REVISTA
CADERNO
VIRTUAL

DA NECESSIDADE DE LIMITES AO TRATAMENTO E COMPARTILHAMENTO DE DADOS POR ÓRGÃOS DE INTELIGÊNCIA DO ESTADO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS EM MATÉRIA PENAL

Amanda Leite de Farias Ponte[1]

Resumo

O presente trabalho analisa a necessidade de imposição de limites bem estabelecidos para o tratamento e compartilhamento de dados por parte dos órgãos de inteligência estatal à luz da Lei Geral de Proteção de Dados em matéria criminal. A Lei nº. 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), em seu art. 4º, §1º, estabelece que o tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais deverá ser objeto de legislação específica e atualmente o anteprojeto de lei que regula o assunto dispõe de forma lacunosa sobre esses limites de atuação e proteção dos titulares de dados. O objetivo central do trabalho baseou-se em aferir se há necessidade de imposição de limites ao tratamento e compartilhamento de dados pelos órgãos de inteligência estatal e como essa limitação deveria se dar sem prejudicar o papel dos órgãos de segurança do Estado e os interesses públicos envolvidos. Adotou-se como metodologia de pesquisa a análise documental e metodologia dedutiva de revisão bibliográfica, buscando-se nas fontes primárias e na bibliografia secundária o suporte e consolidação do conteúdo escolhido.

Palavras-chave: Lei Geral de Proteção de Dados; Dados Pessoais; Limites ao tratamento de dados; Garantias individuais; Persecução penal.

Abstract

The present work analyzes the need to impose well-established limits for the treatment and sharing of data by state intelligence agencies in the light of the General Data Protection Law in criminal matters. Law n. 13.709/2018 – General Data Protection Law (LGPD), in its art. 4,

1 Pós-graduada em Direito Penal e Processo Penal pelo Instituto de Direito Público (IDP). Graduada em Direito pelo Centro Universitário de Brasília (UniCEUB). E-mail: amandalfponte@gmail.com

§1, establishes that the processing of personal data for the purposes of public security, national defense, State security and investigation activities and prosecution of criminal offenses must be the subject of specific legislation and currently the draft law that regulates the matter provides gaps about these limits of action and protection of data subjects. The main objective of the work was based on assessing whether there is a need to impose limits on the treatment and sharing of data by state intelligence agencies and how this limitation should take place without harming the role of state security agencies and the public interests involved. Documental analysis and deductive methodology of bibliographic review were adopted as research methodology, seeking in the primary sources and in the secondary bibliography the support and consolidation of the chosen content.

Keywords: *General Data Protection Law; Personal data; Limits to data processing; Individual guarantees; Criminal.*

INTRODUÇÃO

A Lei nº. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), tem o objetivo de proteger os dados de pessoas físicas e apresenta caráter de norma geral, que deverá ser observada por órgãos da União, dos Estados, do Distrito Federal e dos Municípios.

Em seu art. 4º, inciso III, a LGPD afasta sua aplicação sobre o tratamento de dados pessoais 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.

Já o §1º do art. 4º da referida Lei estabelece que o tratamento de dados pessoais inscritos no inciso III será objeto de legislação específica, a qual estabelecerá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal e os princípios gerais de proteção previstos na lei.

Diante dessa prerrogativa, foi elaborado um anteprojeto de lei pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, em 26 de novembro de 2019, com a finalidade de oferecer parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais.

O presente trabalho visa, portanto, por meio de análise documental e metodologia dedutiva de revisão bibliográfica, examinar a necessidade de imposição de limites ao tratamento e compartilhamento de dados por parte dos órgãos de inteligência do Estado à luz dos preceitos da legislação que trata sobre a proteção de dados, uma vez que há um déficit de proteção dos dados dos titulares, visto que não há regulação específica sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, causando insegurança jurídica.

O objetivo central do trabalho foi responder à seguinte pergunta: "Porque há necessidade de imposição de limites ao tratamento e compartilhamento de dados por órgãos de inteligência Estatal e como essa limitação deverá se dar sem prejudicar o papel da segurança do Estado e os interesses públicos envolvidos?".

Ao final, busca-se constatar se o anteprojeto de lei que regula a Lei de Proteção de Dados em matéria criminal impõe limites ao tratamento de dados pelas autoridades competentes, de modo a observar os ditames e garantias constitucionais que buscam assegurar a proteção ao direito de privacidade dos titulares dos dados, especialmente no tocante a necessidade de observância aos princípios da proporcionalidade, finalidade, necessidade e motivação.

Buscou-se verificar, ainda, qual o entendimento do Supremo Tribunal Federal que vem sendo aplicado nos casos de tratamento e compartilhamento de dados de cidadãos por parte dos órgãos de inteligência estatal e quais os parâmetros, limites ou especificações que são definidos em relação ao tema. Tudo isso, atrelado a problemática causada pelo déficit de proteção dos dados das pessoas físicas que motivou a criação da referida legislação.

1. A LEI GERAL DE PROTEÇÃO DE DADOS

A Constituição Federal de 1988, em seu art. 5º, inciso X, considera invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. Da mesma forma, o inciso XII, do mesmo artigo, garante a inviolabilidade do sigilo postal, de dados e das comunicações telefônicas, salvo por ordem judicial.

Ocorre que apenas a partir da Lei nº. 12.965/2014, conhecida como Marco Civil da Internet (MCI) tornaram-se mais claros os direitos dos usuários da *internet* no Brasil. Essa Lei foi responsável por regular questões como a inviolabilidade e o sigilo de comunicações telemáticas, além da confidencialidade dos registros de conexão e acesso.

Na análise da Lei nº. 12.965/2014 alguns artigos merecem destaque por disciplinarem os princípios que regem o uso da *internet* no Brasil.

O artigo 3º, da Lei nº 12.965/2014[2] dispõe sobre os princípios que regem o uso da *internet*, dentre eles podemos citar: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos na Lei.

Conforme se verifica, desde a vigência da Lei nº 12.965/2014 há uma preocupação com a proteção dos dados pessoais dos indivíduos e a responsabilização dos agentes de acordo com suas atividades.

No contexto brasileiro, o Projeto de Lei nº. 53, de 2018 teve sua aprovação a partir mobilização por parte do Senado, ante o conhecimento, em 2016, dos vazamentos de dados em países estrangeiros protagonizado pela *Cambrigde Analytica*[3], empresa de análise de dados, que teria comprado acesso a informações de usuários do *Facebook*, uma das maiores redes sociais do mundo, usando tais dados para influenciar a eleição presidencial dos Estados Unidos.

---

[2] BRASIL. Lei nº. 12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[3] **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. G1, 2018 < https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml> Acesso em 01 de setembro de 2021.

Esse episódio ganhou atenção mundial e levou os diversos governos a discutir aprovações de leis visando a proteção dos cidadãos e da própria democracia a partir do tratamento, coleta e uso dos dados e responsabilização dos abusos cometidos.

Em 2018, o Congresso Nacional aprovou a Lei nº. 13.709/2018, que dispõe sobre a proteção de dados pessoais, tendo a referida legislação entrado em vigor em 18 de setembro de 2020.

A Lei Geral de Proteção de Dados (LGPD), como ficou conhecida, possui como base o Regulamento Geral da Proteção de Dados europeu (GDPR) – Regulamento nº. 2016/679 –, que está em vigor desde 25 de maio de 2018.

Na União Europeia, o GDPR foi responsável por assegurar aos cidadãos o direito à informação sobre o processamento de seus dados pessoais, local do processamento desses dados e sobre sua finalidade, trazendo uma maior proteção aos titulares de dados.[4]

No Brasil, a Lei Geral de Proteção de Dados (LGPD) foi elaborada com o intuito de garantir a transparência e a utilização adequada de dados pessoais, bem como proteger os direitos fundamentais dos titulares de dados.[5]

A Lei nº. 13.709/2018 está dividida em dez capítulos com a seguinte disposição: Capítulo I – Disposições preliminares; II – Do Tratamento de dados pessoais; III- Dos Direitos do Titular; IV- Do Tratamento de dados pessoais pelo poder público; V- Da transferência internacional de dados; VI – Dos Agentes de tratamento de dados pessoais; VII- Da Segurança e das boas práticas; VIII- Da fiscalização; IV- Autoridade nacional de proteção de dados (ANPD) e do Conselho nacional de proteção de dados pessoais e da privacidade e X- Disposições finais e transitórias.

---

[4]ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. **Proteção de dados pessoais e investigação criminal.** p. 24. Brasília, 2020. Disponível em <http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf> Acesso em 01 de setembro de 2021.

[5] Ibidem.

No art. 2º da LGPD[6] verifica-se os fundamentos que disciplinam a proteção de dados pessoais, sendo eles: I- o respeito à privacidade; II- a autodeterminação informativa; III- a liberdade de expressão, de informação, de comunicação e de opinião; IV- a inviolabilidade da intimidade, da honra e da imagem dos titulares; V- o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor e; VII- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Conforme se verifica, os fundamentos que disciplinam a LGPD são semelhantes aos encontrados na Lei nº. 12.965/2014, conhecida como Marco Civil da Internet (MCI) a exemplo da garantia da liberdade de expressão, comunicação e manifestação de pensamento.

O artigo 6º da LGPD[7] dispõe sobre os princípios que regem a atividade de tratamento de dados pessoais, dentre os quais constam:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

---

[6] BRASIL. **Lei Geral de Proteção de Dados.** Dispõe sobre a Lei de Proteção de Dados e altera a Lei 12.965, de 24 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados (LGPD). Redação dada pela Lei 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

[7] BRASIL. **Lei Geral de Proteção de Dados.** Dispõe sobre a Lei de Proteção de Dados e altera a Lei 12.965, de 24 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados (LGPD). Redação dada pela Lei 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Desta feita, os dados dos usuários só poderão ser tratados quando observados propósitos legítimos, com finalidades informadas ao titular, limitando-se o tratamento ao mínimo necessário para realização de suas finalidades. Ademais, os titulares deverão ter livre acesso as formas de tratamentos desses dados, obtendo informações claras e precisas dos organismos responsáveis pela guarda dessas informações, os quais deverão garantir a não discriminação dos titulares de dados, sob pena de responsabilização e sendo suscetíveis a prestação de contas.

Além do conhecimento dos princípios que regem a LGPD faz-se de extrema importância a conceituação e diferenciação existente na Lei acerca dos diferentes tipos de dados. A LGPD abrange diferentes tipos de dados que são classificados como dados cadastrais (como a identificação do titular), dados de conteúdo (informações financeiras, tributárias etc.), além dos dados considerados como sensíveis.[8]

De acordo com o art. 5º, II, da LGPD, dados pessoais sensíveis são aqueles relativos à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato

[8] ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. **Proteção de dados pessoais e investigação criminal.** p. 16. Brasília, 2020. Disponível em <http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf> Acesso em 01 de setembro de 2021.

ou à organização de caráter religioso, à opinião filosófica ou à opinião política, à saúde ou à vida sexual, às informações genéticas e biométricas quando vinculadas a uma pessoa natural.

A distinção entre dados pessoais e dados pessoais sensíveis se faz de extrema importância pois a tutela em relação ao tratamento de dados relacionados ao segundo grupo deve se dar de forma mais rígida, uma vez que o mal tratamento desses dados são diretamente responsáveis por gerar condutas discriminatórias, abalando o Sistema Democrático de Direito.

Nas palavras da doutrinadora Ana Frazão[9]:

> "(...) o objetivo da LGPD é o de conferir uma ampla proteção ao cidadão e às situações existenciais mais importantes que são afetadas pelo tratamento de dados. Logo, seja em razão do amplo alcance da LGPD, seja em razão da sua preocupação com a tutela das situações existenciais dos titulares de dados, pode-se dizer que foi acolhida concepção convergente com a daqueles que sustentam que a proteção de dados corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante".

Importante ressaltar que todas as informações tuteladas pela LGPD interessam ou podem interessar a investigações criminais e são cotidianamente utilizadas pela Polícia ou pelo Ministério Público nas mais variadas situações.

A despeito disso, a LGPD, da mesma forma que o Marco Civil da Internet, não trouxe regulação da proteção de dados pessoais no âmbito da segurança pública e da persecução criminal, retardando a regulação nessa matéria.

De acordo com o art. 4º, inciso III, da LGPD, a referida lei não se aplica ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Assim, a Lei nº. 13.709/2018 não abrange os problemas relativos à captação, ao tratamento e ao compartilhamento de dados em matéria penal, uma vez que exclui de seu âmbito os dados coletados para fins exclusivos de segurança pública, defesa nacional, segurança

---

[9] FRAZÃO, Ana. **Direitos básicos dos titulares de dados pessoais**. Revista do Advogado, São Paulo, v. 39, n. 144, p. 33-46, nov. 2019. Disponível em < http://200.205.38.50/biblioteca/index.asp?codigo_sophia=155137 > Acesso em 01 de setembro de 2021.

do Estado ou atividades de investigação e repressão de infrações penais, aos quais se exigiu a edição de um diploma legal específico, restando, na prática, a hermenêutica dos ditames normativos sem um controle basilar, conforme se verá a diante.

2. A LEI GERAL DE PROTEÇÃO DE DADOS EM MATÉRIA PENAL

A Lei Geral de Proteção de Dados (LGPD) dispõe sobre o tratamento de dados. No entanto, a referida Lei não se aplica inteiramente a casos de tratamento de dados pessoais para fins exclusivamente de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, inciso III, LGPD). Isso significa que a referida legislação não abarcou operações de tratamentos de dados pessoais no âmbito penal.

Segundo Jacqueline de Souza Abreu, são exemplos de operações de tratamento de dados pessoais realizadas por órgãos estatais para fins de segurança pública as coletas de informações dos titulares de dados envolvidos no sistema de justiça criminal para instrução de um banco de dados de material genético (DNA) e de ampliação de bancos de dados de condenados, além dos dados gerados pela utilização de tornozeleiras eletrônicas.[10]

Ainda nas palavras de Jacqueline de Souza Abreu, dentro dessa categoria podem ser colocadas as operações de tratamento de dados vinculados à coleta de imagens de ambientes públicos por meio de instalação de câmeras de monitoramento, além da utilização de drones para obtenção dessas informações e operações associadas a áreas fronteiras, como controles de passaporte e coleta de imagens e informações biométricas ligadas a atividades de Polícia Federal.[11]

Já os órgãos estatais que tratam dados para fins de persecução penal, estarão encarregados do armazenamento, tratamento e compartilhamento de dados relativos a registros

---

[10] ABREU, Jacqueline de Souza. **Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD.** *In:* DONEDA, Danilo. Tratado de proteção de dados pessoais. Rio de Janeiro: Editora Forense, 2021. <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/cfi/6/84!/4@0:0> Acesso em 31 de agosto de 2021.

[11] Ibidem.

criminais, informações sobre investigações, indiciamentos, medidas cautelares, processos, condenações ou execução da pena.

Nesse ponto, imperioso tecer considerações sobre as diferentes funções e finalidades da persecução penal, da segurança pública, e dos serviços de inteligência, uma vez que possuem clara distinção. Enquanto a persecução penal está voltada para a confirmação de uma suspeita, ou seja, desenvolve-se por um interesse repressivo, buscando apurar uma infração penal e sua autoria, a atividade de segurança pública tem um sentido significativamente diverso. A função precípua dos órgãos de segurança pública é a proteção contra perigos, de modo que o sentido da atividade de segurança pública é preventivo.[12]

No tocante as atividades do serviço de inteligência, são imprescindíveis na coleta e análise de informações necessárias para antecipar perigos e formular políticas de segurança interna ou externa, possuindo margem ampla de investigação com alto poder interventivo na esfera dos dados pessoais, daí a importância de estabelecer parâmetros bem delineados quanto a finalidade da coleta a análise de dados (vinculação à finalidade).[13]

Em relação a esse aspecto da proteção de dados, atualmente tem-se um anteprojeto de lei, elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019 com a finalidade de oferecer balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal.

Na exposição de motivos do referido Anteprojeto de Lei que trata da proteção de dados em matéria penal consta expressamente que:

> "(...) o intuito deste anteprojeto é disciplinar os princípios, as diretrizes e as linhas mestras da proteção de dados no referido âmbito. Busca-se, portanto, harmonizar, de um lado, os deveres do Estado na prevenção e na repressão de ilícitos criminais, protegendo a ordem pública; de outro, assegurar a observâncias das

[12] GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O Direito de Proteção de Dados no Processo Penal e na Segurança Pública**. 1. Ed. – Rio de Janeiro: Marcial Pons, 2021. Págs. 54/56.
[13] Ibidem.

> garantias processuais e as prerrogativas fundamentais dos cidadãos brasileiros no que tange ao tratamento de dados pessoais para tais fins".[14]

Dessa forma verifica-se que a legislação busca disciplinar os princípios e diretrizes do tratamento de dados em matéria criminal, de modo a proteger os cidadãos titulares de dados, garantindo a observância das garantias processuais e das prerrogativas fundamentais desses cidadãos.

O Anteprojeto de Lei apresentado pela Comissão de Juristas atualmente encontra-se estruturado da seguinte forma:(i) âmbito de aplicação da Lei; (ii) condições de aplicação; (iii) base principiológica; (iv) direitos e obrigações; (v) segurança da informação; (vi) tecnologias de monitoramento; (vii) transferência internacional de dados e; (viii) a autoridade de supervisão.

Sobre a proposta apresentada, entende-se que se dedica a realizar um debate importante entre atividades de tratamento de dados pessoais e atividades de segurança pública e persecução penal. O art. 2º da LGPD penal replica os fundamentos da Lei nº. 13.709/2018, acrescentando os fundamentos relativos à presunção de inocência; a confidencialidade e integridade dos sistemas informáticos pessoais; a garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

O Anteprojeto de Lei que dispõe sobre a LGPD em matéria criminal impõe, ainda, a observância a princípios que servirão de limites para o tratamento e compartilhamento de dados pelos órgãos de segurança pública e persecução penal, quais sejam: (I) licitude: embasamento do tratamento em hipótese legal; (II) finalidade: fins devem ser legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; (III) adequação: pertinência do tratamento com suas finalidades; (IV) necessidade: o dados devem ser o mínimo suficiente para consecução dos objetivos do tratamento; (V) proporcionalidade: compatibilidade do tratamento com seus objetivos; (VI) livre acesso: garantia de facilidade e gratuidade aos titulares ao acesso às informações do tratamento de seus dados; (VII) qualidade dos dados: garantia aos titulares de dados de exatidão, clareza, relevância e atualização dos seus dados; (VIII) transparência:

---

[14] O Anteprojeto de Lei está em https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf

garantia aos titulares de informações claras, precisas e acessíveis sobre o tratamento e seu responsável; (IX) segurança: utilização de medidas técnicas e administrativas para a não violação de dados; (X) prevenção: adoção de medidas de prevenção de violações; (XI) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e (XII) responsabilização e prestação de contas: demonstração de medidas que comprovem a observância e a eficácia das normas de proteção de dados.[15]

Diferentemente da Lei nº. 13.709/2018, a LGPD em matéria penal prevê a observância aos princípios da licitude e da proporcionalidade.

Segundo o princípio da proporcionalidade, se o tratamento de dados for necessário para o interesse público, deve ser proporcional ao objetivo visado, respeitando-se, sempre, a proteção dos dados pessoais e os direitos fundamentais e interesses do titular. Dessa forma, ainda que relevante o "interesse público", este não pode sobrepor-se aos direitos fundamentais do indivíduo.

A título de exemplo, a Diretiva 680/2016 da União Europeia, em seu artigo 8º, impõe um dever positivo para o tratamento dos dados, de modo que os órgãos responsáveis pelo tratamento devem especificar o objetivo do tratamento, o dado pessoal a ser tratado e sua finalidade. A finalidade exige o tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, devendo ser compatível com o fim informado, estando o tratamento vinculado a uma finalidade.[16]

Da mesma forma que a lei geral, a LGPD penal distingue os dados pessoais dos dados pessoais sensíveis, trazendo ainda a categoria dos dados pessoais sigilosos, que são aqueles constitucionalmente protegidos por sigilo, como por exemplo, aqueles relativos a operações financeiras, registros de conteúdo de comunicações privadas, geolocalização,

---

[15] BRASIL, Câmara dos Deputados. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal.** Brasília, DF: Câmara dos Deputados, 2019. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf> Acesso em 30 de agosto de 2021.

[16] GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O Direito de Proteção de Dados no Processo Penal e na Segurança Pública**. 1. Ed. – Rio de Janeiro: Marcial Pons, 2021. Págs. 54/56.

atividades e documentos físicos ou digitais em ambientes privados, fontes jornalísticas e segredo estatístico.

Sobre o tratamento dos dados sigilosos, a LGPD penal prevê que o acesso aos referidos dados somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal (art. 14, *caput).*

Nesse sentido, o Anteprojeto de Lei impõe sigilo aos elementos identificadores dos dados pessoais dos investigados e condenados sem trânsito em julgado, de modo que o acesso automatizado e massificado a documentos e peças processuais será vedado, com exceção dos atos decisórios (art. 15, *caput* e §1º), cabendo ao Poder Judiciário, o Ministério Público e as Polícias adotar as medidas de segurança para a proteção desses dados, sob pena de responsabilização.

Na perspectiva penal, os procedimentos de coleta, guarda, processamento, utilização ou transferência de dados pessoais, referem-se não apenas aos dados do autor de uma infração ou a vítima dela, como também aos demais agentes de atuação da esfera criminal, como os dados de testemunhas, peritos ou terceiros, sem nenhuma relação com o fato a ser provado, que poderão ser submetidos a interferência do Estado.[17]

O art. 7º do Anteprojeto de Lei traz a necessidade de distinção clara entre as diferentes categorias de titulares dos dados, dentre os quais constam:

> I – pessoas em relação às quais existem indícios suficientes de que cometeram uma infração penal;
> II – pessoas em relação às quais existem indícios suficientes de que estão prestes a cometer uma infração penal;
> III – pessoas processadas pela prática de infração penal;
> IV – pessoas condenadas definitivamente pela prática de infração penal;
> V – vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal; e
> VI – outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos ou associados das pessoas referidas nos incisos I a V.

---

[17] ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. **Proteção de dados pessoais e investigação criminal.** p. 26. Brasília, 2020. Disponível em <http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf> Acesso em 02 de setembro de 2021.

Como se verifica, inúmeros são os indivíduos titulares de dados submetidos ao tratamento dos dados em matéria criminal. Ocorre que atualmente há um enorme déficit de proteção dos dados desses cidadãos, visto que não há regulação sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de armazenamento e compartilhamento desses dados.

Nesse contexto, o titular dos dados é deixado sem garantias normativas e mecanismos institucionais aplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e até a observância do devido processo legal.

Atualmente o problema que se verifica, além da implementação e efetividade da LGPD em matéria penal, se dá em razão da imposição de parâmetros, ou limites ao tratamento e compartilhamento desses dados especificamente por parte dos órgãos de inteligência do Estado, de modo que as lacunas, à medida que vão surgindo, são submetidas ao Poder Judiciário para apreciação.

3. DO TRATAMENTO E COMPARTILHAMENTO DE DADOS PESSOAIS POR ÓRGÃOS DE INTELIGÊNCIA ESTATAL

O anteprojeto de lei de proteção de dados em matéria penal disciplina, no seu artigo 5º, os conceitos de atividade de segurança pública, a qual abrangeria toda e qualquer atividade exercida para preservação da ordem pública e para prevenção e detecção de infrações penais, e a atividade de persecução penal, que abrangeria toda e qualquer atividade exercida para a investigação, apuração, persecução e repressão de infrações penais por autoridades competentes.

Entretanto, o anteprojeto de lei não é claro acerca da conceituação de atividades de inteligência estatal, embora essa atividade sistemática seja realizada com a finalidade precípua de coletar e analisar informações a fim de orientar a ação estatal.

A Lei nº 9.883, de 7 de dezembro de 1999[18], institui o Sistema Brasileiro de Inteligência (SISBIN) e estabelece como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado.

Conforme dispõe o artigo 1º, §1º da Lei nº. 9.883/1999, o Sistema Brasileiro de Inteligência (SISBIN) tem como fundamentos a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a dignidade da pessoa humana, devendo cumprir e preservar os direitos e garantias individuais e demais dispositivos da Constituição Federal, os tratados, convenções, acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatário, e a legislação ordinária.

As atividades de inteligência possuem, portanto, a função precípua de coleta e análise de informações necessárias para prever ou antecipar perigos e formular políticas de segurança interna ou externa, desse modo, a inteligência está voltada à precaução, prescindindo de um ensejo para sua atuação, exercendo função para além dos limites interventivos que caracterizam proteção contra perigos para a segurança pública e o processo penal.[19]

Gleizer, Montenegro e Viana, afirmam que as atividades de inteligência não estão vinculadas a uma finalidade específica, se tratando de uma atividade que atua em um campo prévio, sem estar submetida a um ensejo para entabular investigação. Segundo os autores:

> (...) serviços de inteligência atuam em um campo prévio, sem que estejam submetidos a um ensejo para entabular investigação, levantar e analisar dados. Essa faculdade de devassar a vida dos cidadãos sem um ensejo concreto põe sobre tensão a noção de Estado de Direito. A forma de equalizar essa desproporção do poder do Estado consiste em submetê-lo a um imperativo de separação.[20]

---

[18] BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. **Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências**. Diário Oficial da União de 08 de dezembro de 1999. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/l9883.htm> Acesso em 03 de abril de 2022.

[19] GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O Direito de Proteção de Dados no Processo Penal e na Segurança Pública**. 1. Ed. – Rio de Janeiro: Marcial Pons, 2021. Págs. 54/56.

[20] Ibidem.

Assim, há um risco associado à cooperação entre os órgãos de inteligência, uma vez que as atividades de inteligência possuem amplo poder de acesso à informação dos cidadãos e, em contrapartida, justamente por ter um caráter preventivo, não se submetem as regras impostas a segurança pública e ao processo penal no tocante a vinculação finalística, segundo o qual o propósito da intervenção precisa ser determinado de antemão.

Nesse sentido, a ABIN, por ser um órgão que tem como função precípua assegurar que o Executivo Federal tenha acesso a informações relativas à segurança do Estado e da sociedade, como aqueles que envolvem defesa interna e externa, além de não se submeter a uma vinculação finalística, não se submeteria a legislação geral, demandando uma legislação específica.[21]

Segundo Lilian Coutinho os serviços britânicos de inteligência, a exemplo do M15, M16 e GCHQ não se submetem à GDPR, operando e processando dados pessoais mediante outras medidas legislativas – *Data Protection Act 2018* - de modo que, diante das peculiaridades da atividade de inteligência, faz-se oportuna uma separação em relação ao tratamento realizado por outros órgãos estatais, a exemplos dos órgãos responsáveis pela segurança pública e persecução penal.[22]

Gleizer, Montenegro e Viana, tratando sobre dogmática constitucional e proteção de dados, dissertam sobre a necessidade da *separação informacional de poderes*, de modo que, por se tratar de funções estatais distintas, persecução penal, segurança pública e inteligência possuem finalidades particulares, devendo observar a necessidade de separação informacional. Nesse sentido, a transferência ou compartilhamento de dados entre persecução penal, segurança pública e inteligência deverá ser a exceção, e não a regra, uma vez que, se o tratamento de dado está vinculado a uma finalidade, e sua transferência fora das hipóteses explicitamente autorizadas configura *desvio de finalidade*.[23]

---

[21] COUTINHO, Lilian. **LGPD e Inteligência: Os Limites no Tratamento de Dados Pessoais Coletados em Fontes Abertas.** Revista Brasileira de Inteligência. Brasília: Abin, n. 15, dez. 2020. Pág. 109.

[22] Ibidem. Pág. 110.

[23] GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O Direito de Proteção de Dados no Processo Penal e na Segurança Pública**. 1. Ed. – Rio de Janeiro: Marcial Pons, 2021. Págs. 54/56.

Em 26 de julho de 2018 foi publicada a Portaria nº. 59 pelo Chefe do Gabinete de Segurança Institucional da Presidência da República. Essa normativa instituiu no âmbito da Agência Brasileira de Inteligência – ABIN, o Programa Nacional de Proteção do Conhecimento Sensível – PNPC, com a finalidade de promover proteção de conhecimentos sensíveis relativos aos interesses e à segurança do Estado.

O intuito do programa seria o de desenvolver atividades preventivas e corretivas de proteção de conhecimentos sensíveis, demonstrando um caráter de prevenção. Ocorre que a referida norma não previu as hipóteses de tratamento e compartilhamento de dados sensíveis pela ABIN com outros órgãos estatais, sendo silente em relação ao tema.

Assim, é importante que o legislador regule a temática e busque um equilíbrio entre a garantia dos direitos individuais dos titulares dos dados e a efetividade dos trabalhos típicos de um serviço de Inteligência, estabelecendo a observância do princípio da finalidade, impedindo tanto a ocorrência de excessos como as deficiências na atuação desses órgãos.

Em 2020, o Supremo Tribunal Federal reconheceu excesso por parte da atividade de inteligência do Ministério da Justiça e Segurança Pública, que foi responsável pela produção e disseminação de dossiê com informações de servidores federais e estaduais, tendo compartilhado os dados armazenados com diversos órgãos, como Polícia Rodoviária Federal, Casa Civil da Presidência da República, Agência Brasileira de Inteligência, Força Nacional de Segurança e outros três centros de inteligência vinculados à SEOPI, nas regiões Sul, Norte e Nordeste, o que gerou Arguição de Descumprimento de Preceito Fundamental (ADPF) ajuizada em 27 de julho de 2020.

O artigo 2º, §1º da Lei nº. 9.883/1999, estabelece que compete ao Sistema Brasileiro de Inteligência o processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo.

Ocorre que o Estado não pode, sob o argumento da prevenção/precaução de crimes e garantia da segurança nacional, invadir a esfera privada do cidadão e armazenar/compartilhar os dados obtidos sem a finalidade e motivação necessária, aptas a possibilitar um controle sobre os atos praticados. O dever de proporcionalidade e razoabilidade deve nortear toda a atividade estatal, sem o qual se mostra incontornável o vício aos preceitos constitucionais.

4. DA IMPOSIÇÃO DE PARÂMETROS AO TRATAMENTO E COMPARTILHAMENTO DE DADOS PELOS ÓRGÃOS DE INTELIGÊNCIA ESTATAL

Em 2016, o parlamento europeu e o conselho da União Europeia estabeleceram a Diretiva nº. 2016/680 para regulamentar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais pelas autoridades para efeitos de segurança pública e persecução penal. No referido documento, constam os princípios orientadores, como o da segurança e integridade da informação, qualidade dos dados, finalidade, necessidade e transparência.

No Brasil, o Anteprojeto de Lei que dispõe sobre a LGPD em matéria criminal impõe a observância aos princípios da licitude; finalidade; adequação; necessidade; proporcionalidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação e responsabilização e prestação de contas.

Além disso, os artigos 45 e 46 do Anteprojeto de Lei que dispõe sobre a LGPD em matéria criminal estabelecem as hipóteses de compartilhamento de dados entre as autoridades competentes:

> Art. 45. (...)
>
> § 1º Ressalvadas as hipóteses legais, é vedado o compartilhamento direto e contínuo de bancos de dados que contenham dados pessoais estabelecidos no âmbito de atividades de segurança pública com órgãos responsáveis pela persecução penal, exceto:
>
> I - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei;
>
> II - para investigação ou processo criminal específico.
>
> § 2º Requisições de acesso a dados entre autoridades competentes para uso compartilhado ocorrerão de forma devidamente motivada quanto ao contexto específico do pedido, à base legal, finalidade, necessidade e proporcionalidade, devendo o registro de acesso e de uso por agentes de autoridades competentes ser mantido por período de no mínimo 5 anos.

> Art. 46. O uso compartilhado de dados pessoais entre uma autoridade competente e um órgão ou entidade da administração pública não competente para os fins desta lei dependerá da demonstração de que o tratamento é compatível com a finalidade original da coleta, observadas as expectativas legítimas de titulares de dados e os objetivos de políticas públicas que ensejaram a coleta original.

Segundo artigo 46, o uso compartilhado de dados pessoais entre uma autoridade competente e um órgão ou entidade da administração pública não competente dependerá da demonstração de que o tratamento é **compatível com a finalidade original da coleta,** ou seja, deverá demonstrar a observância do princípio da finalidade, sob pena de violação ao mencionado artigo.

Assim, os princípios constantes na legislação servirão de balizas para o tratamento e compartilhamento de dados pessoais em matéria criminal, especialmente pelos órgãos de inteligência estatal, impondo certa limitação à atuação dos responsáveis pelo tratamento e compartilhamento desses dados.

Isso porque, os problemas que decorrem da exploração dos dados pessoais são muito mais extensos do que a mera violação do direito à privacidade. Nas palavras de Ana Frazão[24]:

> "(...) os problemas que decorrem da exploração dos dados pessoais são muito mais extensos do que a mera violação da privacidade, especialmente se tal direito for compreendido sob a sua concepção clássica, ou seja, no sentido de intimidade e do direito de ser deixado só. Além da privacidade, há vários desdobramentos da personalidade que são colocados em risco pela economia movida a dados, como a própria individualidade e autonomia. Mais do que isso, não é exagero afirmar que a própria democracia também passa a estar sob ameaça".

Deve-se verificar, assim, a assimetria entre soluções que visam ao interesse público e o empoderamento do titular dos dados pessoais, o qual tem direitos no tocante ao tratamento, coleta e uso desses dados, especialmente os dados considerados sensíveis.

---

[24] FRAZÃO, Ana. **Direitos básicos dos titulares de dados pessoais.** Revista do Advogado, São Paulo, v. 39, n. 144, p. 33-46, nov. 2019. Disponível em < http://200.205.38.50/biblioteca/index.asp?codigo_sophia=155137 > Acesso em 02 de abril de 2022.

Conforme exposto, o Supremo Tribunal Federal enfrentou o tema relativo à limitação da atividade de inteligência do Estado, na oportunidade de julgamento da ADPF 722, que tratou da violação a preceitos fundamentais consubstanciados no direito à liberdade de expressão e o direito à intimidade e à vida privada dos cidadãos.

A ADPF 722 foi provocada pelo Partido Rede Sustentabilidade em detrimento de um relatório produzido pelo serviço de inteligência do Ministério da Justiça e da Segurança Pública, em que constavam dados sensíveis de servidores federais e estaduais integrantes de movimentos antifascismo e de professores universitários, relativos à opção política dos indivíduos. Esses dados foram compartilhados entre órgãos da administração pública, tais como Polícia Rodoviária Federal, Casa Civil da Presidência da República, ABIN, Força Nacional, dentre outros.

Segundo o Ministério da Justiça, a elaboração desse dossiê seria pautada em sua atividade de natureza acauteladora e preventiva, justificada pela necessidade de prevenir, neutralizar e reprimir atos criminosos que atentassem contra a ordem pública e a segurança nacional, o que compatibiliza com as hipóteses de exceção de proibição de tratamento de dados pessoais previstas no art. 4º, inciso III, da LGPD.

Ao julgar o caso, a Relatora Ministra Carmem Lucia entendeu que o serviço de inteligência estatal é necessário para a segurança pública e para a segurança nacional, mas deve agir pautado nos limites constitucionais e legais, pois direitos fundamentais não são objeto de concessão estatal.

Segundo trecho do voto da Relatora:

> (...) Direitos fundamentais não podem ser objeto de ameaça ou lesão, nos termos constitucionais estampados. Nem o Judiciário atua para reparar direitos, senão quando não há mais via jurídica adequada para impedir o dano. O que se busca é que lesões a direitos fundamentais não ocorram, não persistam, não possam ser praticados. O Estado não pode ser infrator. Menos ainda em afronta a direitos fundamentais, que é sua função garantir e proteger. No Estado de direito tem o Poder Judiciário o dever de impedir, quando convocado, ameaça ou lesão a direito.
>
> Também não se demonstra a legitimidade da atuação de órgão estatal de investigar e de compartilhar informações de participantes de movimento político antifascista a pretexto de se cuidar de atividade de inteligência, sem observância do

> devido processo legal e quanto a cidadãos que exercem o seu livre direito de manifestar-se sem incorrer em afronta ao sistema constitucional ou legal.
>
> (...) l. O uso – ou o abuso – da máquina estatal para a colheita de informações de servidores com postura política contrária ao governo caracteriza desvio de finalidade.[25]

No que se refere ao direito à intimidade e à vida privada e a relação existente entre o tratamento de dados pessoais sensíveis, o ministro Gilmar Mendes pontuou, em seu voto, que o serviço de inteligência estatal é importante para o Estado, mas a atividade de inteligência estatal não está imune à necessidade de motivação. Asseverou, ainda, ser um risco a admissão de uma devassa na vida privada das pessoas, mesmo em procedimentos formais da inteligência estatal.[26]

O que se observa no caso apresentado é que os órgãos de inteligência, por possuírem uma natureza preventiva, não necessitando ensejo para entabular investigação, acabam tendo a faculdade de coletar, armazenar e compartilhar os dados obtidos sem que necessitem demonstrar a compatibilidade com a finalidade original da coleta (princípio da finalidade), de modo que se torna mais difícil o controle institucional.

Pelo exposto, verifica-se que a utilização de dados pessoais pelos órgãos estatais de inteligência, especialmente aqueles dados considerados como sensíveis, deverão observar os princípios da finalidade, da necessidade e da motivação, sendo esse o entendimento estabelecido pelo Supremo Tribunal Federal no bojo da ADPF 722/DF.

Pelo princípio da finalidade a coleta de dados pessoais só poderá ser feita para atingir objetivos específicos, explícitos e legítimos diante do escopo da segurança estatal, não

---

[25] BRASIL. Supremo Tribunal Federal. **ADPF n. 722/DF.** Disponível em <http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5967354 > Acesso em 31 de agosto de 2021. Pág. 88/89.

[26] BRASIL. Supremo Tribunal Federal. **ADPF n. 722/DF.** Disponível em <http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5967354 > Acesso em 31 de agosto de 2021. Pág. 88/89.

sendo possível sua utilização com fins ilegítimos e arbitrários, através da deturpação do dever-poder atribuído ao ente público.[27]

Pelo princípio da necessidade preza-se pela limitação do tratamento de dados ao mínimo necessário à realização de suas finalidades, ou seja, não será possível a utilização e o compartilhamento de dados de forma irrestrita. Os usuários de dados possuem direito à limitação do tratamento mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.[28]

Por fim, pelo princípio da motivação, a atuação no tocante a coleta, tratamento e compartilhamentos de dados devem ser justificados, de modo que haja a possibilidade de controle político e judicial em situações de desvio de finalidade.

Diante disso, fica claro que, mesmo para a inteligência estatal, há limites constitucionais que devem ser observados no tratamento e compartilhamento de dados pessoais.

Mais recentemente, em 2020, o Supremo Tribunal Federal deferiu parcialmente medida cautelar na Ação Direta de Inconstitucionalidade (ADI) 6529 para estabelecer que os órgãos componentes do Sistema Brasileiro de Inteligência (SISBIN) somente poderão fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (ABIN) quando for comprovado o interesse público da medida. De acordo com o entendimento majoritário, toda decisão que solicitar os dados de titulares deverá ser motivada, para possibilitar o controle de legalidade pelo Poder Judiciário.[29]

Em 08 de outubro de 2021, o Supremo Tribunal Federal votou o mérito da Ação Direta de Inconstitucionalidade (ADI) 6529, estabelecendo o entendimento de que a) os

---

[27] LOPES, Isabela Maria Pereira; OLIVEIRA, Marco Aurélio Bellizze. **Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018.** Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 2 ed. São Paulo: Revista dos Tribunais, 2020.

[28] ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. **Proteção de dados pessoais e investigação criminal.** p. 21. Brasília, 2020. Disponível em <http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf> Acesso em 02 de abril de 2022.

[29] BRASIL. Supremo Tribunal Federal. **ADI n. 6.529**. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837> Acesso em 07 de abril de 2022.

órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados; b) toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos fundamentais; e, d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN, são imprescindíveis procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abusos.

Conforme se verifica, o entendimento jurisprudencial caminha no sentido de que o tratamento e compartilhamento de dados pelos órgãos de inteligência, em matéria penal, deverá observar os limites delineados pela proteção constitucional, sob pena de incorrer em grave lesão a esses direitos e ameaça ao Estado Democrático de Direito.

Ocorre que, deve-se ter em mente, que o anteprojeto de lei que regula a proteção de dados em matéria penal, embora trate sobre o compartilhamento de dados no âmbito de atividades de segurança pública com órgãos responsáveis pela persecução penal, estabelecendo que é vedado o compartilhamento direto e contínuo sem autorização judicial e fora de propósitos legítimos e específicos (arts. 45 e 46), deixa de estabelecer diretrizes claras em relação aos serviços de inteligência estatal, mostra-se lacunosa, deixando de garantir uma efetiva proteção aos titulares de dados.

CONSIDERAÇÕES FINAIS

A Lei nº. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), tem o objetivo de proteger os dados de pessoas físicas. Em seu art. 4º, inciso III, a LGPD afasta sua incidência sobre o tratamento de dados pessoais 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.

Já o §1º do art. 4º da referida Lei estabelece que o tratamento de dados pessoais inscritos no inciso III será objeto de legislação específica, a qual estabelecerá 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 na lei.

A Constituição Federal de 1988 confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação. Trata-se do chamado direito à privacidade, o qual encontra-se instrumentalizado pelo art. 5º, incisos X e XII, da CF/88.

Nesse sentido, a manipulação e o tratamento de dados em matéria penal deverão observar os limites delineados pela proteção constitucional, sob pena de incorrer em grave lesão a esses direitos e ameaça ao Estado Democrático de Direito.

Surge daí a importância de delinear o alcance da Lei Geral de Proteção de Dados (LGPD) em matéria criminal, bem como a necessidade de imposição de parâmetros ao tratamento de dados por parte do Estado, especialmente no tocante a atuação dos órgãos de Inteligência Estatal, de modo a ensejar uma maior segurança jurídica, bem como diminuir as incertezas na aplicação e interpretação dos dispositivos relacionados ao tratamento de dados.

Ao final, constata-se que o anteprojeto de lei que regula a Lei de Proteção de Dados em matéria criminal, no tocante a imposição de limites ao tratamento e compartilhamento de dados pelos órgãos de Inteligência do Estado, mostra-se lacunosa, deixando de garantir uma efetiva proteção aos titulares de dados.

Embora os artigos 45, §1º e §2º e 46, ambos do anteprojeto de lei de proteção de dados em matéria penal tratem do tema, não são suficientes para estabelecer efetiva proteção aos cidadãos, vez que deixam de limites que garantam uma separação informacional, não trazendo as hipóteses que possibilitariam o tratamento e compartilhamento de dados entre os órgãos de segurança pública, persecução penal e serviços de inteligência estatal.

Identificou-se que o entendimento jurisprudencial que vem sendo consolidado pelo Supremo Tribunal Federal caminha no sentido de que o tratamento e o compartilhamento de dados pelos órgãos de Inteligência deverão observar os princípios da

finalidade, da necessidade e da motivação, de modo a possibilitar um maior controle do Poder Judiciário e evitar violação deliberada a direitos individuais.

Diante disso, fica claro que, mesmo para a inteligência estatal, há limites constitucionais que devem ser observados no tratamento e compartilhamento de dados pessoais, e a legislação atual é lacunosa sobre o tema, além de não estabelecer conceitos bem definidos para garantir a segurança jurídica necessária.

Consequentemente se faz necessário a elaboração de novos estudos para que o presente tema, de grande relevância, continue em evidência e, com isso, sejam elaboradas as especificações necessárias a fim de se evitar abusos, perseguições e utilização da legislação para obtenção de benefícios ilícitos.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Jacqueline de Souza. **Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD.** *In*: DONEDA, Danilo. Tratado de proteção de dados pessoais. Rio de Janeiro: Editora Forense, 2021.

ARAS, Vladimir. **A título de introdução: segurança pública e investigações criminais na era da proteção de dados**. Proteção de dados pessoais e investigação criminal. p. 24. Brasília, 2020. http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf

BRASIL. Câmara dos Deputados. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal.** Brasília, DF: Câmara dos Deputados, 2019. Disponível em <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf>

BRASIL. **Lei Geral de Proteção de Dados.** Dispõe sobre a Lei de Proteção de Dados e altera a Lei 12.965, de 24 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados (LGPD). Redação dada pela Lei 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BRASIL. Lei nº. 12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. **Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências.** Diário Oficial da União de 08 de dezembro de 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9883.htm

BRASIL. Supremo Tribunal Federal. **ADI n. 6.529**. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5972837

BRASIL. Supremo Tribunal Federal. **ADPF n. 722/DF**. Disponível em: http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5967354.

COUTINHO, Lilian. **LGPD e Inteligência: Os Limites no Tratamento de Dados Pessoais Coletados em Fontes Abertas.** Revista Brasileira de Inteligência. Brasília: Abin, n. 15, dez. 2020.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana. **Direitos básicos dos titulares de dados pessoais.** Revista do Advogado, São Paulo, v. 39, n. 144, p. 33-46, nov. 2019. Disponível em: http://200.205.38.50/biblioteca/index.asp?codigo_sophia=155137.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O Direito de Proteção de Dados no Processo Penal e na Segurança Pública**. 1. Ed. – Rio de Janeiro: Marcial Pons, 2021.

GOV.BR. **Guia de boas práticas Lei Geral de Proteção de Dados (LGPD).** 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf.

LOPES, Isabela Maria Pereira; OLIVEIRA, Marco Aurélio Bellizze. **Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018.** Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 2 ed. São Paulo: Revista dos Tribunais, 2020.