

CLOVIS FELIX CURADO JR.
RICARDO PEREIRA CALEGARI
RODRIGO BEZERRA DOWSLEY

**A LACUNA NORMATIVA NO TRATAMENTO DE DADOS PESSOAIS NA DEFESA
NACIONAL E SEGURANÇA DO ESTADO**

Trabalho de Conclusão de Curso apresentado à
Escola Superior de Defesa - *Campus* Brasília,
como exigência parcial para obtenção do título
de Especialista em Altos Estudos em Defesa.

Orientador: Prof. Dr. Paulo Edvandro da Costa
Pinto

Brasília
2021

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado propriedade da ESCOLA SUPERIOR DE DEFESA (ESD). É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que sem propósitos comerciais e que seja feita a referência bibliográfica completa. Os conceitos expressos neste trabalho são de responsabilidade dos autores e não expressam qualquer orientação institucional da ESG.



CLOVIS FELIX CURADO JR.



RICARDO PEREIRA CALEGARI



RODRIGO BEZERRA DOWSLEY

CLÓVIS FELIX CURADO JUNIOR
RICARDO PEREIRA CALEGARI
RODRIGO BEZERRA DOWSLEY

**A LACUNA NORMATIVA NO TRATAMENTO DE DADOS PESSOAIS NA
DEFESA NACIONAL E SEGURANÇA DO ESTADO**


Trabalho de Conclusão de Curso
apresentado à Escola Superior de Defesa,
como exigência parcial para obtenção do
título de Especialista em Altos Estudos
em Defesa.

Trabalho de Conclusão de Curso **APROVADO**:

Brasília, DF, 21 de outubro de 2021



PAULO EDVANDRO DA COSTA PINTO - CMG RI (ESD)
Orientador



JOÃO FRANSWILLIAM BARBOSA - CMG (ESD)
Membro 1



CARLOS RADICCHI - CMG RI (ESD)
Membro 2

20/10/21

A LACUNA NORMATIVA NO TRATAMENTO DE DADOS PESSOAIS NA DEFESA NACIONAL E SEGURANÇA DO ESTADO

Clovis Felix Curado Jr.^{1a}
Ricardo Pereira Calegari^{2a}
Rodrigo Bezerra Dowsley^{3a}

Resumo: A Lei Geral de Proteção de Dados (LGPD) tem como objetivo a proteção dos dados pessoais, de direito público ou privado, inclusive nos meios digitais, buscando garantir a liberdade e privacidade dos direitos fundamentais da pessoa natural. A proteção dos direitos fundamentais está prevista no artigo 5º da Constituição Federal, com destaque aos direitos de liberdade e segurança. Este trabalho tem por objetivo analisar os possíveis riscos que as novas balizas e parâmetros trazidos pela LGPD possam gerar, sobretudo, a partir da hipótese de possíveis interpretações futuras pelos Tribunais Superiores. Nos seus capítulos, restou analisada se haveria incompatibilização nos mandamentos previstos na LAI e na LGPD; apurou possíveis riscos e geração de danos na implementação da LGPD, sobretudo, a partir da hipótese de possíveis interpretações futuras pelos Tribunais Superiores frente ao novo arcabouço legal e, identificou os possíveis impactos da aplicação da LGPD nas instituições e órgãos responsáveis pelas atividades de Defesa Nacional e Segurança do Estado. Concluiu-se, após quatro capítulos de análise e discussões, que é fundamental a edição de uma norma que venha regulamentar o tratamento de dados pela Defesa Nacional e Segurança do Estado, antes que o Poder Judiciário venha ser chamado a fazê-lo.

Palavras-Chave: LGPD; tratamento e proteção de dados; lacuna normativa; defesa nacional.

Abstract: The General Data Protection Law (LGPD) aims to protect personal data, whether public or private, including in digital media, seeking to guarantee the freedom and privacy of the fundamental rights of the natural person. The protection of fundamental rights is provided for in article 5 of the Federal Constitution, with emphasis on the rights of freedom and security. This paper aims to analyze the possible risks that the new beacons and parameters brought by the LGPD generate, above all, based on the hypothesis of possible future interpretations by the Superior Courts. In its chapters, have analyzed whether there would be a mismatch in the commandments fulfilled in the LAI and in the LGPD; identified possible risks and generation of damages in the implementation of the LGPD, above all, based on the hypothesis of possible future interpretations by the Superior Courts against the new legal framework, and identified the possible impacts of the application of the LGPD on the institutions and bodies responsible for the activities of National Defense and State Security. It was concluded, after four chapters of analysis and exercise, that it is essential to issue a rule that will regulate the processing of data by the National Defense and State Security, before the Judiciary Power is called upon to do so.

Keywords: LGPD; data protection; gap in legislation; national defense.

¹ Secretário Especial Adjunto de Administração da Secretaria-Geral da Presidência da República e Especialista em Direito Administrativo, Constitucional, Trabalhista e Processo do Trabalho.

² Reitor da Universidade Católica de Brasília, Doutor em Ensino de Ciências e Matemática e Mestre em Educação Sociocomunitária.

³ Procurador Federal, Coordenador-Geral de Assuntos Estratégicos e Gestão da Procuradoria Federal Especializada junto ao Instituto Nacional do Seguro Social e Especialista em Direito Constitucional.

^a Trabalho de conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Defesa (ESD), Brasília, 2021.

1 INTRODUÇÃO

A Sociedade Contemporânea tem passado por muitas revoluções culturais e tecnológicas, com expressivos impactos nas relações interpessoais. Essa sociedade, que no Brasil pode ser também caracterizada como uma Sociedade da Informação, é ávida consumidora de milhares de informações diárias, em um extraordinário nível de conexão virtual.

Os dados passaram a ser uma nova matriz energética mundial, já que a partir deles é possível identificar e compreender as novas necessidades sociais, bem como utilizá-los para fins diversos, como o comercial, empresarial, político e, até mesmo, o de vulnerabilizar, direta ou indiretamente, a Defesa Nacional e a Segurança do Estado. Nesse contexto, tornou-se necessário, portanto, que fossem criadas estruturas confiáveis e seguras para tutelar a exposição dos dados pessoais, de forma a regular e garantir a não violação de direitos fundamentais dos cidadãos.

Ademais, tornou-se imperioso que o Estado fomentasse mecanismos para não gerar danos ao cidadão e ao próprio erário em razão de eventual má governança dos dados pessoais que cada operação digital utiliza, quando das ofertas de serviços digitais que o governo disponibiliza em larga escala (governo digital), em harmonia com as tendências globais.

Essa má governança dos dados pessoais tem o potencial de impactar, inclusive, a segurança dos cidadãos, das empresas privadas e de entes estatais, visto que as ameaças cibernéticas avançam e se renovam na mesma velocidade que a revolução digital, colocando em risco a sociedade e a administração pública.

Frente à criação de uma legislação específica sobre as questões relacionadas ao compartilhamento de dados e informações, sobretudo em rede (internet), com o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), destacou-se, ainda mais, a necessidade de adaptar a metodologia de tratamento dos dados pessoais cadastrados aos padrões adotados internacionalmente, visando salvaguardar o direito do cidadão à privacidade e ao sigilo das suas informações, bem como resguardar o Estado diante das vulnerabilidades que hoje temos em termos de segurança de dados, sobretudo em sistemas virtualizados.

Assim, como já vinha ocorrendo em várias partes do mundo, tornou-se necessária a implantação de uma regulamentação específica e ampla que garantisse a proteção de dados pessoais, possibilitando ao cidadão o controle sobre como suas informações são utilizadas por organizações, empresas e pelo governo. Essa regulamentação teria o escopo de estabelecer padrões mínimos a serem seguidos quando ocorrer a utilização de um dado pessoal, limitando

esse uso a uma finalidade específica, sempre assegurando ao cidadão protagonismo nas decisões fundamentais quanto aos seus dados.

No Brasil, em resposta a essa nova conjuntura, adveio a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709, de 14 de agosto de 2018), publicada em 15 de agosto de 2018, mas que teve sua vigência plena iniciada 24 (vinte e quatro) meses após sua publicação. Esse importante diploma legal veio dispor sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018)

Nitidamente influenciada pelo Regulamento Geral de Proteção de Dados na União Europeia (RGPD ou GDPR, na sigla em inglês), a LGPD adveio para regular essa nova forma de relações por meios virtuais, elevando a um nível superior a proteção dos dados pessoais e garantindo maior segurança jurídica àqueles – pessoa natural ou pessoa jurídica – que deles tenham que dispor. Portanto, espera-se com a LGPD trazer maior equilíbrio na manipulação e tratamento dos dados entre o titular das informações e aqueles que as utilizam e compartilham.

A LGPD, ao instituir uma série de regras e princípios, demanda uma reanálise e nova compreensão do dever de garantir o acesso às informações da coisa pública, em contraposição à necessidade de se garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado. Portanto, há de se analisar a harmonia da LGPD com a Lei nº 12.527, de 18 de novembro de 2011, também conhecida como Lei de Acesso à Informação (LAI).

Todo esse contexto está inserido em um ambiente cibernético que, conforme consignado no Livro Branco da Defesa Nacional (LBDN), foi selecionado, pela Estratégia Nacional de Defesa (END), como decisivo para a Defesa Nacional. A ameaça cibernética é uma preocupação de defesa na medida em que ela põe em risco a integridade de infraestruturas sensíveis relacionados à segurança nacional.

Como balizador deste dilema entre direitos civis e de acesso aos dados públicos, perpassando a LGPD, se recorrerá à teoria da ponderação de Robert Alexy. Trata-se de uma formulação chamada “lei da ponderação”, que prescreve que quanto maior é o grau da não satisfação de um princípio, maior deve ser a importância da satisfação do outro. A partir desse raciocínio, Alexy desenvolveu um conjunto de regras de argumentação aptas à racionalização das decisões jurídicas. Além disso, ele propõe a ponderação como um modelo de fundamentação, e não de mera decisão, assegurando sua racionalidade.

Assim, por meio do presente trabalho busca-se analisar as possibilidades, oportunidades e os desafios a serem enfrentados na implementação da LGPD, bem como, os seus impactos,

apreciando se essa implementação pode vir a afetar, em última análise, a Segurança e a Defesa Nacionais.

Pretende-se, ainda, verificar a necessidade de regulamentação do tratamento dos dados coletados em consequência das atividades realizadas para fins exclusivos de Defesa Nacional e Segurança do Estado.

Portanto, o objetivo geral do presente trabalho é estudar e avaliar a LGPD em harmonia com o dever de acesso às informações da coisa pública, o dever de garantir o sigilo das informações imprescindíveis à Defesa Nacional e à Segurança do Estado e o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, considerando, ainda, a regra de não aplicabilidade prevista no inciso III do art. 4º desse diploma legal.

Para tanto, em um primeiro momento, analisou-se se haveria incompatibilização nos mandamentos previstos na LAI e na LGPD. Seguidamente, apurou-se possíveis riscos e geração de danos na implementação da LGPD, sobretudo, a partir da hipótese de possíveis interpretações futuras pelos Tribunais Superiores frente ao novo arcabouço legal. Por fim, identificou-se os possíveis impactos da aplicação da LGPD nas instituições e órgãos responsáveis pelas atividades de Defesa Nacional e Segurança do Estado.

2 LGPD E LAI: LEGISLAÇÕES QUE DISCIPLINAM A PUBLICIZAÇÃO E A PROTEÇÃO DE DADOS

Muito antes do advento da LGPD, a Constituição Federal de 1988 (CF/88) já estabelecia como direito fundamental, no inciso X do seu art. 5º, a inviolabilidade da intimidade, da vida privada e da imagem das pessoas, assegurando, ainda, o direito à indenização pelo dano material ou moral decorrente da transgressão dessa inviolabilidade. Ademais, no sentido de garantir o direito de proteção aos dados pessoais, a CF/88 também assegurou que são invioláveis o “sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas” (BRASIL, 1988), salvo quando por ordem judicial ou nas “hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (BRASIL, 1988, art. 5º, XII).

Observa-se, portanto, que a LGPD encontra seu fundamento de validade no texto constitucional, para proporcionar a devida proteção dos direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Por outro lado, a CF/88 também traz, igualmente em caráter de garantia fundamental, o direito do acesso à informação produzida ou custodiada pelos órgãos públicos, seja de interesse

particular, seja de interesse coletivo ou geral, salvo aquela cujo sigilo seja imprescindível à segurança da sociedade e do Estado (art. 5º, XXXIII). Portanto, o princípio da transparência máxima quanto à divulgação das ações governamentais deve ser observado de forma constante na administração pública, excluindo-se, tão somente, as informações que devam ser sigilosas, nos termos da lei. A informação pública, portanto, é propriedade da sociedade, sendo o Estado um mero detentor da informação, que, regra geral, deve disponibilizar essa informação a qualquer cidadão interessado. (BIONI, 2019).

Por sua vez, o inciso II do § 3º do art. 37 garante “o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII”. Para além de remeter à observância do inciso XXXIII do art. 5º da CF/88, a disposição da Carta igualmente também faz remissão ao inciso X do mesmo artigo, que trata da inviolabilidade da intimidade, da vida privada e da imagem das pessoas. Já o § 2º do art. 216 da CF/88 prescreve o dever de a administração pública franquear consulta pública da gestão da documentação governamental, na forma da lei.

Nesse sentido, a promulgação da Lei de Acesso à Informação (Lei nº 12.527, de 2011), que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, veio para regular a efetiva transparência das informações públicas, tendo como principal diretriz a observância da publicidade como regra geral e o sigilo como exceção.

Constata-se, portanto, que o ordenamento jurídico prevê, por um lado, a convivência da obrigação da administração pública de garantir a transparência da informação produzida ou custodiada pelos órgãos públicos e, por outro lado, o direito à privacidade (intimidade) das informações dos cidadãos.

No que se refere ao dever de transparência, frisa-se que, como já visto, o objetivo da LAI é exatamente proporcionar esta ampla publicidade da destinação dada à "coisa pública", permitindo o controle social inerente ao Estado Democrático de Direito. Entretanto, a legislação prevê exceções à regra geral, como veremos a seguir.

Para permitir a excepcionalização da regra geral, a LAI estabelece prazos máximos para restrição de acesso, que vigoram a partir da data da produção da informação, definindo os graus de sigilo da informação, quais sejam: ultrassecreta, secreta ou reservada (art. 24, **caput**, e § 1º). No entanto, para a classificação da informação em determinado grau de sigilo se faz mister observar o interesse público da informação e utilizar o critério menos restritivo possível, considerados a gravidade do risco ou dano à segurança da sociedade e do Estado (art. 24, § 5º).

Especificamente quanto ao tratamento de dados pessoais, a LAI, na sua Seção V, art.31, que trata “Das informações pessoais”, não deixa dúvidas que o tratamento das informações pessoais deve ser feito “com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais” (BRASIL, 2011).

Independentemente de classificação de sigilo, o acesso a esses dados, quando “relativos à intimidade, vida privada, honra e imagem”, será restrito por até 100 (cem) anos, a contar da sua data de produção (art. 31, § 1º, inciso I). Durante o período de restrição, terão acesso a essas informações pessoais apenas os agentes públicos legalmente autorizados e a pessoa a que elas se referirem.

A divulgação dessas informações pessoais ou o acesso a elas por terceiros apenas poderá ser autorizada por lei ou mediante o consentimento expresso da pessoa a que elas se referirem (art. 31, § 1º, inciso II), salvo quando as informações forem necessárias às hipóteses previstas no § 3º do art. 31 da LAI, oportunidades em que a autorização ou consentimento mencionados serão prescindíveis.

No entanto, essa restrição de acesso não poderá ser invocada para prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido ou “em ações voltadas para a recuperação de fatos históricos de maior relevância” (BRASIL, 2011. art. 31, § 4º).

Quanto à LGPD, o ente público ou o particular deve disponibilizar ao titular, por intermédio da figura do controlador, todas as informações referentes aos seus dados “a qualquer momento e mediante requisição” (BRASIL, 2018. art. 18 da LGPD). Em caso de negativas dessas informações, caracterizada estará a infração legal, possibilitando o controle quanto a essa violação à ANPD. Esgotada a esfera administrativa, caberá, igualmente, recorrer ao poder jurisdicional do Estado.

Quanto aos prazos e procedimentos para exercíciolos direitos do titular perante a administração pública, a LGPD faz remissão à legislação específica e, expressamente, à LAI, à Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), e à Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo).

Ademais, quando o tratamento de dados pessoais envolver a obrigação legal da respectiva difusão em transparência ativa, tanto a LGPD (art. 25) como a LAI (art. 8º, § 3º) prescrevem que esses dados devem ser publicados em formato interoperável e estruturado, para o uso compartilhado.

A LAI, que é eminentemente de Direito Público, vincula todos os entes da administração direta e indireta. A LGPD, por sua vez, aplica-se tanto aos entes públicos como à iniciativa

privada. No entanto, como visto acima, em ambos os diplomas legais – e não apenas na LGPD – há diretrizes voltadas ao tratamento de dados pessoais.

Verifica-se, portanto, que a própria LAI, ainda que de forma mais concisa, prevê a proteção de dados, inclusive responsabilizando, pelo uso indevido, aquele que obtiver acesso às informações pessoais (art. 31, § 2º), em conformidade com os mandamentos trazidos pela LGPD.

Por conseguinte, enquanto a LAI determina que os dados públicos devem ser expostos com a finalidade específica de efetivar o princípio da transparência, os mandamentos da LGPD prescrevem que os dados pessoais, ainda que estejam públicos, devem ser protegidos para que não sejam utilizados para finalidade diversa, o que, caso viesse a ocorrer, poderia, inclusive, ensejar a responsabilização do ente que detenha a guarda desses dados.

Nesse sentido, a Controladoria-Geral da União, que concentra os pedidos de dados públicos, mormente por meio do Portal da Transparência do Governo Federal, já descartou quaisquer incompatibilidades entre a LAI e a LGPD.

Ao participar do Seminário Internacional de Proteção de Dados, promovido pela Secretaria de Governo Digital do Ministério da Economia e realizado no dia 28 de abril de 2021, o ouvidor-geral da União, Valmir Dias, destacou que a própria LAI, ainda que de forma mais econômica, já prevê a proteção de dados. Observe-se alguns trechos da sua fala naquela oportunidade:

Não há conflito entre LGPD e LAI. A Lei de Acesso à Informação veio regulamentando a questão constitucional do direito de acesso à informação, mas também já trazia instrumentos de proteção à privacidade no poder público. A LGPD agora detalha instrumentos tanto para o setor privado como para o setor público, como uma ampliação do escopo. E existe a necessidade dessa interação. Mas é tranquilo trabalhar a harmonização dessas normas. Temos que trabalhar o caminho dessa interação. Nesse sentido temos o guia de implementação da LGPD, para que os órgãos se estruturam com base em boas práticas. E que traz em seu teor a Plataforma Fala.br como canal para exercício dos titulares – já temos nessa plataforma adequações alinhadas à LGPD, na proteção dos manifestantes, por exemplo. Além do próprio canal para exercício desses direitos.(SEMINÁRIO, 2021).

Portanto, como visto, não obstante a preocupação de órgãos públicos e seus gestores quanto a um suposto conflito entre a LAI e a LGPD, não se vislumbra antinomias entre os dois diplomas. Pelo contrário, há vários pontos de convergência e a necessidade de aplicação harmônica de ambas as Leis.

3 IMPACTOS DA LGPD NAS INSTITUIÇÕES E ÓRGÃOS RESPONSÁVEIS PELAS ATIVIDADES DE DEFESA E SEGURANÇA DO ESTADO

Os impactos da LGPD na sociedade tendem a ter considerável relevância, haja visto que permearão, com regras rígidas de proteção dos dados pessoais, as relações comerciais e de consumo, bem como as relações com os órgãos governamentais e com as instituições de ensino, por exemplo. Por conseguinte, haverá importantes mudanças de paradigmas no que concerne à proteção e respeito à privacidade do cidadão, inclusive nos meios digitais.

Com efeito, a implementação da LGPD exigirá dos órgãos e entidades uma significativa mudança da cultura organizacional, que deverá perpassar os respectivos níveis estratégico, tático e operacional da instituição. Nessa transformação, deverá ser considerada a garantia da proteção dos dados pessoais e da privacidade dos cidadãos em todos os projetos desenvolvidos por uma organização, desde a sua concepção (*Privacidade by Design*⁴), bem como a promoção de ações de conscientização, para que seja incorporado nas atividades institucionais cotidianas, como princípio inarredável, o respeito à privacidade.

Por outro lado, a LGPD não deixa dúvida de que o legislador optou por não contemplar, no âmbito da sua regência, o tratamento de dados pessoais para fins exclusivos da Segurança Pública, Defesa Nacional, Segurança do Estado e atividades de investigação e repressão de infrações penais. É o que se extrai da leitura do (art. 4º, III, da LGPD):

Art. 4º (...)

(...)

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; (BRASIL, 2018).

3.1 OS IMPACTOS DA APLICAÇÃO DA LGPD NO ÂMBITO DAS ORGANIZAÇÕES PÚBLICAS FEDERAIS

Na avaliação do Tribunal de Contas da União (TCU), as incertezas quanto ao início de vigência da LGPD e quanto à criação da Autoridade Nacional de Proteção de Dados (ANPD), prevista no art. 55-A da LGPD, contribuiram para que os órgãos e entidades públicas não estivessem devidamente estruturados no início da vigência da Lei. Ao que tudo indica, ainda não estão.

⁴Quando da 32ª edição da conferência anual dos Comissários Internacionais de Proteção de Dados e Privacidade (2010), este conceito foi reconhecido como um componente essencial da proteção do direito fundamental de privacidade.

Frente a esse cenário, o TCU autorizou, por meio do Acórdão 2.909/2020 – TCU-Plenário, de relatoria do ministro Augusto Nardes, no âmbito da Tomada de Contas (TC) nº 039.606/2020-1, a instauração de auditoria para analisar o nível de maturidade das organizações públicas no que concerne aos preceitos trazidos pela LGPD, bem como sobre a estruturação da ANPD e a respectiva condução de suas atribuições legais. (BRASIL, 2020a).

Nessa auditoria, o TCU utilizou o método de autoavaliação de controles internos (do inglês *Control Self-Assessment – CSA*), disponibilizando questionário eletrônico para que os gestores avaliassem os controles relacionados à LGPD no âmbito da sua organização, abrangendo aspectos referentes às providências adotadas para buscar adequação dos respectivos processos e procedimentos à LGPD, bem como às medidas efetivamente implementadas para o cumprimento das obrigações que a Lei estabelece.

Como resultado dessa auditoria, que foi realizada em 382 (trezentos e oitenta e duas) organizações públicas federais, incluindo os Conselhos Nacionais de Justiça (CNJ) e do Ministério Público (CNMP), verificou-se, conforme consta do respectivo Relatório de Fiscalização, que a implementação da LGPD ainda é muito incipiente na grande maioria dessas organizações (76,7%), que ainda está no “grau inexpressivo” (17,8%) ou no “grau inicial” (58,9%) do processo de adequação à LGPD. (BRASIL, 2020b).

A incipiência das organizações públicas federais ouvidas, no que tange à respectiva adequação à LGPD, é ainda maior no que diz respeito às providências necessárias para cumprir a legislação no que se refere ao tratamento de dados pessoais.

Destarte, conclui-se que não há, ainda, elementos suficientes para aferir os reais impactos da aplicação da LGPD no âmbito das organizações públicas federais, haja visto a baixa maturidade dessas instituições no que se refere aos preceitos trazidos pela citada Lei.

3.2 OS IMPACTOS DA APLICAÇÃO DA LGPD NO ÂMBITO DOS ÓRGÃOS RESPONSÁVEIS PELAS ATIVIDADES DE DEFESA E SEGURANÇA DO ESTADO

Não obstante a excludente prevista no inciso III do art. 4º da LGPD, deve-se aplicar a LGPD ao tratamento de dados pessoais realizados pelos órgãos responsáveis pela segurança pública, Defesa Nacional, Segurança do Estado e atividades de investigação e repressão de infrações penais, para outros fins que não os exclusivos para essas atividades.

Portanto, os órgãos responsáveis pelas atividades previstas no inciso III do art. 4º também estão subordinados aos ditames da LGPD no que se refere às atividades não realizadas para os fins exclusivos previstos no referido dispositivo legal.

No que se refere aos órgãos responsáveis pela Defesa Nacional e Segurança do Estado, verifica-se que as Forças que constituem as Forças Armadas brasileiras apresentam avanços – tendo como parâmetro a maioria das organizações públicas federais – pelo menos em três das nove dimensões consideradas pelo TCU para elaboração do seu indicador, quando da auditoria autorizada por meio do Acórdão 2.909/2020 – TCU-Plenário (TC nº 039.606/2020-1). Essas dimensões nas quais as Forças Armadas demonstram ter avançado são as relacionadas à “Preparação”, ao “Contexto Organizacional” e à “Liderança”; havendo, ainda, indícios de avanços na dimensão relacionada às “Medidas de Proteção”, sobretudo na FAB.

Nesse sentido, verifica-se que o Exército Brasileiro (EB), a Força Aérea Brasileira (FAB) e a Marinha do Brasil (MB) já estabeleceram diretrizes para orientação sobre aplicação da LGPD no âmbito de suas organizações.

No EB, por exemplo, essas diretrizes foram aprovadas por meio da Portaria nº 088-EME, de 7 de maio de 2020, expedida pelo chefe do Estado-Maior do Exército (EME), com a finalidade de orientar a aplicação da LGPD “aos processos internos, aos meios de Tecnologia da Informação e Comunicações (TIC) e à revisão de atos normativos internos do Exército Brasileiro”, sempre em conformidade com as “disposições da Diretriz Estratégica Organizadora do Sistema de Informação do Exército”, tendo como um dos objetivos “possibilitar o adequado tratamento de informações pessoais no âmbito do Exército Brasileiro”, para além de:

Proteger as informações pessoais de integrantes do Exército Brasileiro, de usuários do serviço público, que por força normativa forneçam informações pessoais aos órgãos internos da Força, e das informações pessoais oriundas de compartilhamento de dados entre órgãos e entidades da Administração Pública. (BRASIL, 2020c).

Verifica-se, portanto, que uma das premissas dessas diretrizes é a de que “as unidades do Exército Brasileiro estão diretamente afetadas pela LGPD, pois se considera que todas realizam tratamento de dados pessoais, nos diversos processos internos que veiculam tais informações”.(BRASIL, 2020c).

Sem prejuízo, há tratamentos de dados internos, mormente os utilizados para o exercício das atividades finalísticas do Exército Brasileiro, que se enquadram nas exceções previstas no inciso III do art. 4º da LGPD.

No que se refere à estrutura de governança de proteção de dados pessoais, a Portaria nº 088-EME, de 2020, prescreve que cabe ao EME, dentre outras atribuições, “orientar, monitorar e avaliar, no nível de direção geral, as atividades relacionadas com a adequação à LGPD”; e “ligar-se, no exercício das atribuições de órgão controlador, à ANPD”. (BRASIL, 2020c).

Já os órgãos de direção setorial (ODS), o Órgão de Direção Operacional (ODOp) e os órgãos de assistência direta e imediata (OADI) exercem a atribuição de órgão operador de que trata a LGPD (artigos 5º, incisos VII e IX, 37 e 38 e outros), sendo responsáveis pelo tratamento de dados pessoais em nome do controlador e pelo ciclo de vida da informação de seu interesse. São esses órgãos que nomeiam militar para o exercício da atribuição de encarregado pela proteção e operações de tratamento de dados pessoais.

Já na FAB, foi editada a Portaria nº 899/GC3, de 28 de agosto de 2020, expedida pelo comandante da Aeronáutica, que “aprova a edição da Diretriz que dispõe sobre a Governança da Proteção de Dados Pessoais do Comando da Aeronáutica”, a qual se aplica a todas as Organizações do Comando da Aeronáutica.

Para além de trazer, de forma bastante delineada e explicativa, as fases do ciclo de vida do tratamento dos dados (coleta, retenção, processamento, compartilhamento e eliminação), a Portaria nº 899/GC3, de 2020, também avança na metodologia de análise de riscos e nas boas práticas em segurança das informações, incorporando o conceito da Privacidade desde a Concepção (do inglês *Privacyby Design*), “o qual implica que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo.” (BRASIL, 2020d).

Por fim, a Portaria do Comando da Aeronáutica estabelece toda a sua estrutura de governança de proteção de dados pessoais, definindo, de forma expressa, o comandante da Aeronáutica, que é o dirigente máximo da instituição, como o Controlador de que trata a LGPD (artigos 5º, incisos VI e IX, 8º, § 2º, 9º, incisos III, IV e V, 10, 37, 38, 41 e outros).

Na MB, o chefe do Estado-Maior da Armada (CEMA) expediu a Circular nº 06/2021, de 31 de março de 2021, tratando sobre a implantação da LGPD naquela Força e estabelecendo, em seus anexos, diretrizes para sua implantação. A exemplo das diretrizes estabelecidas para as demais Forças, foram consolidadas nas referidas diretrizes da MB os principais aspectos da LGPD, bem como apresentadas as particularidades afetas àquela Força. Embora nessas diretrizes, editadas pelas Forças Armadas, haja a previsão de expedição de relatórios de impactos e de avaliação e monitoramento, no âmbito dos levantamentos para elaboração do presente trabalho não foi possível identificar se os mesmos de fato foram elaborados, sendo certo que o acesso a esses relatórios não foi franqueado ao público, nem tampouco aos autores deste trabalho.

Verifica-se, portanto, que a implementação da LGPD nas Forças Armadas, a exemplo do que ocorre na maioria das organizações públicas federais, também é, ainda, incipiente.

Corroboram essa conclusão as respostas do Ministério da Defesa ao questionário conduzido, em 2021, pela Secretaria de Governo Digital do Ministério da Economia, com vistas a traçar um diagnóstico de privacidade junto às organizações públicas federais. Nessas respostas, de acordo com a metodologia empregada pela Secretaria de Governo Digital, sopesando 7 (sete) dimensões, o Ministério da Defesa atingiu o “Índice da Adequação à LGPD” de 0,34 (em uma escala de 0,0 a 1,0), alcançando apenas o “Nível Básico”.

Destarte, da mesma forma que ocorre nas demais organizações públicas federais, conforme apontado no Relatório da Fiscalização nº 232/2020, autorizada pelo TCU por meio do Acórdão 2.909/2020–TCU-Plenário (TC nº 039.606/2020-1), o nível maturidade das Forças Armadas no que se refere à adequação à LGPD ainda não é suficiente para avaliar os impactos efetivos da sua implementação no âmbito dessas organizações militares.

3.3 OS EFEITOS DA AUSÊNCIA DE REGULAMENTAÇÃO DO TRATAMENTO DE DADOS PESSOAIS PREVISTO NAS ALÍNEAS “B” E “C” INCISO III DO ART. 4º DA LGPD

A excludente prevista no inciso III do art. 4º da LGPD ganha maior relevância em razão do fato de que é a administração pública que detém a posse e controla todos os dados pessoais inseridos nas atividades relacionadas no referido dispositivo, haja visto que essas atividades se revestem de caráter eminentemente estatal. Se por um lado essa não incidência tenha o condão de preservar a administração pública de qualquer responsabilidade quanto aos tratamentos realizados para os fins exclusivos que relaciona, por outro pode vir a gerar outros riscos e vulnerabilidades, seja o titular dos dados pessoais inseridos nesse contexto, seja para o próprio Estado, conforme se passa a tratar.

Os riscos quanto ao titular dos dados pessoais inseridos nesse contexto decorrem da amplitude de possibilidades de utilização de dados pessoais para os fins previstos no inciso III do art. 4º, que não terão o devido tratamento sob a alegação de que é preciso garantir a segurança dessas atividades. Entretanto, esse mesmo argumento pode ser utilizado como justificativa para possíveis violações da privacidade, motivo pelo qual a própria LGPD, no § 1º do seu art. 4º, determina a regulação do tratamento desses dados por lei específica, que “deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.” (BRASIL, 2018).

Importante destacar que o §2º do art. 4º da LGPD veda que o tratamento nas circunstâncias enumeradas no inciso III do referido artigo seja realizado por pessoa de direito

privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, hipótese que deve ser informada à ANPD, sem prejuízo da observância da limitação imposta no § 4º do art. 4º, que assim dispõe:

Art. 4º (...)

(...)

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (BRASIL, 2018).

Os riscos para o Estado, nesse aspecto, decorrem também das situações em que os fins exclusivos previstos no inciso III do art. 4º cessam, podendo, a partir de então, trazer a incidência da LGPD para os dados acumulados, a respeito dos quais o órgão que os tem sob sua guarda têm de dar satisfação à sociedade. É o caso, por exemplo, do tratamento de dados pessoais usados para fins de uma operação de Garantia da Lei e da Ordem – GLO⁵ que chegou ao seu fim. Com o fim da operação, a excludente decai e há que se mapear esses dados e estabelecer o seu tempo de guarda, dentre outras atividades.

Um outro ângulo a ser observado, para que não haja um entendimento distorcido da excludente prevista no inciso III do art. 4º da LGPD, é que a Lei não se aplica apenas ao tratamento de dados pessoais realizado para fins exclusivos das atividades que relaciona. Portanto, ainda que o tratamento de dados pessoais seja utilizado para fins de segurança pública, Defesa Nacional, Segurança do Estado ou atividades de investigação e repressão de infrações penais, mas não para fins exclusivos dessas atividades, esse tratamento atrairá a aplicação da LGPD.

Nesse sentido, a mencionada Portaria nº 899/GC3, de 2020, expedida pelo comandante da Aeronáutica, ao tratar, em seu item 6, das “Hipóteses em que a Lei não se Aplica”, assim alerta:

O Art. 4º da LGPD definiu as hipóteses nas quais os seus dispositivos não se aplicam, os quais serão descritos nos subitens a seguir, devendo-se, entretanto, levar em conta que nenhuma hipótese aqui descrita tem caráter absoluto, porquanto o tratamento de dados pessoais que, aparentemente, esteja enquadrado numa hipótese de não aplicação da lei, pode sim, em dada medida, estar incorrendo em alguma das outras hipóteses que a lei prevê e que serão descritas no item 7. Neste sentido, é importante observar que todos os dispositivos contidos no Art. 4º usam o advérbio “exclusivamente”, ou o adjetivo “exclusivo”, para esclarecer que os fins previstos pela norma não podem se desviar em nada dessas previsões legais, porque, se o fizerem,

⁵Garantia da Lei e da Ordem – GLO: operação prevista na Constituição Federal (art. 142) realizada exclusivamente por ordem expressa do presidente da República, autorizando o uso das Forças Armadas para determinado fim extraordinário de segurança pública, em graves situações de perturbação da ordem.

podem estar incorrendo nas hipóteses nas quais a LGPD se aplica. (BRASIL, 2020d)

Portanto, frente ao que a importância e complexidade da matéria indica, os órgãos de Defesa Nacional e Segurança do Estado não podem prescindir de uma legislação específica, conforme previsto no § 1º do art. 4º da LGPD, que assegure, por um lado, a circulação de dados pessoais entre os vários organismos militares envolvidos, mas sem que deixe de ser observada, por outro lado, a preservação da privacidade dos cidadãos. (BRASIL, 2018).

Isto porque, embora as organizações públicas estejam isentas das multas previstas de serem aplicadas pela ANPD, os possíveis impactos provocados por eventual divulgação imprópria de dados pessoais podem resultar em ações judiciais, com potencial consequência de dano ao erário. Ademais, em razão da relevância mundial alcançada pelo tema proteção de dados, sobretudo após a aprovação do GDPR pela União Europeia, os países que não proveem mecanismos de proteção de dados pessoais, para além de poderem perder oportunidades comerciais (retaliação como mecanismo de indução ao cumprimento dos preceitos de privacidade), também poderão inviabilizar cooperações internacionais nessa seara de atuação.

Essa necessidade é potencializada diante das vulnerabilidades verificadas no âmbito das organizações públicas federais no que concerne à segurança da informação, que, de um modo geral, ainda são insuficientes para assegurar a devida proteção dos dados pessoais, conforme já evidenciado pelo TCU nos Acórdãos nºs 4.035/2020-TCU-Plenário⁶ (TC 001.873/2020-2) e 1.109-TCU-Plenário⁷ (TC 036.620/2020-3).

Em razão dessas fragilidades de segurança da informação, recentemente, por exemplo, já após a vigência da LGPD, o Brasil foi vítima de vários ataques que resultaram em vazamento e exposição de milhares de dados pessoais de brasileiros em vários órgãos públicos, conforme amplamente noticiado na mídia nacional.

⁶ BRASIL. Tribunal de Contas da União. **Acórdão nº 4.035/2020**. Plenário. Relator: Ministro Vital do Rêgo. Sessão de 08/12/2020. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-2442373%22>. Acesso em: 22.ago.2021.

⁷ BRASIL. Tribunal de Contas da União. **Acórdão nº 2.737/2020**. Plenário. Relator: Ministro Vital do Rêgo. Sessão de 12/05/2021. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-2473503%22>. Acesso em: 22.ago.2021.

4 PONDERAÇÃO JURÍDICA ACERCA DA LACUNA NORMATIVA RELACIONADA AO TRATAMENTO DE DADOS DE QUE TRATA O INCISO III DO ART. 4º DA LGPD

Do já exposto, não se percebe antagonismos entre a LAI e a LGPD, mas vários pontos de convergência e a necessidade de aplicação harmônica de ambas.

Ademais, verificou-se que a LGPD excluiu do seu âmbito da sua regência o tratamento de dados pessoais para fins exclusivos da segurança pública, Defesa Nacional, Segurança do Estado e atividades de investigação e repressão de infrações penais.

Para preencher essa lacuna, a LGPD prescreve, no § 1º do seu art. 4º, que o tratamento desses dados específicos deverá ser regido por legislação específica, a qual preverá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nessa Lei. (BRASIL, 2018). Como esse regramento ainda não existe, aumenta-se a insegurança jurídica no que concerne ao tratamento desses dados.

Conforme salienta Dworkin (2007, p.29), diante da imprevisibilidade das contingências de um “sistema de ordens”, algumas normas serão inevitavelmente vagas ou pouco claras, o que permitirá aos julgadores a criação de novas regras. Assim, essa lacuna permite uma possível interpretação dos Tribunais (notadamente do Supremo Tribunal Federal - STF) de que a LGPD é aplicável, ainda que, parcialmente, nesses casos referidos.

Verifica-se, portanto, que embora a LGPD não tenha mencionado de quem ou de qual órgão partirá a iniciativa de elaboração dessa legislação específica, essa terá de ser construída para regulamentar as operações de tratamento dos dados porventura coletados, exclusivamente, em consequência das atividades previstas no inciso III do seu art. 4º.

O fundamento para a elaboração de uma legislação específica está na premência e necessidade efetiva de se conferir segurança jurídica aos órgãos e instituições que detêm as competências legais para exercerem essas atividades. Desta forma, poderão desempenhar suas atribuições e deveres institucionais com segurança jurídica, sem prejuízo dos direitos fundamentais e princípios gerais de proteção dos titulares de dados obtidos em virtude das atividades finalísticas e do devido processo legal.

Enquanto persistir essa lacuna, no entanto, para que esse tratamento integre o ordenamento jurídico, considerando experiências pretéritas, é importante a utilização da ponderação jurídica.

Como há o dever de garantir o acesso às informações da coisa pública, com a necessidade de garantia do sigilo das informações imprescindíveis à segurança da sociedade e

do Estado, bem como, numa terceira frente legislativa, o dever de proteger os direitos fundamentais de liberdade e de privacidade no que concerne aos dados pessoais e o livre desenvolvimento da personalidade da pessoa natural, a problemática enfrentada neste trabalho é que determinados casos fáticos podem levar à conclusão da existência de direitos fundamentais conflitantes, cuja solução jurídica demanda a utilização de ponderação jurídica.

Portanto, há um emaranhado jurídico de princípios e regras que podem, a depender do contexto fático, constituir um campo fértil para interpretações jurídicas distintas, com preponderância de um ou de outro princípio e de uma ou outra regra, notadamente diante da lacuna legislativa ainda não preenchida pelo Poder Executivo federal.

4.1 DO DIREITO À PRIVACIDADE

No contexto específico do art. 4º, III, da LGPD, há o comando explícito de que as normas que protegem os direitos fundamentais de liberdade e de privacidade no que concerne aos dados pessoais e o livre desenvolvimento da personalidade da pessoa natural, contidas nesse regramento, são inaplicáveis. Diante dessa lacuna legislativa ainda não preenchida, incumbe compreender o direito à privacidade.

Para Herrán Ortíz(1998), esse direito, que surge com a revolução burguesa (francesa), não é um conceito facilmente identificável, tendo em vista a evolução das aspirações individuais de uma esfera reservada da sua vida. Hoje, a luta pela defesa da vida privada se converteu numa defesa e controle da informação pessoal, que pode revelar os mais íntimos comportamentos ou hábitos individuais.

Portanto, a privacidade é compreendida como a liberdade do indivíduo de decidir por um isolamento da sua vida em sociedade. (HERRÁN ORTIZ, 1998). A dualidade intimidade-privacidade é definida da seguinte forma:

Intimidade não é, na verdade, um sinônimo de privacidade, ainda que se considere às vezes deste modo ao não existir termo apropriado para a noção original de *privacy*. Poderia dizer-se que a privacidade é uma noção sociológica, ao definir-se com referências ao exterior formado por uma pluralidade [...], e, ao contrário, a intimidade é um conceito psicológico que alude a um ‘mundo’ que se desenvolve no próprio interior. Neste sentido, a privacidade conteria a intimidade (HERRÁN ORTÍZ, 1998, p.100, tradução nossa).

Já para Aragón Reyes (2001), a dimensão nuclear do conceito de dignidade da pessoa depende claramente do contexto das circunstâncias históricas, temporais ou situacionais, de forma que o seu alcance efetivo está intimamente ligado às mesmas. A referência à dignidade humana propõe-se como guia para uma interpretação adequada dos direitos fundamentais

(humanos), seja pelo legislador, por um Tribunal Constitucional ou por qualquer agente público. (ARAGÓN REYES, 2001).

Assim, Guichot (2009, p.178) defende que:

Garantir a vida privada, hoje, precisa do reconhecimento ao indivíduo de um poder de controle sobre todos os seus dados pessoais, consistente em proibições (de obtenção, uso e comunicação sem consentimento) e direitos ou faculdades (de informação, acesso, retificação e cancelamento). (tradução nossa).

A liberdade negativa de John Locke, na perspectiva de Cardoso (2016), numa compreensão liberal, seria “a não interferência do Estado na liberdade e na propriedade dos indivíduos, exceto em caso de danos à sociedade e possui uma concepção limitada dos direitos do cidadão. É preciso, portanto, reconhecer um mínimo espaço de liberdade pessoal inatingível por qualquer pessoa, de forma que se definiria a fronteira entre o que é vida pública e o que é vida privada. Para HerránOrtíz(1998, p.8) “a intimidade constitui um bem pessoal que, de modo algum, pode ser renunciado pelo indivíduo sem sofrer em sua dignidade humana”. Quanto menos se conhece da vida pessoal, mais se usufrui da intimidade. A intimidade seria uma esfera tão interior do indivíduo, que apenas a este caberia a sua revelação. (HERRÁN ORTIZ, 1998).

O direito à privacidade é decorrente da própria dignidade humana, contida na Declaração Universal dos Direitos Humanos, de 10 de dezembro de 1948, que, em seu artigo 1º, afirma que “Todos os seres humanos nascem livres e iguais em dignidade e em direitos. São dotados de razão e consciência e devem agir em relação uns aos outros com espírito de fraternidade”. (UNITED NATIONS, 1948). Já o artigo 12º prescreve que “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação”, complementando que “Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” (UNITED NATIONS, 1948).

Havendo dados íntimos acessíveis e tratáveis pela administração pública, decorre a necessidade de ocultamento público desses dados (e até mesmo um limite à administração pública), como meio de proteção do direito à intimidade. O sigilo (segredo) se caracteriza por essa necessidade de ocultamento do que há de ser apartado do público ou proteção do tratamento da administração pública; ou seja, daquilo que é privado, ainda que num aspecto histórico-temporal relativo.

Mas qual seria este limite quanto ao tratamento de dados? Para HerránOrtíz (1998), a vida privada seria uma “esfera de retiro e isolamento”, sem intromissão de terceiros (incluindo a administração pública), enquanto a intimidade seria uma esfera mais sagrada do indivíduo (do seu interior), um “mundo próprio”, inalcançável até mesmo aos olhos dos demais. Mas hoje,

contudo, já se superou essa concepção de esfera reservada inatingível, para uma faculdade de decisão e escolha do indivíduo do que pode ser compartilhado, de forma que ele teria um aspecto negativo (não intromissão) e outro positivo (controle).

Para Guichot (2009, p. 178), necessita-se de ferramentas que protejam a vida privada, com “um poder de controle sobre todos os seus dados pessoais, consistente em proibições (de obtenção, uso e comunicação sem consentimento) e direitos ou faculdades (de informação, acesso, retificação e cancelamento)” (tradução nossa). Seria uma autodeterminação do direito à informação, que pode ser considerado um direito da personalidade. (HERRÁN ORTÍZ, 1998). A LGPD se mostra como um marco legal nesse sentido, propiciando a proteção dessa autodeterminação.

4.2 DO DIREITO AO ACESSO À INFORMAÇÃO

A obrigatoriedade imposta à administração pública de respeitar o princípio da publicidade consta dos artigos 5º, XXXIII, § 3º, II, e 39 da CF/88. Nesses dispositivos há a referência expressa ao respeito aos incisos X e XXXIII do art. 5º, que tratam da inviolabilidade da intimidade e da vida privada e do direito de acesso às informações custodiadas pelo poder público de interesse particular, coletivo ou geral. Já de plano, a CF/88 prevê o tratamento ponderado das normas de publicidade e de privacidade.

Portanto, quais informações devem ser impedidas do franqueamento público ou, até mesmo, do tratamento público? O próprio inciso XXXIII do art. 5º, que impõe o dever de transparência, já traz a primeira hipótese de sigilo constitucionalmente obrigatório: quando for imprescindível à segurança da sociedade e do Estado. Mas aqui não houve o esclarecimento quanto aos limites do tratamento dos dados pessoais (íntimos) pela administração pública.

Segundo Moraes (2019), há uma inviolabilidade constitucional da privacidade, de forma que se deve proteger o cidadão contra: a interferência em sua vida privada, familiar e doméstica; os ataques à honra e reputação; a perspectiva falsa; o uso de nome, identidade e imagem; a espionagem; a violação das correspondências; transmissão de informações resguardadas por sigilo profissional; além da integridade física e mental e liberdade intelectual e moral.

O direito de acesso à informação pública (e pela administração pública), para Panoeiro (2014, p.12), “é essencial no Estado Democrático, pois se por um lado ele permite aos cidadãos conhecer e controlar todos os atos da Administração Pública, por outro reequilibra um pouco as forças de poder na sociedade.”

O contexto constitucional é de coexistência do direito de acesso à informação, do dever de transparência imposto à administração pública e do direito à privacidade das informações íntimas. Guichot (2019, p.12) afirma que:

O legislador, por natureza, é chamado a realizá-la, mas, quando se omite nesta tarefa de harmonização sistemática, o operador do Direito enfrenta uma tarefa de enorme complexidade, a de compatibilizar, em cada caso, estes valores, bens, direitos e princípios e determinar até onde deve chegar o sacrifício de cada um destes.(tradução nossa).

Portanto, diante da lacuna normativa prevista no art. 4º, III, da LGPD, e ante à respectiva inexistência de norma específica (§1º do art. 4º), existe um vasto quadro de possibilidades interpretativas, que podem ser, e até já foram, objeto de interpretação pelo STF.

4.3 DO PONDERAÇÃO JURÍDICA DAS REGRAS E PRINCÍPIOS APLICÁVEIS AO CASO

Nos debates jurídicos acerca da natureza deôntica dos princípios, Alexy (2008, p.87) define que:

Regras e princípios serão reunidos sob o conceito de norma, porque ambos dizem o que deve ser. Ambos podem ser formulados por meio das expressões deônticas básicas do dever, da permissão e da proibição.

Para Dworkin (2007), princípios e regras distinguem-se quanto à natureza da orientação que oferecem, sendo as regras aplicáveis à maneira do tudo-ou-nada.

Assim, os princípios, observados como mandamentos de otimização, podem ser satisfeitos em graus variados a depender das possibilidades fáticas e jurídicas, e essa (possibilidade jurídica) seria determinada pelo resultado dos princípios e das regras colidentes. Assim, o ponto decisivo para a distinção entre princípios e regras é que:

Princípios são normas que ordenam que algo seja realizado na maior medida do possível dentro das possibilidades jurídicas e fáticas existentes. Princípios são, por conseguinte, mandamentos de otimização, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas. O âmbito das possibilidades jurídicas é determinado pelos princípios e regras colidentes. (ALEXY, 2008, p. 90).

Desta forma, a regra é ou não válida, concluindo-se que “princípios são sempre razões *prima facie* e regras são, se não houver o estabelecimento de alguma exceção, razões definitivas” (ALEXY, 2008, p. 106).

Alexy (2008, p. 104) acrescenta que:

Princípios exigem que algo seja realizado na maior medida do possível dentro das possibilidades jurídicas e fáticas existentes. Nesse sentido, eles não contêm um mandamento definitivo, mas apenas *prima facie*. Da relevância de um princípio em um determinado caso não decorre que o resultado seja aquilo que o princípio exige para esse caso. Princípios representam razões que podem ser afastadas por razões antagônicas. A forma pela qual deve ser determinada a relação entre razão e contra-razão não é algo determinado pelo próprio princípio. Os princípios, portanto, não dispõem da extensão de seu conteúdo em face dos princípios colidentes e das possibilidades fáticas.

Não é correta a “compreensão de que os princípios são razões para regras e as regras são razões para decisões concretas (normas individuais)”, apesar de ter, “à primeira vista, algo plausível.”(ALEXY, 2008, p. 107). Da mesma forma, o grau de generalidade não é idôneo para diferenciar regras de princípios. Apesar de os princípios serem relativamente gerais, é possível tanto um princípio menos geral, assim como uma regra mais geral.

Neste contexto estudado, necessária a aplicação da ponderação jurídica, que, também para Alexy (2008, p. 167), assim se caracteriza:

Quanto maior for o grau de não-satisfação ou de afetação de um princípio, tanto maior terá que ser a importância da satisfação do outro. Essa regra expressa uma lei que vale para todos os tipos de sopesamento de princípios e pode ser chamada de lei do sopesamento. Segundo a lei do sopesamento, a medida de não-satisfação ou de afetação de um princípio depende do grau de importância da satisfação do outro.

Interpretando as normas até então vigentes, como o Código Civil, no que tange à eventual responsabilização pela não proteção de dados, será necessária uma revalorização da compreensão normativa. Assim, conforme leciona Ferreira Filho (2010, p.197-198):

É importante, porém, revalorizar a lei. Tem-se perdido de vista que a ela compete desdobrar os princípios consagrados pela Constituição, visando excluir o arbítrio do aplicador do direito e, em consequência, dar segurança aos membros da comunidade. Ela é que permitirá a estes conhecer com precisão o que é lícito e o que é ilícito. Ademais, ela é a manifestação essencial da democracia, pois exprime o que, desde Rousseau, se designa por vontade geral.

A dificuldade é, por meio da ponderação jurídica, compatibilizar o dever de transparência imposto à administração pública e o direito de acesso à informação em face da administração pública, como decorrência do princípio constitucional da publicidade, com o direito à privacidade.

Se o legislador, naturalmente, deve harmonizar as normas constitucionais por meio da legislação infraconstitucional, em caso conflitante, incumbe ao operador do Direito a complexa tarefa de compatibilizá-los por meio da ponderação jurídica, de forma a gerar o menor dano possível às regras e aos princípios constitucionais envolvidos.

Compreendida a ponderação jurídica para preenchimento da lacuna normativa, ante a inexistência de norma específica, prevista no art. 4º, III, §1º, da LGPD, rememoramos que o STF já enfrentou uma lacuna normativa com decisão clara de aplicação de uma norma de forma supletiva.

4.3.1 Do julgamento do Mandado de Injunção nº 708

Se, nas palavras de Hart (2009, p. 183), “um supremo tribunal tem a última palavra ao dizer o que é o direito, e, uma vez que o tenha declarado, a afirmação de que o tribunal ‘errou’ não tem consequências dentro do sistema: o fato não altera os direitos ou os deveres de ninguém”, devemos rememorar que o STF, no julgamento do MI nº 708, já analisou um caso de lacuna normativa, com a aplicação de regramento de forma “supletiva”. Nesse julgado, restou considerada inconstitucional a omissão legislativa referente à regulamentação do direito de greve dos servidores públicos.

Conforme se observa da ementa do julgado, considerou-se que o Direito Comparado permite ao Poder Judiciário adotar medidas normativas como alternativa legítima de superação de omissões inconstitucionais, sem que a proteção judicial efetiva a direitos fundamentais se configure como ofensa ao modelo de separação de poderes. Havia, da mesma forma que no objeto de estudo do presente trabalho, uma lacuna que demandou uma ponderação jurídica para deliberar entre regras e princípios antagônicos. Observe-se:

4.1 [...] Na hipótese de aplicação dessa legislação geral ao caso específico do direito de greve dos servidores públicos, antes de tudo, afigura-se inegável o conflito existente entre as necessidades mínimas de legislação para o exercício do direito de greve dos servidores públicos civis (CF, art. 9º, caput, c/c art. 37, VII), de um lado, e o direito a serviços públicos adequados e prestados de forma contínua a todos os cidadãos (CF, art. 9º, §1º), de outro. Evidentemente, não se outorgaria ao legislador qualquer poder discricionário quanto à edição, ou não, da lei disciplinadora do direito de greve. O legislador poderia adotar um modelo mais ou menos rígido, mais ou menos restritivo do direito de greve no âmbito do serviço público, mas não poderia deixar de reconhecer direito previamente definido pelo texto da Constituição. Considerada a evolução jurisprudencial do tema perante o STF, em sede do mandado de injunção, não se pode atribuir amplamente ao legislador a última palavra acerca da concessão, ou não, do direito de greve dos servidores públicos civis, sob pena de se esvaziar direito fundamental positivado. Tal premissa, contudo, não impede que, futuramente, o legislador infraconstitucional confira novos contornos acerca da adequada configuração da disciplina desse direito constitucional.

4.2 Considerada a omissão legislativa alegada na espécie, seria o caso de se acolher a pretensão, tão-somente no sentido de que se aplique a Lei nº 7.783/1989 enquanto a omissão não for devidamente regulamentada por lei específica para os servidores públicos civis (CF, art. 37, VII). (BRASIL, 2017).

Desta forma, o STF determinou a aplicação, no que couber, dos parâmetros constantes da Lei nº 7.783/1989, até que sobreviesse regulamentação específica sobre o tema de greve dos servidores públicos civis.

Ou seja, mesmo que a legislação que disciplinava a aplicação de determinados regramentos a um grupo específico fosse inaplicável ao outro, para que não houvesse a violação de direito com assento constitucional (no caso o direito de greve), pela omissão legislativa, restou aplicado supletivamente este regramento.

4.3.2 Da possível ponderação jurídica quanto ao art. 4º, III, § 1º, da LGPD

Compreendida a necessidade de preenchimento de lacunas normativas, a ponderação jurídica será a ferramenta interpretativa hábil a compatibilizar o dever de transparência imposto à administração pública e o direito de acesso à informação em face da administração pública, como decorrência do princípio constitucional da publicidade, com o direito à privacidade, ante a lacuna normativa ainda não preenchida (art. 4º, III, §1º da LGPD).

Esse vácuo normativo pode inviabilizar a proteção do direito à privacidade de forma absoluta no tratamento de dados para fins exclusivos de Defesa Nacional ou Segurança do Estado? É possível que o STF entenda que a omissão legislativa é tão gravosa, diante de hipotético vazamento de dados pessoais e, até mesmo, mau tratamento de dados dos cidadãos, a ponto de determinar a aplicação supletiva das regras da LGPD ao tratamento de dados pelos órgãos responsáveis pela Defesa Nacional e Segurança do Estado?

Essa lacuna normativa pode permitir que o STF, da mesma forma do que decidido nos MI nº 708, entenda aplicável à LGPD ao tratamento de dados dos cidadãos, mesmo nos casos de Defesa Nacional e Segurança do Estado, até que sobrevenha a regulamentação específica conforme determina o art. 4º, III, §1º da LGPD.

É possível que o STF pondere que o direito à privacidade, constitucionalmente protegido, demande uma proteção, ainda que mínima, no tratamento de dados relacionados aos casos de Defesa Nacional e Segurança do Estado. Rememore-se que, nesse MI nº 708, o STF deixou claro que “o legislador poderia adotar um modelo mais ou menos rígido, mais ou menos restritivo do direito [...], mas não poderia deixar de reconhecer direito previamente definido pelo texto da Constituição”. (BRASIL, 2017).

Ora, o direito à privacidade existe não só no texto constitucional, mas até mesmo na Declaração Universal dos Direitos Humanos, como já visto.

Nesse sentido, essa lacuna normativa permite que o Poder Judiciário crie “regras”, integrando o Ordenamento Jurídico lacunoso, construindo interpretações jurídicas acerca dos limites dos tratamentos de dados dos cidadãos na Defesa Nacional e Segurança do Estado. Pode ser que se interprete que a LGPD, em face da omissão legislativa, é aplicável também nas questões relacionadas à Defesa Nacional e Segurança do Estado.

Na mesma linha de raciocínio, o STF, na Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 635, por meio da Tutela Provisória Incidental na Medida Cautelar, no voto do ministro Edson Fachin, analisando o requerimento de que não fossem realizadas “operações policiais em comunidades durante a epidemia do covid-19, a não ser em hipóteses absolutamente excepcionais, que devem ser devidamente justificadas por escrito pela autoridade competente”, ponderou que “o uso da força só é legítimo se for comprovadamente necessário para proteção de um bem relevante, como a vida e o patrimônio de outras pessoas”. Tal linha de interpretação pode vir a prejudicar a END (na visão da LBDN), colocando em risco “a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional”. Pode, também, torná-la ineficiente ou até mesmo não operacional por um determinado período, inviabilizando alguma ação de Defesa Nacional e Segurança do Estado.

Conclui-se, portanto, que a omissão normativa contida no art. 4º, III, §1º da LGPD pode levar à aplicação supletiva da LGPD de forma até mesmo absoluta no tratamento de dados (mesmo que sigilosos), pelos órgãos que atuam na Defesa Nacional e Segurança do Estado, o que pode vir a comprometer a atuação desses órgãos.

As experiências obtidas nos julgamentos do MI nº 708 e da ADPF nº 635 demonstram que, a fim de evitar cenário que permite este amplo espectro interpretativo, o ideal seria a edição da referida norma que regulamenta o tratamento de dados pela Defesa Nacional e Segurança do Estado, ainda que seja adotado um modelo mais ou menos rígido, mais ou menos restritivo do direito. Caso contrário, é possível que isto ocorra de forma jurisprudencial e da forma não pretendida pela a END.

5 CONSIDERAÇÕES FINAIS

A LGPD, que instituiu várias regras e princípios protetivos dos dados pessoais, demandou uma reanálise e nova compreensão do dever de garantir o acesso às informações da coisa pública, enquanto se garante o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e se protege os direitos fundamentais de liberdade e de privacidade. No

aprofundamento do estudo dessa nova realidade, restou concluída a harmonizada LGPD com a LAI, diplomas que guardam importantes pontos de convergência, devendo ser aplicados de forma harmônica.

Não obstante o EB, a FAB e a MB já terem estabelecido diretrizes para orientação sobre a aplicação da LGPD no âmbito de suas organizações, de forma geral, pode-se concluir, das auditorias e diagnósticos promovidos pelo TCU e pelo Ministério da Economia, que sua implementação ainda é muito incipiente na absoluta maioria dessas organizações, não havendo, ainda, no que concerne aos preceitos trazidos, maturidade suficiente para aferir os reais impactos da aplicação desta legislação no âmbito das organizações públicas federais.

O art. 4º, III, da LGPD, contudo, criou uma lacuna normativa que ainda não foi suprida, já que excluiu da sua regência o tratamento de dados pessoais realizados para fins exclusivos das atividades finalísticas de segurança pública; Defesa Nacional; Segurança do Estado; ou atividades de investigação e repressão de infrações penais. Esse contexto cria uma insegurança jurídica no tratamento desses dados, tendo em vista que a LGPD tem como objetivo proteger direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, que possuem tutela constitucional.

O STF, em diversos precedentes jurisprudenciais, mais especificamente nos julgamentos do MI nº 708 e da ADPF nº 635, a fim de evitar cenários que permitiam um amplo espectro interpretativo, criou “regras” preenchendo as lacunas normativas. Conforme asseverado no julgamento do MI nº 708, “o legislador poderia adotar um modelo mais ou menos rígido, mais ou menos restritivo do direito de greve no âmbito do serviço público, mas não poderia deixar de reconhecer direito previamente definido pelo texto da Constituição”. (BRASIL, 2017).

Os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural são bens jurídicos protegidos constitucionalmente. Esse contexto de lacuna normativa é um vasto campo de criação de regras pelo STF. As consequências (e até mesmo as regras), ainda imprevisíveis, criadas de forma jurisprudencial, podem impactar sobremaneira a atuação da Defesa Nacional e Segurança do Estado, de forma não pretendida pela END, à semelhança do que ocorreu no caso da ADPF nº 635.

Conclui-se, com o presente trabalho, que é extremamente importante e urgente a edição de norma que venha a regulamentar o tratamento de dados pela Defesa Nacional e Segurança do Estado, ainda que seja adotado um modelo mais ou menos rígido ou mais ou menos restritivo do direito, a fim de que o Poder Judiciário não venha a ser chamado a fazê-lo.

Com essa necessária regulamentação, conforme argumentado no item 3.3 do Capítulo terceiro deste trabalho, contribuir-se-ia para que seja(m): a) assegurada, por um lado, a circulação de dados pessoais entre os vários organismos militares envolvidos, sem que deixe de ser observada, por outro lado, a preservação da privacidade dos cidadãos; b) evitados possíveis impactos provocados por eventual divulgação imprópria de dados pessoais, incluindo a inviabilização de oportunidades comerciais (retaliação como mecanismo de indução ao cumprimento dos preceitos de privacidade), bem como de cooperações internacionais nessa seara de atuação; e c) fortalecida a segurança da informação no tratamento desses dados, para propiciar a devida proteção dos dados pessoais.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros, 2008.

ARÁGON REYES, Manuel. **Temas básicos de derecho constitucional**. Tribunal constitucional y derechos fundamentales. Madrid: Civitas, 2001. t. 3.

BAPTISTA, Ricardo Córdoba. **Privacy by design**: privacidade incorporada aos projetos. Disponível em: <https://jus.com.br/artigos/83496/privacy-by-design-privacidade-incorporada-aos-projetos/2>. Acesso em: 6 ago.2021.

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

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 maio 2021.

BRASIL. Comando da Aeronáutica. **Portaria nº 899/GC3, de 28 de agosto de 2020**. Aprova a edição da Diretriz que dispõe sobre a Governança da Proteção de Dados Pessoais do Comando da Aeronáutica. Brasília, DF: COMAER, 2020d. Disponível em: [file:///C:/Users/user/Downloads/Z__COVID_226-BCA-ANEXO%202%20-%20DCA%2016-6%20\(GABAER\).pdf](file:///C:/Users/user/Downloads/Z__COVID_226-BCA-ANEXO%202%20-%20DCA%2016-6%20(GABAER).pdf). Acesso em: 8 ago. 2021.

BRASIL. Exército Brasileiro. **Portaria nº 088-EME, de 7 de maio de 2020**. Aprova a Diretriz de Orientação para Aplicação da Lei Geral de Proteção de Dados Pessoais no Exército Brasileiro (EB20-D-02.013). Brasília, DF:EB, 2020c. Disponível em: http://webcache.googleusercontent.com/search?q=cache:lFrJu7LyZXwJ:www.sgex.eb.mil.br/sistemas/boletim_do_exercito/copiar.php%3Fcodarquivo%3D1791%26act%3Dbre+&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 8 ago. 2021.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº

11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 30 abr. 2021.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional.** Brasília: MD, 2016a.

BRASIL. Supremo Tribunal Federal. **Mandato de Injunção 708/DF.** Impetrante: Sindicato dos trabalhadores em educação do Município de João Pessoa. Impetrado: Congresso Nacional. Relator: Min. Gilmar Mendes. 25 de outubro de 2017. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=558551>. Acesso em: 8 ago. 2021.

BRASIL. Tribunal de Contas da União. Secretaria de Fiscalização de Tecnologia da Informação (Sefti). Relatório de Fiscalização. **Fiscalização nº 232/2020.** TC n. 039.606/2020-1. Relator: Ministro Augusto Nardes. Brasília.2020b.

BRASIL. Tribunal de Contas da União. **Acórdão nº 4.035/2020.** Plenário. Relator: Ministro Vital do Rêgo. Sessão de 08/12/2020. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-2442373%22>. Acesso em: 22.ago.2021.

BRASIL. Tribunal de Contas da União. **Acórdão nº 2.737/2020.** Plenário. Relator: Ministro Vital do Rêgo. Sessão de 12/05/2021. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-2473503%22>. Acesso em: 22.ago.2021.

BRASIL. Tribunal de Contas da União. **Acórdão nº 2.909/2020.** Plenário. Relator: Ministro Augusto Nardes. Sessão de 28 de outubro de 2020a. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/redireciona/acordao-completo/%22ACORDAO-COMPLETO-2437249%22>. Acesso em: 22ago.2021.

Brasília, DF: **Presidência da República** [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 30 set. 2021.

CARDOSO, Marco Aurélio. **Liberdade negativa:** uma reflexão contemporânea. 2006. Disponível em: https://projetos.extras.ufg.br/conpeex/2006/porta_arquivos/posgraduacao/0545193-MarcoAur%C3%A9lioCardoso.pdf. Acesso em: 8 ago. 2021.

CAVOUKIAN, Ann. **Privacy by design:** the 7 foundational principles. Information and Privacy Commissioner of Ontario, jan.2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 6 ago.2021.

CONDEIXA, Fábio. **Comentários à lei de Acesso à Informação**. Disponível em: <https://jus.com.br/artigos/21436/comentarios-a-lei-de-acesso-a-informacao>. Acesso em: 20 jul. 2021.

DWORKIN, Ronald. **Levando os direitos a sério**. 2. ed. São Paulo: Martins Fontes, 2007.

FERREIRA FILHO, Manoel Gonçalves. **Princípios fundamentais do direito constitucional**: o estudo da questão no início do século XXI, em face do direito comparado e, particularmente, do direito positivo brasileiro. São Paulo: Saraiva, 2010.

GUICHOT, Emilio. **Publicidad y privacidad de la información administrativa**. Cizur Menor (Navarra): Thomson Civitas, 2009.

HART, H.L.A. **O conceito de direito**. São Paulo: Martins Fontes, 2009.

HERRÁN ORTÍZ, Ana Isabel. **La violación de la intimidad en la protección de datos personales**. Madrid: Dykinson, 1998.

MORAES, Alexandre de. **Direito constitucional**. 25. ed. São Paulo: Atlas, 2019.

PANOEIRO, Claudio de Castro. **Corrupción, transparência governamental y derecho de acceso a la información**: un análisis comparativo de la ley de transparencia y acceso a la información brasileña. 2014. Dissertação (Mestrado Universitário em Corrupción y Estado de Derecho) – Posgrado Estado de Derecho y Buen Gobierno, Universidad d Salamanca, Salamanca, Espanha, 2014.

SEMINÁRIO Internacional de Proteção de Dados “Once-only, But Privacy First”. [Brasília, DF: MP Streaming], 2021. 1 vídeo (3h22 min). Disponível em: <https://www.youtube.com/watch?v=VROskx8FdtM>. Acesso em 20 jul. 2021.

UNITED NATIONS. HumanRights. Office of the High Commissioner. **Universal Declaration of Human Rights**, 1948. Disponível em: <https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>. Acesso em: 8 ago. 2021.