

Isso posto, por dados sensíveis, expressos no art. 5º, II<sup>14</sup> da Lei, compreende-se aqueles que devem ser tratados de forma diferenciada, primando por sua segurança e com bases legais distintas, tais como o consentimento específico<sup>15</sup> (expresso e informado) do titular em determinados casos, tendo em conta a possibilidade do acesso de terceiros (alheios ao titular) a dados suscetíveis de mau uso.

### **3. A CONCILIAÇÃO ENTRE PROTEÇÃO À VIDA, SAÚDE PÚBLICA E A PROTEÇÃO DE DADOS PESSOAIS EM TEMPOS DA PANDEMIA DO NOVO CORONAVÍRUS.**

Em que pese o dever-poder do Estado à prestação do direito fundamental à saúde e à proteção da vida, a coleta e manipulação de dados sob essas perspectivas não exime os entes

---

<sup>14</sup> “Art. 5º, II - Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (...)” (BRASIL, 2018, s/p).

<sup>15</sup> “Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: (...) f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (...)” (BRASIL, 2018, s/p).



públicos de atuarem no exercício do pleno respeito ao Estado Democrático de Direito, devendo primar, também, pelo direito do cidadão à sua privacidade.

Entretanto, como observado anteriormente, a LGPD sobrepõe a imposição do tratamento de dados sensíveis sem o consentimento do indivíduo (art. 11) à inviolabilidade da privacidade de dados, ao prever casos específicos em que o consentimento não é considerado requisito absoluto, tais como: “(i) ser necessário à execução de políticas públicas; (ii) para a proteção da vida ou da incolumidade física do titular ou de terceiro; e, principalmente, (iii) para a tutela da saúde”.

Esta anteposição, contrária às normas de confidencialidade e sigilo, encontra legitimidade em situações de emergência ou de interesse humanitário, de forma que a utilização dos dados pessoais seja pontual e tenha o propósito literal de conter ou minimizar os riscos à saúde e proteger a vida humana, e que ocorra minimamente, priorizando sempre que possível a anonimização e pseudonimização dos dados.

### **3.1 A PROTEÇÃO DE DADOS E SUA INFLUÊNCIA NAS MEDIDAS TECNOLÓGICAS UTILIZADAS NA CONTENÇÃO DA DOENÇA.**

A China, país que identificou o primeiro caso causado pelo vírus, adotou aplicativo que cruza dados da Comissão Nacional de Saúde, do Ministério dos Transportes e da Agência de Aviação Civil para identificar pessoas que estiveram em contato com outras infectadas ou com suspeita, com o propósito de se antecipar à disseminação do vírus por meio do mapeamento, rastreamento e notificação prévia a possíveis infectados, traduzindo-se em forma eficaz de controle do avanço da doença na população (CARBINATTO, 2020).

A medida de vigilância digital, embora pareça excessiva, pois limitou a circulação de infectados, reconstruindo suas rotas de forma impositiva, foi estabelecida em consonância com os princípios e diretrizes pautadas na legislação chinesa como o Regulamento de Segurança das Informações Pessoais e nas leis de Cibersegurança e de Criptografia.

Atualmente, os diferentes graus de vigilância adotados por diversas nações, como medida de contenção da pandemia causada pela disseminação pela covid-19, trazem questões importantes



pertinentes à privacidade de dados pessoais e como esses são tratados. Nesse contexto, é evidente a importância do uso de dados pessoais para a elaboração de políticas públicas voltadas para a contenção do vírus, mas sempre se atendo à finalidade de sua utilização para que não sejam utilizados de forma que ofenda direitos fundamentais do cidadão.<sup>16</sup>

Antes de os entes governamentais pensarem em tecnologias de monitoramento que interagem e interferem diretamente no tratamento de dados pessoais, acobertados pelo interesse público diante da grave ameaça à população, faz-se necessário que sejam cumpridos altos padrões de segurança da informação e da proteção de dados desde o momento da colheita até a sua exclusão da base de dados (*Privacy by Design*). A possibilidade de o ente público captar dados sem autorização da população deve ser analisada rigorosamente sob aspectos importantes tais como: o que deve ser coletado, como e por quem deve ser coletado, de forma a evitar danos irreparáveis à sociedade.

Outra conjectura a ser observada diz respeito aos estudos e pesquisas realizados por pessoas jurídicas de direito privado, como os realizados por universidades privadas e laboratórios farmacêuticos, na intenção de ampliar o conhecimento sobre o vírus e suas especificidades, na busca por medicamentos e vacinas que possam contribuir no combate a epidemias. A LGPD impõe que a manipulação de dados pessoais seja estritamente realizada para o fim proposto, uma vez que à entidade privada será permitido o acesso não somente relacionados à própria existência da contaminação do indivíduo pelo vírus, como também a outras enfermidades e históricos de saúde, para a efetiva contribuição à compreensão do desenvolvimento da doença.

Em âmbito internacional, pode-se citar como exemplo os estudos realizados pela Verity (holding do Google), organização de pesquisa que se dedica aos estudos das ciências da vida (SATO, 2020). O acesso da plataforma Google aos dados obtidos de testes de covid-19 foi questionado em relação à sua real utilização: se necessariamente destinados à supressão da doença e ao benefício e assistência às entidades públicas.

Contanto que conduzidas as atividades na busca do bem comum e dentro das práticas exigidas, internacionalmente, de padrão de segurança de proteção de dados pessoais, respaldada

---

<sup>16</sup> O “*General Data Protection Regulation*” (GDPR) consente que autoridades sanitárias processem dados pessoais no contexto de epidemia desde que respeitadas a legislação de cada país-membro.



pela situação de emergência frente à crise de saúde pública mundial, não obsta empecilho à empresa de tecnologia, considerando que muitos dos órgãos governamentais não possuem mecanismo ou sofisticação técnica equiparável com o de uma empresa como a Google (SATO, 2020).

No cenário brasileiro, recentemente, dados de 16 milhões de brasileiros diagnosticados com Covid-19 ou que tiveram suspeita da doença foram expostos em uma plataforma da internet, em vazamento do Ministério da Saúde, devido a um descuido de segurança que tornou públicas as senhas de acesso a bancos de dados epidemiológicos, desenvolvido para fins de análise preditiva da pandemia. Os bancos de dados expostos continham, além de registros de CPF(s) e endereços, informações de natureza privada particular, tais como históricos médicos pessoais (CAMBRICOLI, 2020).

A observância das normas protetivas, em especial por aqueles que tratam diretamente as informações de saúde pessoal, é fundamental, visto que o vazamento de dados pessoais ou sua utilização de forma ilícita ou imprópria, além de abrir espaço para tratamentos discriminatórios, podem colocar em risco a reputação e mesmo a própria saúde física ou mental de seus titulares.

Desde a decretação de estado de calamidade pública, acompanha-se rotineiramente divulgações ao público, realizadas pelo Ministério da Saúde e/ou Institutos de Pesquisa paralelos, de números de infectados e mortos em decorrência do coronavírus, considerando os casos relatados por localidades e regiões, sem que, de alguma forma, sejam repassadas informações específicas que possam de alguma forma servir para identificar os indivíduos envolvidos.

Embora a pessoa infectada não possa se opor ao compartilhamento de seu nome e demais informações, o Ministério da Saúde, em consonância aos princípios defendidos pela LGDP, pode compartilhar tais informações, por objetivarem instruir a população para que possam adotar medidas de segurança, como o buscar seu próprio diagnóstico, ou mesmo medidas preventivas, como a prática de isolamento social, porém sem se descuidar de que sejam apresentadas de forma anônima ou pseudonimizadas.

Outro episódio questionável diz respeito ao anúncio do Ministério da Ciência e Tecnologia, realizado no mês de abril de 2020, envolvendo a celebração de acordo entre o Governo Executivo Federal e cinco operadoras de telefonia de grande porte destinado a



possibilitar o acesso a dados de geolocalização extraídos de aparelhos celulares dos particulares, sem seu consentimento, para fins de monitoramento do deslocamento da população durante o período de pandemia. Essa medida foi posteriormente declinada pelo próprio governo federal (SCHREIBER, 2020).

Não obstante o contexto epidemiológico, tal medida extremada de vigilância em massa, mas também adotada por outros países democráticos, poderia ser melhor executada se desenvolvida de forma mais segura, sob o conglomerado de deveres jurídicos já dispostos na Lei Geral de Proteção de Dados<sup>17</sup>, ainda não vigente à época, que impõem parâmetros seguros e transparentes sobre o que pode e o que não pode ser praticado em relação ao tratamento de dados pessoais, sob a ótica da proteção à privacidade.

Como último exemplo, outra providência adotada pelo governo brasileiro diz respeito à edição da Medida Provisória nº 954 de 17/04/2020, que liberava o compartilhamento de dados não anonimizados, de tratamento das empresas de telefonia fixa e móvel, com o Instituto Brasileiro de Geografia e Estatística (IBGE). Observa-se que a normativa não definia como ou para que finalidade os dados coletados seriam utilizados ou mesmo mecanismos técnicos de segurança que pudessem ser implementados, consistente com a consolidação de vigilância desmedida que poderia trazer legitimidade ao governo federal de, por exemplo, rastrear rivais políticos ou membros de grupos minoritários (ARAÚJO; BANDEIRA, 2020).

Devida a ausência de comprovação de interesse público legítimo e ao não oferecimento de condições para avaliação da real necessidade, adequação e proporcionalidade da medida, o Supremo Tribunal Federal decidiu suspender a medida, referendando pedido de liminar contido em Ação Direta de Inconstitucionalidade, ajuizada pela Ordem dos Advogados do Brasil – OAB (ADI nº 6387/MC DF)<sup>18</sup>.

---

<sup>17</sup> Ainda não vigentes devido à aprovação do Senado Federal pelo adiamento da vigência da Lei para o mês de agosto de 2021, tendo como principal argumento, questão levantada por pesquisas, indicando que a grande maioria das empresas brasileiras ainda não estão preparadas para atender às exigências da LGPD e que as medidas de isolamento adotadas em razão da atual pandemia contribuíram para dificultar o atendimento das exigências impostas pela normativa.

<sup>18</sup> “Nesse contexto, e a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel, com o caráter precário próprio aos juízos perfunctórios e sem prejuízo de exame mais aprofundado quando do julgamento do mérito, defiro a medida cautelar requerida, ad referendum do Plenário desta Suprema Corte, para suspender a eficácia da Medida Provisória n. 954/2020” (BRASIL, 2020, s/p).



Por conseguinte, considerando os exemplos das situações supramencionadas, evidencia-se que a legítima segurança jurídica destinada ao tratamento de dados, em atenção às exigências da “*General Data Protection Regulation*” (GDPR), somente será exequível se decorrente de normativa (LGPD) que proporcione base legal e legitimidade para que a manipulação de dados no atual contexto de pandemia causada pelo coronavírus seja estritamente voltada para essa finalidade (Danilo Doneda)<sup>19</sup>.

#### 4. CONSIDERAÇÕES FINAIS

O papel da proteção de dados em epidemiologias ou em calamidades envolvendo questões de saúde pública tem justificado a prática de adoções tecnológicas por entes públicos e privados, desde que sejam utilizadas com o propósito de favorecer o engajamento de pesquisas e estudos, voltados para restauração da segurança e saúde da coletividade, e sem que haja o exercício arbitrário do poder de vigilância em detrimento da privacidade do indivíduo.

Nesse sentido, a observância das normas protetivas, em especial por aqueles que tratam diretamente as informações de saúde pessoal, é fundamental, considerando que o vazamento de dados pessoais ou sua utilização de forma ilícita ou imprópria, além de abrir espaço para tratamentos discriminatórios, podem colocar em risco a reputação e mesmo a própria saúde física ou mental de seus titulares.

Os diferentes graus de vigilância adotados por diversas nações, como medida de contenção da pandemia causada pela disseminação da covid-19, trazem questões importantes pertinentes à privacidade de dados pessoais e como esses são tratados. Nesse contexto, é evidente a importância do uso de dados pessoais para a elaboração de políticas públicas voltadas para a contenção do vírus, mas sempre se atendo à finalidade de sua utilização para que não sejam utilizados de forma que ofenda direitos fundamentais do cidadão.<sup>20</sup>

---

<sup>19</sup> “Estando a proteção de dados vocacionada à proteção do cidadão, a sua disciplina compreende dispositivos capazes de legitimar a utilização de seus dados pessoais em situações nas quais o seu interesse ou o da sociedade é prioritário, como ocorre em situação como a que estamos passando.” (DONEDA, 2020, s/p).

<sup>20</sup> O “*General Data Protection Regulation*” (GDPR) consente que autoridades sanitárias processem dados pessoais no contexto de epidemia desde que respeitadas a legislação de cada país-membro.



Em conclusão, além da adequação do cenário brasileiro à perspectiva das “novas democracias”, a abertura da vigência da LGPD consiste em episódio de extremo interesse público, tendo em conta a vultosa quantidade de manipulação nacional e internacional de dados pessoais em tempos de disseminação generalizada do vírus denominado covid-19, em especial consideração aos dados sensíveis, traduzindo-se como legislação imprescindível para a garantia da seguridade de informações inerentes à intimidade do indivíduo, durante e pós fase pandêmica, consolidando-se como instrumento de restrição a eventuais danos ao direito à privacidade, compreendido como fundamental pela Magna Carta de 1988.

## REFERÊNCIAS

ARAÚJO, Maria Menezes de; BANDEIRA, Natália Ferreira Freitas. Na Pandemia é possível flexibilizar as balizas da proteção de dados pessoais? Jota, 01 de jun. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/na-pandemia-e-possivel-flexibilizar-as-balizas-da-protecao-de-dados-pessoais-01042020>. Acessado em 05 de jun. de 2020.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. Malheiros Editores LTDA. 29ª Edição. São Paulo/2014.

BRASIL. Supremo Tribunal Federal. AGR. no recurso extraordinário nº 271.286-8. Paciente: Cândida Silveira Saibert e outros. Relator: Ministro Celso de Melo. Rio Grande do Sul, 12 de set. de 2000. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=335538>. Acessado em 02 de jun. de 2020.

BRASIL. Presidência da República. Casa Civil. Subchefia para assuntos Jurídicos. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Brasília, 2002.

BRASIL. Presidência da República. Casa Civil. Subchefia para assuntos Jurídicos. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Brasília, 2011. Disponível em:



[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm). Acessado em 03 de jun. de 2020.

BRASIL. Constituição da República Federativa do Brasil : texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nos 1 a 6/94, pelas Emendas Constitucionais nos 1/92 a 91/2016 e pelo Decreto Legislativo no 186/2008. – Brasília : Senado Federal, Coordenação de Edições Técnicas, 2016.

BRASIL. Presidência da República. Casa Civil. Subchefia para assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília, 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm). Acessado em 01 de jun. de 2020.

BRASIL. Supremo Tribunal Federal. Medida cautelar na ação direta de Inconstitucionalidade 6387. Paciente: Marcos Vinícius Furtado Coelho e outros. Relatora: Ministra Rosa Weber. Brasília, 24 de abr. de 2020. Disponível em: <https://www.conjur.com.br/dl/adi-6387.pdf>. Acessado em 02 de jun. de 2020.

CAMBRICOLI, Fabiana. Vazamento de senha do ministério expõe dados de 16 milhões de brasileiros. UOL, 26 de fev. de 2020. Disponível em: <https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2020/11/26/vazamento-de-senha-do-ministerio-expoe-dados-de-16-milhoes-de-pacientes-de-covid.htm>. Acessado em 01 de jun. de 2020.

CARBINATTO, Bruno. China está usando tecnologias de vigilância em massa para combater coronavírus. Super Interessante, 25 de mar. de 2020. Disponível em: <https://super.abril.com.br/tecnologia/china-esta-usando-tecnologias-de-vigilancia-em-massa-para-combater-coronavirus/>. Acessado em 05 de jun. de 2020.

DAMO, Paola Salvatori. Pandemia do novo coronavírus à luz da lei geral de proteção de dados. Migalhas, 14 de abr. de 2020. Disponível em: <https://www.migalhas.com.br/depeso/324507/pandemia-do-novo-coronavirus-a-luz-da-lei-geral-de-protecao-de-dados>. Acessado em 01 de jun. de 2020.



DONEDA, Danilo. A proteção dos dados em tempos de coronavírus. Jota. 25 de mar. de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020>. Acessado em 02 de jun. de 2020.

MALDONADO, Viviane Nóbrega. LGPD – **Lei Geral de Proteção de Dados – Manual de Implementação**. Editora Revista dos Tribunais / RT. 1ª Edição. São Paulo/2018.

MARQUES, Natália. Lei geral de proteção de dados e a pandemia do novo coronavírus. Migalhas, 08 de abr. de 2020. Disponível em: <https://www.migalhas.com.br/depeso/324035/lei-geral-de-protecao-de-dados-e-a-pandemia-do-novo-coronavirus>. Acessado em 01 de jun. de 2020.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados no Brasil: Análise contextual detalhada. Jota. 14 de jul. de 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>. Acessado em 02 de jun. de 2020.

OIKAWA, Andrezza Hautsch. Coronavírus e proteção de dados pessoais. 20 de mar. de 2020. Disponível em: <https://www1.folha.uol.com.br/opiniao/2020/03/coronavirus-e-protecao-de-dados-pessoais.shtml>. Acessado em 01 de jun. de 2020.

PICELLI, Roberto Ricomini. Saúde na lei de proteção de dados: proibições e permissões. Jota, 31 de jul. de 2019. Disponível: [https://www.jota.info/paywall?redirect\\_to=//www.jota.info/opiniao-e-analise/artigos/saude-na-lei-de-protecao-de-dados-proibicoes-e-permissoes-31072019](https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/saude-na-lei-de-protecao-de-dados-proibicoes-e-permissoes-31072019). Acessado em 05 de jun. de 2020.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei 13.709/2018**. Editora Saraiva. 1ª Edição. São Paulo/2018.

SATO, Luíza. A lei de proteção de dados em tempos de coronavírus. CIO from IDG, 08 de abr. de 2020. Disponível em: <https://cio.com.br/a-lei-geral-de-protecao-de-dados-em-tempos-de-coronavirus/>. Acessado em 01 de jun. de 2020.



SANTOS, Rafa. Uso de dados pessoais para combate à coronavírus gera dúvidas. Conjur.com.br, 02 de abr. de 2020. Disponível em: <https://www.conjur.com.br/2020-abr-02/uso-dados-pessoais-combate-covid-19-gera-duvidas>. Acessado em 02 de jun. de 2020.

SCHREIBER, Anderson. Privacidade na pandemia: por que adiar a LGPD é um erro? Jota, 22 de abr. de 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/privacidade-na-pandemia-por-que-adiar-a-lgpd-e-um-erro-22042020>. Acessado em 02 de jun. de 2020.

SOARES, Paulo Vinícius de Carvalho; MELO, Leonardo Albuquerque. Como conciliar saúde e proteção de dados em tempos de coronavírus. Migalhas, 20 de mar. de 2020. Disponível em: <https://www.migalhas.com.br/depeso/322099/como-conciliar-saude-e-protecao-de-dados-em-tempos-do-coronavirus>. Acessado em 01 de jun. de 2020.