Data de aprovação: _____/_____/_____

PROTEÇÃO DE DADOS E PODER PÚBLICO:
A APLICABILIDADE DA LGPD ÀS ORGANIZAÇÕES PÚBLICAS

Ana Flávia Cocentino Azevedo[1]
Msc. Edinaldo Benício de Sá Júnior[2]

RESUMO

O presente artigo tem como objetivo analisar juridicamente as possibilidades de aplicação da LGPD ao Setor Público, a fim de compilar informações quanto à adequação de instituições que compõem a esfera pública à proteção de dados pessoais, em consonância com a normativa supracitada, por meio de pesquisas documentais e bibliográficas. Nesse sentido, há, portanto, a pretensão de definir meios de adequação à Lei Geral de Proteção de Dados juridicamente corretos, além de delimitar quais seriam as metodologias aplicáveis à adequação das instituições que integram o Poder Público. Com isso, há a intenção de materializar por meio da pesquisa desenvolvida um compilado de úteis informações que esclareçam e colaborem com a implantação dessa norma considerada por muitos complexa e repleta de diferentes nuances, em especial no que tange às organizações públicas, contemplando tema de relevante interesse social e jurídico.

Palavras-chave: Lei Geral de Proteção de Dados. Proteção de Dados. Setor Público.

---

[1] Acadêmica do Curso de Direito do Centro Universitário do Rio Grande do Norte. Bacharel em Administração pela UFRN. Email: anaflaviacazevedo@gmail.com
[2] Advogado OAB-RN | Mestre em Direito pela UFRN | Professor | E- mail: beniciodesa.adv@gmail.com

ABSTRACT

This article aims to analyze the possibilities of applying the LGPD in the Public Administration, in order to compile information regarding the adequacy of institutions that make the public sphere to the protection of personal data, in line with the aforementioned regulations, through research documents and bibliography. In this sense, there is the intention of defining correct ways of adaptation to the General Data Protection Law, in addition to delimiting what would be the methodologies applicable to the adequacy of the institutions that make part of the Public Power. With this, there is the objective of materializing, through the research developed, a compilation of useful information that clarifies and collaborates with the implementation of this norm considered by many complex and full of different points, contemplating a relevant topic of social and legal interest.

Keywords: General Data Protection Law. Data Protection. Public administration.

1. INTRODUÇÃO

Diante dos avanços tecnológicos latentes em nossa sociedade, proveniente em grande parte da globalização e ampla utilização da internet, se fez necessária a normatização da utilização de dados a fim de proteger os indivíduos, mitigando abusos por parte dos detentores de informações de terceiros.

Nesse contexto, surge a LGPD, Lei Geral de Proteção de Dados, Lei n.º 13.709, de 14 de agosto de 2018, apresentando conceitos importantíssimos e regulamentando as relações com esses aglomerados de dados pessoais. Nesse sentido, o presente artigo surge com o objetivo de desenvolver uma análise jurídica da aplicabilidade da norma ao setor público, mediante estudo de jurisprudência, artigos científicos, leis e bibliografia.

Assim, a fim de alcançar o objetivo proposto, este trabalho é dividido em três capítulos. No primeiro deles, é contemplado o contexto histórico-normativo da temática em análise, considerando a relevância de compreender os fatos e aspectos legislativos antecedentes que levaram à publicação da lei vigente.

Segundo a norma supracitada, em seu artigo 5º, é considerado dado pessoal toda informação relacionada a pessoa natural identificada ou identificável, ou seja, ainda que não esteja explicitamente exposto o nome de um indivíduo, se o dado permite a identificação do mesmo através de outras informações trata-se de dado pessoal, e, portanto, deverá ser protegido.

Assim, o segundo capítulo do presente artigo discute a LGPD perante o Poder Público. Alguns autores defendem que a norma se aplica a todos que realizam tratamento de dados pessoais, sejam organizações públicas ou privadas. Desse modo, cabe também às organizações de caráter público identificar meios para viabilizar sua adequação à norma, considerando todas as suas particularidades. Para tanto, um subtópico do capítulo reforça esse entendimento, por meio da apresentação dos princípios que regem a Lei.

Além disso, a normativa em análise apresenta também a conceituação de dados pessoais sensíveis, que exigem maior cuidado e proteção, pois, discorrem sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico, desde que vinculados à uma pessoa natural.

Nesse sentido, esses dados pessoais são considerados sensíveis à medida que podem sujeitar o titular dos dados a práticas discriminatórias. E ainda, afirma que o tratamento desses dados deverá observar bases legais mais restritivas em comparação com os dados pessoais.

Nesse diapasão, o terceiro capítulo do presente trabalho discute as bases legais que viabilizam tal feito. Importa mencionar que a LGPD contempla no seu artigo 7º as hipóteses de tratamento de dados pessoais. O tratamento de dados, ainda segundo a norma, art. 5º, X, refere-se à toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Já as hipóteses contemplam algumas possibilidades de suma importância, como o fornecimento do consentimento por parte do titular, o cumprimento de obrigação legal ou regulatória pelo controlador, dentre outras. Há ainda, prevista nas hipóteses de tratamento de dados, na LGPD, art. 7º, III, quando feito pela administração pública, o tratamento de dados necessário à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. E ainda, na LGPD, art. 7º, IX, no atendimento de interesses legítimos do controlador.

Quando discutimos a aplicabilidade da Lei Geral de Proteção de Dados no Setor Público é importante considerar as hipóteses previstas no art. 7º da norma, e, além disso, refletir sobre as demais situações nas quais as instituições que compõem o poder público precisam se valer da utilização, coleta, processamento, armazenamento de dados, e demais atos de tratamento de dados.

Importa ressaltar, que a discussão é de suma importância uma vez que o tema teve seu impacto reforçado pelo entendimento de que a proteção aos dados pessoais constitui direito fundamental ao constatar que o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, ao passo que infere-se da consideração dos riscos que a automatização do tratamento traz à proteção da personalidade, levando em conta as garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, em consonância com a proteção da intimidade e da vida privada.

Assim, não restam dúvidas quanto ao notável ganho ao estabelecer rotas de adequação às normas, uma vez que são direitos indispensáveis aos indivíduos.

Ainda assim, se fez necessário o estabelecimento de uma normativa específica que objetivasse resguardar os direitos dos titulares de dados, bem como estabelecer diretrizes e normas que assegurassem a devida cautela ao se trabalhar com dados de terceiros.

2. DA PROTEÇÃO DE DADOS PESSOAIS: CONTEXTO HISTÓRICO NORMATIVO

O contexto social, político e econômico do século XXI reforça a importância de proteger dados. Informações são hoje um dos mais importantes e valorosos itens que uma organização pode dispor. Há uma grande demanda por profissionais que coletem, tratem, adequem, modifiquem, filtrem, ou seja, que trabalhem com dados, a fim de transformá-los no produto que as organizações necessitam.

Nesse sentido, Doneda (2011), contempla a possibilidade de dividir as normas que contemplam a proteção de dados pessoais em quatro gerações. A princípio, havia uma preocupação direcionada aos bancos de dados, que nos anos 70 ganharam espaço na sociedade e também à limitação da utilização e controle de informações por parte do Estado. Desse modo, voltava-se para o crescimento constante da utilização de novas tecnologias e processamento de dados, sem concentrar esforços na proteção do cidadão titular de dados.

Já na geração seguinte, o olhar se volta à privacidade dos indivíduos e no controle do acesso de terceiros aos dados, projetando mecanismos de controle para que os sujeitos pudessem tutelar seus próprios direitos individuais.

Por sua vez, a terceira geração de normativas ganhou um enfoque no princípio da liberdade, de modo que a fornecer ao titular condições de, por meio da autodeterminação, conhecer e manifestar posicionamento acerca da coleta e tratamento de seus dados.

Ao final, Doneda (2011) menciona ainda a quarta geração de leis que discutem a proteção de dados pessoais, enfatizando a aplicabilidade de técnicas que proporcionem equilíbrio entre as partes envolvidas no tratamento (o controlador e o titular de dados), de modo a minimizar as discrepâncias percebidas pelo desequilíbrio presente entre o ente responsável pelo tratamento e o indivíduo.

Assim, observa-se que as normas no Brasil que contemplam a questão da proteção de dados pessoais são anteriores à LGPD, inclusive é o país signatário de acordos internacionais anteriores à legislação específica, como a Convenção de Berna, de 1886 e também existem leis internas que guardam relação com o tema me alguns de seus artigos, como o Código de Defesa do Consumidor, o Marco Civil da Internet e o Decreto sobre Comércio Eletrônico.

Nesse contexto, Babiere (BABIERE, 2020) explicita a importância de observar que os dados, diferente de outros ativos organizacionais, podem ser copiados ou replicados. Isso não ocorre com outros recursos, como bens móveis, imóveis, mas no meio digital é possível replicar dados em sistemas, extraí-los, transferi-los. E isso, por si só, gera uma demanda robusta por mecanismos que possibilitem a proteção desse ativo.

Ainda nesse sentido, o autor esclarece que os dados precisam de um contexto para serem compreendidos, e ao ser fornecido esse complemento tem-se uma informação, que ao ser inserida dentro de um universo de outros dados se torna conhecimento.

Segundo Lóssio e Santos, diante da transformação digital, as organizações precisam se reconstruir, adequando seus processos internos (LIMA, 2021). Isso se aplica não somente às empresas privadas, mas também às instituições que compõem o poder público e ainda aquelas que integram o

terceiro setor. As mudanças percebidas pelo advento da internet, que promoveu consigo o alto e constante tráfego de dados de todas as espécies, gerou a necessidade de análise minuciosa dos processos que tratam essas fontes de riqueza que é a informação.

Assim, o que muito vale exige sua devida proteção. Para Pinheiro (PINHEIRO, 2020), o desenvolvimento de um modelo de negócio inserido na economia digital gerou uma dependência significativa dos fluxos de dados, especialmente dos dados relacionados aos indivíduos, uma vez que os avanços tecnológicos e a globalização possibilitaram essas modificações, de modo que, se fez necessária a elaboração de regulamentações que versassem sobre a proteção de dados pessoais.

Dessa forma, foi preciso repactuar o compromisso das instituições com os seres humanos, que hoje compõem também uma comunidade digital, habitam os meios virtuais, e anseiam por proteção e garantia de direitos humanos fundamentais, como o da privacidade, intimamente relacionados com os gigantescos fluxos de dados existentes no atual contexto social globalizado.

Foi na União Europeia que o debate acerca da formulação de normas que resguardam os direitos de privacidade, essencialmente quanto aos dados pessoais, surgiu. Intensificado pelo partido “The Greens”, em abril de 2016 foi promulgado o Regulamento Geral de Proteção de Dados Pessoais Europeu (GDPR), contemplando a proteção dos indivíduos quanto ao tratamento dos dados os quais seriam os titulares e a livre circulação desses.

Com isso, todas as empresas, países, e demais atores que possuíam relações com entes inseridos na União Europeia precisariam se adequar às normas apresentadas, de modo que, para manter suas relações com os entes europeus se fez necessária a adaptação aos preceitos de proteção de dados instituídos naquela esfera do continente. Estados e empresas que não apresentassem normas internas nos moldes da GDPR teriam dificuldades de negociar com seus pares da União Europeia, podendo, inclusive, sofrer com sanções e barreiras econômicas.

O regulamento citado tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de união econômica, possibilitando progresso econômico e social e consolidação e convergência das economias visando o bem-estar das pessoas físicas além de assegurar

um razoável nível de proteção das pessoas e evitar divergências que constituam obstáculos à livre circulação de dados pessoais no mercado interno. Além disso, objetiva garantir a segurança jurídica e transparência no tratamento de dados pessoais, impondo obrigações e responsabilidades aos controladores e processadores dos dados.

Desse modo, houve um incentivo vigoroso para que as demais nações produzissem normas de cunho similar, gerando a aprovação de leis, como é o caso, no Brasil, da Lei n. º 13.709, aprovada em agosto de 2018 e com vigência a partir de agosto de 2020. A norma surge com o fito de construir um ambiente de segurança jurídica através da padronização de normativas e condutas inerentes às atividades que englobam o tratamento de dados pessoais.

A própria norma, em seu art. 1º, ressalta que tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, em consonância com a legislação europeia supracitada e as demais normativas que dela decorrem.

Ademais, a lei brasileira, em seu artigo 5º apresenta uma série de conceitos fundamentais para a boa compreensão de seu regramento. Dentre eles, está a ideia de dado pessoal (art. 5º, I) , que é nada mais que a informação relacionada a pessoa natural identificada ou identificável. Ou seja, é dado pessoal tudo aquilo que permite a identificação do indivíduo, mesmo que não esteja expressamente mencionado o seu nome. Por exemplo, o dado que rotula alguém por cargo que ocupa não precisa estar nominado para permitir a identificação, como o prefeito da cidade de São Paulo no ano de 2022. Não é necessário rotular nominalmente para que seja possível identificar a quem pertence tal informação, que por si só já é um dado pessoal, pois, ainda que não diretamente, permite identificar o titular dos dados fornecidos.

Além disso, a legislação conceitua no art. 5º, X, o que seria o tratamento de dados pessoais, que engloba uma série de ações que ensejam proteção. São elas: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Isso significa

que, ainda que uma organização não trabalhe com os dados, apenas os armazene, deverá estabelecer medidas claras e definidas para promover sua proteção.

Tal proteção configura um direito fundamental, garantido pela promulgação da Emenda Constitucional Nº 115/2022, que explicitamente elencou a proteção de dados pessoais como garantia fundamental, fixando a competência privativa da União para legislar sobre o tema, que foi inserido no art. 5º da Constituição Federal do Brasil. Esse feito consolidou um entendimento que já vinha se confirmando no Supremo Tribunal Federal, reforçando ainda mais a relevância do tema e necessidade de adequação às normas produzidas.

Para Sarlet (LIMA, 2020), a proteção de dados é, em síntese, a proteção da pessoa humana, e a consequência imediata do advento da internet foi a ilusão de que esse seria um ambiente neutro e seguro. A partir disso, é possível refletir sobre os perigos que permeiam o mundo digital, que hoje, movimenta bilhões de reais todos os anos, e tem extrema força política, social, induz movimentos, tem estrondosa influência comportamental, sendo capaz de modificar opiniões e posicionamentos. Para a autora, os dados pessoais são ativos financeiros, mola propulsora da atualidade, o que implica em um latente interesse dos mais diversos atores em tratar dados pessoais, detendo, assim, uma fonte de poder.

Nesse contexto, as legislações vigentes são aplicáveis a todos os entes que tratam dados, ou seja, não somente empresas privadas precisarão se adequar. As normas supracitadas devem ser devidamente cumpridas por organizações públicas, empresas de economia mista e também as que compõem o terceiro setor.

Isso gera um desafio diferente para cada contexto, uma vez que ao observar a legislação e intencionar aplicá-la ao universo público é preciso considerar as variáveis que diferenciam as organizações públicas das privadas, pois, o motivo pelo qual os dados são armazenados, modificados, coletados, organizados etc, é muito diferente quanto objetiva-se a prestação de um serviço público eficiente. O que motiva a existência de organizações desse tipo não é a busca incessante por lucros, e sim a manutenção de uma grande variedade de serviços e atividades oferecidas à população.

Dessa forma, se faz necessário analisar como se dá a melhor forma de implementação de normas, como a Lei Geral de Proteção de Dados, considerando as características das atividades exercidas pelos órgãos que integram a União, os Estados e os Municípios, bem como o Distrito Federal. Avaliar métodos de aplicação e a própria legislação é fundamental para possibilitar a melhor adequação, viável aos moldes dos serviços prestados pela administração pública.

3. DA LEI GERAL DE PROTEÇÃO DE DADOS PERANTE O PODER PÚBLICO

Segundo Patricia Peck (2020), a lei geral de proteção de dados se aplica a todos que realizam o tratamento de dados pessoais, independente de serem organizações públicas ou privadas e independente dos meios, desde que o tratamento dos dados ocorra no território nacional, ou tenha como objetivo a oferta ou fornecimento de bens ou serviços ou tratamento de dados de indivíduos localizados no território nacional, ou ainda, que os dados tenham sido coletados no território nacional.

Diante da aplicabilidade, as organizações devem, portanto, identificar métodos adequados para implementação dessas normas nas suas respectivas esferas de atuação. Para tanto, se faz necessário identificar como atender os requisitos previstos de forma sustentável e duradoura.

Segundo Garcia (2020), uma opção é a utilização da metodologia BEST (business engaged security transformation), que apresenta uma abordagem adaptável ao sistema de gestão que atende à LGPD e foi concebida pela Fundação Vanzolini, baseado na promoção da conscientização e engajamento dos colaboradores.

Nessa abordagem, cada profissional deve contribuir para com a segurança dos sistemas de informação, responsabilizando-se pela solução implementada, considerando as restrições e especificidades decorrentes de cada área de atuação e suas particularidades. Nesse diapasão, ao objetivar a implantação da Lei Geral de Proteção de Dados no setor público se faz necessário considerar suas variantes específicas, decorrente das atividades

inerentes ao Poder Público, que inevitavelmente diferenciam-se das presentes no âmbito privado.

Segundo o Guia Orientativo da Autoridade Nacional de Proteção de Dados (ANPD), Tratamento de Dados Pessoais pelo Poder Público (2022), ao ser realizado pelas organizações que compõem o setor público o tratamento de dados pessoais possui muitas peculiaridades de modo que se faz necessário alinhar prerrogativas estatais típicas com os princípios, regras e direitos estabelecidos na legislação vigente.

A Lei N.º 13.709/18, define o termo “Poder Público” de forma ampla, contemplando no seu rol órgãos ou entidades dos entes federativos e dos três poderes, além das Cortes de Contas e do Ministério Público. Além desses, inclui ainda os serviços notariais e de registro, as empresas públicas e as sociedades de economia mista, desde que não estejam atuando em regime de concorrência ou operacionalizem políticas públicas no âmbito de sua execução.

Ainda segundo a norma, essas organizações devem observar o disposto na LGPD, ressalvadas as hipóteses previstas no art. 4º da Lei (tratamento realizado para fins exclusivo de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais), ou seja, a depender da hipótese de tratamento em uma mesma organização pode-se ter a aplicabilidade e a não aplicabilidade das restrições e demais regras impostas.

Há, ainda, a possibilidade aplicável apenas ao Poder Público, da ANPD solicitar informe específico sobre o âmbito, natureza dos dados e outros detalhes considerando relevantes para sua atuação, além de promover auditorias, a fim de garantir a conformidade das instituições dessa natureza perante o tratamento de dados pessoais.

Ademais, importa mencionar que os servidores públicos, em consonância com o art. 28 do Decreto Lei N.º 4.657/92, ao infringir a LGPD serão passíveis de responsabilização administrativa pessoal e autônoma. Assim, os casos, por exemplo, de venda de banco de dados, alteração de cadastro inadequada ou supressão de informações, para fins ilegítimos, poderão levar o servidor que praticou ato ilegal a ser responsabilizado.

3.1 DOS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Observa-se no art. 6º da Lei Geral de Proteção de Dados os princípios que fundamentam a norma, de modo que são indispensáveis para a boa compreensão do tema e devem ser analisados de forma complementar perante os artigos 23 a 30 do Capítulo IV, que apresentam normas direcionadas ao Poder Público.

Nesse sentido, o art. 6º, I, apresenta o princípio da finalidade e adequação, possibilitando inferir que o tratamento de dados pessoais deverá ocorrer a atingir propósito direcionados, específicos, claros e informados ao titular dos dados, não podendo o Poder Público apoderar-se desses dados com determinada finalidade e posteriormente utilizá-los para outro fim. Assim, aplicando o princípio em específico à esfera pública constata-se ainda que, nesse caso, a finalidade deve ser pública, além de legítima, específica, explícita e informada.

Ao contemplar a necessidade de vinculação da justificativa apresentada inicialmente ao tratamento efetivamente realizado tem-se a discussão acerca da possibilidade da utilização secundária perante outros propósitos legítimos.

Nesse sentido, a ANPD, em consonância com o Regulamento Geral sobre Proteção de Dados da União Europeia, recomenda que seja avaliada a compatibilidade entre a finalidade originária e a secundária, considerando para tanto o contexto e as circunstâncias do caso concreto, a existência de conexão fática ou jurídica entre ambas, a natureza dos dados pessoais - sugerindo cautela ao tratar-se de dados sensíveis -, os impactos percebidos pelos titulares e o interesse público e competências legais do entes envolvidos no tratamento posto, em observância ao art. 23 da LGPD.

Outrossim, há o princípio da necessidade, que aponta para a realização do tratamento de dados apenas nos casos em que verdadeiramente se faça imperioso a movimentação nos dados pessoais. Dessa forma, deve-se realizar as operações de tratamento com a menor quantidade possível a fim de atingir determinado objetivo específico.

Nesse sentido, aplicando-se tal princípio ao setor público cria-se a obrigação às entidades e órgãos públicos de checar periodicamente dados

coletados dos cidadãos que compõem bancos de dados e não são efetivamente necessários, a fim de minimizar o armazenamento excessivo de informações dispensáveis.

Por fim, o princípio da transparência, previsto no art. 6º, VI da Lei pertinente, manifesta-se com a finalidade de possibilitar ao titular dos dados tratados a disponibilização de informações quanto ao tratamento de seus dados. Nesse sentido, o princípio do livre acesso, que está presente também no art. 6º, IV, assegura aos titulares a previsão de consultar a os dados em tratamento, a forma, finalidade.

Diante disso, é possível constatar que, embora guardem muita semelhança, os princípios supracitados se diferenciam quanto à postura dos entes envolvidos, de modo que ao referir-se ao princípio da transparência observa-se a necessidade da postura ativa da organização pública em disponibilizar informações, enquanto no livre acesso é dada a possibilidade ao titular dos dados de ativamente solicitar o acompanhamento do tratamento de seus dados, ao menos ao haver pertinência.

Nesse sentido, a Lei N.º 14.129/2021 também estabeleceu normas quanto à publicidade de operações de tratamento de dados pessoais, ao pontuar que plataformas do governo devem dispor de ferramentas de transparência e controle de tratamento de dados, que sejam acessíveis aos cidadãos, de modo a consubstanciar as obrigações previstas na LGPD.

Assim, considerando as diretrizes que permeiam os princípios regentes da Lei Geral de Proteção de Dados é possível aferir os pontos indispensáveis de observância a fim de adequar organizações inseridas no Setor Público ao regramento previsto na norma em vigor, além de subsidiar tomadas de decisão perante temas controversos ou situações fáticas de difícil resolução, a partir de uma leitura conjunta dos princípios e normas vigentes.

Ademais, importa ressaltar a importância dos princípios norteadores, uma vez que são elementares na busca de uma interpretação adequada das normas em análise. Isso porque os princípios condicionam a análise realizada, e mais ainda quando se trata de uma norma recente, ainda com muitas análises a se realizarem, com poucas decisões proferidas acerca do tema e poucas jurisprudências consolidadas. Nesse cenário, fundamental se faz a interpretação adequada a partir dos princípios elencados previamente.

4. BASES LEGAIS DA LGPD: HIPÓTESES DE APLICAÇÃO DA NORMA NO SETOR PÚBLICO

Considerando a relevância do art. 7º da Lei Geral de Proteção de Dados, que apresenta as hipóteses nas quais poderá ocorrer o tratamento de dados pessoais é imprescindível ao aplicar a norma ao contexto do poder público enquadrar a situação fática dentro de uma dessas possibilidades elencadas no supracitado artigo, quando possível. (BRASIL, 2018)

Nesse sentido, se faz necessário analisar ainda o art. 11 da LGPD, que contempla as hipóteses de tratamento dos dados sensíveis. Tais artigos devem ser interpretados conjuntamente e em observância aos princípios norteadores das condutas do ente público.

Segundo Carvalho (2019), a Lei Geral de Proteção de Dados, bem como as bases legais que justificam o seu tratamento, podem ser aplicadas a situações diversas e não se restringem às relações de consumo, aplicando-se, portanto, também as situações presentes no Setor Público.

Para Serafino (2020), o tratamento de dados de terceiros é possível desde que haja a autodeterminação informativa, isto é, o titular deverá ter conhecimento acerca das atividades de tratamento realizadas com seus dados e a finalidade do tratamento deve pautar-se em alguma base legal.

Um relevante conceito que deve ser considerado na aplicabilidade da legislação no setor público é o consentimento do titular de dados. Segundo o art. 5º, XII, da LGPD, o consentimento pode ser conceituado como “a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”, e ainda, ao inserir-se na hipótese de dado sensível, o consentimento deve ser fornecido de forma específica e destacada, com os fins específicos a que se destina.

Já Boni (2020), assinala que o fato do consentimento precisar ser inequívoco enseja a necessidade de obter sua confirmação por meio de demonstração do controlador, resguardando a informação que o titular manifestou sua autorização para o tratamento específico e tal autorização

pode ser demonstrada por meio de vídeos, gravação de áudio ou outro meio claro de constatação do consentimento.

Ou seja, é necessário que o titular dos dados expressamente manifeste seu conhecimento acerca do tratamento que ocorrerá com seus dados, mediante apresentação específica do seu destino, com explícita concordância ou recusa. Ademais, a qualquer tempo o fornecedor dos dados poderá revogar o consentimento apresentado e solicitar a exclusão daqueles previamente concedidos.

Dessa forma, o tratamento de dados pessoais por parte do poder público nem sempre terá o consentimento como a base legal mais indicada, considerando que, muitas vezes, o tratamento de dados por parte de instituições que compõem o setor público se dá com o intuito de prestar um serviço cujo tratamento é obrigatório para cumprimento de obrigações legais.

Em outras palavras, há excepcionalidade nessas situações diante do papel exercido pelo ente que exerce prerrogativas estatais típicas, que exigem o tratamento de dados para manutenção da ordem do Estado. Entretanto, caberá a utilização do consentimento como base legal de forma eventual, quando a situação divergir do modelo supramencionado, certificando-se que não serão observados prejuízos ao interesse público. (BRASIL, 2022)

Uma outra base legal que, ao ser aplicada ao setor público, deve ser utilizada em casos eventuais é o legítimo interesse. Sua fundamentação consiste no art. 7º, IX da norma em análise e não se aplica ao tratamento de dados pessoais sensíveis.

Essa base legal permite o tratamento de dados pessoais quando for necessário para atender interesses legítimos do controlador ou de terceiros, e por não ser rígida, exige uma análise de proporcionalidade entre os interesses do controlador e do terceiro interessado e os direitos e expectativas do titular, podendo ainda este se manifestar em discordância com o tratamento quando este se der respaldando-se na hipótese de legítimo interesse. De modo que, não é recomendável utilizar-se dessa base legal para tratar dados no âmbito público de forma compulsória ou para cumprimento de obrigações e atribuições legais.

Isso porque nesse tipo de situação a ponderação necessária é dificultada, pois, a própria lei já a estabelece. Assim, bases legais como a execução de políticas públicas e cumprimento de obrigação legal são mais utilizadas pelo Poder Público.

Ainda assim, o legítimo interesse poderá ser utilizado em casos excepcionais, quando os dados não são utilizados compulsoriamente e o tratamento não se basear no exercício de prerrogativas típicas estatais.

Nesse sentido, faz-se pertinente expor a hipótese de tratamento pautada no cumprimento de obrigação legal ou regulatória, que está prevista no art. 7º, II, da Lei Geral de Proteção de Dados, bem como no art. n.º 11, II, a, da mesma lei. Porém, ao aplicar essa base legal no contexto do poder público se faz necessário diferenciar duas possibilidades distintas de ocorrência em virtude da espécie de norma jurídica que pauta a obrigação discutida. As possibilidades são: norma de conduta, que rege um comportamento, estabelecendo fato ou hipótese legal com consequências em caso de descumprimento; e as normas de organização, que estruturam os entes em suas competências e atribuições.

Diante disso, a diferença entre as duas possibilidades é que na primeira o tratamento se faz imprescindível para atender uma determinação legal, e, assim, não é necessário vínculo direto entre o tratamento de dados e o exercício de atribuições e competências do controlador. Já na segunda hipótese, o tratamento dos dados se faz necessário para permitir que o ente cumpra seu papel perante a sociedade, de modo a possibilitar o exercício de suas atividades de forma prática, cumprindo com a finalidade pública e garantindo a proteção do interesse público.

Ainda, importa mencionar que a Lei Geral de Proteção de Dados, no art. nº 23, menciona que o tratamento de dados pessoais ocorre no setor público com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, atendo-se à prestação dos devidos serviços executados. (BRASIL, 2018)

Nessa perspectiva, Otero (2019), reforça a necessidade das instituições que compõem o setor público identificarem as bases fundamentais que justifiquem o tratamento de dados por parte da organização, uma vez que, para o autor, essa é uma regra básica a ser

seguida por todos os entes que compõem a Administração Pública quando se trata da necessidade de tratamento e uso compartilhado de dados que se fazem indispensáveis para a execução de política públicas diversas.

O autor reconhece que em muitos casos o ente público acaba por realizar a retenção de dados que não se fazem mais necessários, mantendo em seus bancos informações desatualizadas e obsoletas tornando a atividade de adequação à Lei Geral de Proteção de Dados (2018) mais delicada.

Nesse sentido, ao discutir a aplicabilidade das bases legais às atividades exercidas pelos entes público, Otero (2019) recorda que, em sua perspectiva, o interesse legítimo não pode ser utilizado como base legal para o tratamento de dados pessoais no serviço público, de modo que se faz necessário um aprofundamento no tema para que as instituições procedam com as adequações necessárias, uma vez que, para o atendimento coeso na norma, é fundamental a definição de regras claras, algo até então parcialmente ausente na discussão da LGPD.

De acordo com Xavier (2022), fundamental é o papel da Autoridade Nacional de Proteção de Dados nessa árdua tarefa de identificar as hipóteses de tratamento, as bases legais que justificam a utilização dos dados dos indivíduos. Isso porque, incumbe à ANPD a missão de regulamentar as questões que por qualquer motivo estejam obscuras, ensejando o esclarecimento por meio das autoridades competentes para tanto.

Assim, considerando o cenário complexo de aplicação da norma no setor público, exige-se ainda mais atenção e dedicação das instituições e de todos os servidores que compõem esse sistema para que seja possível a devida adaptação frente à norma que é nova, complexa e enseja cuidados, especialmente ao se identificar lacunas quanto à devida orientação dos entes que passam por esse processo adaptativo de adequação à nova Lei Geral de Proteção de Dados.

O papel da ANPD, definido no art. n.º 55-J da Lei 13.709 de 2018 (BRASIL), contempla essa árdua tarefa de esclarecer, conforme se faça necessário, e com os meios possíveis as medidas à serem adotadas pelas instituições, de modo a facilitar sua conformidade institucional com a supracitada norma.

5. CONSIDERAÇÕES FINAIS

Em consonância com as informações apresentadas, especialmente ao que tange a legislação vigente, depreende-se a aplicabilidade da norma ao Poder Público, de modo direcionado, específico.

É necessário destacar as particularidades que permeiam a discussão do tema quando da aplicação aos entes que não compõem o mercado privado, e por conseguinte, que não desempenham suas atividades com o intuito puro e simples de obter lucro. As atividades realizadas pelas instituições do Poder Público são, naturalmente, diferentes daquelas realizadas pelo setor privado, e isso gera reflexos que se impõem também perante o tratamento de dados pessoais. De toda forma, há que se vislumbrar a aplicabilidade da norma no cenário em discussão.

Isso porque não se pode desconsiderar a importância da finalidade do tratamento dos dados pessoais, que respalda e norteia a Lei Geral de Proteção de Dados, e ao deparar-se com o setor público tem-se uma série de atividades desenvolvidas que tratam dados pessoais mas que tem por finalidade o interesse público, legítimo, diferenciando-se abissalmente do tratamento realizado por empresas privadas.

Nesse contexto, em recente julgado, o STF firmou entendimento, na análise conjunta da Ação Direta de Inconstitucionalidade (ADI 6649) e da Arguição de Descumprimento de Preceito Fundamental (ADPF 695), que é possível o compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal, em reforço a ideia que no âmbito público o olhar se diferencia do âmbito privado.

Além disso, nessa decisão, foi enfatizada a importância da hipótese de tratamento e atenção ao interesse do usuário, uma vez que segundo o relator, Ministro Gilmar Mendes, a permissão de acesso a dados pressupõe propósitos legítimos, específicos e explícitos para seu tratamento e deve ser limitada a informações imprescindíveis ao atendimento do interesse público.

Ou seja, os entes que compõem a Administração Pública, ainda que agindo no cumprimento de suas funções, respaldado em seu interesse legítimo de prestar determinado serviço à sociedade, devem, assim como qualquer outra instituição que realiza tratamento de dados pessoais, justificar

o tratamento, identificar a hipótese legal que permite o tratamento, informar ao usuário que tipo de tratamento e por qual motivo será realizado, além de prezar por todos os cuidados que garantam que a movimentação dos dados ocorrerá de maneira segura, seja ela de coleta, utilização, acesso, processamento, arquivamento, ou qualquer uma das formas previstas no art. 5º, X, da Lei nº 13.709/2018.

Portanto, cumpre ressaltar a relevante importância que a adequação às normas vigentes tem perante a segurança de dados de indivíduos, em especial no que se refere às instituições públicas, considerando que muitos dos dados fornecidos são necessários para realização de atividades básicas e essenciais aos usuários, como o fornecimento de dados para obter um documento, para ingressar com uma ação judicial, para realizar uma denúncia, garantir um benefício. Assim, são dados que, muitas vezes, são essenciais para o estabelecimento de algum serviço que o cidadão necessita, podendo inclusive conter dados sensíveis, e que merecem especial atenção do Poder Público na garantia de sua proteção.

Por fim, ressalta-se que, diante da inquestionável importância da proteção dos dados pessoais dos cidadãos, as instituições que compõem o setor público do país não podem ficar inertes, e devem atuar vislumbrando a total adequação às normas vigentes, levando em consideração, por óbvio, suas particularidades que a diferenciam das demais organizações do mercado.

Ademais, estão as autoridades competentes, como a Autoridade Nacional de Proteção de Dados, incumbidas de cooperar com essas instituições a fim de orientá-las e, assim, possibilitar sua correta adequação às normas vigentes que objetivam proteger e resguardar os direitos inerentes aos titulares de dados no país.

REFERÊNCIAS

BABIERI, Carlos. **Governança de Dados: Prática, conceitos e novos caminhos**. Rio de Janeiro: Alta Books, 2020.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade.** nº 6649/DF - Distrito Federal. Relator: Ministro Gilmar Mendes. 2022.

BRASIL, Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental.** nº 695/DF - Distrito Federal. Relator: Ministro Gilmar Mendes. 2022.

BRASIL. **Constituição**: República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais** (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia Orientativo**. **Tratamento de Dados Pessoais pelo Poder Público**. Brasília: ANPD, 2022.

BONI, Gabriela. **O consentimento como base legal para o tratamento de dados à luz da LGPD**. Revista Jus Navigandi, Teresina, ano 25, n. 6345, 14 nov. 2020. Disponível em: <https://jus.com.br/artigos/86621>. Acesso em: 11 de maio de 2022.

CARVALHO, Luiz et al. **Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais**. Anais do VII Workshop de Transparência em Sistemas. SBC, 2019. Disponível em: <https://sol.sbc.org.br/index.php/wtrans/article/view/6438> Acesso em junho de 2022.

CORREA, Luiz Felipe Batista. **Análise jurídica dos limites do consentimento com base na Lei Geral de Proteção de Dados (LGPD)**. Disponível em: <https://www.conteudojuridico.com.br/consulta/artigos/58271/anlise-jurdica-dos-limit

es-do-consentimento-com-base-na-lei-geral-de-proteo-de-dados-lgpd>. Acesso em maio de 2022.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico Journal of Law. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em junho de 2022.

GARCIA, Lara Rocha. **Lei Geral de Proteção de Dados Pessoais (LGPD) : guia de implantação**. São Paulo : Blucher, 2020.

LIMA, Ana Paula Moraes Canto. **LGPD aplicada**. São Paulo: Atlas, 2021.

LIMA, Cintia Rosa Pereira de. **Comentários à lei geral de proteção de dados**: Lei n. 13.709/2018, com alteração da lei. 18.853/2019. São Paulo: Almedina, 2020.

OTERO, Rodrigo Guynemer Lacerda. **A LGPD e seus efeitos no setor público.** Brasília: SERPRO. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2019/lgpd-setor-publico-efeitos> . Acesso em: julho de 2022.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13709/2018 (LGPD)**. 2 ed. São Paulo: Saraiva Educação, 2020.

XAVIER, Fábio Correa. **LGPD no Setor Público: bases legais para o tratamento de dados pessoais.** 2022. Disponível em: <https://www.migalhas.com.br/depeso/360877/lgpd-no-setor-publico-bases-legais-para-o-tratamento-de-dados> Acesso em novembro de 2022.