A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NO SETOR PÚBLICO

Hemily Samila da Silva Saraiva[1]
Raquel Teixeira de Brito[2]

RESUMO

O presente artigo científico trata, em bases gerais, da Lei Geral de Proteção de Dados pessoais (LGPD) e a implementação dessa legislação no setor público. A necessidade de tutela aos dados pessoais é um dos maiores desafios contemporâneos que a Administração Pública enfrenta, no sentido de promover a adequação das atividades de tratamento de dados pessoais às disposições perpetradas pela LGPD, sob possibilidade de responsabilização em caso de inadequação a tais medidas. Nesse contexto, aborda-se tanto as medidas necessária à implementação da normativa, quanto à responsabilização da Administração Pública, caso não se adeque as medidas preconizadas. O estudo da temática é de suma importância e de interesse social, tendo em vista a necessidade de assegurar o controle, a fiscalização e a segurança dos dados pessoais, sensíveis ou não, não apenas do cidadão comum, como também dos servidores públicos. Apesar de haver normativas sobre o assunto, na LGPD e em leis setoriais, ainda são imprescindíveis estudos mais aprofundados com a finalidade de propor meios de aplicação prática. Como procedimentos metodológicos utilizam-se a pesquisa do tipo qualitativo e nível de investigação descritivo, através da análise bibliográfica, jurisprudencial e dispositivos normativos atinentes ao tema.

Palavras-chave: Lei Geral de Proteção de Dados (LGPD); Setor Público; Implementação; Inovação; Sanções.

[1] Advogada. Pesquisadora-bolsista da Escola do Governo do Estado do Rio Grande do Norte. Mestranda em Constituição e Garantia de Direitos e Especialista em Direito Administrativo pela Universidade Federal do Rio Grande do Norte – UFRN. Especialista em Direito Civil e Empresarial pela Universidade Potiguar – UNP e Especialista em Processo Civil pelo Centro Universitário do Rio Grande do Norte – UNI/RN. Membro do Instituto de Direito Administrativo Seabra Fagundes (IDASF). E-mail: saraivahemily@gmail.com

[2] Advogada. Pesquisadora-bolsista da Escola do Governo do Estado do Rio Grande do Norte. Especialista em Direito Civil e Processo Civil pela Universidade Futura. Habilitada em Direito do Petróleo, Gás Natural e Biocombustíveis pela Agência Nacional do Petróleo - ANP. Graduada em Direito pela Universidade Federal do Rio Grande do Norte - UFRN. E-mail: raquel-2013@ufrn.edu.br

1. INTRODUÇÃO

O presente trabalho abordará a problemática atinente à implementação da Lei Geral de Dados (LGPD) no setor público, proposta por meio da Lei Federal n.º 13.709 de 14 de agosto de 2018, vigente desde 18 de setembro de 2020, a qual trouxe inúmeras nuances a serem observadas não apenas no setor privado, mas também pelo público. A busca da tutela de dados pessoais é uma realidade amparada pela legislação, que demanda esforços da Administração Pública no sentido de promover a adequação das atividades de tratamento de dados pessoais às disposições perpetradas pela LGPD, sob possibilidade de responsabilização em caso de inadequação a tais medidas.

Em razão da recente entrada em vigor da legislação em comento, o Brasil, assim como diversos países que adequaram tardiamente seu ordenamento jurídico às legislações de proteção de dados, apresenta um quadro de instabilidade institucional acerca no armazenamento de dados pessoais, razão pela qual a LGPD veio fortalecer e reafirmar garantias fundamentais, com o intuito de assegurar direitos como a inviolabilidade de dados e o direito à privacidade.

Diante disso, a presente pesquisa visa estudar as medidas necessárias para a implementação da LGPD no setor público, bem como dispor sobre o tipo de responsabilidade civil se aplicará aos agentes de tratamento, e quais são as sanções previstas na Lei em caso de inadequação à normativa.

Para se alcançar o objetivo pretendido, no primeiro item se analisará o panorama geral da lei geral de proteção de dados no Brasil, especificando como tal Lei aborda o tratamento de dados no setor público. Posteriormente, passa-se a estudar quais medidas de implementação seriam necessárias e as consequências em caso de não adequação a LGPD.

No que tange às medidas de adequação, a legislação preocupou-se, em sessão própria com a temática, as quais devem ser observadas e seguidas pelo setor público, objetivando resguardar o direito à privacidade dos cidadãos[3]. A LGPD surge trazendo mudanças no uso e na coleta de dados pessoais, tendo por ideia geral a função de educar para a cidadania na seara digital, buscando a proteção da coletividade.

A presente pesquisa se justifica por se tratar de tema atual, relevante e necessário no contexto hodierno. A questão do vazamento de dados pessoais no setor público é algo que merece ser discutido, para que a Administração Pública não fique a mercê dessa prática. A implantação da LGPD no setor público se torna uma realidade, imprescindível para o controle, fiscalização e a segurança, daí o dever dos órgãos públicos se adequarem a esta Lei.

Para o desenvolvimento do presente trabalho, será utilizada como metodologia a revisão bibliográfica, a partir de livros, de artigos científicos, da legislação infraconstitucional e constitucional, bem como da jurisprudência. A abordagem de tais meios de pesquisa se dará de forma qualitativa e nível de investigação descritivo, uma vez que buscará, por intermédio de uma interpretação e compreensão do problema posto à luz da literatura examinada, extrair conclusões pautadas em conceitos e teorias,

[3]A LGPD dedicou um capítulo exclusivo à Administração Pública, estabelecendo regras para o compartilhamento de dados pessoais por entidades públicas, bases legais autorizativas de tratamentos desses dados, transparência e sanções.

descrevendo os resultados levantados e as variáveis que se fazem presentes nesse levantamento.

2. PANORAMA GERAL DA LEI GERAL DE PROTEÇÃO DE DADOS E O TRATAMENTO DE DADOS NO SETOR PÚBLICO

A sociedade da informação sugere a ideia de uma sociedade estruturada a partir da informação, que se constitui como a fonte geradora do mercado. Assim, de acordo com Laura Schertel Mendes, "vivemos em uma economia da informação pessoal desde a década de 70", onde "a crise da produção em massa e o surgimento da economia de especialização flexível, que se caracteriza pela diversificação da produção para diferentes produtos e diferentes clientes" revelam a importância dos dados pessoais no mercado de consumo atual (MENDES, 2014, p. 84-85). Ante a relevância dos dados pessoais para a economia mundial, surge a afirmação: "Dados são o novo petróleo", em tradução livre para a original "*Data is the new oil*", criada e defendida por Clive Humby, que é um matemático e empresário britânico no campo da ciência de dados e estratégias de negócios centradas no cliente**.**

Nesse contexto, a Constituição Federal de 1988 (CF/88), apesar de não trazer de forma expressa em seu texto a proteção de dados pessoais como um direito fundamental, não se pode dizer que a proteção dos dados não recebeu amparo constitucional (MENDES, 2014), pois a temática é abordada na Constituição em diversos dispositivos, como por exemplo, na consagração do direito à liberdade de expressão (art. 5º, IX), a inviolabilidade da vida privada e da intimidade (art. 5º, X), a inviolabilidade do sigilo da correspondência e das comunicações telefônicas e de dados (art. 5º, XII) e o direito à informação (art. 5º, XIV), assim como a ação de *habeas data* (art. 5º, LXXII).

No entanto, tais dispositivos constitucionais não possuem efetividade para tutelar os direitos de pessoas naturais em face dos potenciais riscos decorrentes da atividade de tratamento de dados pessoais (MENDES, 2014). A ação de habeas data, por exemplo, visa assegurar aos indivíduos, o acesso às informações constante de registros ou bancos de dados de entidades governamentais de caráter público, bem como a possibilidade de retificação de tais dados (art. 5º, LXXII, CF), razão pela qual não é um instrumento ágil e eficaz o suficiente para garantir a proteção de dados pessoais, pois "ela proporciona uma tutela completamente anacrônica e ineficaz quanto à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação" (ENDC, 2010, p. 51).

Diante da necessidade de positivação de direito fundamental à proteção de dados, o Supremo Tribunal Federal (STF), decidiu que "toda e qualquer atividade de tratamento de dados deve ser devidamente acompanhada das devidas salvaguardas sob pena de ser uma interferência desproporcional na esfera pessoal dos brasileiro (a)s" (BIONI, 2020, p. 01).

Ao se posicionar dessa forma, a Suprema Corte findou por elevar a proteção de dados pessoais ao *status* de direito fundamental em consonância com a Proposta de Emenda à Constituição n.º 17/2019, que foi aprovada, de forma unânime, em Comissões

Parlamentares e pelo plenário do Senado Federal e na Comissão Especial da Câmara dos Deputados, e aguarda a sua apreciação no plenário desta última Casa Legislativa (BIONI, 2020).

Pode-se esclarecer que a LGPD é uma norma que visa assegurar um direito fundamental, por hora, não expresso, mas que está há poucos passos de ser positivado em nosso texto constitucional por meio da PEC n.º 17/2019, a qual "altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais", modificando, assim o inciso XII do art. 5º da CF[4].

Inclusive, o STF, ao julgar conjuntamente, em 24/04/2020, a medida cautelar na Ação Direta de Inconstitucionalidade (ADI) ns.º 6.387, 6388, 6389, 6393, 6390, declarou a inconstitucionalidade da MP n.º 954/2020[5], chancelando a autonomia do direito fundamental à proteção de dados pessoais, que já era reconhecida na General Data Protection Regulation (GDPR), no CONSIDERANDO n.º 1º do Regulamento[6].

Nesse contexto, urge destacar que a LGPD foi elaborada tendo como base o sistema adotado na União Europeia, qual seja, o Regulamento 2016/679 da GDPR, e as novas legislações sobre proteção de dados pessoais surgiram logo após o escândalo envolvendo *Cambridge Analytica* e o *Facebook*[7].

No que diz respeito ao tratamento de dados pessoais, direito amparado pela LGPD, podemos afirmar que o tratamento se resume em todas as operações realizadas com dados pessoais[8], englobando também ou dados sensíveis[9]. Por tratamento, entende-se tudo que é possível ser realizado com o dado, seja no momento de entrada ou na saída do banco desses dados. A prática da coleta, do armazenamento e da transferência seriam meios de tratamentos. Logo, a legislação ao dispor sobre o tratamento de dados pessoais, sejam tais dados advindos de meio físico ou de meios digitais, podendo serem tratados por pessoa natural[10] ou por pessoa jurídica de direito público ou privado, assume o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

---

[4] O art. 5º, XII da CF ficaria com a seguinte redação: "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**, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais**." (grifos acrescidos)**.**

[5] Tal normativa traz em seu texto o dever das operadoras de telefonia a repassarem a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) dados identificados de seus usuários de telefonia fixa e móvel, o que acarreta milhões de brasileiros, durante a pandemia COVID-19.

[6] CONSIDERANDO n.º 1º, da GDPR, diz que "A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental".

[7] O fatídico envolveu usuários que participaram de um aplicativo de teste psicológico na rede social, no qual entregaram, voluntariamente e sem conhecimento, suas informações e dados relativos aos amigos do perfil na rede social.

[8] Os tratamentos de dados pessoais somente podem ser realizados nas hipóteses do art. 7º, da LGPD.

[9] O tratamento dos dados sensíveis está presente no art. 11, da LGPD e poderá ocorrer nas hipóteses lá previstas.

[10] Uma vez que a Lei trata de dados relativo à pessoa natural, os dados das pessoas falecidas não são por ela tratados, pois de acordo o art. 6º do Código Civil de 2002, a existência da pessoa natural termina com a morte. Logo, pessoa natural é todo ser humano vivo.

O art. 7º, inciso I, da mencionada Lei traz que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular. Isso busca dar soberania aos titulares dos dados, permite que o usuário tenha alguns direitos que antes não eram resguardados, podendo solicitar alteração dos dados fornecidos, revogar e pedir a exclusão.

A autodeterminação informativa possibilita o particular controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos ao titular de direitos, possibilitando manter o controle sobre suas próprias informações. Assim, objetivando a legitimação do tratamento de dados pessoais, o consentimento livre e expresso dos titulares dos dados se tornam essencial. Não obstante, conforme dispõe o art. 7º, III, da LGPD, a Administração Pública é poupada da exigência do consentimento para a coleta de dados pessoais e 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 necessários ao desenvolvimento das atividades do órgão.

Nesse contexto, acerca do tratamento de dados sensíveis pela Administração Pública, poderá ocorrer, sem fornecimento de consentimento do titular, tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos, conforme art. 11, inciso II, alíneas “a” e “b”, da LGPD. Deve ser dada publicidade a essa possibilidade (art. 11, §2º, da Lei), trazendo esclarecimentos sobre o tratamento de dados (art. 23, inciso I, da Lei).

Importante mencionar quais seriam as entidades públicas responsáveis para o tratamento de dados pessoais e sensíveis. A LGPD utiliza como referência Lei Federal de Acesso à Informação (LAI) n.º 12.527, de 18 de novembro de 2011, parágrafo único do art. 1º, para disciplinar as pessoas jurídicas de direito público, que seriam: os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público, bem como 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.

No entanto, nos termos do art. 24, e seu parágrafo único, da Lei Federal n.º 13.709/2018, não se enquadram nesses benefícios às empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, as quais seguirão o tratamento previsto as pessoas privadas, exceto se estiverem operacionalizando políticas públicas e no âmbito da execução dessas políticas.

Acerca dos serviços notariais e de registro, exercidos em caráter privado, por delegação do Poder Público, a lei determina o mesmo regime as pessoas jurídicas de direito público. Ela “equiparou os cartórios (serviços notariais e de registro exercidos em caráter privado por delegação do Poder Público) as pessoas jurídicas de direito público, dando a eles o mesmo nível de tratamento diferenciado”, conforme art. 23, § 4º, da norma (SALES; TSUZUKI, 2020, p. 78).

Logo, a Administração Pública como custodiante dos dados dos cidadãos, deve assegurar, nível de proteção apropriada para proteger os dados custodiados e/ou tratados, promovendo assim, o uso ético, seguro e responsável dos dados pessoais. Dessa forma, recai sobre os órgãos públicos a iniciativa de implementar uma série de

medidas - as quais serão abordadas abaixo - em consonância com a LGPD, proporcionando uma verdadeira mudança na cultura organizacional.

3. AS MEDIDAS DE IMPLEMENTAÇÃO DA LGPD NO ÂMBITO PÚBLICO

A LGPD foi um marco normativo à proteção de dados pessoais, estabelecendo, desde 2018[11], regulamentação sobre o tratamento e compartilhamento de dados, permitindo penalidades no que atine ao vazamento e uso indevido desses dados. A não conformidade à legislação pode trazer diversos problemas a Administração Pública, daí a adequação ser uma necessidade, no qual o setor público e privado não podem se eximir.

No instante em que haja uma coleta de dados, a Lei tutela uma finalidade, objetivando proteger o livre desenvolvimento da personalidade da pessoa natural, englobando não só o direito à privacidade, mas a intimidade e à autodeterminação informativa, essa última foi ampliada com a decisão da Corte Alemã, em 1983[12].

Danilo Doneda menciona que a necessidade de funcionalização da proteção da privacidade ocasionou a proteção de dados pessoais, que tem em sua origem pressupostos ontológicos muito parecidos aos da própria proteção da privacidade: pode-se dizer que a proteção de dados pessoais é a sua "continuação por outros meios"." (DONEDA, 2019, p. 44)

Nessa linha de intelecção, Raphael de Matos Cardoso (2020, p. 217) diz que o controle dos dados do indivíduo seria o meio de atender ao direito fundamental da privacidade:

> O atributo básico do direito à privacidade seria a capacidade de o indivíduo controlar a circulação de informações a seu respeito. A privacidade não é a simples ausência de conhecimento alheio sobre os fatos da vida privada do indivíduo, mas o controle exercido sobre essas informações e esses dados pessoais. A privacidade significa o conjunto de informações do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em quais condições.

Diante disso, a LGPD tem um interpretação voltada à privacidade,[13] visando concretizar a necessidades da sociedade da informação e promover o uso ético, seguro e responsável dos dados pessoais por parte daqueles que os custodiam e/ou tratam, recai

[11] Antes disso, algumas leis setoriais trataram sobre o assunto: A Lei de Acesso à Informação, de n.º 12.527/2011; a Lei do Cadastro Positivo, n.º 12.414/2011; a Lei do Marco Civil da Internet, n.º 12.965/2014.

[12] Vide **BVERFGE 65, 1**. SCHWABE, Jürgen; MARTINS, Leonardo. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Konrad-Adenauer-Stiftung, 2005, p. 233 a 245. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf/view. Acesso em: 02 ago. 2020.

[13] O art. 2, inciso I da Lei disciplina a proteção de dados pessoais tendo como fundamento o respeito à privacidade.

sobre os órgãos públicos e privados o dever de implementar uma série de medidas para que possam se adequarem ao disposto neste novo contexto legal. A implementação dessas medidas no setor público deve ocorrer de maneira estruturada e planejada, envolvendo todo o órgão público, promovendo, assim, uma verdadeira mudança na cultura organizacional.

A discussão não é exclusiva da área de segurança da informação ou da área jurídica do órgão, a responsabilidade pelo cumprimento da Lei é de todo o órgão público, desde a Autoridade Máxima, passando pelas áreas meio e fim. Assim, todo projeto de adequação do órgão público à LGPD tem caráter multidisciplinar, multissetorial e impacto no órgão público como um todo.

Nesse viés, o objetivo geral a ser operacionalizado é um estudo sobre o órgão público, suas competências legais, atividades finalísticas e atividades meio, a fim de identificar onde paira sua atuação e delimitar a aplicabilidade da LGPD no órgão público, bem como as limitações (vedações) às quais está submetido, para assim, propor medidas de segurança e de adequação sólidas e eficazes. É nesse sentido que "todo o produto ou serviço desenvolvido deverá pensar, antes de tudo, em *como proteger as informações sensíveis*, estabelecendo uma *segurança ponta-a-ponta*, *em respeito à privacidade do usuário."* (HEINEN, 2020, p. 412).

Podem-se abordar algumas medidas de segurança trazidas pela Lei, o que abrange: i) a adoção de medidas técnicas que garantam o tratamento de dados de forma segura; ii) o desenvolvimento de processos internos que permitam a criação e manutenção de registros das operações de tratamento de dados; iii) conservação dos dados visando atender a finalidade pela qual foram coletados e cumprir com obrigações legais regulatórias; e iv) informar o titular caso haja alguma alteração na finalidade para a coleta de dados. Essas são apenas algumas medidas que deverão ser adotadas em razão da necessidade de adequação à LGPD.

A implementação da governança e privacidade de dados é mínima para que se possa proteger os dados pessoais sem invadir a esfera de proteção do cidadão. Diante disso, como implementar a LGPD na Administração Pública para atingir esse princípio norteador?

A adequação do órgão público ao disposto na LGPD requer a adoção de medidas sistêmicas de segurança, e que impactem em toda a organização, as quais, segundo o Escola Nacional de Administração Pública (ENAP, 2019, p. 7-8), podem ser implementadas em quatro dimensões organizacionais: i) dimensão estratégica: momento em que será necessário definir medidas de adequação do órgão em relação à finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (art. 6º da LGPD); ii) dimensão organizacional: será definida uma estrutura organizacional multidisciplinar, que seja suficientemente capaz para apoiar a implementação das medidas de adequação definidas. Essa estrutura, por si só já é uma medida de adequação; iii) dimensão operacional: serão definidas as medidas de adequação que devem ser incorporadas aos processos organizacionais, os quais lidam e/ou de alguma forma afetam os dados pessoais custodiados pelo órgão público; iv) a criação de um Comitê para tratar do tema Proteção de Dados, podendo ser aproveitado estruturas já existentes, em analogia ao que ocorre no Executivo Federal, como por exemplo o

Comitê Central de Governança de Dados, conforme disposto pelo art. 21 do Decreto nº 10.046/2019 ou o Comitê de Governança, Riscos e Controles conforme disposto pela Instrução Normativa Conjunta MP/CGU n° 01/2016, ou ainda o Comitê de Governança Digital disposto pelo art. 2º do Decreto nº 10.332/2020.

No "Comitê" a ser criado, devem participar os representantes de todas áreas meio e fim do órgão público, que terão como material base os resultados referentes aos itens "i" e "ii". Por sua vez, o item "iii" será plenamente desenvolvido após a criação do Comitê, que terá como função primordial o gerenciamento das metas a serem atingidas com vistas a programar efetivamente as medidas de adequação e segurança da LGPD no setor público.

Logo, pode-se dizer que a implementação da LGPD no setor público inicia-se a partir do planejamento, após compreender os riscos e problemas na instituição pública acerca do uso de dados, passa-se a buscar um programa de privacidade. De forma mais detalhada, Juliano Heinen (2020) teoriza acerca da implementação de um programa de privacidade no setor público. Para ele, são necessárias algumas providências: i) deve haver o apoio da alta gestão da instituição, sendo aconselhável a criação de comitês multidisciplinares que fariam o monitoramento da Lei e a "ponte" entre os setores que trabalhem com os dados; ii) nomear um encarregado da proteção de dados que será o gerente do programa; iii) realizar mapeamento dos dados sensíveis ou pessoais; iv) desenvolver uma política de privacidade de dados, para realizar o tratamento de dados indicando a finalidade do seu manuseio; v) implementar vários programas voltados a proteção de dados e infraestrutura da informação abarcando: um sistema eficiente de respostas a possíveis violações; um programa que contenha um plano seguro de eliminação das informações, salvo se na devam ser guardados em algumas situações regulamentadas; vi) a implantação da " *Data protection officer*" (DPO) para esclarecer os titulares dos dados e orientar a instituição.

Ainda sob a ótica do mesmo autor, para se mapear os dados tutelados pela LGPD deve-se analisar o banco de dados da instituição, classificando-os, objetivando orientar em como coletar, processar, armazenar, compartilhar ou publicar a informação. Para tanto, deve-se observar: "Quais os dados sensíveis ou pessoais são manipulados por cada área/agente da instituição; Qual a finalidade empregada a estes dados; Quem é o responsável por eles; Qual é o fluxo dessa informação; Quanto tempo os dados são retidos; Em que formato eles são retidos" (HEINEN, 2020, p. 416).

Um quesito importante para auxiliar no tratamento de dados seria o Relatório de Impacto a Proteção de Dados Pessoais (RIPDP), previsto no art. 5º, XVII, da Lei, que consiste no documento do controlador contendo a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Esse documento deverá indicar os resultados e sobre o projeto de privacidade.

Em síntese, vislumbra-se importante para a implementação da LGPD no setor público diretrizes que se preocupem em: i) capacitar os servidores para atuarem na Administração Pública; ii) realizar mapeamentos e relatórios de impactos de proteção de dados; iii) ter uma organização com as políticas e os procedimentos dos dados em seus sistemas, no sentido de saber por onde trafegam, como são armazenados,

compartilhados e seu descarte; iv) investir constantemente em segurança da informação e novas metodologias[14].

O art. 6º estabelece o dever do Estado para o tratamento de dados pessoais observando a boa-fé e os princípios definidos na LGPD. Assim, cabe a Administração Pública:

> a adoção de medidas técnicas e administrativas para proteção desses dados (princípio da segurança), inclusive que possam prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (princípio da prevenção) e que adote medidas eficazes capazes de comprovar a observância das normas de proteção de dados pessoais (princípio da responsabilização e prestação de contas), proibindo qualquer tratamento para fins discriminatórios, ilícitos e abusivos (principio da nao discriminacao). (SALES; TSUZUKI, 2020, p. 79).

Um dos maiores desafios contemporâneos da Administração Pública consiste em proteger os dados pessoais dos cidadãos. A compatibilidade entre os dados coletados e sua finalidade em vista dos serviços oferecidos, não raro suscitam a possibilidade de abuso pelo Estado diante dessa prerrogativa. A infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos geram impactos enormes, além das multas de valor alto. A necessidade de mudança na sistemática organizacional será inevitável nas estruturas de toda a Administração Pública. O fortalecimento do processo de inovação, com ênfase na segurança da informação deve ser incentivado.

4. A RESPONSABILIDADE DA ADMINISTRAÇÃO EM RAZÃO DA INADEQUAÇÃO À LGPD E AS SANÇÕES PREVISTAS NA LEI

Como mencionado, a Lei Geral de Proteção de Dados (LGPD) teve como base o Regulamento Geral sobre proteção de dados (RGPD) que, detalha de forma mais específica e rigorosa acerca das altas multas em caso de violação desses dados, até 20 milhões de euros ou 4% da sua receita, buscando maior licitude, lealdade e transparência dos dados pessoais.

Em âmbito nacional, a LGPD passa a punir empresas por vazamento de dados pessoais, podendo haver várias sanções, como a multa simples; multa diária; advertência; bloqueio dos dados pessoais; publicização da infração; e eliminação dos dados pessoais.[15] Essas multas podem ser aplicadas isoladamente ou cumulativamente. No que atine ao setor público, a tutela dos dados anda em linha tênue, no qual já há sistemas de Governo e órgãos públicos sendo invadidos e dados de servidores públicos vêm sendo utilizados para o cometimento de fraudes.

O ataque hacker, no dia 03 de novembro de 2020, envolvendo o Superior Tribunal de Justiça (STJ) resultou na interrupção de diversos julgamentos que ocorriam

---

[14] Como o *framework* no desenvolvimento de seus sistemas e serviços. "O diagnóstico dos dados da organização deve ser feito em conformidade com os frameworks que possam fornecer uma estrutura para conformidade (...) determinadas qualificações, ou mesmo o procedimento já adotado pela instituição, poderão facilitar a programação pretendida, mas também deverão se adaptar a ela" (HEINEN, 2020 p. 415).

[15] As sanções administrativas estão preconizadas no art. 52 a 54 da LGPD.

por videoconferência e na suspensão de prazos processuais. A preocupação foi de um vazamento em massa de dados copiados. Ao que parece, a invasão aos sistemas do STJ utilizou o *ransomware* - um programa malicioso que sequestram dados e exige resgate para devolvê-los. Isso demonstra a vulnerabilidade na segurança envolvendo o setor público no Brasil[16].

Outro caso recente ocorreu com o Tribunal Superior Eleitoral (TSE), no dia de eleições municipais em todo o Brasil, no qual hackers, denominados "*Cyber Team*", vazaram informações internas do Tribunal com o objetivo de mostrar a vulnerabilidade do Estado no quesito segurança. Tais dados apenas mostraram a estrutura do banco de dados, não havendo a exposição dos dados dos cidadãos.[17] Apesar do problema, o TSE afirma que a eleição não foi prejudicada[18].

Notícia do dia 24 de setembro de 2019, presente no sítio eletrônico do G1, divulga que operação investiga esquema que fraudava dados em tribunais federais e do Distrito Federal, no qual suspeitos invadem sistemas e abriram contas, para transferir parte do salário e efetuar compras, inclusive o financiamento de automóveis, em nome de servidores públicos. Prejuízo estimado é de R$ 1 milhão[19]. Existem outros casos parecidos como esse de vazamento de dados do sistema de órgãos públicos, e como podem ainda ocorrer demais casos[20].

A LGPD traz em seu escopo a aplicação de sanções, não obstante, os casos que envolvem entidades e órgãos públicos não estão sujeitos às sanções de multa, apenas à advertência, publicização da infração, bloqueio dos dados pessoais e eliminação dos dados a que se refere à infração, nos termos do art. 52, § 3º. Esse dispositivo vai além do fato de se coletar dados pessoais dos servidores públicos, haja vista que responsabiliza os servidores públicos responsáveis pelo vazamento de dados. Assim, o § 3º referenciado acima menciona a não aplicação de multa pela ANPD, mas pune aqueles servidores, seja por culpa ou dolo, podendo ser penalizados nas esferas da improbidade administrativa e criminal.

Por sua vez, os arts. 31 e 32 da Lei Geral de Proteção de dados tratam que quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informes com medidas cabíveis

---

[16] "Calcula-se que 255 mil processos tramitam na corte. Não há ainda informações se o cibercriminoso conseguiu fazer cópia de todo esse volume, mas essa é uma possibilidade que preocupa a Corte. Além disso, há um "risco elevado" de o hacker ter conseguido fazer o download de documentos com informações dos servidores do tribunal". Essa informação pode ser vislumbrada no sítio eletrônico do UOL. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/11/09/ataque-no-stj-hacker-continua-com-o-controle-de-documentos-sigilosos.htm.Acesso em: 22 nov. 2020.

[17] Informacao disponivel em: https://olhardigital.com.br/fique_seguro/noticia/apos-negar-ataque-tse-tem-bancos-de-dados-vazado-por-hackers/110224. Acesso em: 23 nov. 2020.

[18] Informacao disponivel em: https://www.uol.com.br/tilt/noticias/redacao/2020/11/16/bugs-do-tse-nao-colocam-eleicao-em-risco-entenda-4-pontos-do-vazamento.htm. Acesso em: 23 nov. 2020.

[19] Essa informação pode ser vislumbrada no sítio eletrônico do G1. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/09/24/operacao-investiga-esquema-que-fraudava-dados-em-tribunais-federais-e-do-df.ghtml. Acesso em: 20 nov. 2020.

[20] Para maiores estatísticas vide o sítio eletrônico do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). Disponível em: https://www.ctir.gov.br/. Acesso em: 20 nov. 2020.

para fazer cessar a violação, bem como poderá solicitar a agentes do Poder Público a publicação de 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 setor Público.

Ante a realidade da revolução digital, observa-se um avanço no que diz respeito à legislação brasileira em matéria de Direito e novas tecnologias. No entanto, não seria forçoso dizer que, do ponto de vista retórico, indagar se a inteligência artificial e os direitos à privacidade representam incoerência entre si, consoante vasta vulnerabilidade do cidadão e servidor público em razão do uso inadequado dessas tecnologias de inteligência artificial por instituições e, inclusive, pelos próprios servidores públicos, como mencionado, que teriam o dever de tutela de dados da Administração Pública.

A responsabilidade do agente de tratamento de dados está disciplinada entre os artigos 42 a 45, os quais estabelecem as regras referentes à responsabilidade civil dos agentes de tratamento de dados pessoais. O controlador ou o operador, o que inclui os órgãos e entidades públicos, empresas públicas e sociedades de economia mista, respondem por dano em razão do exercício de atividade de tratamento de dados pessoais. Tal atividade abrange os casos de violação à legislação de proteção de dados pessoais, bem como por não adoção de medidas técnicas de segurança. O operador responde solidariamente pelos danos causados quando: i) descumprir as obrigações da legislação de proteção de dados; ii) não tiver seguido as instruções lícitas do controlador. (ITS, 2019)

> Tanto o controlador (aquele que toma das decisões sobre tratamento de dados) como operador (aquele que realiza o tratamento em nome do colaborador) são responsáveis pelo tratamento das informações. Então, é salutar que a organização constitua um departamento ou instrua um agente específico que faça a comunicação e auxilie nesta interlocução entre os operadores/controladores e os titulares de dados e a ANPD, o que se denomina de Data Protection Officer - DPO" (HEINEN, 2020, p. 419)

Por sua vez, o art. 43 da LGPD dispõe que o agente quando provar que o tratamento de dados não aconteceu, não houve violação à LGPD ou caso o dano advenha exclusivamente da culpa do titular dos dados ou de terceiro. Visando resguardar a veracidade das informações, a Autoridade Nacional poderá solicitar aos agentes do Poder Pública a publicação de relatórios de impacto à proteção de dados pessoais, quando necessário, desde que respeitados os segredos comerciais e industriais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

É importante destacar a respeito da responsabilidade dos agentes de tratamento, que conforme dispõe o art. 42 e o art. 44, da LGPD, fora adotada a responsabilidade civil objetiva, visto que recai sobre os agentes de tratamento a obrigação de indenizar os danos causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador.

Cumpre destacar que a Autoridade Nacional de Proteção de Dados (ANPD), conforme previsão do art. 55 da LGPD, é a autoridade que atuará como um órgão a serviço do cidadão e da salvaguarda de seus direitos, bem como uma ponte entre a

sociedade e o governo, possibilitando que as pessoas enviem dúvidas, sugestões, denúncias ligadas à LGPD para apuração. Além disso, exercerá a relevante função de orientar e apoiar os órgãos e empresas quanto ao tratamento dos dados pessoais dos cidadãos e com isso assegurará maior segurança jurídica no que diz respeito à proteção de dados pessoais.

No entanto, apesar de a LGPD estar em vigor, às sanções administrativas estão suspensas até 1º de agosto de 2021, período reservado à estruturação da Autoridade, que ainda está em processo de composição, haja vista que a primeira Diretoria da Autoridade fora indicada em 20 de outubro de 2020[21], e os trâmites continuam até que seja definida a composição, o que vem limitando a plena eficácia, regulamentação e fiscalização dos dispositivos intrínsecos à lei. Ademais, editou-se recentemente o Decreto Federal nº. 10.474, de 26 de agosto de 2020, que regulamenta com maior especificidade a estrutura e as atribuições da ANPD.

5. CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD) ao dispor sobre a proteção de dados pessoais propõe um diálogo em consonância com os direitos fundamentais assegurados na Constituição da República de 1988 (CF/88). Assim, em razão do desenvolvimento da Sociedade da Informação, tal Lei surgiu com o intuito de atender a necessidade de circulação de dados pessoais de modo mais seguro, respeitando o direito à privacidade e mitigando os riscos desse processo.

Ao se abordar a necessidade de implementação da LGPD, não apenas no setor privado, como também no setor público, pois em ambos os caso se visa proteger os dados pessoais de cidadãos e a sociedade como um todo, haja vista que tais dados, sensíveis ou não, possuem poder, principalmente de cunho econômico.

Como abordado, as medidas de implementação da LGPD no setor público, pode ser resumida tanto em diretrizes previstas em lei como em boas práticas a serem seguidas, como, por exemplo, a capacitação de servidores para atuarem na Administração Pública; a realização de mapeamentos e relatórios de impactos de proteção de dados; organização com as políticas e os procedimentos dos dados em seus sistemas, no sentido de saber por onde trafegam, como são armazenados, compartilhados e seu descarte; e no investimento constante em segurança da informação e novas metodologias.

De igual modo, é importante destacar que, caso a Administração Pública não promova as medidas de adequação necessárias ou em caso de seus agentes de tratamento incorrer em algum dano aos titulares dos dados, em decorrência do tratamento de dados pessoais, a Autoridade Nacional de Proteção de Dados (ANPD) poderá enviar informes com medidas cabíveis para fazer cessar a violação, bem como solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de

[21]Conforme se pode vislumbrar em informação disponível em: RODRIGUES, Edilson. Senado confirma primeira diretoria da Autoridade Nacional de Proteção de Dados. Agência Senado, Brasília, 20 nov. 2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/10/20/senado-confirma-primeira-diretoria-da-autoridade-nacional-de-protecao-de-dados>. Acesso em: 20 nov. 2020.

dados pessoais pelo setor público. Além disso, é possível ainda que o agente de tratamento venha a responder pelos danos na modalidade de responsabilidade civil objetiva.

Em que pese à necessidade de promoção das medidas de adequação, em virtude da natureza propedêutica de muitos dispositivos da LGPD, sem regras definidas acerca de sua aplicação prática, surgem as dificuldades de sua implementação, pois a lei não disserta a respeito das ações de natureza tecnológica, das mudanças regulatórias ou fiscais necessárias, especialmente nesse primeiro momento em que tudo é novo e necessita de direcionamentos.

Assim, a evolução tecnológica e a natural introdução de novas operações de tratamento de dados demandam um processo contínuo de adequação e aperfeiçoamento de procedimentos e medidas protetivas de dados pessoais, com a finalidade de acompanhar as tecnologias mais recentes capazes de assim dar cumprimento às disposições da LGPD, para que a Administração Pública apresente a segurança de dados necessária a proteger direitos fundamentais.

Portanto, embora a LGPD ofereça relevantes salvaguardas aos titulares de dados pessoais, ela acabou por criar um extenso rol de obrigações e responsabilidades aos agentes que realizam tratamento de dados, o que, conciliado à natureza principiológica da Lei e ao princípio da publicidade e eficiência que rege a Administração Pública, exigirá dos administradores públicos elevada capacidade de gestão e integração de sua equipe, além de efetivo empenho e capacitação dos servidores públicos.

REFERÊNCIAS

ALBERS, Marion. A complexidade da Proteção de Dados. **Direitos Fundamentais & Justiça**. Porto Alegre, v. 10, n. 35, p. 19-45, jul./dez. 2016.

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

BIONI, Bruno Ricardo. A IMPORTÂNCIA DA PEC DE PROTEÇÃO DE DADOS MESMO APÓS O HISTÓRICO JULGAMENTO DO STF. **GenJurídico**, 2020. Disponível em: < http://genjuridico.com.br/2020/06/23/importancia-pec-de-protecao-de-dados/>. Acesso em: 17 nov. 2020.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Brasília, DF: ENDC, 2010. (Caderno de Investigações Científicas, v. 2). Disponível em: https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-deprotecao-de-dados-pessoais.pdf. Acesso em: 10 nov. 2020.

BRASIL. Escola Nacional de Administração Pública (ENAP). **Proteção de Dados Pessoais no Serviço Público:** O Ciclo de Vida dos Dados Pessoais. Brasília, 2019. Disponível em: <https://www.escolavirtual.gov.br/curso/290>. Acesso em: 02 ago. 2020.

BRASIL. Instituto de Tecnologia e Sociedade. **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E SETOR PÚBLICO:** Um guia da Lei 13.709/2018, voltado para os órgãos e entidades públicas. Rio de Janeiro: ITS, 2019. Disponível em: <https://itsrio.org/wp-content/uploads/2019/05/LGPD-vf-1.pdf>. Acesso em: 10 de nov. 2020.

BVERFGE 65, 1. SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Konrad-Adenauer-Stiftung, 2005, p. 233 a 245. Acesso em: http://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf/view. Acesso em: 02 ago. 2020.

CARDOSO, Raphael de Matos. O desembarque da privacidade e da intimidade na LGPD. In: **LGPD e administração pública:** uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**. Joaçaba, v. 2, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://www.researchgate.net/publication/277241112_A_protecao_dos_dados_pessoais_como_um_direito_fundamental. Acesso em: 17 nov. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da lei geral de dados. 2 ed. Revista dos Tribunais, 2019.

HEINEN, Juliano. Planejando a implementação de um programa de privacidade a partir da Lei Geral de Proteção de Dados (LGPD) - Lei 13.709/2018. *In*: **LGPD e administração pública:** uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

OLIVEIRA, Ricardo Alexandre de. Lei Geral de Proteção De Dados Pessoais e seus impactos no ordenamento jurídico. **Revista dos Tribunais**, São Paulo, n. 998, p. 241-261, dez. 2018.

SALES, Stela Chaves Rocha; TSUZUKI, Camila Akemi. Cidadania em xeque: entre o interesse público e a proteção de dados pessoais. *In*: **Direito Público Digital: O Estado e as novas tecnologias:** desafios e soluções. São Paulo: Thomson Reuters Brasil, 2020.