

Pontifícia Universidade Católica de São Paulo
PUC-SP

José Jerônimo Nogueira de Lima

LGPD e Administração Pública: regulação e aplicação

Mestrado em Direito Administrativo

São Paulo

Dezembro - 2020

Pontifícia Universidade Católica de São Paulo
PUC-SP

José Jerônimo Nogueira de Lima

LGPD e Administração Pública: regulação e aplicação

Mestrado em Direito Administrativo

Tese apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de Mestre em Direito Administrativo sob a orientação do Prof. Dr. Márcio Cammarosano.

São Paulo

Dezembro - 2020

Pontifícia Universidade Católica de São Paulo
PUC-SP

Defesa da dissertação do mestrando José Jerônimo Nogueira de Lima, intitulada “LGPD e Administração Pública: regulação e aplicação”, sob a orientação do Professor Márcio Cammarosano, apresentado à banca examinadora em 21 de dezembro de 2020.

Os membros da Banca Examinadora consideram o candidato: _____

Prof. Dr. Márcio Cammarosano – PUC/SP

Prof. Dr. Maurício Garcia Palhares Zockun – PUC/SP

Prof. Dr. Flávio Henrique Unes Pereira – IDP/DF

São Paulo

Dezembro - 2020

Agradecimentos

Ao Professor Márcio Cammarosano, por todo o ensinamento e atenção disponibilizada para a realização do trabalho.

Agradeço aos meus pais, Vera e Carlos, pelo estímulo constante para a continuidade dos estudos.

A Débora, minha namorada e companheira de todas as horas, por todo o esforço, compreensão e auxílio, posto que sem ela não seria possível a realização do mestrado, em especial, pelo amor e cuidado conferido aos nossos pequenos Joca e Chico.

Resumo

O objetivo do trabalho intitulado “LGPD e Administração Pública: regulação e aplicação” é evidenciar aspectos relacionados à Lei Geral de Proteção de Dados Pessoais, especialmente os inerentes ao órgão regulador e as situações em que a lei é aplicada, ou não, à Administração Pública, por meio de pesquisa à doutrina, jurisprudência, trabalhos acadêmicos e matérias jornalísticas. As conclusões revelam uma necessidade de atribuir maior independência à Autoridade Nacional de Proteção de Dados, na qualidade de regulador, bem como de observância aos princípios constitucionais e da lei geral de proteção de dados pela Administração, tanto nas hipóteses em que a lei se aplica ao Poder Público, quanto nas hipóteses em que não se aplica.

Palavras-chave: Administração Pública. LGPD. ANPD. Regulação. Aplicação.

Abstract

The objective of the work entitled “LGPD and Public Administration: regulation and application” is to highlight aspects related to the General Law for the Protection of Personal Data, especially those inherent to the regulatory body and the situations in which the law is applied, or not, to Public Administration, through research on doctrine, jurisprudence, academic works and journalistic articles. The conclusions reveal a need to give greater independence to the National Data and Protection Authority, as a regulator, as well as compliance with constitutional principles and the general data protection law to the Administration, both in the cases in which the law applies to the Government, as well as in the cases in which it does not apply.

Keywords: Public Administration. LGPD. ANPD. Regulation. Application.

Sumário

1. Do sistema normativo de proteção de dados pessoais e seus princípios
 - 1.1. Constituição Federal e o direito à privacidade
 - 1.2. Habeas data
 - 1.3. Lei dos arquivos públicos
 - 1.4. Código de Defesa do Consumidor
 - 1.5. Lei do Cadastro Positivo
 - 1.6. Marco Civil da Internet
 - 1.7. Lei Geral de Telecomunicações e Lei de Interceptações Telefônicas
 - 1.8. Sigilo das operações financeiras
 - 1.9. Demais diplomas normativos setoriais
 - 1.10. Lei Geral de Proteção de Dados Pessoais e seus princípios
 - 1.10.1. Princípio da finalidade
 - 1.10.2. Princípio da adequação
 - 1.10.3. Princípio da necessidade
 - 1.10.4. Princípio do livre acesso
 - 1.10.5. Princípio da qualidade dos dados
 - 1.10.6. Princípio da transparência
 - 1.10.7. Princípio da segurança
 - 1.10.7. Princípio da prevenção
 - 1.10.8. Princípio da não discriminação
 - 1.10.9. Princípio da responsabilização
 - 1.11. Conclusão
2. Autoridade Nacional de Proteção de Dados
 - 2.1. Organização administrativa
 - 2.1.2. Competência da ANPD
 - 2.2. Panorama da regulação exercida pelas Agências Reguladoras Federais
 - 2.2.1. Histórico das Agências Reguladoras
 - 2.2.2. Da regulação exercida pelas Agências Reguladoras
 - 2.2.3. Poder Normativo das Agências Reguladoras
 - 2.2.4. Análise de impacto regulatório
 - 2.2.5. Poder Sancionatório das Agências Reguladoras
 - 2.2.6. Da autonomia das Agências Reguladoras
 - 2.2.7. Da autonomia formal das Agências Reguladoras
 - 2.2.8. Da “nova lei das Agências Reguladoras” (Lei nº 13.838/2019)
 - 2.2.9. Conclusão Parcial
 - 2.3. Da experiência internacional
 - 2.3.1. GDPR: a exigência de uma autoridade de dados autônoma para a transferência transnacional de dados
 - 2.3.2. A autonomia regulatória exigida pela GDPR e OCDE
 - 2.4. Regulação prevista na LGPD
 - 2.4.1. Corregulação
 - 2.4.2. Regulação estatal e o paradigma do Banco Central do Brasil
 - 2.4.3. Do déficit de autonomia institucional da ANPD
 - 2.4.4. Autonomia administrativa
 - 2.4.5. Da natureza de órgão público como um risco à autonomia da ANPD. Caso do “dossiê antifascista”
 - 2.4.6. Da política de pessoal

- 2.4.7. Autonomia financeira
- 2.5. Conclusão

3. Hipóteses de não aplicação da LGPD em relação à Administração Pública

- 3.1. Interesse público x interesse privado: a compatibilização de direitos na LGPD
- 3.2. Da garantia de aplicação da legislação específica e dos princípios da proteção de dados
- 3.3. O Poder Público no exercício de tratamento de dados para fins de segurança pública e defesa nacional: há competência fiscalizatória e sancionatória por parte da ANDP?
- 3.4. Tratamento de dados por pessoa jurídica de direito privado sob a tutela do Poder Público
- 3.5. Experiência internacional – modelo adotado pela GPDR
- 3.6. Defesa Nacional e Segurança do Estado
 - 3.6.1. Ataques cibernéticos
 - 3.6.2. Ameaça terrorista
 - 3.6.3. Da nova estrutura da ABIN e a ADI nº 6529
- 3.7. Segurança pública e atividades de investigação e repressão de infrações penais
 - 3.7.1. Dos bancos de dados de perfil genético, multibiométrico e de impressões digitais previstos na lei anticrime
 - 3.7.2. Investigação com base em dados de geolocalização: *geofencing* ou busca reversa
 - 3.7.3. Criptografia: julgamento do caso Whatsapp
- 3.8. Conclusão

4. Da aplicação da LGPD ao Poder Público

- 4.1. Administração Direta
 - 4.1.1. Da aplicação aos Poderes Legislativo, Tribunal de Contas, Judiciário, Ministério Público e Defensoria Pública
- 4.2. Serviços notariais e de registro
- 4.3. Administração Indireta
 - 4.3.1. Aplicação da LGPD em relação às empresas estatais
 - 4.3.2. Especificidades da proteção de dados das estatais que prestam serviço público
- 4.4. Regime jurídico do tratamento dados pelo Poder Público
 - 4.4.1. Prerrogativa: desnecessidade de obtenção do consentimento do titular para o tratamento de dados
 - 4.4.2. Condicionamentos: cumprimento dos pressupostos previstos na LGPD
 - 4.4.3. A busca do interesse público no tratamento de dados pelo Poder Público
 - 4.4.4. Dever de informação e prestação de contas
- 4.5. Diplomas legais e Princípios aplicáveis ao Poder Público
 - 4.5.1. Lei de acesso à informação e eventual conflito com a LGPD
 - 4.5.2. Do tratamento de dados no âmbito das políticas públicas de enfrentamento do COVID-19
 - 4.5.3. Do tratamento de dados pessoais sensíveis pelo Poder Público
- 4.6. Regime jurídico do compartilhamento de dados pelo Poder Público
 - 4.6.1. Interoperabilidade como garantia do compartilhamento de dados

- 4.6.2. Do compartilhamento de dados no âmbito das políticas de enfrentamento do Covid-19
- 4.6.2. Extensão do compartilhamento de dados: das políticas públicas ao poder de polícia
- 4.6.3. Do compartilhamento de dados no âmbito do MPF na operação Lava Jato. O compartilhamento como política do controle de operações de tratamento de dados
- 4.6.4. Necessidade de estabelecimento de regras de governança para o compartilhamento de dados pelo Poder Público. Casos SERPRO e ABIN
- 4.6.5. Conclusão

Introdução

A passagem da sociedade industrial marcada pela produção fabril, fundada na estruturação mecanizada e pelo modelo fordista de produção, para a sociedade pós-industrial baseada na prestação de serviços, denominada *capitalismo leve* por Zygmunt Bauman, levou também a alteração das formas de relacionamento social e de interações econômicas.¹

Verifica-se no estágio atual da modernidade, ou da pós-modernidade, uma mudança de paradigma nos moldes em que tratado por Thomas S. Kuhn como decorrência de uma revolução tecnológica determinante para a alteração da tradição vigente, onde a criação de mecanismos capazes de processar e transmitir informações em quantidade e velocidade jamais imaginável consolidou uma nova forma de organização econômica e social baseada na informação, substituindo os meios que outrora mantinham a sociedade industrial.²³

Sobre o atual estágio da sociedade, o qual Zygmunt Bauman denominou como modernidade líquida, considerando a fluidez dos acontecimentos nos campos econômico e social, há uma análise do autor com relação às obras Admirável Mundo Novo de Aldous Huxley e 1984 de George Orwell no sentido de que, nada obstante a diferença de mundos retratados pelos autores visionários e distópicos, a visão de ambos se unia sobre o pressentimento de um futuro estritamente controlado, com mais vigilância ao ponto de homens e mulheres não terem o controle sobre suas vidas.⁴

O atual momento não sugere o extremo controle, mas reflete um crescente nível de vigilância pelos diversos meios, em um contexto em que os dados pessoais são compartilhados, customizados, tratados e amplamente utilizados por corporações e pelo próprio Estado sem que seja disponibilizado aos cidadãos o acesso e o conhecimento pleno à forma de utilização desses dados.

Shoshana Zuboff cunhou o atual estágio da sociedade coma expressão “capitalismo de vigilância”, considerando a invasão das diversas plataformas na vida privada dos indivíduos, onde a interação nas redes passa a ser a matéria-prima de um mercado que

¹ BAUMAN, Zygmunt. *Modernidade líquida*. Trad. Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

² KUN, Thomas S. *A estrutura das revoluções científicas*. São Paulo: Editora Perspectiva S.A., 1998.

³ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais e a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020. p. 4.

⁴ BAUMAN, op. cit.

tem como base a extração e o tratamento descontrolado de dados pessoais, sendo o atual cenário denominado pela autora como *Big Other*, pelo fato dessa vigilância ser realizada de forma ampla e pulverizada pelos diversos *players* do mercado⁵.

Há no atual contexto econômico e político uma ampla discussão acerca da titularidade e a forma de tratamento e compartilhamento dos dados pessoais, os quais se converteram em um grande ativo para a denominada economia da informação, onde a ciência aplicável a organização desses dados (big data) viabilizou a sistematização dos hábitos dos cidadãos, por meio de algoritmos capazes de automatizar tendências pessoais⁶.

Frank Pasquale (apud FRAZÃO, 2019, p. 42) resume de maneira contundente a forma com que os dados pessoais são tratados pelas diversas plataformas: “No seu livro Turing’s Cathedral, Jorge Dyson afirma que o Facebook define que somos, a Amazon define o que queremos e o Google define o que pensamos.”⁷.

No plano político internacional, foram divulgadas denúncias de coleta e tratamento abusivo de dados, a exemplo das revelações do ex-agente da National Security Agency Edward Snowden de um grande sistema de vigilância da população americana, bem como a suspeita de manipulação das eleições americanas de 2016, embora inexista evidências concretas de que o *Facebook* e a *Cambridge Analytics* tenham interferido no resultado das eleições. Os exemplos mencionados evidenciam como as plataformas detêm grandes quantidades de dados e significativo poder de determinação da vontade dos seus usuários, sendo assim hipoteticamente capazes de inclusive interferir em processos políticos, o que representa um risco real aos Estados e a democracia.⁸⁹

É dentro desse contexto que a União Europeia (UE) promulgou o Regulamento Geral de Proteção de Dados Europeu nº 679, aprovado em 27 de abril de 2016 (GDPR), com o objetivo de “harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre

⁵ ZUBOFF, Shoshana. *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*. *Journal of Information*, 04 abr. 2015, p. 85. Disponível em: <<https://cryptome.org/2015/07/big-other.pdf>>. Acesso em: 05 maio 2020.

⁶ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais e a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020. p. 10-12.

⁷ Frank Pasquale apud FRAZÃO, Ana. Fundamentos da Proteção dos Dados Pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 42.

⁸ Idem, p. 46.

⁹ Entenda o caso de Edward Snowden, que revelou espionagem nos EUA. *Globo.com*, 14 fev. 2014. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 23 mar. 2020.

circulação de dados pessoais entre os Estados-Membros”. Os países que mantêm relações comerciais com a Europa se viram obrigados a editar normativo com conteúdo adequado ao regulamento europeu, do contrário poderiam ter algum tipo de dificuldade comercial junto aos países membros da União Europeia, a exemplo da impossibilidade de receber dados pessoais de cidadãos europeus, por não terem nível correspondente de proteção de dados.¹⁰¹¹.

A experiência da autorregulação dos dados pessoais pelo mercado evidenciou ser insuficiente, na medida em que as empresas utilizavam dos dados pessoais de forma abusiva, por vezes de forma discriminatória, a exemplo da recente multa aplicada pelo Departamento de Proteção e Defesa do Consumidor (DPDC) a Decolar.com pela prática conhecida como *geo pricing* e *geo blocking*, ante o emprego de tarifas e disponibilização de ofertas de acordo com a localização geográfica do consumidor, evidenciado no caso que computadores de São Paulo tinham tarifas até 29% superiores aos ofertados aos localizados em Buenos Aires para as mesmas acomodações.

Foi diante de um amplo debate acerca da titularidade e da forma com que os dados pessoais são tratados não só pelas empresas como também pelos governos, que tivemos a criação da Lei Geral de Proteção de Dados Pessoais no Brasil (Lei nº 13.709, de 14 de agosto de 2018) editada com o objetivo de proteger os dados de pessoas físicas, com fundamento nos direitos fundamentais da liberdade de expressão, privacidade e o livre desenvolvimento da personalidade da pessoa natural (artigo 1º e 2º). A lei brasileira não se restringiu ao meio virtual, mas a todos os meios pelos quais os dados das pessoas podem ser extraídos, no entanto, é no meio virtual que se verifica as maiores preocupações acerca da proteção de dados.¹²

O estudo tem a finalidade de analisar as questões relacionadas a implementação da LGPD em relação a Administração Pública, nos seus aspectos regulatórios e executivos, considerando a complexidade do tema que deverá ser objeto de específico tratamento pelas diversas unidades político-administrativas integrantes da Federação. A título de exemplo, cita-se a atual controvérsia acerca da as iniciativas de combate ao COVID-19

¹⁰ Regras para a proteção de dados pessoais dentro e fora da UE. *União Europeia*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection_pt. Acesso em: 30 mar. 2020.

¹¹ PINHEIRO, Patrícia Peck. *Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD)*. São Paulo: Saraiva, 2018. p. 212.

¹² FRAZÃO. Ana. Fundamentos da Proteção dos Dados Pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 31-32.

que envolveram a parceria estatal, nos mais diversos níveis, com operadoras de celulares para monitorar aglomerações que, apesar de envolver supostamente dados agregados que seriam anonimizados, suscitou questionamentos acerca da possibilidade da individualização pessoal e da obtenção de dados considerados sensíveis pela LGPD, como a informação acerca da saúde do cidadão, o que levantou questões acerca da transparência de tais ações e do nível de proteção da privacidade no tratamento desses dados.

No que respeita a metodologia, foi adotado como padrão a pesquisa doutrinária, jurisprudencial e a análise de casos atuais com grande repercussão no tema da proteção de dados pessoais.

O estudo é dividido em quatro tópicos. A primeira parte, conceitual, trata das normas aplicáveis ao tratamento de dados pela legislação que antecedeu a edição da LGPD e, com relação à esta última, faz-se uma análise acerca dos princípios que informam a aplicação da lei.

Em um segundo momento, é abordado os aspectos estruturais da Autoridade Nacional de Proteção de Dados (ANPD), na qualidade de regulador criado para dar efetividade a proteção de dados no Brasil, especialmente a necessidade de atribuir autonomia institucional a ANPD, considerando que a regulação será exercida inclusive em relação a Administração Pública em seus diversos níveis.

O terceiro tópico trata das hipóteses em que a lei excepciona a proteção ao tratamento de dados pela Administração, o que não exclui a necessidade de controle de adequação e finalidade da utilização destes dados considerando a garantia constitucional assegurada aos direitos fundamentais inerentes à privacidade e à intimidade.

Por fim, são analisados as situações e os desafios a aplicação da LGPD no tratamento e compartilhamento de dados realizados pelos entes públicos, com suas complexidades de ordem material e jurídica.

1. Do sistema normativo de proteção de dados e seus princípios

1.1. Constituição Federal e o direito à privacidade

Desde os artigos de Samuel Warren e Louis Brandeis denominado *The right to privacy* de 1890 (Apud VAINZOF, 2019, p. 25), a privacidade foi compreendida como um direito do indivíduo, o direito a ser deixado só (*right to be let alone*), sendo que, segundo Rony Vainzof, o referido ensaio apontava como as novas tecnologias como a máquina fotográfica poderia adentrar ao domínio da vida privada, conceito que ganhou abrangência e posituação nos diversos ordenamentos jurídicos.”¹³

No atual contexto, temos verificado como as tecnologias relacionadas com o tratamento de dados pessoais se tornou um verdadeiro ativo da atual sociedade da informação para as empresas atuarem com mais eficiência no mercado, identificando com precisão os perfis de consumo dos indivíduos, voltando à tona a discussão acerca do direito à privacidade, considerando que as atuais tecnologias utilizam do cruzamento de dados pessoais cadastrais, análise de comportamento em redes sociais, compras com cartões de crédito, informações de geolocalização, ultrapassando muitas vezes o limite da vida privada.¹⁴

O direito à privacidade no Brasil possui status constitucional, estando devidamente previsto no artigo 5º, inciso X da Constituição que dispõe: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Cabe ressaltar que, seguindo a mesma lógica do dispositivo constitucional, prevê o art. 21 do Código Civil: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

Na sua visão tradicional, o direito à privacidade era definido como *right to be alone* e assemelhava com o direito de propriedade, mas sua atual leitura o aproxima com o princípio da dignidade humana (art. 1º, III, CF), em uma perspectiva extrapatrimonial sob

¹³ Samuel Warren apud VAINZOF, Rony. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 25.

¹⁴ Idem, p. 26.

a lógica de assegurar o indivíduo da manipulação irrestrita de seus dados pessoais pelas mais diversas plataformas públicas ou privadas.¹⁵

A Constituição previu no seu artigo 5º, XII o sigilo de meios como a correspondência, comunicações telegráficas, dados e comunicações telefônicas, sendo a proteção de dados pessoais até a edição da LGPD era realizada pela legislação infraconstitucional de maneira fragmentária, por específicos sigilos, a exemplo das informações recebidas por médicos, advogados, bancos e a administração tributária¹⁶. A lógica que vigia é que os dados cadastrais não estavam abrangidos pela garantia constitucional da privacidade, salvo exceções consideradas em diplomas esparsos, conforme posição de Tércio Sampaio Ferraz Júnior:

Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos – como nome, endereço, profissão, idade, estado civil, filiação, número de registro público, etc., condicionam o intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido.¹⁷

A questão da proteção de dados pessoais assumiu tamanha importância no atual estágio da chamada sociedade da informação, que há inclusive Proposta de Emenda Constitucional (PEC 17/2019) conferindo autonomia normativa a proteção de dados pessoais como um direito fundamental, com a intenção de conferir um regime jurídico próprio a questão, atribuindo a União a competência privativa para legislar acerca da disciplina dos dados pessoais.¹⁸

Cabe ressaltar, nesse ponto, que Portugal prevê em sua constituição o direito de proteção de dados pessoais (art. 35), sendo que segundo Canotilho (apud CUEVA, 2019, p. 88) o direito aos dados pessoais compreende as seguintes faculdades:

¹⁵ FILHO, Carlos Edison do Rêgo Monteiro; CASTRO, Diana Paiva de. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Coordenação). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 326.

¹⁶ SILVA, Carlos Bruno Ferreira da. *Proteção de Dados e Cooperação Transacional. Teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014. p. 213-215.

¹⁷ FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. In: PIZOLIO, Reinaldo. GAVALDÃO JR., Jayr (Org.). *Sigilo Fiscal e Bancário*. São Paulo: Quartier Latin, 2005. p. 28.

¹⁸ BRASIL. PEC 17/2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 25 mar. 2020.

(a) o direito de acesso, ou seja, o direito de conhecer os dados constantes de registros informáticos, quaisquer que eles sejam (públicos ou privados); (b) o direito ao conhecimento da identidade dos responsáveis, bem como o direito aos esclarecimentos sobre a finalidade dos dados. (c) o direito de contestação, ou seja, direito à rectificação dos dados e sobre a identidade e endereço do responsável. (d) o direito de actualização (cujo escopo fundamental é a correcção do conteúdo dos dados em caso de desactualização); (e) finalmente, o direito à eliminação dos dados cujo registro é interdito.¹⁹

O Supremo Tribunal Federal, por sua vez, ao analisar a medida cautelar na ADI nº 6387, referendou a decisão liminar da Ministra Rosa Weber que suspendeu a eficácia da MP nº 954/2020, a qual determinava que as empresas de telecomunicação disponibilizassem dados de nomes, números de telefone, dos seus usuários para fins de estatística oficial do COVID-19, sob o fundamento de violar a privacidade, valor constitucional previsto nos artigos 5º, incisos X e XII da Constituição e positivado no art. 2º, I e II, da LGPD.²⁰

O voto do Ministro Edson Fachin na ADPF nº 403, a qual analisa a constitucionalidade de determinações judiciais de acesso a conteúdo de comunicações de mensagens protegidos por criptografia, bem como da sanção de suspensão das atividades de aplicativos de mensagens, no caso o Whatsapp, citando o voto proferido pela Ministra Rosa Weber na ADI nº 6387, ressaltou a necessidade de atualizar o alcance dos direitos e garantias fundamentais no contexto das novas tecnologias, oportunidade em que consignou que a proteção “constitucionalmente assegurada ao direito à privacidade é, portanto, elevada, digna dos direitos que detêm a mais ampla primazia no ordenamento nacional.”²¹

Assim, o direito à privacidade é um direito com assento constitucional nos artigos 5º, incisos X e XII da Constituição, sendo que a proteção de dados pessoais constitui seu desdobramento com pretensão atual de alçar específica previsão constitucional, conforme se verifica da PEC 17/2019, considerando a importância que a proteção dos dados

¹⁹ José Joaquim Gomes Canotilho apud CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 88.

²⁰ BRASIL. Supremo Tribunal Federal. ADI nº 6387, Rel. Ministra Rosa Weber, julgamento 07 maio 2020.

²¹ BRASIL. Supremo Tribunal Federal. ADPF nº 403, Rel. Ministra Edson Fachin, julgamento 28 maio 2020.

peçoais vem adquirindo no contexto social e econômico, notadamente no que diz respeito aos limites de sua manipulação tanto pelas entidades privadas quanto públicas.

1.2. Habeas data

O habeas data previsto artigo 5º, LXXII da Constituição Federal de 1988 tem a finalidade de assegurar o conhecimento das informações do interessado constantes em bancos de dados de entidades governamentais ou de caráter público, bem como a retificação desses dados quando verificada inexatidão.

A Lei nº 9.507/97 que regula o habeas data prevê, além das hipóteses de conhecimento e retificação, possibilidade de contestação ou explicação sobre fato controverso (art. 7, III), sendo que a jurisprudência admite também o seu manejo como meio de complementação de informações de registros incompletos.²² O artigo 8º da lei, na esteira da jurisprudência consolidada na súmula 02 do STJ, impôs como condição da ação a prova da recusa pelo sujeito passivo, o que na visão de Alexandre de Moraes (apud SILVA, 2014, p. 233) representou uma limitação do direito de acesso ao Poder Judiciário e uma restrição ao direito de informação que é protegido pelo instituto.²³²⁴

Quanto a abrangência do cabimento do habeas data, apesar da tentativa o legislador de conceituar o termo banco de dados de “caráter público” verificada no parágrafo único do art. 1º da Lei nº 9.507/97, a ambiguidade verificada acerca do alcance do instituto motivou uma postura positiva da doutrina e jurisprudência para estender o seu cabimento para além dos órgãos públicos, entendimento que prosperou de forma decisiva com a redação levada a efeito pelo artigo 43, §4º do Código de Defesa do Consumidor que equiparou os arquivos de consumo aos de entidades de caráter público, para fins de aplicação do habeas data²⁵.

José Afonso da Silva atuou como assessor dos relatores da Constituição de 1988, sendo testemunha histórica da formulação e do contexto que determinou a redação final do artigo 5º, LXXII da Constituição Federal que instituiu o instituto do *habeas data*²⁶:

²² BRASIL. Superior Tribunal de Justiça. HD 147-DF, Rel. Ministro Arnaldo Esteves Lima, julgamento em 14 jun. 2007.

²³ BRASIL. Superior Tribunal de Justiça. Súmula 02: Não cabe o habeas data (CF, art. 5., LXXII, letra "a") se não houve recusa de informações por parte da autoridade administrativa.

²⁴ SILVA, Carlos Bruno Ferreira da. *Proteção de Dados e Cooperação Transacional. Teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014. p. 60-61.

²⁵ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 267-274.

²⁶ Art. 5º.

(...) propusemos perante a Comissão Provisória de Estudos Constitucionais (Comissão Afonso Arinos) um Anteprojeto de Constituição cujo art. 17 reconhecia o direito nos termos seguintes: “1. Toda pessoa tem direito de acesso aos informes a seu respeito registrado por entidades públicas ou particulares, podendo exigir a retificação de dados, e a sua atualização. 2. É vedado o acesso a terceiros a esse registro. 3. Os informes não poderão ser utilizados para tratamento de dados referentes a convicções filosóficas ou políticas, filiações partidárias ou sindical, fé religiosa ou vida privada, salvo quando se tratar do processamento de dados estatísticos não individualmente identificáveis. 4. Lei federal definirá quem pode manter registros informáticos, os respectivos fins e conteúdo”. No art. 31 instituímos o remédio constitucional específico: “Conceder-se-á habeas data pra proteger o direito à intimidade contra abusos de registros informáticos públicos e privados, curto e seco, como se vê. O Anteprojeto da Comissão acolheu a declaração do direito no seu art. 17 com aperfeiçoamentos e o remédio no art. 48: “Dar-se-á habeas data ao seu legítimo interessado para assegurar os direitos tutelados no art. 17.” Daí saiu para o debate constituinte, andando o direito e sua garantia específica em dispositivos separados até que no Projeto da Comissão de Sistematização fosse aprovado num único dispositivo, ou seja: reconhecia-se o direito mediante sua garantia específica (art. 6º, §52). Daí sofreu modificações para pior até o texto do atual art. 5º, LXXII (...).²⁷

Segundo Carlos Bruno Ferreira da Silva esse esquitejamento do instituto durante o processo constituinte, reflete a pouca propensão doutrinária e jurisprudencial atual do instituto avançar na proteção dados, posto que restrito a finalidade que determinou sua criação de conhecimento e retificação de informações pessoais existentes em banco de dados, baseado no histórico recente de revelação dos arquivos da ditadura que existiu no Brasil entre 1964 e 1985, sendo que para o autor a utilidade prática do habeas data é praticamente inexistente, substituído na práxis processual pelo mandado de segurança, tendo em vista que aquele exige prova da recusa das informações conforme súmula 02 do STJ, o que resultou na baixa adesão a utilização do instituto conforme se verifica na quantidade pouco expressiva de expedientes em trâmite nos tribunais superiores.²⁸

Luís Roberto Barroso (Apud DONEDA, 2019, p. 267) atribui ao habeas data uma significação essencialmente simbólica, pelo fato do direito que visa tutelar ser passível de tutela por outros instrumentos jurídicos, representando uma manifestação do constituinte contra o que denominou *comunidade de informações* existente no ciclo militar-autoritário

LXXII - conceder-se-á *habeas data*:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

²⁷ SILVA, José Afonso da. *Curso de direito constitucional positivo*. 26. ed. São Paulo: Malheiros, 2006. p. 454.

²⁸ SILVA, Carlos Bruno Ferreira da. *Proteção de Dados e Cooperação Transacional. Teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014. p. 60-61.

marcada pelo abuso de informações que diferentes organismos armazenavam sobre as pessoas por meios ilícitos e para fins condenáveis.²⁹

O habeas data foi criado com a finalidade de viabilizar o conhecimento e a possibilidade de alteração de dados em poder de órgãos públicos e de bancos de dados de caráter público, no entanto, a sua ampla adoção foi limitada pelas condições impostas ao seu cabimento, notadamente pela necessidade de prova da recusa de acesso pelo sujeito passivo, o que desestimou o seu uso e determinou a utilização de outros instrumentos jurídicos, como o mandado de segurança.

1.3. Lei dos arquivos públicos

A Lei nº 8.159/91 dispõe sobre a política nacional de arquivos públicos e privados de interesse de público e social, conceituando “arquivos públicos” no seu artigo 7º e “arquivos privados de interesse social no seu artigo 12, prevendo como regra o direito de acesso aos interessados (art. 4º), disposições sobre a eliminação de arquivos públicos (art. 9º), a organização dos arquivos nacionais (art. 17), bem como o acesso e sigilo dos documentos públicos no seu artigo 22 a 24 recentemente revogados pela Lei nº 12.527/2011 (lei de acesso à informação).

Arquivos públicos são documentos recebidos e produzidos por órgãos públicos no exercício de suas funções, compreendendo tanto o documento arquivado em mídia física quanto digital. A regra do direito de acesso a tais documentos previsto no artigo 4º da Lei nº 8.159/91 é relativizada pelas normas inerentes ao sigilo impostas pelos seus artigos 22 a 24 em relação a documentos que cuja divulgação coloquem em risco a segurança da sociedade e do Estado e àqueles necessários a proteção da privacidade e a honra das pessoas, cuja classificação foi determinada pelo Decreto Federal nº 4.553/2002 em ultrassecretos, secretos e confidenciais.

As disposições inerentes ao sigilo atribuído aos arquivos públicos previstas na Lei nº 8.159/91 e Decreto Federal nº 4.553/2002 foram revogadas pela Lei nº 12.527/2011 (lei de acesso à informação).

1.4. Código de Defesa do Consumidor

²⁹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 267.

O artigo 45 da LGPD prevê a aplicação do Código de Defesa do Consumidor nas hipóteses de violação de direitos de titular de dados no âmbito das relações de consumo que, por sua vez, impõe a responsabilidade objetiva do fornecedor em relação ao dano causado ao consumidor (art. 14).

Quando a violação de direito de titular de dados configurar uma relação de consumo, se aplica na hipótese o Código de Defesa do Consumidor no que respeita a responsabilidade civil objetiva, no entanto, não se exclui os direitos assegurados LGPD como a Responsabilização e Prestação de Contas do agente de tratamento de dados que, por sua vez, determina que este último não apenas cumpra as determinações legais, mas também demonstre o seu cumprimento, mesmo que não haja descumprimento ou ilegalidade³⁰.

Nesse formato, o titular de dados inserido numa relação de consumo está há um só tempo assegurado tanto pela LGPD quanto pelo CDC, o que lhe hipoteticamente garante uma dupla proteção frente ao tratamento de seus dados pessoais.³¹

Deve ser ressaltado a preocupação do legislador pátrio na edição do CPC na década de 90 com a proteção dos bancos de dados dos consumidores, inserindo nas disposições do código o artigo 43 com inspiração no *National Consumer ACT* pelo *Fair Credit Reporting Act – FCRA* de 1970, o qual estabelece limites ao uso da informação sobre o consumidor pelo fornecedor, a exemplo do registro de dados negativos que não poderia superar 5 anos, a necessidade de comunicação escrita sobre o tratamento de informação do consumidor em determinados casos, bem como o direito de acesso, informação e correção de dados.³²

Grande parte dos questionamentos que surgiram no período diziam respeito aos cadastrados negativos de crédito. Nesse sentido, no REsp 22.337-8/RS o Ministro Ruy Rosado já fazia menção, em 1995, ao direito de autodeterminação informativa nos moldes do modelo alemão, viabilizando o direito de acesso e retificação. Em 2001, por ocasião do julgamento do REsp 306.570, a Ministra Eliana Calmon reconheceu em seu voto que “o contribuinte ou o titular da conta bancária tem direito à privacidade em relação aos seus dados pessoais”. Por fim, no REsp 1.168.547/RJ, julgado em 2011, o Relator

³⁰ TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2019. p. 304.

³¹ Idem.

³² DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Revista dos Tribunais. p. 266-267.

Ministro Luis Felipe Salomão ressaltou a existência de um novo conceito de privacidade e a necessidade de consentimento do interessado para a divulgação de informação pessoal a seu respeito.³³

Verifica-se, no que respeita a proteção de dados prevista no artigo 43 do CDC, o início da regulação da proteção de dados pessoais, nada obstante restrita as relações de consumo, sendo que o regime jurídico da proteção de dados prevista na LGPD representa um avanço mesmo no microsistema de proteção ao consumidor, especialmente pela positivação dos princípios gerais da proteção de dados (art. 6), notadamente o da finalidade, adequação, necessidade, não discriminação, responsabilização e prestação de contas.

1.5. Lei do cadastro positivo

A Lei nº 12.414/2011 conhecida como Lei do Cadastro Positivo trouxe disposições acerca da “formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito”, ampliando as garantias referentes aos bancos de dados de consumidores, especialmente:

(...) a) o direito de obter o cancelamento do cadastro; b) o direito de conhecer os principais elementos e critérios considerados para análise de risco; c) o direito de ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento; d) o direito de solicitar ao consulente a revisão da decisão realizada exclusivamente por meios automatizados e) o direito de ter os seus dados pessoais utilizados de acordo com a finalidade para a qual foram coletados.³⁴

A controvérsia acerca do cadastro positivo ficou por conta do sistema de avaliação de risco de crédito denominado score de crédito ou *credit score*, um algoritmo que utiliza de diversos bancos de dados para aferir o grau de solvência do consumidor, questão que determinou o julgamento de dois recursos repetitivos e uma súmula pelo Superior Tribunal no Justiça.

No primeiro recurso repetitivo julgado, no caso o RESP nº 1.457.199/RS, foi fixada a tese de que o sistema de *credit score* é lícito e autorizado pela lei do cadastro positivo,

³³ CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 89.

³⁴ Idem, p. 89.

sendo desnecessário o consentimento do consumidor consultado, no entanto, ressaltou a necessidade de fornecer ao consumidor os critérios valorados pelo algoritmo, devendo ser utilizado para a finalidade exclusiva de acesso ao crédito, sendo que o uso abusivo poderia ensejar a responsabilidade objetiva e solidária do fornecedor, do responsável pelo banco de dados, da fonte e do consulente.

No RESP nº 1.306.736/RS, julgado na sistemática do recurso repetitivo, foi fixada a tese de que a ação cautelar para exibição de documentos no sistema *credit scoring* dependeria de requerimento anterior para obtenção dos dados ou tentativa de fazê-lo e que a recusa do crédito se deu pela pontuação que lhe foi atribuído pelo sistema.

Finalmente, o STJ editou a súmula 550 dispondo que o sistema de avaliação de crédito dispensa o consentimento do consumidor, o qual pode solicitar esclarecimentos sobre as informações pessoais valoradas e a respectiva fonte.³⁵

A LGPD manteve-se coerente com a Súmula 550 do STJ ao excepcionar a necessidade de consentimento do titular para fins de proteção ao crédito (art. 7, X), de forma que no atual regime aplicável ao sistema de cadastro positivo de crédito, é assegurado ao consumidor o acesso as informações e ao método valorativo da sua avaliação de crédito, no entanto, não é exigido seu consentimento prévio para a utilização do sistema de aferição de seu grau de solvência.

1.6. Marco civil da internet

A Lei nº 12.965/2014 denominada “Marco Civil da Internet” estabelece os princípios, garantias, direitos e deveres para o uso da internet, introduzindo no ordenamento jurídico brasileiro algumas balizas à proteção de dados pessoais, permitindo prerrogativas básicas para a proteção de seu conteúdo que foram posteriormente sistematizadas com maior amplitude pela LGPD.

O artigo 3º do Marco Civil da Internet assegura a um só termo no uso da internet os direitos constitucionais da liberdade de expressão e da privacidade, como basilares a uma convivência democrática no ambiente virtual, introduzindo no ordenamento jurídico a distinção entre o direito à privacidade e à proteção dos dados pessoais nos incisos II e III,

³⁵ BRASIL. Superior Tribunal de Justiça. Súmula 550: A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

absorvendo a tendência de considerar este último um direito autônomo, inclusive com pretensão de alçar específica previsão constitucional, conforme se verifica da PEC 17/2019, considerando o atual contexto social e econômico onde a proteção de dados pessoais vem adquirindo especial relevância.³⁶

Com relação especificamente a política de proteção de dados pessoais, atribuiu a lei um regime restritivo a transferência de dados a terceiros condicionados ao *consentimento livre, expresso e informado* do titular de dados (art. 7, VII e IX), com a necessidade dos provedores de conexão e aplicações de internet informarem com clareza e completude a forma como ocorre a coleta, uso, armazenamento e tratamento dos dados pessoais, justificada sempre sua utilização para finalidades específicas autorizadas por lei (art. 7, VIII) e, finalmente, o artigo 7, X com redação definida pelo artigo 60 da LGPD previu a possibilidade de exclusão dos dados pessoais mediante requerimento do titular ao término da relação entre as partes.

O artigo 10 do Marco Civil da Internet ao tratar da guarda dos dados pessoais pelos provedores de conexão e aplicações de internet, fundado no direito à privacidade, assegurou que o acesso a terceiros dos registros e informações relacionados a tais dados fossem resguardadas pela reserva de jurisdição, concedidos estritamente para o fim de formar conjunto probatório em processo judicial cível ou penal (art. 22) e respeitados os direitos a liberdade de expressão e a privacidade previstos no artigo 7º. O provedor de aplicações de internet deverá manter os registros de acesso a aplicações de internet, sob sigilo, pelo prazo de 6 (seis) meses (art. 15), sendo que administrador de provisão de conexão de internet manterá os registros de conexão pelo prazo de 1 (um) ano (art. 13).

O artigo 11, por sua vez, assegura que qualquer operação referente ao tratamento de dados ocorrida em território nacional, deverá observar a legislação brasileira, notadamente os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações.

No que respeita ao regime de sanções previstas no artigo 12 pelo descumprimento das normas previstas nos artigos mencionados 10 e 11 do marco civil da internet, verifica-se a advertência (art. 12, I), multa de até 10% do faturamento (art. 12, II), suspensão e proibição temporária de atividades que envolvam o tratamento de dados pessoais (art. 12, III e IV). Com relação ao regime das sanções no que respeita ao tratamento de dados, deve ser considerado que a LGPD trouxe previsão específica acerca do tema, de tal forma

³⁶ SILVA, Carlos Bruno Ferreira da. *Proteção de Dados e Cooperação Transacional. Teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014. p. 238.

que eventuais infrações às regras relacionadas a proteção de dados, em especial no que respeita ao seu tratamento, atrai o regime sancionatório previsto na Lei Geral de Proteção de Dados.³⁷

O Supremo Tribunal Federal iniciou o julgamento da ADIn^o 5527, Relator Ministra Rosa Weber, e da ADPF n^o 403 cujo Relator é o Ministro Edson Fachin, a qual analisa a constitucionalidade dos artigos 7^o, II, 10, § 2^o e o art. 12 do Marco Civil da Internet, dispositivos invocados para justificar decisões judiciais determinando o acesso a mensagens protegidas pela criptografia aos aplicativos de troca de mensagens, no caso o Whatsapp, bem como penalidades de suspensão temporária de serviços, sendo que o voto dos Ministros Edson Fachin e Rosa Weber concluíram não ser possível ordem judicial afastar a aplicação de criptografia aos aplicativos de mensagens. O julgamento foi interrompido em razão do pedido de vista do Ministro Alexandre de Moraes.³⁸

Por fim, devemos consignar as disposições do Marco Civil da Internet em relação ao Poder Público previsto nos seus artigos 24 a 28, com especial referência as diretrizes a serem adotadas pela Administração, tais como a interoperabilidade de serviços e sistemas, inclusive entre os diversos entes federativos, de maneira a viabilizar intercâmbio de dados (art. 24, III e IV) e a prestação de serviços de “forma integrada, eficiente, simplificada e por múltiplos canais de acesso” (art. 24, X), sendo que os dispositivos aplicáveis ao Poder Público encerram uma tentativa de sedimentação de um cenário de Administração Eletrônica, mediante o estímulo a virtualização dos serviços colocados à disposição da sociedade.³⁹

O Marco Civil da Internet representou a gênese da regulação dos dados pessoais no ordenamento jurídico brasileiro, mediante a consagração do conceito e das faculdades básicas inerentes ao próprio direito que já estava amplamente estabelecido em outros países, notadamente a União Europeia que já possuía à época a Diretiva 95/46/CE do

³⁷ O descumprimento das regras de proteção de dados previstos na LGPD pode determinar a intervenção da ANPD para fazer cessar a infração (art. 31), bem como as seguintes sanções a ser aplicada pelo regulador: (i) advertência; (ii) publicização da infração; (iii) bloqueio dos dados pessoais a que se refere a infração até a sua regularização; (iv) eliminação dos dados pessoais a que se refere a infração; (v) suspensão parcial e temporária do funcionamento do banco de dados a que se refere a infração (vi) suspensão temporária do exercício da atividade de tratamento dos dados pessoais; (vii) proibição parcial ou total do exercício de tratamento de dados (art. 31 e 52).

³⁸ Relatores consideraram inconstitucional quebra de sigilo das comunicações em aplicativos de mensagens. *Supremo Tribunal Federal*, Brasília, 28 maio 2020. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444384&ori=1>. Acesso em: 10 ago. 2020.

³⁹ SILVA, Carlos Bruno Ferreira da. *Proteção de Dados e Cooperação Transacional. Teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014, p. 243.

Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, representando assim um embrião da proteção de dados pessoais no sistema jurídico que veio a ser amplamente sistematizada pelo advento da LGPD.

1.7. Lei Geral de Telecomunicações, Lei de Interceptações Telefônicas e Lei das Organizações Criminosas

A Lei Geral de Telecomunicações (Lei nº 9.472/97) estabelece no seu artigo 3º o direito dos usuários à privacidade de seus dados pessoais, sendo que o serviço de telefonia abrange as chamadas e a internet, de tal forma que os concessionários congregam uma grande quantidade de dados dos seus usuários, tais como nome, CPF, endereço, número do telefone, chamadas realizadas e recebidas e, em alguns casos a conta corrente do usuário para o débito bancário.⁴⁰

Dados pessoais como nome e endereço podem ser objeto de divulgação por se tratar de informação de caráter público, que integra uma lista de assinantes nos termos do artigo 96, IV da LGT, o qual deve se opor a divulgação caso não seja do seu interesse a publicidade de tais dados (art. 3, VI). O artigo 72, §1º da LGT protege as informações pessoais dos usuários de forma abrangente, submetendo sua transferência a terceiros ao consentimento do titular, sendo permitido seu uso estatístico, desde que mediante a adoção de técnicas de anonimização.

A Lei das Organizações Criminosas (Lei nº 12.850/2013) possibilita (artigo 15) o acesso a dados cadastrais de investigado inerentes a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet, e administradoras de cartão de crédito, por parte da autoridade policial e do Ministério Público, sem a necessidade de autorização judicial.

Deve ser registrado, também, a possibilidade das Comissões Parlamentares de Inquérito (CPI) terem acesso aos dados cadastrais e aos registros telefônicos dos usuários de telefonia, conforme definido pelo Supremo Tribunal Federal por ocasião do julgamento do Mandado de Segurança nº 23.452, Relator Min. Celso de Mello, ao interpretar o artigo 58, §3º da CF que prevê as CPIs “poderes investigatórios próprios de

⁴⁰ Art. 3º O usuário de serviços de telecomunicações tem direito:

(...)

IX - ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço;”

autoridades judiciais”, desde que exerça tal mister da mesma forma que um juiz, com motivação e sujeito ao controle pelo STF. No entanto, o mesmo não ocorre em relação as interceptações telefônicas, tendo em vista a reserva de jurisdição levada a efeito no artigo 5º, XII da CF.

A Lei de Interceptação Telefônica e Telemática (Lei nº 9.296/96), ratificando a reserva de jurisdição da comunicação de dados prevista no artigo 5º, XII da CF, assegura no seu artigo 1º que as interceptações telefônicas serão cabíveis apenas para utilização como prova em investigação criminal e dependerá de ordem judicial, assegurado o segredo de justiça.

Nesse sentido, o Supremo Tribunal Federal assentou que o regime das comunicações de dados (informações dinâmicas), está submetido a reserva de jurisdição conforme preceitua o artigo 5º, XII da CF, o que não se aplica ao sigilo de dados (informações estáticas) que, nada obstante acobertado pela garantia do sigilo (art. 5º, X), não está sujeito a reserva de jurisdição, podendo a lei estabelecer regimes específicos relacionados à exceção ao sigilo dos dados em si mesmo, armazenados em mídias como computadores, pen drives, HD externo.⁴¹

Dessa forma, a Lei Geral de Telecomunicações (Lei nº 9.472/97) assegura o direito dos usuários à privacidade de seus dados pessoais, o que é de grande relevância, considerando o volume de dados pessoais que armazenados pelos concessionários, sendo que o acesso por terceiros a tais dados se submete, em regra, a reserva da jurisdição, ressalvado as hipóteses previstas na Lei das Organizações Criminosas (acesso a dados cadastrais do investigado pela autoridade policial e Ministério Público), bem como em relação as Comissões Parlamentares de Inquérito cujo acesso a dados cadastrais e aos registros telefônicos dos usuários de telefonia é possível, desde que de forma motivada e sujeito ao controle judicial.

1.8. Sigilo das operações financeiras

O artigo 1º da LC nº 105/2001 prevê, como regra, que as instituições financeiras “conservarão sigilo em suas operações ativas e passivas e serviços prestados.”

No entanto, a LC nº 105/2000 prevê limitações ao sigilo, especialmente para os fins de: preservação do sistema creditício mediante informações para embasar análise de

⁴¹ BRASIL. Superior Tribunal de Justiça. HC nº 135041. Rel. Min. Rosa Weber. Julgamento em 25 set. 2019.

riscos (art. 1º, §3º, I e II); realização de poder de polícia pelos órgãos de fiscalização do sistema financeiro (art. 2º, §§ 1º e 3º); e, finalmente, na comunicação de ilícitos penais e administrativos, sendo que nessa última hipótese a limitação ao sigilo vem prevista de forma mais detalhada na lei de prevenção à lavagem de dinheiro (lei nº 9.613/1998).⁴²

O Supremo Tribunal Federal definiu por ocasião do julgamento do RE nº 1.055.941/SP, julgado na sistemática da repercussão geral (Tema 990), acerca da possibilidade do compartilhamento de dados bancários e fiscais obtidos pelo Fisco com o Ministério Público para fins penais, sem a necessidade de interveniência do Judiciário, devendo o órgão de persecução penal resguardar o sigilo dos dados obtidos. Na oportunidade, foi definido que o compartilhamento de dados bancários e fiscais pelo Fisco não violava o direito a intimidade e do sigilo de dados previsto no art. 5º, incisos X e XII, da Constituição Federal.

O sigilo de dados bancários junto às entidades que compõem o sistema financeira é regra, temperada por exceções previstas no artigo 1º da LC nº 105/2001, bem como e para fins específicos de persecução criminal ao Ministério Público que pode acessar tais dados em poder do Fisco, obtidos por este último junto as instituições financeiras no legítimo exercício de fiscalizar os contribuintes.

1.9. Demais diplomas normativos setoriais

Cabe mencionar outras normas que trataram da questão dos dados pessoais antes do advento da LGPD, tais como a Lei nº 12.737/2012 (Lei Carolina Dieckman) que tipificou como crime a invasão de dispositivos informáticos, bem como atos com caráter normativo como o Decreto Federal nº 6.135/2007 que criou o Cadastro Único para programas sociais do Governo Federal, prevendo o sigilo de dados das famílias beneficiadas, o Decreto Federal nº 6.425/2008 que dispõe sobre o censo anual da educação e o sigilo dos dados pessoais apurados no censo; Decreto Federal nº 6.523/2008 que regulamenta o SAC (Serviço de Atendimento ao Consumidor) e assegura o sigilo dos dados e sua utilização para finalidade exclusiva de atendimento.

1.10. Lei Geral de Proteção de Dados Pessoais e seus princípios

⁴² SILVA, Carlos Bruno Ferreira da. *Proteção de Dados e Cooperação Transacional. Teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014. p. 221.

A Lei Geral de Proteção de Dados Pessoais no Brasil (Lei nº 13.709, de 14 de agosto de 2018) foi editada com o objetivo de proteger os dados de pessoas físicas, com fundamento nos direitos fundamentais da liberdade de expressão, privacidade e o livre desenvolvimento da personalidade da pessoa natural (arts. 1º e 2º). A LGPD se aplica, como regra, a todos os procedimentos de tratamento de dados realizados no território brasileiro (art. 3º), sendo as exceções previstas no seu artigo 4º.

Conforme artigo 5, X da LGPD o tratamento de dados abrange “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.”

Nos termos do artigo 6º da LGPD, as atividades de tratamento de dados deverão ser regidas, além da boa-fé, pelos seguintes princípios: finalidade (art. 6, I); adequação (art. 6, II); necessidade (art. 6, III); livre acesso (art. 6, IV); qualidade (art. 6, V); transparência (art. 6, VI); segurança (art. 6, VII); prevenção (art. 6, VIII); não discriminação (art. 6, IX); e, finalmente, responsabilização e prestação de contas (art. 6, X).

Os princípios previstos na LGPD informam e determinam toda a legislação e a interpretação das regras de proteção de dados que, por ser uma lei que objetiva a proteção de dados pessoais, não só, mas com especial atenção em relação a meios tecnológicos inovadores, onde há uma ciência aplicável a organização desses dados (big data) por meio de algoritmos capazes de automatizar tendências pessoais, verifica-se que a lei procurou, para além de criar regras específicas para a regulação no atual contexto social e econômico, estabelecer princípios para sua aplicação, de maneira a evitar sua prematura desatualização. Nos itens seguintes, serão abordados os princípios aplicáveis ao tratamento de dados na LGPD.

1.10.1. Princípio da finalidade

O princípio da finalidade está previsto no artigo 6, I da LGPD e determina que o tratamento de dados pessoais deve ser realizado “para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”.

Segundo Danilo Doneda, o princípio da finalidade determina que a utilização dos dados deve obedecer à finalidade informada ao titular antes de sua coleta, sendo de grande

relevância prática, na medida em que restringe a transferência a terceiros, além de fixar um critério de razoabilidade na utilização de determinados dados considerando sua finalidade.⁴³

Rony Vainzof esclarece que tal princípio é estabelecido de forma semelhante no GPDR como “Limitação da Finalidade” (Purpose Limitation), segundo o qual os dados pessoais devem ser tratados de forma compatível à finalidade que determinou sua coleta, inclusive o artigo 25 do GPDR prevê que o controlador deve aplicar medidas técnicas que assegurem por padrão (privacy by default), só sejam tratados dados pessoais necessários para cada finalidade específica do tratamento.⁴⁴

Dessa forma, o princípio da finalidade determina que os dados pessoais são tratados de forma legítima quando respeitada a finalidade informada ao seu titular no momento da coleta dos dados, não podendo ocorrer tratamento posterior para finalidade diversa da informada ao seu titular.

1.10.2. Princípio da adequação

O princípio da adequação previsto no artigo 6, II da LGPD pretende preservar a relação entre a finalidade informada ao titular e o tratamento dispensado, com o objetivo de evitar a desvirtuação do procedimento realizado durante a realização do tratamento dos dados.⁴⁵⁴⁶

No caso, a inadequação de um procedimento de tratamento de dados é verificada quando há o uso secundário e fora do contexto do tratamento, ou seja, alheio à finalidade que determinou o início do processo de tratamento de dados.⁴⁷

1.10.3. Princípio da necessidade

⁴³ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 182.

⁴⁴ VAINZOF, Rony. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 139.

⁴⁵ Art. 6.

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

⁴⁶ COTS, Marcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais Comentada*. 3. ed. São Paulo: Revista dos Tribunais, 2019. p. 80.

⁴⁷ VAINZOF, Rony, op. cit., p. 139.

O artigo 6, III atribui ao princípio da necessidade o sentido de restringir o tratamento de dados “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”.

Tal princípio positivado na LGPD tem duas facetas: o aumento da responsabilidade àquele que coleta e realiza o tratamento de dados, bem como representa um óbice a coleta de dados não imprescindíveis à finalidade almejada.⁴⁸

O princípio em questão está intimamente ligado a uma premissa de limitação de dados coletados para um fim determinado, previsto na GPDR como princípio da minimização dos dados e considerado em decisão do Superior Tribunal de Justiça que declarou abusiva a cláusula contratual, em contrato de prestação de serviços de cartão de crédito que autoriza a instituição compartilhar dados de consumidores com outras entidades financeiras, sem a possibilidade de opção ao titular de manifestar oposição ao compartilhamento.⁴⁹

1.10.4. Princípio do livre acesso

O controle do uso dos dados pelo seu titular guarda seu fundamento na autodeterminação informativa, sendo garantido a este o livre acesso pelo princípio previsto no artigo 6, IV da LGPD, o qual assegura a “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”

O conteúdo jurídico do mencionado princípio é integrado pelo artigo 9º da lei que prevê a consulta facilitada e gratuita sobre a forma e duração do tratamento de dados, bem como à integridade dos dados do titular, o quais deverão ser fornecidos de forma clara, adequada e ostensiva por meio da requisição prevista no artigo 18 da LGPD.

1.10.5. Princípio da qualidade dos dados

⁴⁸ FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Weverton Gabriel Gomes. Princípios que regem o tratamento de dados no Brasil. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020. p. 130.

⁴⁹ BRASIL. Superior Tribunal de Justiça. REsp nº 1348532. Rel. Ministro Luis Felipe Salomão, julgamento em 10 de out. 2017: “Não se cuida de desconsiderar a possibilidade de restrição ou conformação de direito fundamental, mas do cuidado em preservar o núcleo essencial do direito. É imprescindível, no âmbito da moderna concepção de proteção de dados, limitar tanto o conteúdo como a quantidade de informação que é tratada pelas entidades de proteção a o crédito”.

Os dados pessoais colocados em conjunto em um processo de tratamento, representam um compilado de informações sobre determinadas pessoas, notadamente a classe social do indivíduo, se possui ou não antecedentes criminais, se é partidário ou apartidário, ateu ou religioso, HIV positivo ou negativo, heterossexual ou homossexual, consumidor de álcool, entre outras diversas características pessoais que necessariamente refletem nas considerações afetas a determinadas pessoas.⁵⁰

Daí a importância da lei assegurar no artigo 6, V da LGPD a qualidade dos dados pessoais, para que as informações acerca do indivíduo, em seu conjunto, reflitam necessariamente qualificações exatas acerca das suas reais características pessoais.

1.10.6. Princípio da transparência

O princípio da transparência (art. 6, VI) assegura aos titulares que o acesso das informações seja assegurado de forma clara, acessível sobre todos os aspectos relacionados ao tratamento de dados realizados.

Sobre o tema, Rony Vainzof cita o caso da Promotoria de Justiça de Defesa do Consumidor de Belo Horizonte/MG, no Processo Administrativo MPMG-0024.18.0027027-3 que resultou na multa de R\$ 7.930.801,72 em relação a uma drogaria, por condicionar a realização de descontos ao fornecimento do CPF pelo consumidor, hipótese onde a ausência de transparência foi ressaltada na decisão administrativa com fundamento no Código de Defesa do Consumidor.⁵¹

A transparência dos dados do titular deve ser proporcional à capacidade de tratamento de dados pelo controlador, o qual deve observar os artigos 9, 18 e 19 da LGPD que determinam quais informações devem ser prestadas de ofício ou mediante requerimento dos titulares.

1.10.7. Princípio da segurança

O princípio da segurança (art. 6, VII) impõe ao agente de tratamento de dados a responsabilidade pelos procedimentos que lhe são próprios, a utilização de meios e

⁵⁰ VAINZOF, Rony. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 149.

⁵¹ Idem, p. 150.

tecnologias que assegurem a proteção dos dados pessoais de acesso a terceiros, notadamente os expedientes invasivos utilizados por hackers, bem como eventos acidentais ou propositais de destruição, perda, alteração e extravio de dados pessoais.⁵²

Em tais situações, pela indevida exposição de dados pessoais, os agentes de tratamento de dados ficam sujeitos as sanções administrativas previstas nos artigos 52 e seguintes da LGPD, bem como a responsabilização civil (arts. 42/45), sendo que no juízo de avaliação da gravidade de eventual incidente deve ser considerado a comprovação de que foram adotadas as medidas adequadas para preservação da privacidade dos titulares dos dados (art. 48, §3º).

Rony Vainzof defende a implantação, por parte da Autoridade Nacional de Proteção de Dados (ANPD), de padrões técnicos mínimos para segurança das informações tratadas, de acordo com as características específicas do tratamento e do atual estágio da tecnologia, em especial, no que respeita aos dados sensíveis dos titulares, citando como exemplo normas setoriais importantes como o art. 13 do Decreto 8.771/2026 que regulamentou o Marco Civil da Internet e fixou padrões de segurança dos provedores de internet, sendo dessa maneira salutar que a entidade reguladora definisse obrigações de forma linear aos agentes que realizam operações de tratamento de dados.⁵³

1.10.8. Princípio da prevenção

O princípio da prevenção (art. 6, VIII) determina sejam adotadas medidas “para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”, de forma que tal princípio está intimamente ligado com o da segurança, partindo da premissa de que a atuação do agente de tratamento deve se dar de forma preventiva, mitigando a possibilidade de ocorrência de eventos que coloquem em risco os dados pessoais de seus titulares.⁵⁴

As medidas de prevenção devem ser observadas desde a concepção do produto ou serviço até sua execução, conforme prevê o artigo 46, §2º da LGPD que absorveu o conceito da chamada *Privacy by Design* que, segundo sua idealizadora Ann Caoukian,

⁵² FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Weverton Gabriel Gomes. Princípios que regem o tratamento de dados no Brasil. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020. p. 132.

⁵³ VAINZOF, Rony. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 149.

⁵⁴ FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Weverton Gabriel Gomes., op. cit., p. 132.

deveria ser pautado pelos seguintes princípios: (i) proatividade e atuação voltada a prevenção e não à correção; (ii) privacidade como padrão; (iii) privacidade incorporada ao design; (iv) funcionalidade total; (v) segurança de ponta a ponta, em todo o ciclo da informação; (vi) visibilidade e transparência; (vii) respeito à privacidade do usuário, devendo considerar este último como o foco do tratamento de dados.⁵⁵

Bruno Ricardo Bioni ressalta que a concepção do sistema de tratamento de dados, a partir da metodologia conhecida como *Privacy by Design*, corresponde à ideia de que a proteção de dados deve orientar a concepção de um produto ou serviço considerando para tanto a adoção de tecnologias que viabilizem a proteção das informações pessoais:

Veja-se, por exemplo, a criptografia que assegura a confidencialidade das comunicações. Ou, ainda, a anonimização de dados pessoais que quebra ou pelo menos dificulta o vínculo de identificação entre um dado sujeito ao qual está atrelado, bem como mecanismos de navegação anônima que impedem rastreamento do usuário. Em todos esses exemplos, a arquitetura dos sistemas de informação é um instrumento hábil para proteger os dados pessoais do cidadão.⁵⁶

A adoção desse modelo de proteção de dados requer, especialmente no âmbito dos diversos entes públicos, a adoção de regras de governança de dados que inviabilizem o extravio destes a terceiros, evitando eventos como o verificado na Secretaria de Saúde de Arapongas (Paraná), onde houve a divulgação da lista dos infectados pelo COVID-19, com o nome do paciente, endereço, data em que receberam o resultado e o local onde foram atendidos.⁵⁷

Dessa forma, com vistas a aplicação do princípio da prevenção, a LGPD prevê que os agentes poderão formular regras de boas práticas e governança com condições de organização, normas, padrões técnicos, ações educativas, mecanismos internos de supervisão e mitigação de riscos, regras estas que deverão ser publicadas, atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela Autoridade Nacional de

⁵⁵ CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles*. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf>. Acesso em: 12 jul. 2020.

⁵⁶ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento*. 2. ed. Rio de Janeiro: Editora Forense, 2019. p. 168.

⁵⁷ Lista de pessoas infectadas com o novo coronavírus foi divulgada na internet. *Globo.com*, 12 jul. 2020. Disponível em: <https://g1.globo.com/pr/norte-noroeste/noticia/2020/07/12/lista-de-pessoas-infectados-com-o-novo-coronavirus-em-arapongas-foi-divulgada-na-internet.ghtml>. Acesso em: 15 jul. 2020.

Proteção de Dados (ANPD), a qual deverá estimular a adoção de padrões técnicos que viabilizem o controle pelos titulares dos dados pessoais.⁵⁸

1.10.9. Princípio da não discriminação

Nos EUA um programa de computador chamado COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), analisa a probabilidade de reincidência criminal do indivíduo com base em dados, no entanto, muitas questões têm surgido acerca dos critérios utilizados pelos algoritmos que é gerido por uma empresa privada, especialmente diante de acusações de refletir um risco maior de reincidência para negros.⁵⁹

No Brasil, o Departamento de Proteção e Defesa do Consumidor (DPDC) aplicou multa no valor de R\$ 7.500.000,00 a Decolar.com pela prática conhecida como *geo pricing* e *geo blocking*, ante o emprego de tarifas e disponibilização de ofertas de acordo com a localização geográfica do consumidor, evidenciado no caso que computadores de São Paulo tinham tarifas até 29% superiores aos ofertados aos localizados em Buenos Aires para as mesmas acomodações.⁶⁰

Diante destas e outras situações identificadas no processo de tratamento de dados, previu o artigo 6, IX da LGPD a vedação a “realização do tratamento para fins discriminatórios ilícitos ou abusivos”, o que evidentemente não afasta a possibilidade de discriminações no processo de tratamento de dados para o fim de estabelecer distinções legalmente admitidas, como a coleta de informações de passageiro acerca de restrições alimentares, por questões religiosas ou de saúde, para o fim de lhe assegurar uma refeição adequada.⁶¹

Deve ser ressaltado, finalmente, que a LGPD assegura ao titular de dados solicitar a revisão de decisões baseadas em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20), devendo o

⁵⁸ VAINZOF, Rony. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coordenação). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 159.

⁵⁹ Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA. *BBC News*, 31 out. 2016. Disponível em: <https://www.bbc.com/portuguese/brasil-37677421>. Acesso em: 12 jul. 2020.

⁶⁰ Decolar.com é multada por prática de geo pricing e geo blocking. Ministério da Justiça, 12 jun. 2018. Disponível em: <https://www.justica.gov.br/news/collective-nitf-content-51>. Acesso em: 12 jul. 2020.

⁶¹ VAINZOF, Rony, op. cit., p. 166.

controlador fornecer sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada (art. 20, §1º).

1.10.10. Princípio da responsabilização e prestação de contas

A LGPD (art. 6, X) impõe ao agente de tratamento de dados o dever de demonstrar a “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”.

De acordo com o mencionado dispositivo da LGPD, não basta cumprir a lei, é preciso que as medidas adotadas para tal fim se mostrem comprovadamente eficazes, de tal maneira que os agentes terão responsabilidade pelos dados em seu poder durante do ciclo de vida do tratamento de dados, devendo adotar programas de conformidade que assegurem não só a segurança no sigilo dados, mas que viabilizem o registro das operações de tratamento que realizarem (art. 37), pois, além do fato de que a ANPD poderá solicitar tais informações (art. 55, J, IV), é possível a inversão do ônus da prova em favor do titular (art. 42, § 2º), sendo o agente de tratamento obrigado a reparar qualquer dano patrimonial ou moral, individual ou coletivo, que causarem em violação à LGPD.⁶²

A luz desse princípio, a figura da Autoridade Nacional de Proteção de Dados (ANPD) ganha especial relevância como instituição responsável pela regulação exercida em relação aos agentes econômicos e ao setor público quando no exercício de tratamento de dados, pois, dentre as competências da ANPD inclui-se a de requisitar informações, a qualquer tempo, aos agentes que realizam tratamento de dados pessoais (art.55, J, IV), bem como aplicar as sanções na hipótese de tratamento de dados realizados em descumprimento a LGPD (art.55, J, VI).

1.11. Conclusão

O direito à privacidade possui assento constitucional nos artigos 5º, incisos X e XII da Constituição, sendo que a proteção de dados pessoais constitui seu desdobramento com pretensão atual de alçar específica previsão constitucional, conforme se verifica da PEC 17/2019, sendo a LGPD editada com o objetivo de proteger os dados de pessoas

⁶² VAINZOF, Rony. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coordenação). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 166-168.

físicas, com fundamento nos direitos fundamentais da liberdade de expressão, privacidade e o livre desenvolvimento da personalidade da pessoa natural (arts. 1º e 2º).

O histórico da proteção de dados no Brasil abrange a criação de mecanismos (habeas data) e a edição de diversos diplomas normativos, com destaque à Lei de Acesso à Informação e ao Marco Civil da Internet, os quais podem ser considerados a gênese da proteção de dados pessoais no sistema jurídico que veio a ser amplamente sistematizada pelo advento da LGPD.

Cabe ressaltar que o artigo 4º da LGPD excepciona aplicação lei em algumas hipóteses, tais como o tratamento de dados realizados para fins de segurança pública (art. 4, III, a); defesa nacional (art. 4, III, b); segurança do Estado (art. 4, III, c); atividades de investigação e repressão de infrações penais (art. 4, III, d), circunstâncias que, nada obstante inaplicável a regulação prevista a LGPD, está obviamente amparada pela garantia constitucional da privacidade prevista nos artigos 5º, incisos X e XII, de modo a evitar uma eventual postura estatal abusiva no tratamento de dados quando no exercício de tais atividades.

Finalmente, nos casos em que aplicável a LGPD, deve-se considerar as regras e os princípios previstos na lei, notadamente o princípio da responsabilização e prestação de contas que empresta especial importância à figura da Autoridade Nacional de Proteção de Dados (ANPD), instituição responsável pela regulação levada a efeito em relação aos setores público e privado e com um grande plexo de competências fiscalizatórias e sancionatórias (art. 55), a exigir seja atribuído ao regulador um modelo institucional que favoreça sua autonomia, de forma a viabilizar o efetivo exercício das competências que lhe foram conferidas pela LGPD.

2. Da Autoridade Nacional de Proteção de Dados

2.1. Organização administrativa

O artigo 55-A da Lei Geral de Proteção de Dados Pessoais, na redação conferida pela Lei nº 13.853/2019, estabeleceu a criação, sem aumento de despesas, da Autoridade Nacional de Proteção de Dados (ANPD) com a natureza de “órgão da administração pública federal, integrante da Presidência da República”.

A conformação da ANPD como órgão é transitória (artigo 55-A, §1º), podendo ser “transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República” em até 2 (dois) anos da entrada em vigor da estrutura regimental da ANPD (art. 55 -A, §2º).

A ANPD terá estrutura regimental definida pela Presidência da República (art. 55-G), cargos em comissão e função de confiança remanejados de outros órgãos e entidades da Administração Federal (art. 55-H) e, nesse período de transição para uma possível readequação institucional para o formato de autarquia especial, a ANPD irá contar com apoio técnico e administrativo da Casa Civil (art. 55-G, §1º).

A Autoridade Nacional de Proteção de Dados será composta pelos seguintes órgãos: (1) Conselho Diretor, órgão máximo de direção, (2) Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, (3) Corregedoria, (4) Ouvidoria, (5) órgão de assessoramento jurídico próprio e (6) Ouvidoria, sendo a competência e composição dos dois primeiros órgãos previstos na LGPD e os demais dependentes de criação por ato normativo posterior.

O Conselho Diretor, órgão máximo de direção da entidade, é composto de 5 membros (art. 55-D), nomeado pela Presidência da República, após aprovação do Senado Federal (art. 55-D, §1º), com reputação ilibada e formação compatível (art. 55-D, §2º) e mandato de quatro anos (art. 55-D, §3º), com a possibilidade de perda do cargo por renúncia, condenação judicial transitada em julgada ou aplicação de pena de demissão em processo disciplinar (art. 55-E), sujeito as causas que configuram o conflito de interesses, após exercício do mandato, previstas no art. 6º da Lei nº 12.813, de 16 de maio de 2013 (art. 55-F).

O Conselho Nacional de Proteção de Dados e Privacidade é órgão multissetorial, com as competências previstas no artigo 58-B da LGDP, notadamente (1) propor

diretrizes para elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para atuação da ANPD, (2) elaborar relatórios, estudos, realizar debates, audiências públicas e realizar ações para divulgação da proteção de dados⁶³⁶⁴.

O artigo 55-H assegurou a autonomia técnica e decisória da ANPD. Com relação ao seu custeio, a lei de proteção de dados previu que suas receitas seriam decorrentes de: (1) dotações orçamentárias; (2) doações, legados, subvenções; (3) do resultado de aplicações de receitas no mercado financeiro; (3) negócios jurídicos celebrados com entidade públicas e privadas, nacionais e internacionais; (4) o produto da venda de materiais de caráter técnico elaborado pelo órgão.

2.1.2. Competência da ANPD

O artigo 55-J da LGPD prevê um rol das atribuições regulatórias da ANPD, organizadas no quadro abaixo em competências de coordenação das políticas para a implementação da LGPD, atribuições de fiscalizatórias, normativas e sancionatórias.

COMPETÊNCIAS DA ANPD (Art. 55-J)	
COORDENAÇÃO	<ul style="list-style-type: none">- elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (inc. III);- promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança (inc. VI);- promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade (inc. VII);- ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento (inc. XIV);- comunicar às autoridades competentes as infrações penais das quais tiver conhecimento (inc. XXI);- comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal (inc. XXII);

⁶³ LUCCA, Newton de; LIMA, Cintia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e Privacidade. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020. p. 383.

⁶⁴ O Conselho Nacional de Proteção de Dados e Privacidade tem composição paritária, sendo integrado por: (I) Administração Pública: 5 membros do Administração Federal, 1 do Senado, 1 da Câmara dos Deputados, 1 do CNJ, 1 do CNMP e 1 membro do Comitê Gestor de Internet do Brasil; (II) sociedade civil: 3 membros da sociedade civil com atuação em proteção de dados pessoais, 3 de instituições de pesquisas; 3 de confederações sindicais, 2 do setor empresarial e 2 de entidades representativas do setor laboral.

	<ul style="list-style-type: none"> - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais (inc. VII); - promover ações de cooperação com autoridades de proteção de dados de outros países (inc. IX); - articular-se com autoridades reguladoras (inc. XXIII);
FISCALIZATÓRIAS	<ul style="list-style-type: none"> - zelar pela proteção dos dados pessoais, nos termos da legislação (inc. I); - fiscalizar (inc. IV); - solicitar do poder público informações sobre as atividades de tratamento de dados (inc. XI); - realizar auditorias ou determinar sua realização (inc. XIX); - garantir que o tratamento de dados de idosos seja feito de forma simples (inc. XIX); - emitir opiniões técnicas e solicitar relatório de impacto à Administração (art. 4, § 3º);
NORMATIVAS	<ul style="list-style-type: none"> - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais (inc. XIII); - editar normas, orientações e procedimentos (inc. XVIII); - deliberar administrativamente sobre a interpretação da LGPD (XX);
SANCIONATÓRIAS	<ul style="list-style-type: none"> - aplicar sanções, nas hipóteses de descumprimento da lei, mediante processo administrativo, sendo assegurado o contraditório, a ampla defesa e o direito a recurso (inc. IV); - apreciar pedidos dos titulares de dados contra os controladores (inc. V); - celebrar compromisso com agentes de tratamento para eliminar irregularidades (inc. VII); - implementar mecanismos simplificados para o registro de reclamações sobre o tratamento de dados pessoais (XXIV).

Fonte: elaboração própria

Pela textura das competências atribuídas a ANPD pela lei de proteção dados pessoais, fica evidente a sua importância dentro do cenário da legislação que está a implementar, pois, a Autoridade Nacional de Proteção de Dados é a figura central para a aplicação da lei, em um contexto em que os agentes de tratamento de dados pessoais, tanto do setor público como do privado, estarão sujeitos à sua atividade regulatória, especialmente no campo sancionatório.⁶⁵

⁶⁵ Conforme o artigo 52 da LGPD, as penalidades pelas infrações a lei são: a advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração (infração não aplicável aos Entes Públicos); multa diária, observado o limite total aplicável a multa (infração não aplicável aos Entes Públicos); publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a

2.2 Panorama da regulação exercida pelas Agências Reguladoras Federais

2.2.1. Histórico das Agências Reguladoras

A reforma administrativa proposta no Plano Diretor da Reforma do Aparelho do Estado de 1995, com finalidade de reduzir o déficit público e redefinir a atuação estatal nas áreas econômicas e sociais, mediante a adoção de “ instrumentos de política social, proporcionando maior abrangência e promovendo melhor qualidade para os serviços sociais”, aliado ao ideário de reforma econômica viabilizadora da concorrência internacional no cenário de globalização determinou a diminuição do Estado com a privatização de serviços básicos, conforme explica Fábio Ulhoa Coelho⁶⁶:

O economista liberal diria, portanto, que o Estado está reduzindo porque, caso não o fizesse, as empresas brasileiras iriam encarar a competição com as empresas internacionais, que vivem num cenário liberal. Num mundo globalizado, estas empresas são as nossas concorrentes. Se o empresário brasileiro deve pagar mais contribuições sociais para a Previdência, ele não pode praticar preço competitivo com os dos seus concorrentes globais. A globalização força a reliberalização do Estado, na visão dos teóricos liberais.

De uma forma ou de outra, optando pela análise marxista ou pela análise liberal, o fato é que o Estado está se livrando de um ônus que, durante o século XX, chamou para si, que é o da manutenção de algumas comodidades para todos os cidadãos: a Educação, a Saúde, a Previdência Social etc.⁶⁷

Com base nesse quadro de mudança do paradigma de intervenção estatal no domínio econômico e social, foi editada a Lei nº 8.987/1995 que alterou o regime das concessões para viabilizar a participação da iniciativa privada na prestação de serviços públicos e a edição as Emendas Constitucionais nº 8/95 e 9/5 que permitiram a participação privada nos setores de telecomunicações e exploração de petróleo⁶⁸.

regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
⁶⁶ BRASIL. Plano Diretor da Reforma do Aparelho do Estado. Brasília: Presidência da República, 1995. Disponível em: <<http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/plano-diretor-da-reforma-do-aparelho-do-estado-1995.pdf>>. Acesso em: 25 mar. 2020.

⁶⁷ COELHO, Fábio Ulhoa. Reforma do Estado e Direito Concorrencial. In: SUNDFELD, Carlos Ari. *Direito Administrativo Econômico* (Org.). São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 193.

⁶⁸ NUSDEO, Ana Maria de Oliveira. Agências Reguladoras e Concorrência. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 159.

As agências reguladoras não são sinônimos de serviços privatizados, mas sua introdução no Brasil coincidiu com a agenda de privatizações ocorridas no final da década de 90, a exemplo das agências dos setores de telecomunicações (ANATEL) e energia elétrica (ANEEL) para a regulação de um setor relevante da economia, mas não ficou restrita aos serviços públicos privatizados se estendendo inclusive para atividades privadas de interesse público, como podemos verificar da ANS criada na qualidade de ente regulador dos serviços privados de saúde⁶⁹.

2.2.2 Da regulação exercida pelas Agências Reguladoras

A atividade regulatória exercida pelas Agências Reguladoras é uma forma de intervenção estatal na ordem econômica, onde o poder público não atua diretamente como provedor dos serviços básicos, em uma ordem de coisas onde a regulação era exercida pelo ponto de vista do gestor dos serviços, mas dentro de um novo modelo onde há a separação entre o provedor das utilidades públicas e os agentes encarregados de regular essa nova atividade, deslocando a atividade regulatória para entes com relativa autonomia em relação ao poder central⁷⁰.

A regulação exercida pelas Agências Reguladoras é ampla e complexa e não envolve apenas a atividade regulamentar setorial, segundo exegese do artigo 174 da CF que atribui ao Estado não só o papel de “agente normativo” como também de “regulador da atividade econômica”, de forma que a atividade regulatória não se exaure na regulamentação normativa⁷¹.

Nesse sentido, de rigor a menção ao entendimento de Floriano de Azevedo Marques, segundo o qual a atividade regulatória envolve tanto atividades regulamentares, quanto de organização, fiscalização, sancionatórias e de conciliação:

A atividade de regulação estatal envolve – dentro das balizas acima divisadas – funções muito mais amplas que a função regulamentar (consistente em disciplinar uma atividade mediante a emissão de comandos normativos, de caráter geral, ainda que com

⁶⁹ SUNDFELD, Carlos Ari. Introdução as Agências Reguladoras. In: SUNDFELD, Carlos Ari. *Direito Administrativo Econômico* (Org.). São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 19-22.

⁷⁰ NETO, Floriano de Azevedo Marques. A Nova Regulação Estatal e as Agências Independentes. In: SUNDFELD, Carlos Ari. *Direito Administrativo Econômico* (Org.). São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 78.

⁷¹ _____ . Agências Reguladoras. Instrumentos do fortalecimento do Estado. *Associação Brasileira de Agências de Regulação*, 20 jan. 2019. Disponível em: <http://abar.org.br/mdocs-posts/agencias-reguladoras-instrumentos-do-fortalecimento-do-estado/>. Acesso em: 02 abr. 2020.

abrangência meramente setorial). A regulação estatal envolve, como veremos adiante mais amiúde, atividades coercitivas, adjudicatórias, de coordenação e organização, funções de fiscalização, sancionatórias, de conciliação (composição e arbitragem de interesses), bem como o exercício de poderes coercitivos e funções de subsidiar e recomendar a adoção de medidas.⁷²

Segundo Vital Moreira (apud Neto) “o conceito de regulação deve abranger todas as medidas de condicionamento da atividade económica, revistam ou não de forma normativa.”⁷³

2.2.3. Poder Normativo das Agências Reguladoras

Esse conceito amplo de regulação por parte de uma entidade dotada de relativa autonomia, vinculada ao Poder Executivo, suscitou questionamentos acerca da sua legitimidade institucional para o exercício de atividades que *per se*, pela regra clássica da separação de poderes, estaria fora das competências institucionais do Executivo, notadamente as atividades normativas intrínsecas a atividade regulatória.

A competência ínsita as Agências Reguladoras, especialmente com relação aos poderes normativos, não contrastam e nem supõem a subtração de funções próprias do Poder Legislativo ou uma hipotética delegação de função, mas constituem uma evolução do princípio da legalidade numa sociedade complexa e em questões profundamente técnicas, onde cabe a lei em sentido estrito, editada pelo Legislativo, editar conteúdos mais amplos, verdadeiros *standarts* passíveis de serem integrados pela Administração no dia-a-dia da atividade diante da sua complexidade e dinamicidade, pautada pelos critérios objetivos delimitados pela lei.⁷⁴

Alexandre Santos de Aragão defende que:

A necessidade de descentralização normativa, principalmente de natureza técnica, é a razão de ser das entidades reguladoras independentes, ao que podemos acrescentar o fato de a competência normativa, abstrata ou concreta, integrar o próprio conceito de regulação.⁷⁵

⁷² NETO, Floriano de Azevedo Marques. Agências Reguladoras. Instrumentos do fortalecimento do Estado. Associação Brasileira de Agências de Regulação, 20 jan. 2019. Disponível em: <http://abar.org.br/mdocs-posts/agencias-reguladoras-instrumentos-do-fortalecimento-do-estado/>. Acesso em: 02 abr. 2020.

⁷³ Idem.

⁷⁴ _____ . A Nova Regulação Estatal e as Agências Independentes. In: SUNDFELD, Carlos Ari. *Direito Administrativo Econômico* (Org.). São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 94-95.

⁷⁵ ARAGÃO, Alexandre Santos de. *Agências Reguladoras e a evolução do Direito Administrativo Econômico*. Rio de Janeiro: Forense, 2002. p. 380.

Ainda segundo o mencionado autor, o fundamento constitucional do poder normativos das agências decorreria de um conceito amplo do regulamento de execução previsto no artigo 84, IV, *in fine* da CF (expedição de “decretos e regulamentos para fiel execução da lei), a partir de *standarts* legislativos de conteúdo aberto, a exemplo do art. 3º, VIII, da Lei nº 9.427/96 que atribui à ANEEL a competência de impor “restrições, limites ou condições” aos negócios dos agentes envolvidos. Tal posição é delimitada no seguinte excerto, no qual Aragão faz menção ao pensamento de Caio Tácito:

Sintetizando a nossa opinião a respeito da controvérsia, podemos adotar a lição de CAIO TÁCITO, pela qual “regulamentar não é só reproduzir analiticamente a lei, mas ampliá-la e complementá-la, segundo o seu espírito e conteúdo, sobretudo nos aspectos que a própria lei, explícita ou implicitamente, outorga à esfera regulamentar.”⁷⁶

Maurício Zockun e Carolina Zancaner Zockun apontam que, a par das situações de sujeição geral “cominada por lei que impõem dado comportamento a toda a sociedade de modo geral e impessoal”, a denominada sujeição especial ocorre em situações onde o Estado produz “normas jurídicas destinadas a disciplinar sua atuação nas relações jurídicas intestinas”, instituto distinto da discricionariedade, porquanto que este último consiste no espaço de liberdade nos limites da lei, enquanto que a sujeição especial decorre da ausência de expressa autorização legal.⁷⁷

Segundo mencionados autores, a sujeição especial guarda seu fundamento constitucional no artigo 84, VI, *a* da CF que autoriza ao Poder Executivo a dispor, por ato infralegal, sobre a organização e o funcionamento da Administração Federal, sujeitando tanto o particular que voluntariamente se insere na estrutura orgânica da Administração, quanto os que são impositivamente colocados sob o espectro dessas relações (ex. casos dos presos, alunos dos estabelecimentos oficiais de ensino, enfermos em hospitais públicos), citando ainda o caso das Agências Reguladoras, onde o concessionário e permissionário voluntariamente se colocam sob a estrutura e a sujeição das normas fixadas por essas autarquias.⁷⁸

⁷⁶ ARAGÃO, Alexandre Santos de. *Agências Reguladoras e a evolução do Direito Administrativo Econômico*. Rio de Janeiro: Forense, 2002. p. 414-416.

⁷⁷ ZOCKUN, Maurício; ZOCKUN, Carolina Zancaner. *A relação de sujeição especial no direito brasileiro*. Revista de Direito Administrativo e Constitucional. Curitiba, n. 77, jul./set. 2019, p. 127-131.

⁷⁸ Idem, p. 130-132.

A tese da sujeição especial se aplica sem discussões aos serviços públicos que foram delegados à iniciativa privada, por se tratar de situação em que o particular voluntariamente adere à estrutura orgânica estatal, pelo vínculo do contrato, no entanto, nas hipóteses de atividades privadas de interesse público, a exemplo das atividades regulamentadas pela Agência Nacional de Saúde Suplementar (ANS), a atividade não é de titularidade exclusiva do Estado (art. 199 da CF), de tal maneira que o particular que atua no setor de saúde complementar, por exemplo, exerce sua atividade no mercado e não se dispõe a atuar debaixo da estrutura estatal como ocorre na delegação dos serviços públicos.

Isso porque, a par da existência dos serviços públicos, que são atividades desempenhadas diretamente ou indiretamente pelo Estado (por delegação à iniciativa privada), as quais são caracterizadas pelo vínculo orgânico com o Estado nos termos do artigo 175 da CF de 1988, temos os serviços de “utilidade pública” ou as chamadas “atividades privadas de interesse público” que não são serviços públicos, por faltar o vínculo orgânico com o Estado pelo fato de não incumbir ao poder público, mas que “estão no meio termo” entre o serviço público e as atividades eminentemente privadas, estas últimas não sujeitas a controle ou, quando muito, a um controle de polícia administrativa geral, “que apenas verifica se a atividade não fere a ordem pública, a saúde pública, a segurança pública etc., não a funcionalizando especifica e comissivamente ao interesse público”.⁷⁹

As atividades de interesse público são prestadas pelo particular por direito próprio, mas o Estado a sujeita a um “controle constante e que pode em alguns aspectos imiscuir-se em elementos contratuais da prestação da atividade”, para que ela não só não agrida a ordem pública, como ocorre nas atividades eminentemente privadas, como também contribua para sua realização.⁸⁰

Segundo Alexandre Santos de Aragão, o que distingue as atividades privadas de interesse público do serviço público, é o fato daquelas se encontrarem protegidas pelo direito fundamental da livre iniciativa, podendo ser instrumentalizadas pelo Estado para realização de políticas públicas, mas não forçadas a executá-las, enquanto que no serviço público a prestação pode ser delegada quando e como o poder público decidir e não há

⁷⁹ ARAGÃO, Alexandre Santos de. Atividades Privadas Regulamentadas. In: ARAGÃO, Alexandre Santos de (Org.). *O Poder Normativo das Agências Reguladoras*. 2. edição. Rio de Janeiro: Forense, 2011. p. 170.

⁸⁰ Idem.

nenhum direito empresarial à atividade que constranja o Estado, o qual pode inclusive retomar sua prestação direta.⁸¹

A par da mencionada distinção, as atividades de interesse público estão sujeitas a exigência de prévia autorização (art. 170, parágrafo único, da CF) e a uma forte regulação (art. 174 da CF), que alcança aspectos essenciais da atividade, como fixação de preços a usuários (ex. táxis) e conteúdo mínimo das prestações (saúde), no entanto, tal regulação deve ser limitada pelo direito fundamental da livre iniciativa (art. 170 da CF).⁸²

Nos serviços públicos, por sua vez, não há um direito preexistente, uma garantia empresarial fundamental tal como a livre iniciativa que limite a regulação estatal ou garanta ao particular direitos ao exercício da atividade, sendo todos os direitos decorrente do contrato de concessão, de tal forma que o Estado pode deixar de delegar a atividade ou, quando delegada, retomá-la, o que não é possível na atividade privada de interesse público, pois, nada obstante a prerrogativa regulatória estatal (art. 174), há que respeitar um mínimo, o núcleo essencial do direito fundamental à livre iniciativa (art. 170).⁸³

Dessa forma, verifica-se uma competência regulatória mais ampla nos serviços públicos do que nas atividades privadas de interesse público, posto que enquanto o concessionário ou permissionário adere a estrutura estatal pela via do contrato, sujeito a uma maior ingerência estatal, o particular que exerce uma atividade privada de interesse público, a exemplo dos prestadores de saúde complementar, estão sujeitos a uma regulação limitada pela garantia fundamental da propriedade e da livre iniciativa.

É importante ressaltar que a regulação exercida pela ANPD é exercida de forma transversal não só em relação à Administração Pública, notadamente no que se refere a políticas públicas exercidas diretamente ou indiretamente, como também sobre os setores econômicos que realizam tratamento e compartilhamento de dados pessoais, sejam atividades puramente privadas ou de interesse público, de tal forma que deve haver um necessário equilíbrio nas competências normativas do regulador.

Nesse sentido, andou bem a LGPD ao prever no seu texto que as condicionantes administrativas impostas pela ANPD ao agente de tratamento privado, devem observar “a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei” (§ 1º, art.

⁸¹ ARAGÃO, Alexandre Santos de. Atividades Privadas Regulamentadas. In: ARAGÃO, Alexandre Santos de (Org.). *O Poder Normativo das Agências Reguladoras*. 2. edição. Rio de Janeiro: Forense, 2011. p. 170-171.

⁸² Idem, p. 170.

⁸³ Idem, p. 170.

55J), bem como a necessidade das normas da ANPD serem precedidas de consulta pública e análise de impacto regulatório (§2º, art. 55J).

2.2.4. Análise de impacto regulatório

Conforme leciona Paulo César Melo da Cunha (apud Filho, 2011, p. 65) “Toda regulação representa uma intervenção imperativa traduzida em uma restrição de liberdade dentro de uma atividade empresarial.” Nesse sentido, observa o autor: “A proposta, assim, é buscar, à luz do princípio da proporcionalidade, o ponto ótimo para reduzir o impacto na interferência estatal na propriedade e atividade privadas e, ao mesmo tempo, viabilizar a admissão daqueles que têm interesse em ingressar e permanecer no mercado regulado.”⁸⁴

Segundo Luiz Alberto Blanchet e Priscila Lais Ton Bubniak:

A Análise de Impacto Regulatório (AIR), definida pela Organização para Cooperação e Desenvolvimento Econômico (OCDE, 2008), como “ferramenta regulatória que examina e avalia os prováveis benefícios, custos e efeitos das regulações novas ou alteradas” sob uma primeira perspectiva, apresenta-se como um importante mecanismo para definição do objeto de regulação, bem como justificção da intervenção. Ademais, visa evitar problemas, como contrariedade entre normas administrativas; insegurança jurídica; dificuldades geradas em matéria de compliance; restrições à pura inovação dos agentes econômicos e sociais; riscos decorrentes de desdobramentos não previstos no conteúdo regulatório; distorções mercadológicas perpetradas por agentes econômicos interessados em prejudicar competidores por meio da regulação; favorecimento de pequenos grupos em detrimento do interesse público; captura regulatória e lobby.⁸⁵

No Brasil, a ANVISA foi a primeira agência a implementar o AIR em 2008, por meio da Portaria nº 422/08, posteriormente absorvida pela ANEEL (Resolução Normativa nº 540/2013), ANATEL (Resolução 612/2013), ANCINE (Resolução de Diretoria Colegiada nº 52/13), ANAC (Instrução Normativa nº 61/2012), ANP (Portaria nº 255/2013) e ANTAQ (Resoluções de nº 197/2009, nº 3.585/2014 e nº 3.000/2009).⁸⁶

⁸⁴ FILHO, José dos Santos Carvalho. O Poder Normativo das Agências Reguladoras. In: ARAGÃO, Alexandre Santos de (Org.). *O Poder Normativo das Agências Reguladoras*. 2. edição. Rio de Janeiro: Forense, 2011. p. 65.

⁸⁵ BLANCHET, Luiz Alberto, BUBNIAK, Priscila Lais Ton. *Análise de Impacto Regulatório: uma ferramenta e um procedimento para a melhoria da regulação*. Pensar, Fortaleza, v. 22, n. 3, set/dez. 2017, p. 1-15.

⁸⁶ Idem.

O artigo 5º da Lei de Liberdade Econômica (Lei 13.874, de setembro de 2019) previu expressamente o instituto da AIR, uniformizando sua aplicação pelas agentes regulatórias, com a finalidade de aferir a razoabilidade do impacto econômico do ato normativo, sendo regulamentado no âmbito federal pelo Decreto nº 10.411, de 30 de junho de 2020.

De qualquer forma, a previsão expressa da análise de impacto regulatório na LGPD (§2º, art. 55J), como condição à materialização da competência normativa pela ANPD, representa importante garantia aos agentes de tratamento privados, na medida em que reforça a necessidade do equilíbrio normativo, a busca da razoabilidade frente “a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei” (§1º, art. 55J).

2.2.5. Poder Sancionatório das Agências Reguladoras

Dentro da atividade regulatória, é próprio do agente regulador o poder de aplicar sanções, bem como dirimir conflitos individuais e coletivos sem que isso implique em subtração de funções do Poder Judiciário, até porque o judiciário não é o único foro de mediação e solução de conflitos, como já ocorre nos Tribunais Arbitrais e comissões de conciliação. As decisões do regulador, por sua vez, não afastam seu controle judicial, nos termos em que previstos no artigo 5º, XXXV, da CF.⁸⁷

No que respeita especialmente ao poder sancionatório da ANPD, o artigo 52 da LGPD prevê as penalidades pela infração à lei pelos agentes de tratamento de dados, após procedimento que assegure a ampla defesa, mediante critérios que considerem as condições pessoais e a postura do infrator, a natureza e gravidade das infrações e a proporcionalidade da sanção (§1º, art. 52), sem prejuízo de sanções previstas em legislações específicas (§2, art. 52).⁸⁸ A ANPD deverá editar regulamento acerca das

⁸⁷ SUNDFELD, Carlos Ari. Introdução às Agências Reguladoras. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 31.

⁸⁸ Advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração (infração não aplicável aos Entes Públicos); multa diária, observado o limite total aplicável a multa (infração não aplicável aos Entes Públicos); publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI -

sanções pela infração à LGPD, com a metodologia do cálculo das sanções de multa, a ser submetido à consulta pública (art. 53).

A LGPD restringiu as penalidades aplicáveis à Administração Pública pela infração à lei às seguintes sanções: advertência (art. 52, I); publicização da infração (art. 52, IV); bloqueio (art. 52, V) e a eliminação dos dados pessoais a que se refere a infração (art. 52, VI), suspensão do funcionamento banco de dados pelo prazo de 6 meses (art. 52, X), suspensão da atividade de tratamento de dados objeto da infração pelo prazo de 6 meses (art. 52, XI), proibição, parcial ou total, da realização de tratamento de dados (art. 52, XII). Não são aplicáveis ao Poder Público as sanções pecuniárias de multa simples e multa diária (art. 52, II e III).

Cabe ressaltar, finalmente, que o §5 do artigo 53 prevê que o produto da arrecadação das multas aplicáveis pela ANPD será destinado ao Fundo de Defesa de Direitos Difusos, e não para o orçamento de ente regulador, circunstância que prejudica sua autonomia financeira, conforme será tratado em capítulo próprio.

2.2.6. Da autonomia das Agências Reguladoras

A autonomia atribuída as agências reguladoras em relação ao Poder Executivo é traço característico desse novo modelo de intervenção estatal, aliás, sua neutralidade na qualidade de regulador, qualificada pela capacidade de tomar decisões técnicas sem a interferência de um ator político, é requisito exigido pelo mercado para ingressar em um dado setor com competitividade. Marcos Augusto Perez consolidou, com muita propriedade, os traços característicos das Agências Reguladoras:

Concluindo, podemos resumir nosso entendimento da seguinte forma: (1) as agências reguladoras do Direito Brasileiro foram inspiradas no modelo das *administrative agencies* do Direito norte-americano; (2) as agências reguladoras, no Direito brasileiro, são autarquias de regime especial, ou seja, pessoas jurídicas de direito público, criadas por lei e com autonomia gerencial, administrativa e financeira ampliada em relação às autarquias comuns; (3) as agências reguladoras, no Direito brasileiro, possuem independência hierárquica em relação à Administração Direta, independência assegurada em razão de seus dirigentes possuírem mandato e estabilidade na função; (4) as agências, no Direito brasileiro, acumulam funções de regulamentação, de fiscalização, sancionatórias e contenciosas; (5) a finalidade das agências, em nosso Direito, é coordenar a intervenção estatal em um determinado setor da economia, preservando a

suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

competição entre os particulares e fiscalizando a execução de serviços públicos executados pela iniciativa privada; (6) é essencial às agências, e nosso Direito contempla regras nesse sentido, a fixação de um processo racional e transparente de tomada de decisões.⁸⁹

A outorga de autonomia as Agências Reguladoras tiveram como objetivo a criação de um modelo de regulação mais eficiente em setores de especial interesse da sociedade, evitando a “captura” do regulador pela influência política ou do mercado.⁹⁰

No mesmo sentido, Carlos Ari Sunfeld anota que o regime especial da agência qualificado pela sua autonomia, viabilizou a criação de um ambiente de segurança a investidores para a aquisição de ativos estatais em um sistema de concorrência, um modelo de controle e influências que asseguram uma atuação democrática e atenta aos interesses gerais. Na visão do autor, o fator fundamental para garantir a autonomia das agências é a estabilidade dos seus dirigentes, materializada nos mandatos conferidos por ocasião da nomeação sem a possibilidade de exoneração *ad nutum*.⁹¹

Celso Antonio Bandeira de Mello registra que a qualificação autarquias “sob regime especial” atribuída as agências reguladoras que a difere das demais autarquias, diz respeito a investidura e a estabilidade dos mandatos dos seus dirigentes, tendo em vista que os demais caracteres do instituto relacionados a autonomia administrativa e ausência de subordinação hierárquica é ponto comum nas autarquias em maior ou menor grau⁹².

Maria Sylvia Zanella Di Pietro define o regime especial conferido as agências reguladoras como sendo, em regra, a maior autonomia em relação a Administração Direta, a estabilidade dos seus dirigentes e ao caráter final de suas decisões⁹³.

Floriano de Azevedo Marques Neto, por sua vez, entende que a concretização da autonomia das agências reguladoras é verificada pela adoção de um desenho institucional que proporcione:

i) a estabilidade dos dirigentes; ii) a autonomia da gestão do órgão; iii) o estabelecimento de fontes próprias de recursos para o órgão, se possível, geradas do

⁸⁹ PEREZ, Marcos Augusto. *As Agências Reguladoras no Direito brasileiro: origem, natureza e funções*. Revista de Direito Administrativo e Constitucional. Curitiba, ano 2, n. 5 (2000), p. 59-66.

⁹⁰ ARAGÃO, Alexandre Santos de. *Agências Reguladoras e a evolução do Direito Administrativo Econômico*. Rio de Janeiro: Forense, 2002. p. 365.

⁹¹ SUNDFELD, Carlos Ari. Introdução às Agências Reguladoras. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 24.

⁹² MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 178.

⁹³ PIETRO, Maria Sylvia Zanella Di. *Direito Administrativo*. 23. ed. São Paulo: Editora Atlas, 2009. p.469.

próprio exercício da atividade regulatória; iv) a não-vinculação hierárquica a qualquer instância de governo; v) a inexistência de instância revisora hierárquica dos seus atos, ressalvada a revisão judicial⁹⁴.

Em análise acerca do regime jurídico especial da Agência Nacional de Telecomunicações (ANATEL), Benedicto Porto Neto ressaltou o elevado grau de autonomia da agência, considerando as seguintes características: (i) autonomia administrativa e financeira; (ii) ausência de subordinação hierárquica; e (iii) estabilidade dos seus dirigentes.⁹⁵

A Lei nº **9.986, de 18 de julho de 2000** trouxe disposições relacionados a gestão das Agências Reguladoras Brasileiras, incorporando os institutos considerados relevantes a autonomia da Entidade, conforme Luís Roberto Barroso:

No geral, a lei endossa as linhas de entendimento que se haviam cristalizado na doutrina, prevendo: (i) nomeação de conselheiro ou diretor, pelo Presidente da República, com aprovação do Senado Federal, atendidos os requisitos da nacionalidade brasileira, reputação ilibada, formação universitária e elevado conceito no campo de especialidade dos cargos (arts. 5º); (ii) quarentena, com o impedimento ao ex-dirigente, terminado o mandato, de prestar qualquer tipo de serviço no setor público ou nas empresas integrantes do setor regulado pela agência (art. 8º); (iii) estabilidade: os conselheiros e diretores somente perderão o mandato em caso de renúncia, de condenação judicial transitada em julgado ou de processo administrativo disciplinar (art. 9º).⁹⁶

A Lei nº 13.848, de 25 de junho de 2019 alterou dispositivos relativos ao regime jurídico das Agências Reguladoras, com a finalidade de aperfeiçoar o sistema vigente com vistas a “preservar sua autonomia e independência, imprescindíveis ao seu bom funcionamento”, tendo absorvido no seu artigo 3º o ponto convergente na doutrina acerca da autonomia das Agências Reguladoras, ao prever que sua “natureza especial” é caracterizada pela: (i) ausência de subordinação hierárquica, (ii) autonomia decisória, administrativa, financeira e funcional, (iii) bem como a investidura dos seus dirigentes para cumprimento de mandato por prazo certo.⁹⁷

⁹⁴ NETO, Floriano de Azevedo Marques. A Nova Regulação Estatal e as Agências Independentes. In: SUNDFELD, Carlos Ari. *Direito Administrativo Econômico* (Org.). São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 88.

⁹⁵ NETO, Benedicto Porto. A Agência Nacional de Telecomunicações. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 287-288.

⁹⁶ BARROSO, Luis Roberto. Apontamentos sobre as agências reguladoras. In: MORAES, Alexandre. (Org) et alii. *Agências reguladoras*. São Paulo: Atlas, 2002. p. 111-112.

⁹⁷ BRASIL. Justificativa constante do texto inicial da PLS 52/2013. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/111048>>. Acesso em: 20 abr. 2020.

2.2.7. Da autonomia formal das Agências Reguladoras

Pesquisadores de diversas matizes como Fabrizio Gilardi, Luiz Gutierrez e Alexandre Gueventher buscaram definir critérios para mensurar o grau de autonomia das Agências Reguladoras, sendo comum a identificação de indicadores lastreados na autonomia formal, de caráter objetivo e considerando o desenho institucional da entidade, levando em conta aspectos relacionados a: (i) estabilidade dos seus dirigentes (forma de nomeação, estabilidade e tempo de mandato dos diretores); (ii) autonomia administrativa e orçamentária e (iii) ausência de subordinação hierárquica.⁹⁸

Luiz Gutierrez procedeu a análise da governança regulatória de 25 países da América Latina em 2003, com dados obtidos entre 1980 e 1997, considerando o aspecto autonomia da autoridade regulatória no setor de telecomunicações⁹⁹. Na ocasião e com base nos fatores utilizados, o Brasil ficou ranqueado em 5º lugar, atrás de Argentina (1º), Barbados (2º), Belize (3º) e Bolívia (4º).¹⁰⁰

No Brasil, uma das primeiras pesquisas acerca da qualidade regulatória realizada por Correa et al (2006) levou em consideração indicadores para análise da autonomia formal, baseada no modelo institucional da agência, bem como a autonomia de fato, focada em procedimentos adotados pelas entidades para concluir, em síntese, que os atributos formais não asseguram uma atuação autônoma da agência, devendo ser levado em consideração indicadores relacionados a procedimentos decisórios adotados na prática da sua atuação, ou seja, os atributos relacionados a autonomia de fato.¹⁰¹

No presente estudo é realizado um recorte acerca dos indicadores relacionados à autonomia formal, relacionada ao modelo institucional atribuído por lei à Agência, não que a autonomia de fato, substantiva, não seja importante, mas porque o foco de análise

⁹⁸ GILARDI, F. The Formal Independence of Regulators: a comparison of 17 countries and 7 sectors. *Swiss Political Science Review*, v. 11, n. 4, p. 139-167, 2005. GUTIERREZ, L. Regulatory Governance in the Latin American Telecommunications Sector. *Utilities Policy*, n. 11, 2003. GHEVENTER, A. *Autonomia versus controle: origens do novo marco regulatório antitruste na América Latina e seus desafios sobre a democracia*. Belo Horizonte: Editora da UFMG, 2005.

⁹⁹ Os indicadores utilizados por Luiz Gutierrez foram: (1) autonomia (autonomia para recrutar seu próprio pessoal); (2) accountability (possibilidade de questionamento), (3) clareza da competência da agência (clareza de atribuições para imposição de obrigações); (4) transparência e participação (realização de audiências públicas e publicidade decisória); (5) marco legal regulatório (todos os indicadores anteriores devem estar claros no marco legal de criação da agência).

¹⁰⁰ GUTIERREZ, L. Regulatory Governance in the Latin American Telecommunications Sector. *Utilities Policy*, n. 11, 2003.

¹⁰¹ CORREA, P. et al. Regulatory governance in infrastructure industries: a assessment and measurement of Brazilian regulators. Washington: World Bank, World Bank Publications, 2006.

é a Autoridade Nacional de Proteção de Dados, regulador que ainda não se encontra instrumentalizado e em funcionamento, de forma que não há parâmetros para a análise acerca dos procedimentos que serão adotados pela instituição.

Mariana Batista da Silva em monografia sobre a autonomia das agências reguladoras, realizou a análise acerca da autonomia formal das agências a partir dos seus desenhos institucionais, com base no modelo proposto por Alexandre Gueventher.¹⁰² Abaixo as variáveis consideradas pela pesquisadora com suas conclusões:

Tabela 1: índice de Autonomia Formal

Variável	Descrição	Codificação
Mandato	O mandato dos diretores é superior ou igual a quatro anos?	1 (sim) 0,5 (≤ quatro anos) 0 (sem mandato fixo)
Indicação	A indicação dos diretores é compartilhada?	1 (sim) 0 (não)
Demissão	A demissão é apenas possível com sentença?	1 (sim) 0,5 (início do mandato) 0 (não)
Recondução	A recondução é proibida?	1 (sim) 0 (não)
Experiência	É necessário que os diretores possuam conhecimento específico na área de regulação?	1 (sim) 0 (não)
Autorização	A agência toma decisões sem a necessidade de autorização do governo?	1 (sim) 0 (não)
Revisão	As decisões da agência são passíveis de revisão apenas no Judiciário?	1 (sim) 0 (não)
Recursos	O orçamento é definido pela própria agência?	1 (sim) 0 (não)
Pessoal	A agência tem o comando da sua política de pessoal?	1 (sim) 0 (não)
Procedimentos	Os procedimentos da agência só podem ser modificados com anuência do Legislativo?	1 (sim) 0 (não)

Fonte: Mariana Batista da Silva (2010, p. 53)

¹⁰² SILVA, Mariana Batista da. *Independência após a delegação? Uma análise exploratória da interferência política nas Agências Regulatórias Brasileiras*. 2010. Dissertação (Mestrado em Ciência Política). Universidade Federal de Pernambuco, Recife, 2010.

Tabela 2: Autonomia formal das Agências Reguladoras Brasileiras

Agência	Mandato	Indicação	Demissão	Recondução	Experiência
ANEEL	1	1	0,5	0	1
ANATEL	1	1	1	0	1
ANP	1	1	1	0	1
ANVISA	0,5	1	0,5	0	1
ANS	0,5	1	0,5	0	1
ANA	1	1	0,5	0	1
ANTAQ	1	1	1	0	1
ANTT	1	1	1	0	1
ANCINE	1	1	1	0	1
ANAC	1	1	1	0	1

Agência	Autorização	Revisão	Recursos	Pessoal	Procedimentos
ANEEL	0	1	0	1	0
ANATEL	1	1	0	1	0
ANP	1	1	0	1	0
ANVISA	1	1	0	1	0
ANS	1	1	0	1	0
ANA	0	1	0	1	0
ANTAQ	0	1	0	1	0
ANTT	0	1	0	1	0
ANCINE	0	0	0	1	0
ANAC	0	1	0	1	0

Fonte: Mariana Batista da Silva (2010, p. 55/56)

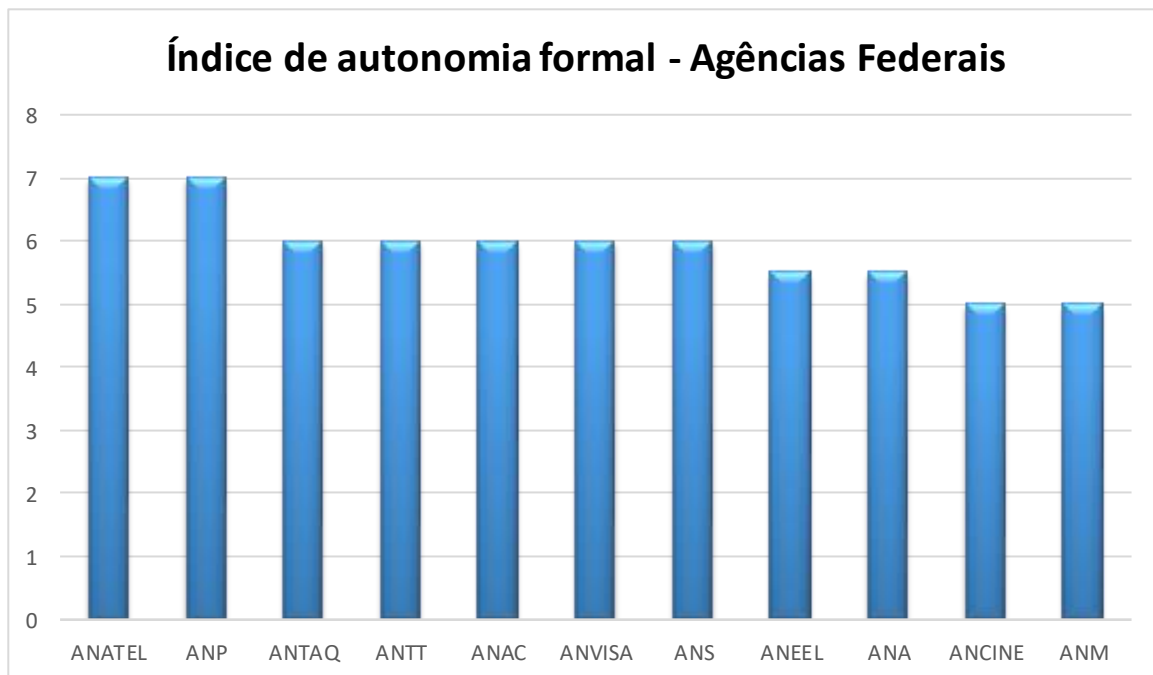
Dos 10 indicadores utilizados pela pesquisadora, cinco não tiveram variação entre as agências: (i) **orçamento** baseados em recursos próprios, como taxas e multas, bem como recursos orçamentários do tesouro, sendo necessária a observação quanto ao contingenciamento do orçamento da Agência pelo Executivo que reflete redução na sua autonomia orçamentária; (ii) a **política de pessoal**, por meio de legislação própria, detendo a diretoria autonomia para alocação de recursos humanos; (iii) **experiência específica no campo de atuação**; (iv) **indicação seguida de aprovação pelo Senado Federal**; (v) **possibilidade de modificação de procedimentos** da Agência pelo Executivo por meio de Medidas Provisórias¹⁰³.

As diferenças ficam por conta do status dos diretores: (i) **mandatos** fixos, sendo que apenas duas agências possuem mandato inferior a quatro anos (ANVISA e ANS); (ii) **demissão** por sentença judicial e também em alguns casos no início do mandato; (iii) impossibilidade de **recondução**, o que torna os diretores mais independentes por não ser

¹⁰³ Cita-se a título de exemplo a reversão da delegação de poderes para estabelecer os termos do contrato de concessão realizada pelo Governo Federal em relação a ANEEL em 2003, em meio à crise elétrica, por meio de Medida Provisória.

possível a renovação do mandato; (iv) necessidade de **aprovação** de suas decisões pelo Governo; (v) **impossibilidade de revisão** das suas decisões pelo Governo.

A título ilustrativo destaca-se o gráfico abaixo acerca do grau de autonomia das Agências Reguladoras Brasileiras, com base nos indicadores utilizados por Batista que levaram em conta o modelo proposto por Alexandre Gueventher, oportunidade que incluímos a recém criada Agência Nacional de Mineração (ANM) utilizando os mesmos indicadores, mas sem considerar a ANPD, posto que será objeto de estudo em capítulo próprio.



Fonte: elaboração própria

A conclusão acerca do grau de autonomia formal das agências, levando em conta os diversos modelos institucionais, é de que sob tais indicadores, há uma autonomia relativamente alta das Agências Reguladoras, sendo que as principais restrições estariam nas questões envolvendo a estabilidade dos seus diretores, a relativa autonomia orçamentária decorrente do contingenciamento de recursos e retenções de receitas próprias das Agências pelo Governo e a possibilidade de intervenção política nos procedimentos e competências da Agência por meio da edição de Medidas Provisórias.

2.2.8. Da “nova lei das Agências Reguladoras” (Lei nº 13.838/2019)

A Lei nº 13.848, de 25 de junho de 2019 dispõe sobre a gestão, a organização, o processo decisório e o controle social das agências reguladoras, constituindo um marco legal das Agências Reguladoras Brasileiras. A mencionada lei prevê sua aplicação, como regra, às autarquias especiais caracterizadas como Agências Reguladoras e criadas a partir de sua vigência (artigo 2º, parágrafo único).

O artigo 3º da Lei nº 13.848/2019 estatuiu o entendimento consagrado na doutrina de que a natureza “especial” conferida a as agências reguladoras é determinada pela: (i) ausência de subordinação hierárquica, (ii) autonomia decisória, administrativa, financeira e funcional, (iii) bem como a investidura dos seus dirigentes para cumprimento de mandato por prazo certo.

Com relação ao status dos dirigentes, a Lei nº 13.848/2019 fixou o prazo mandato em cinco anos de forma linear para todas as agências reguladoras, regras de transição para a não coincidência dos mandatos, regras para a vacância, vedou a recondução ao cargo, aumentou a chamada quarentena de quatro para seis meses, estabeleceu requisitos relacionados a efetiva experiência profissional e formação compatível com o cargo, bem como vedou a nomeação de caráter político (art. 42)

No que respeita a autonomia administrativa e de pessoal da Agência Reguladora, ressaltou a lei ser de responsabilidade dos seus gestores “a representação da agência, o comando hierárquico sobre o pessoal e os serviços e o exercício de todas as competências administrativas correspondentes” (art. 42).

O §2º do artigo 3º da nova lei das Agências Reguladoras prevê que sua autonomia administrativa é caracterizada por competências listadas no dispositivo, a exemplo da solicitação ao Ministério da Economia para: (i) autorização para realização de concursos públicos; (ii) provimento de cargos; (iii) alterações no quadro pessoal e plano de carreiras. No entanto, a subordinação à tomada de decisões em políticas de gestão de pessoal a Administração Central pode, em maior ou menor medida, revelar uma incompatibilidade da Agência em dispor de forma autônoma da sua organização administrativa¹⁰⁴.

De qualquer forma, no seu aspecto geral a lei procura munir as Agências Reguladoras de mecanismos visando estruturar sua autonomia em relação ao poder central, revelando a preocupação do legislador pátrio acerca da autonomia do agente regulador. Tanto é assim que o §6º do artigo 37 da Lei 13.878/2019 prevê que a delegação

¹⁰⁴ GARNICA, Vitor Gabriel; KEMPFER, Marlene. *O fenômeno da captura e a independência das Agências Reguladoras no Brasil*. Revista Brasileira de Filosofia do Direito. Belém, v. 5, n. 2, Jul/Dez 2019, p. 43-60.

de poderes regulatórios próprios de Agências Federais somente poderá ser realizada se reguladores estaduais, distrital e municipais gozarem “de autonomia assegurada por regime jurídico compatível com o disposto nesta Lei”.

A Lei nº 13.848/2019 aponta para uma tendência onde “o poder legislativo tem tentado, por meio de sua atividade legislativa, diminuir a influência do poder executivo sobre as agências reguladoras”, o que pode ser verificado pela finalidade constante da justificativa do projeto que deu origem a lei, pelas alterações no modelo institucional das Agências levadas a efeito pelo mencionado diploma legal, bem como pela positivação do conceito de autarquia de natureza “especial”, atrelando-o aos indicadores de autonomia que a diferencia das demais autarquias, de forma a absorver o conceito doutrinário.¹⁰⁵

2.2.9. Conclusão Parcial

Podemos concluir que a autonomia atribuída as agências reguladoras em relação ao Poder Executivo é traço peculiar desse modelo de intervenção estatal, cuja neutralidade, característica inerente a capacidade de tomar decisões técnicas sem a interferência de um ator político, é requisito para a regulação dentro de um dado setor, especialmente em sistemas onde o Poder Público está sujeito a regulação ao lado de atores do mercado, como na situação objeto do estudo onde o Estado atua tanto como regulador, na figura da Autoridade Nacional de Proteção de Dados, como regulado, posto que a Administração Pública e suas entidades, nos mais diversos níveis, realizam o tratamento e o compartilhamento de dados pessoais.

A autonomia da Agência Reguladora, condição para o exercício da regulação em condições de neutralidade em relação ao poder político e econômico, pode ser estabelecida a partir de um modelo institucional em sua criação que proporcione uma autonomia formal a Agência, a partir de arquétipos já concebidos pela doutrina e pela legislação aplicável, a par de requisitos de índole substantiva afetos aos procedimentos decisórios que também são considerados para aferir a autonomia da Agência, mas cuja a verificação só é possível mensurar a partir do funcionamento e análise das práticas decisórias da entidade.

¹⁰⁵ SALINAS, Natasha Schmitt Caccia. *A intervenção do Congresso Nacional na Autonomia das Agências Reguladoras*. Revista Estudos Institucionais. Rio de Janeiro, v. 5, n.2, maio/dez. 2019, p. 586-614.

Com relação aos modelos institucionais concebidos pela doutrina para aferir a autonomia da Agência em relação ao poder político, a Lei nº 13.848, de 25 de junho de 2019, absorveu no seu artigo 3º o ponto convergente na doutrina acerca da autonomia das Agências Reguladoras, ao prever que sua “natureza especial” é caracterizada pela: (i) ausência de subordinação hierárquica, (ii) autonomia decisória, administrativa, financeira e funcional, (iii) bem como a investidura dos seus dirigentes para cumprimento de mandato por prazo certo.

2.3. Da experiência internacional

2.3.1. GPDR: a exigência de uma autoridade de dados autônoma para a transferência transnacional de dados

O debate sobre o tema da proteção de dados pessoais na União Europeia (EU) resultou na promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu nº 679, aprovado em 27 de abril de 2016 (GPDR), o que levou os países não integrantes do bloco a adequarem sua legislação interna, tendo em vista que a referida norma contém exigências no sentido de que tais países devem contar com uma legislação compatível, sob pena de terem prejudicada a relação comercial com os integrantes da União Europeia.¹⁰⁶

O artigo 45, 1 do Regulamento 679/2016 (GPDR) prevê: “Pode ser realizada uma transferência de dados para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.”

A autonomia da autoridade nacional de proteção de dados, é um dos requisitos para que a Comissão de Proteção Dados Pessoais da UE avalie a adequação do nível de proteção atribuído por um dado país em relação à GPDR.¹⁰⁷

¹⁰⁶ PINHEIRO, Patrícia Peck. *Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD)*. São Paulo: Saraiva, 2018. p. 196/225.

¹⁰⁷ Artigo 45, 2, b do Regulamento 679/2016 (GPDR): A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internaional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros;

Ao apreciar o sistema de proteção dados de países da América Latina, ainda sob a vigência do artigo 25 Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 que previu regra semelhante à da GPDR, a Comissão Europeia reconheceu que o nível de proteção de dados assegurada na Argentina e no Uruguai era compatível ao estabelecido na União Europeia, analisando especialmente a adequação entre as legislações e a existência de um órgão autônoma para fiscalizar a execução da lei.¹⁰⁸ Tal exigência ficou bastante evidente na decisão da Comissão em relação ao Uruguai:

URUGUAI: DECISÃO DE EXECUÇÃO DA COMISSÃO, de 21 de agosto de 2012, nos termos da Diretiva 96/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai, no que se refere ao tratamento automatizado de dados [notificada com o número C (2012) 5704]. (texto relevante para efeitos do EEE) (2012/484/EU).

(6) As normas de proteção de dados pessoais da República Oriental do Uruguai baseiam-se em grande medida nas normas da Diretiva 95/46/CE e encontram-se estabelecida na Lei 18.331 de proteção de dados pessoais e ação de habeas data (Ley nº 18.331 de protección de datos personales y acción de habeas data), de 11 de agosto de 2008, que é aplicável tanto às pessoas singulares como às pessoas coletivas).

(7) A referida lei é regulamentada pelo Decreto nº 414/2019, de 31 de agosto de 2009, aprovado no intuito de clarificar diversos elementos da lei e regular a organização, os poderes e o funcionamento da autoridade nacional de proteção de dados. O preâmbulo deste Decreto indica que, quanto a esta questão, a ordem jurídica nacional deve ser adaptada ao regime jurídico comparável mais comumente aceite, sobretudo o estabelecido pelos países europeus através da Diretiva 95/46/CE. [...]

(10) A aplicação das normas de proteção de dados é garantida pela existência de vias de recurso administrativas e judiciais, em especial pela ação de habeas data, que permite à pessoa a quem se referem os dados intentar uma ação judicial contra o responsável pelo tratamento de dados, a fim de exercer o direito de acesso, retificação e supressão, e *por um controlo independente efetuado pela Unidade Reguladora e de Controlo de Dados Pessoais (Unidad Reguladora y de Control de Datos Personales – URCDP), que tem poderes de investigação, intervenção e sanção, seguindo o disposto no artigo 28º da Diretiva 95/46/CE, e que de forma totalmente independente*. Além disso, qualquer parte interessada pode recorrer aos tribunais para pedir uma indenização por danos sofridos em consequência do tratamento ilícito dos seus dados pessoais.¹⁰⁹

¹⁰⁸ AGENTINA: 2003/490/CE: Decisão da Comissão, de 30 de junho de 2003, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa a adequação do nível de proteção de dados pessoais na Argentina (texto relevante para efeitos do EEE). Jornal Oficial nº L 168 de 05/07/2003 p. 0019-0022.

¹⁰⁹ LUCCA, Newton de; LIMA, Cintia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e Privacidade. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020. p. 389.

¹⁰⁹ Idem, p. 378-379.

O acordo de privacidade denominado *privacy shield* firmado entre EUA e UE em 12 de julho de 2016, para transferência para os Estados Unidos de dados de cidadãos europeus para fins comerciais, foi anulado pelo Tribunal de Justiça da União Europeia em decisão proferida em 16 de julho de 2020, sob o entendimento de que os requisitos de acesso a tais dados pelas autoridades americanas não tinham o mesmo nível de proteção previsto na União Europeia. Tal decisão dificulta o envio de dados de cidadãos europeus aos EUA, bem como evidencia uma postura da União Europeia de exigir um alto nível de proteção aos dados pessoais para manutenção de relações comerciais com os demais países, o que certamente refletirá no Brasil, o qual deve assegurar nível compatível de proteção de dados.¹¹⁰¹¹¹

Cabe ressaltar que na América Latina apenas a Argentina e o Uruguai contam com o reconhecimento da Comissão Europeia de Proteção de Dados, de que os modelos legislativos e regulatórios adotados nos respectivos países são compatíveis com o Europeu, sendo que a Argentina criou a “Direção Nacional de Proteção de Dados” do Ministério da Justiça, e o Uruguai a “Unidad Reguladora y de Control de Datos Personales (URCDP), órgão vinculado a agência reguladora “Agência para el Desarrollo del Gobierno de Gestión Electronica y la Sociedade de la Información y del Conocimiento (AGESIC).¹¹²

2.3.2. A autonomia regulatória exigida pela GPDR e OCDE

O artigo 52 da GPDR prevê que as autoridades nacionais de proteção de dados atuarão com autonomia (art. 52, 1) e sem qualquer tipo de interferência externa (art. 52, 2), razão pela qual determina que as autoridades de proteção de dados deverão ser dotadas de recursos humanos; técnicos, financeiros e estruturais necessários a realização de suas atribuições (art. 52, 4), quadro próprio de pessoal subordinado a sua diretoria (art. 52, 5) e autonomia financeira, de forma a assegurar “sua independência e que disponha de

¹¹⁰ Commercial sector: EU-US Privacy Shield. *European Commission*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en. Acesso em: 20 jul. 2020.

¹¹¹ Impactos da decisão da Corte de Justiça da União Europeia sobre transferência de dados pessoais. *Lexlatin*, 17 jul. 2020. Disponível em: <https://br.lexlatin.com/opiniao/impactos-da-decisao-da-corte-de-justica-da-uniao-europeia-sobre-transferencia-de-dados>. Acesso em: 20 jul. 2020.

¹¹² LUCCA, Newton de; LIMA, Cintia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e Privacidade. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020. p. 380.

orçamentos anuais separados e públicos”, mesmo que provisionados pelo orçamento geral estatal (art. 52, 6).

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE), cujo ingresso é uma das prioridades do atual governo, apresentou um relatório a membros do governo federal denominado “A Caminho da Era Digital no Brasil”, onde pontuou aspectos sensíveis relacionadas ao desenho institucional da ANPD e expediu recomendações visando assegurar sua autonomia, tais como: (i) reavaliar sua estruturação como órgão vinculado à Presidência da República; (ii) garantir que as nomeações para o Conselho Diretor sejam baseadas em critérios técnicos e; (iii) garantir um orçamento adequado e previsível à ANPD.¹¹³

A autonomia regulatória da Autoridade Nacional de Proteção de Dados prevista na LGPD não é, sob uma visão ampla, tão somente um requisito para a efetivação dos direitos da personalidade no controle de dados pessoais assegurados no artigo 2º da Lei nº 13.709/2018, como também condição para a reciprocidade no recebimento de dados de cidadãos europeus, exigência determinante para a competição das empresas brasileiras no cenário internacional, bem como para o ingresso do Brasil em organizações internacionais, a exemplo da OCDE, de tal maneira que não basta existir uma lei sobre o tema, mas deve ser estabelecidos mecanismos para viabilizar a atuação eficiente e autônoma da ANPD.

2.4. Regulação prevista na LGPD

2.4.1. Corregulação

A LGPD previu que a regulação em matéria de tratamento de dados não seria exclusivamente estatal, permitindo a regulação por parte dos agentes de tratamentos de dados, por si ou por meio de associações constituídas para esse fim, a chamada autorregulação (artigo 50). Considerando a já existente regulação estatal por meio da

¹¹³ A Caminho da Era Digital no Brasil. *OECD-ilibrary*. Disponível em: <https://www.oecd-ilibrary.org/docserver/45a84b29-pt.pdf?expires=1607261489&id=id&acname=guest&checksum=777E12D39468C4466F5844ACCADE5975>. Acesso em: 05 dez. 2020.

ANPD, a paralela autorregulação da atividade de tratamento de dados pelos próprios agentes constitui a chamada correção¹¹⁴.

Floriano de Azevedo Marques Neto registra que a regulação exercida pelo Estado pode se dar em relação a serviços públicos (telecomunicações, energia elétrica), bens públicos escassos ou estratégicos (petróleo, recursos hídricos) atividades que envolvam risco sistêmico (setor financeiro e securitário), atividades de interesse geral (saúde suplementar ou vigilância sanitária), ou ainda a regulação que não incide sobre um setor específico, mas de forma transversal em relação as atividades econômicas como um todo à vista da proteção de um interesse específico (sistemas de defesa do consumidor e da concorrência).¹¹⁵

A regulação estatal a ser realizada no sistema de proteção de dados não é setorial por não discriminar um *locus* específico de aplicação, mas ocorre de forma transversal, englobando os mais variados setores da economia com vistas a proteção do valor juridicamente consagrado dos dados pessoais.

A regulação a cargo do mercado previsto na LGDP seria realizada individual e diretamente pelos agentes de tratamentos de dados, ou mesmo por associações, por meio da elaboração de regras de boas práticas e de governança sobre dados pessoais, as quais podem ser reconhecidas pela ANPD (artigo, 50, §3º). Tal hipótese caracterizaria uma espécie de autorregulação induzida, onde a regulação é exercida por setores organizados da sociedade, por incentivo estatal e reconhecimento legal, como uma forma de reduzir a intervenção estatal.¹¹⁶

A previsão da autorregulação no sistema da proteção dos dados pessoais é válida, pois, o objeto regulado é notoriamente complexo, envolve aspectos altamente tecnológicos, mão de obra especializada, sendo considerado atualmente o grande ativo da

¹¹⁴ Luciano Portal Santana a nota que “Um sistema de correção se caracteriza quando a a autorregulação ocorre num segmento em que o Estado não abdica de suas funções normativa e supervisora. A atuação regulatória, privada e pública, neste sistema terá maior eficácia na medida em que a ação privada for complementar à pública e vice-versa” (SANTANNA, Luciano Portal. *Autorregulação supervisionada pelo Estado: desenvolvimento de um sistema de correção para o mercado de corretagem de seguros, resseguros, capitalização e previdência complementar aberta*. Revista de Direito Administrativo, Rio de Janeiro, v. 257, p. 183-211, mai. 2011. ISSN 2238-5177. Disponível em: <<http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/8591/7327>>. Acesso em: 26 abr. 2020.)

¹¹⁵ NETO, Floriano de Azevedo Marques. *Regulação Econômica e suas modulações*. Revista de Direito Público da Economia, Belo Horizonte, ano 7, n. 28, out./dez. 2009, p. 27-42.

¹¹⁶ Floriano de Azevedo Marques Neto realiza a seguinte distinção acerca da autorregulação: (1) autorregulação delegada, mediante a transferência legal de competência regulatória para os particulares (ex.: OAB); (2) autorregulação induzida que ocorre quando o poder público incentiva e a lei reconhece a regulação pelo particular (institutos de certificação de processos e produtos); (3) autorregulação espontânea verificada no setor privado sem qualquer atuação estatal (ex. autorregulação profissional sem previsão legal). (Idem)

denominada economia da informação, onde a ciência aplicável a organização desses dados viabilizou a sistematização dos hábitos de consumo dos cidadãos, por meio de algoritmos capazes de automatizar tendências pessoais, o que proporcionou aos atores do mercado a possibilidade de se empreender de forma estratégica. Dessa forma, a regulação a ser exercidos pelos próprios agentes de tratamento pode ser assertiva, na medida em que eles detêm o controle acerca das informações técnicas relacionadas ao tratamento de dados pessoais.

Nos setores onde ocorre a correção, convivendo a regulação estatal e a autorregulação, pode-se estabelecer arranjos por meio de parcerias para a utilização de mecanismos da regulação econômica por parte da regulação estatal, a exemplo de estudos, pareceres, estrutura e tecnologia do sistema integrante da autorregulação, o que nos parece salutar diante da complexidade do objeto regulado, minimizando de alguma forma a assimetria de informações do regulador estatal¹¹⁷.

Tramita no Senado Federal o Projeto de Lei nº 6212, de 2019, de Relatoria do Senador Antonio Anastasia, atualmente na Comissão de Constituição, Justiça e Cidadania, que visa alterar a LGPD com a finalidade de “suplantar os problemas e insuficiências da autorregulação pura, tais como o déficit de legitimidade democrática, a baixa coibição de externalidades negativas e, especialmente, a baixa coercitividade”.¹¹⁸

Segundo o Projeto de Lei nº 6212, de 2019, uma norma de autorregulação deve ser submetida à homologação da ANPD para tornar vinculante o ato normativo ao agente que o produziu, ou no caso de associação, aos seus associados, o que excluiria a aplicação de sanções agente de tratamento de dados que demonstrar ter cumprido o normativo aprovado pelo regulador estatal. Nos termos do Projeto, a ANPD poderia aprovar o regramento, rejeitá-lo ou sugerir modificações.

O mencionado Projeto de Lei prevê o estabelecimento de requisitos à criação de atos normativos pelo regulador econômico, tais como, a avaliação de impacto regulatório e a realização de consulta pública, com vistas a “assegurar que elas sejam fruto de uma deliberação *bottom-to-up*, isto é, de baixo (do setor regulado) para cima (ANPD).”¹¹⁹

¹¹⁷ NETO, Floriano de Azevedo Marques. Regulação Econômica e suas modulações. Revista de Direito Público da Economia, Belo Horizonte, ano 7, n. 28, out./dez. 2009, p. 27-42.

¹¹⁸ BRASIL. PL nº 6212/2019. Disponível em: < <https://www25.senado.leg.br/web/atividade/materias/-/materia/139980>>. Acesso em: 25 abr. 2020.

¹¹⁹ PEREIRA, Flávio Henrique Unes; CRUVINEL, Renan. A correção na Lei Geral de Proteção de Dados. *O Estado de São Paulo*, São Paulo, 03 dez. 2019. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/a-corregulacao-na-lei-geral-de-protecao-o-de-dados/>. Acesso em: 25 abr. 2020.

A autorregulação no sistema de proteção de dados pessoais é um modelo adequado, posto que o setor regulado detém a expertise acerca das práticas e tecnologias relacionados ao tratamento de dados pessoais, minimizando assim uma assimetria de informações por parte do regulador estatal, bem como um déficit de autossuficiência administrativa, financeira e de pessoal altamente especializado na estrutura da ANPD, imposto pelo desenho institucional que lhe foi atribuído *a priori* pela LGPD.

2.4.2. Regulação estatal e o paradigma do Banco Central do Brasil

A regulação estatal no sistema de proteção de dados não é setorial por não atuar sobre um determinado setor econômico, mas ocorre de forma transversal abrangendo variados domínios que realizam o tratamento de dados, a exemplo áreas de saúde, telecomunicações, indústria, entre outros.

Um ponto importante acerca da regulação a ser realizada pela ANPD diz respeito ao fato de que ela não se exaure nos setores econômicos, mas aplica-se inclusive aos diversos Entes Estatais e suas Entidades no exercício de tratamento de dados.¹²⁰

A LGPD prevê exceções a sua aplicação aos Entes Estatais, notadamente o tratamento de dados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, o qual será objeto de legislação específica e observadas as restrições acerca da impossibilidade de tratamento de tais dados por pessoas jurídicas de direito privado (artigo 4º). No entanto, a par das exceções mencionadas, a regra é a submissão da atividade de tratamento de dados pessoais por parte da Administração Pública a LGPD.

O tratamento de dados pessoais pelo Poder Público deverá observar o atendimento da sua finalidade pública, notadamente a execução de políticas públicas e as competências legais, devendo ser respeitados os princípios previstos na LGPD (art. 23 a 30).

O descumprimento por parte da Poder Público das regras de proteção de dados previstos na LGPD pode determinar a intervenção da ANPD para fazer cessar a infração (art. 31), bem como as seguintes sanções a ser aplicada pelo regulador: (i) advertência; (ii) publicização da infração; (iii) bloqueio dos dados pessoais a que se refere a infração até a sua regularização; (iv) eliminação dos dados pessoais a que se refere a infração; (v) suspensão parcial e temporária do funcionamento do banco de dados a que se refere a

¹²⁰ Lei nº 13.709/2018: Art. 1º. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

infração (vi) suspensão temporária do exercício da atividade de tratamento dos dados pessoais; (vii) proibição parcial ou total do exercício de tratamento de dados (art. 31 e 52).

O fato da Administração Pública estar sujeita a aplicação da LGPD e a regulação levada a efeito pela ANPD, reforça a necessidade de lhe atribuir um desenho institucional que lhe assegure a autonomia formal, de forma a assegurar uma atuação autônoma em relação ao ente político sujeito a fiscalização.

Nesse sentido, cabe trazer a título de comparação o Banco Central do Brasil que, na qualidade de primeiro órgão brasileiro de regulação setorial, criado pela Lei Federal nº 4.595, de 31 de dezembro de 1964, promove a regulação das instituições financeiras públicas e privadas (artigo 10, IX).¹²¹

O Banco Central do Brasil é uma autarquia federal cuja diretoria composta por cinco membros, sendo seu presidente escolhido pelo Conselho Monetário Nacional dentre os seus integrantes (art. 14 da Lei Federal nº 4.595/1964). Integram o Conselho Monetário Nacional o: (i) Ministro da Fazenda, na qualidade de Presidente; (ii) Presidente do Banco Central do Brasil; (iii) Presidente do BNDES; (iv) outros sete membros nomeados pelo Presidente da República que exercerão mandato de sete anos, com a possibilidade de exoneração desde que justificada por motivos relevantes (art. 6º da Lei Federal nº 4.595/1964).

O modelo institucional atribuído ao Banco Central do Brasil favorece à intervenção política, na medida em que seus dirigentes são escolhidos pelos integrantes de um órgão diretamente vinculados a Administração Central. Nesse sentido, de rigor a observação de Conrado Hubner Mendes:

Verifica-se do conteúdo da Lei 4.595, citada, que o Banco Central, em praticamente toda sua esfera de ação, é claramente subordinado às decisões do Conselho Monetário Nacional, o que acaba suprimindo qualquer desejo de considerar essa autarquia como uma autoridade independente do corpo político central. Na verdade, o Banco Central não parece ser mais nada do que uma ramificação especializada do Ministério da Fazenda, mas que está inteiramente condicionada por políticas econômicas decididas pelo Conselho Monetário Nacional. Podemos citar, a título de fundamentação, diversos artigos

¹²¹ NETO, Floriano de Azevedo Marques. *Agências Reguladoras. Instrumentos do fortalecimento do Estado. Associação Brasileira de Agências de Regulação*, 20 jan. 2019. Disponível em: <http://abar.org.br/mdocs-posts/agencias-reguladoras-instrumentos-do-fortalecimento-do-estado/>. Acesso em: 02 abr. 2020.

legais, onde estão claras as restrições que este ente sofre no exercício de suas competências: art. 9º, art. 11, V e VIII, e art. 13, entre outros.¹²²

Um exemplo notório da fragilidade da regulação exercida pelo Banco Central, em função do seu *déficit* de autonomia, é verificado no notório caso das “pedaladas fiscais” que levou ao *impeachment* da Presidente Dilma Roussef em 2016 e que permitiu que a dívida não contabilizada do governo junto a bancos públicos relativos a programas sociais fosse diferida no tempo, numa manobra que envolveu os três maiores bancos públicos do país: Banco do Brasil, BNDES e Caixa Econômica Federal.

O Tribunal de Contas da União decidiu na ocasião que as dívidas postergadas junto ao Banco do Brasil, à Caixa Econômica Federal, ao BNDES e ao FGTS fossem registradas pelo Banco Central do Brasil na Dívida Líquida do Setor Público (DLSP) “a qual é calculada mensalmente pelo Banco Central e serve de base à apuração dos resultados primário e nominal, para fins de avaliação do cumprimento das metas fiscais estabelecidas na lei de diretrizes orçamentárias (art. 4º, § 1º, da LC 101/2000).”¹²³

Deve ser ressaltado, ainda, que pagamento das chamadas pedaladas fiscais foi realizado pelo Governo Federal no final de 2015, com recursos do Banco Central do Brasil decorrentes de valorização cambial de ativos de reservas cambiais, ganho escritural que desde 2008 em virtude da MP nº 435/2008 convertida na Lei nº 11.803/2008 é alocado como recursos na conta única do Tesouro junto ao Banco Central. No final do ano de 2015, o Ministério do Planejamento incorporou R\$ 103 bilhões do BC em um expediente que permitiu o pagamento das pedaladas fiscais no montante de R\$ 72,4 bilhões.¹²⁴

A situação levada a efeito pelas pedaladas fiscais revelam: (i) a fragilidade da fiscalização do BCB em relação aos bancos públicos na sua relação com o Tesouro; e (ii) as falhas da relação entre o BCB e o governo, notadamente no que respeita a forma de

¹²² MENDES, Conrado Hubner. Reforma do Estado e Agências Reguladoras: Estabelecendo os Parâmetros de Discussão. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000, p. 127-128.

¹²³ BRASIL. Tribunal de Contas da União. Acórdão n. 825/2015. Processo 021.643/2014-8. Rel. Ministro José Múcio Monteiro, Plenário, sessão 15 abr. 2015, ata n. 13/2015.

¹²⁴ OLIVEIRA, Gisele; SALOMÃO, Alexa. Como o governo usou o BC para pagar as pedaladas. *O Estado de S. Paulo*, São Paulo, 06 fev. 2016. Disponível em: <https://www.estadao.com.br/infograficos/economia,como-o-governo-usou-o-bc-para-pagar-as-pedaladas,541349>. Acesso em: 01 maio 2020.

distribuição de lucros pelo Banco Central do Brasil, o que é atribuído ao seu desenho jurídico de baixa autonomia a viabilizar a intervenção política pelo poder central.¹²⁵

Diversos são os Projetos de Lei que tramitam no Congresso Nacional e objetivam atribuir autonomia ao Banco Central, como o PL 80, de 2017, de Relatoria do Senador Airton Sandoval que objetivou o tratamento regulatório equivalente entre bancos públicos e privados, arquivado em virtude do final da legislatura, bem como o PL 19, de 2019, de Relatoria do Senador Plínio Valério e o PLP 200, de 1989, de autoria do então Deputado Itamar Franco, em tramitação, os quais visam impor requisitos para acesso e atribuir estabilidade ao exercício do cargo de Presidente e Diretor do Banco Central do Brasil.

O que se pretende demonstrar nessa parte do estudo é que quando se trata de atuação regulatória estatal, onde o Estado exerce tanto o papel de regulador como de regulado, como é o caso do Banco Central e os bancos públicos, a autonomia institucional atribuída ao regulador tem papel fundamental no sucesso de uma regulação autônoma, evitando uma pernicioso captura regulatória pela intervenção política verificada nas mais variadas formas e viabilizada pela ausência de autonomia administrativa, técnica, financeira ou de pessoal.

2.4.3. Do déficit de autonomia institucional da ANPD

A Lei nº 13.853/2019 não atribuiu a Autoridade Nacional de Proteção de Dados Pessoais um desenho institucional que viabilize sua autonomia formal, institucional, em uma análise comparativa em relação as Agências Regulatórias Federais.

Com base nos indicadores utilizados por Batista apresentados anteriormente e que levaram em conta o modelo proposto por Alexandre Gueventher, são apresentadas as variáveis acerca do grau de autonomia formal da ANPD (Tabela 1: índice de Autonomia Formal).¹²⁶

Tabela 3: Autonomia formal da ANPD

Agência	Mandato	Indicação	Demissão	Recondução	Experiência
---------	---------	-----------	----------	------------	-------------

¹²⁵ DURAN, Camila Villard. Fragilidades jurídicas na relação BC – bancos públicos. *Jota*, 10 maio 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/fragilidades-juridicas-na-relacao-bc-bancos-publicos-10052017>. Acesso em: 01 maio 2020.

¹²⁶ SILVA, Mariana Batista da. *Independência após a delegação? Uma análise exploratória da interferência política nas Agências Regulatórias Brasileiras*. 2010. Dissertação (Mestrado em Ciência Política). Universidade Federal de Pernambuco, Recife, 2010. p. 53.

ANPD	0,5	1	1	0	1
------	-----	---	---	---	---

Fonte: elaboração própria

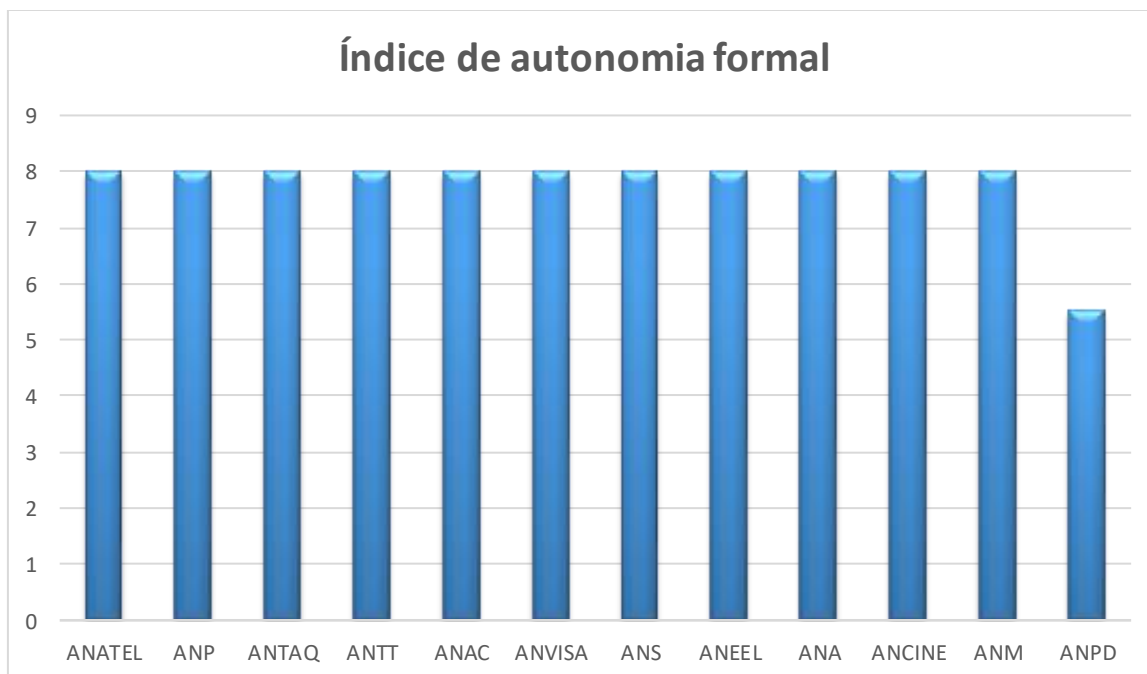
Agência	Autorização	Revisão	Recursos	Pessoal	Procedimentos
ANPD	1	1	0	0	0

Fonte: elaboração própria

Com relação aos 10 indicadores utilizados pela pesquisadora, cumpre observar que: (i) os **mandatos** são fixos, nada obstante pelo período de quatro anos; (ii) a **indicação** dos diretores é compartilhada com o Senado Federal; (iii) a **demissão** só é possível mediante decisão judicial ou processo administrativo disciplinar; (iv) a **recondução** dos diretores não é proibida; (v) é exigida **experiência** dos representantes na área da regulação; (vi) não é necessária **autorização** do poder central para tomada de decisões; (vii) as decisões são passíveis de **revisão** pelo poder judiciário; (viii) os **recursos** orçamentários não são definidos pela ANPD; (ix) a entidade não tem autonomia sobre sua política de **pessoal**; e (x) há possibilidade de modificação de **procedimentos** do regulador pelo Executivo por meio de Medidas Provisórias.

Tais informações são consolidadas no gráfico abaixo que consolida as informações acerca do grau de autonomia formal das Agências Reguladoras Federais, atualizado com a Lei nº 13.848/2019 que promoveu uma alteração linear e qualitativa na autonomia institucional das Agências, com base nos indicadores utilizados por Batista apresentados anteriormente e que levaram em conta o modelo proposto por Alexandre Gueventher, com a inclusão da ANPD¹²⁷.

¹²⁷ SILVA, Mariana Batista da. *Independência após a delegação? Uma análise exploratória da interferência política nas Agências Regulatórias Brasileiras*. 2010. Dissertação (Mestrado em Ciência Política). Universidade Federal de Pernambuco, Recife, 2010. p. 53.



Fonte: elaboração própria

Pela consolidação dos indicadores aplicados por Batista, verifica-se que a ANPD apresenta um desenho institucional levado a efeito pela LGPD que propicia uma reduzida autonomia formal frente ao modelo institucional das Agências Reguladoras Federais, nada obstante se tratar de um formato transitório que pode ser alterado (art. 55 da LGPD), e é desejável que o seja, para lhe atribuir uma roupagem de regime autárquico especial que lhe propicie maior autonomia em relação ao poder central.

2.4.4. Autonomia administrativa

O artigo 55-G da LGPD prevê que cabe ao Presidente da República dispor sobre a estrutura regimental da ANPD, com sua disponibilização administrativa e de pessoal, o que foi efetivado por ocasião da edição do Decreto nº 10.474, de 26 de agosto de 2020, o qual aprovou a estrutura regimental do órgão, bem como seu quadro de cargos em comissão e funções de confiança.

2.4.5. Da natureza de órgão público como um risco à autonomia da ANPD. Caso do “dossiê antifascista”

O contexto de austeridade fiscal em que editada a MP nº 869/2018 convertida na Lei nº 13.853/2019 determinou a criação “sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República”.

A criação de uma autoridade regulatória, com vistas a atuar de forma autônoma, mas com a qualificação de órgão vinculado a Presidência da República revela uma contradição, posto que os órgãos públicos consistem em unidades abstratas que sintetizam atribuições estatais, verdadeiras repartições internas sem personalidade jurídica, vinculados entre si pelo “*liame unificador da hierarquia*” a uma autoridade superior.¹²⁸

A definição da ANPD como órgão público integrante da Presidência da República é uma qualificação que, *prima facie*, não condiz com a autonomia funcional, administrativa e decisória que a Lei nº 13.848/2019 recentemente atribuiu às Agências Reguladoras como condição do exercício de sua autonomia decorrente de sua natureza especial.

Com relação a competência decisória da ANPD, nada obstante delimitação do espaço de atuação do regulador levada a efeito no artigo 55-J, de forma a afastar uma sobreposição de competências dentro da pessoa jurídica que esta última integra na qualidade do órgão, seria adequado que a lei contivesse previsão expressa no sentido de reconhecer a ANPD como última instância administrativa, de forma a assegurar sua autonomia decisória prevista no artigo 55-B.

Cabe ressaltar que a previsão legal acima mencionada encerraria eventual controvérsia acerca da possibilidade de manejar recurso hierárquico contra decisões da ANPD, dada sua natureza jurídica de órgão integrante da Administração Central, evitando em mesma medida a interferência política comprometedora de sua autonomia. Nesse sentido, de rigor a menção do entendimento de José Roberto Pimenta Oliveira:

Por outro lado, não há expressa dicção legal declarando a Agência como última instância administrativa decisória no setor, na Lei 9.427, de 1996, competindo-lhe apenas “dirimir, no âmbito administrativo, as divergências entre concessionárias, permissionárias, autorizadas, produtores independentes e autoprodutores, bem como esses agentes e seus consumidores”. A ANEEL, através da Resolução 233, de 14.7.1998, considerou que “a instância máxima de recurso, nas matérias submetidas à alçada da Agência, será a Diretoria” (art. 45).

¹²⁸ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 144-155.

Desse modo, em termos de interferência política no Poder Executivo, na direção da autarquia, dado o pioneirismo do modelo, a independência restou comprometida.¹²⁹

A configuração jurídica de órgão integrante da Administração Centralizada atribuída a ANPD pela LGPD, atrai questionamentos acerca do déficit de autonomia daquela instituição, cujas repercussões são dimensionadas sob dois aspectos: (i) as exigências de outros países, como os Estados-Membros da União Europeia acerca da necessidade de um regulador autônomo, como condição a transferência de dados pessoais entre as nações; e (ii) a garantia da proteção dos direitos individuais frente a atuação do Poder Público, na medida em que assume ambos os papéis de regulador e regulado. Sobre essa questão:

Aliás, a vinculação à Presidência da República, por si só problemática, carrega em si dificuldades específicas: pode não haver suficiente autonomia e independência institucional exigidas de outros países de modo a assegurar a cooperação jurídica internacional para a transferência de dados pessoais entre nações. Pode ser o caso, em especial, para os Estados-Membros da União Europeia sob a disciplina da GDPR. Outra crítica com a qual alinhamos, diretamente relacionada à primeira, diz respeito à inescapável redução da capacidade de regulação e fiscalização, por parte da ANPD, do tratamento de dados pessoais pelo Poder Público. Se o ente perdeu importante parcela de autonomia e independência, em especial dada a inexistência de mecanismos mínimos estabelecidos internacionalmente, como garantir que haverá proteção de direitos individuais frente a atuação do Poder Público?¹³⁰

Algumas posturas adotadas na elaboração das normas aplicáveis a ANPD sugerem que a atribuição de uma reduzida autonomia a ANPD não é casual, tendo em vista que a MP nº 869/2018 que criou a ANPD e a constituiu como órgão integrante da Presidência da República, procedeu ao mesmo tempo revogação dos parágrafos primeiro e segundo do artigo 7º da LGPD, a qual determinava que “o titular de dados deveria ser informado pelo Poder Público acerca das hipóteses em que seria admitido o tratamento de seus dados” e que a ANPD deveria regulamentar a forma de disponibilização destes dados, posto que tal medida reduziu de uma só vez e de forma injustificável a transparência do

¹²⁹ OLIVEIRA, José Roberto Pimenta. Reforma do Estado e Direito Concorrencial. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000. p. 343.

¹³⁰ VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 732.

uso de dados pela Administração e o controle regulatório a ser exercido pela ANPD em relação ao tratamento de dados realizados pelo Estado.¹³¹

No atual contexto político, a circunstância da ANPD ter sido configurada como órgão vinculado ao Chefe do Executivo Federal exacerba ainda mais os questionamentos acerca da sua autonomia, tendo em vista acontecimentos recentes, a exemplo do chamado “dossiê antifascista” criado no âmbito do Ministério da Justiça e Segurança Público e que consolidou dados pessoais de adversários políticos. O Supremo Tribunal Federal, por ocasião da análise do pedido de liminar deduzido na ADPF 722, determinou a suspensão de qualquer ato com objetivo de coletar e compartilhar informações de cidadãos, sob o entendimento de se tratar de uso abusivo da máquina estatal, realizado em desvio de finalidade.¹³²

A questão que se coloca, a partir de um fato verificado no chamado “dossiê antifascista”, elaborado por um órgão vinculado ao Presidente da República é: teria a ANPD, a qual possui a natureza de órgão vinculado à Presidência da República, a necessária autonomia para fiscalizar atos praticados pelos demais órgãos e entidades também vinculados a mesma autoridade ?

Por fim, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), cujo ingresso é uma das prioridades do atual governo, apresentou o relatório “A Caminho da Era Digital no Brasil”, onde pontuou aspectos sensíveis relacionadas ao desenho institucional da ANPD e expediu recomendações visando assegurar sua autonomia, especialmente reavaliar sua estruturação como órgão vinculado à Presidência da República, considerando o déficit de autonomia que decorre dessa vinculação.¹³³

A natureza provisória atribuída a ANPD de “órgão da administração pública federal, integrante da Presidência da República”, suscita questionamentos acerca da autonomia administrativa, funcional e decisória da ANPD dado os reflexos jurídicos decorrentes desta qualificação jurídica, necessariamente subordinada a uma autoridade

¹³¹ VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 732.

¹³² Ministra Camem Lúcia vota para proibir Ministério da Justiça de elaborar dossiê contra antifascistas. Supremo Tribunal Federal, 19 ago. 2020. Disponível em: <http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449906&ori=1>. Acesso em: 10 set. 2020.

¹³³ A Caminho da Era Digital no Brasil. *OECD-ilibrary*. Disponível em: <https://www.oecd-ilibrary.org/docserver/45a84b29-pt.pdf?expires=1607261489&id=id&acname=guest&checksum=777E12D39468C4466F5844ACCADE5975>. Acesso em: 05 dez. 2020.

superior pelo vínculo da hierarquia, cujos reflexos ainda não se sabe porquanto a entidade não foi constituída pelo Poder Executivo, no entanto, há o receio da organização administrativa atribuída a ANPD prejudicar sua autonomia, inviabilizando o reconhecimento internacional e, em mesma medida, se revelar insuficiente para a proteção de direitos individuais na fiscalização da política de tratamento de dados pelo Poder Público.

2.4.6. Da política de pessoal

A política de pessoal, assim como a dotação orçamentária e o arranjo administrativo da ANPD, será regulado por ato do Presidente da República, conforme o disposto no artigo 55-G da LGPD.

No atual contexto de crise fiscal, há uma tendência de que a ANPD seja equipada com uma estrutura enxuta, sendo que especialistas avaliam que a instituição irá contar com cerca de 10% do efetivo da ANATEL (aproximadamente 400 funcionários), o que seria algo em torno de 40 funcionários, bem como uma estrutura predominante digital com o fim de redução de encargos administrativos. Mencionado Decreto ainda está em fase de estudos, no entanto, membros do Senado Federal protocolaram junto ao Presidente da República o Requerimento 123, 2020, visando a realização de debates temáticos para subsidiar a edição do mencionado Decreto Presidencial.¹³⁴¹³⁵

O Decreto que vier a ser editado deverá estruturar a ANPD com pessoal permanente, suficiente, e tecnicamente capacitado para o exercício de sua finalidade institucional, considerando a complexidade técnica que a atividade requer, o que necessariamente vai envolver um esforço remuneratório para tornar o cargo atraente sob o ponto de vista do mercado. A título comparativo, verifica-se que o Decreto nº 13.709, de 14 de agosto de 2020, o qual aprovou a estrutura dos cargos em comissão do órgão, previu a remuneração de um cargo DAS de nível 5 para os Diretores do Conselho Diretor da ANPD, o que equivale atualmente a R\$ 13.623,39, valor que seria um limite remuneratório que poderia tornar o cargo pouco atrativo para especialistas do mercado

¹³⁴ GUTIERREZ, Andrei. Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Org.). *Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 403.

¹³⁵ BRASIL. Requerimento nº 123, 2020. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=8073590&ts=1585142422472&disposition=inline>>. Acesso em: 01 maio 2020.

nessa área de atuação, bem como para servidores com maior experiência e conhecimento técnico aceitarem o encargo de diretores da Agência.¹³⁶

Cabe ressaltar que a LGPD não trata da política de pessoal da ANPD, conferindo tal atribuição ao Presidente da República por meio da edição de ato competente (artigo 55-G da LGPD), sendo salutar que o chefe do Poder Executivo, no exercício de sua competência de organizar os órgãos da Administração Federal prevista na Constituição Federal (artigo 84, IV, a, da CF), delegasse expressamente aos diretores da ANPD a atribuição de gerir os recursos humanos a cargo da instituição, reforçando assim sua autonomia administrativa.

2.4.7. Autonomia financeira

Com relação as receitas da ANPD, a lei de proteção de dados previu seu financiamento por meio de: (1) dotações orçamentárias; (2) doações, legados, subvenções; (3) do resultado de aplicações de receitas no mercado financeiro; (3) negócios jurídicos celebrados com entidade públicas e privadas, nacionais e internacionais; (4) o produto da venda de materiais de caráter técnico elaborado pelo órgão.

Cabe ressaltar o veto ao dispositivo da **Lei nº 13.853, de 8 de julho de 2019** que possibilitava a instituição da possibilidade de cobrança de emolumento por serviços prestado (art. 55-L, V), ou seja, de taxa pelo exercício de poder de polícia.

De acordo com a mensagem de veto, a natureza transitória de órgão da Administração Direta da ANPD não possibilitaria a cobrança de emolumentos pelos serviços prestados para fins de composição de sua receita, a qual deveria ser arcada com recursos orçamentários da União.¹³⁷

A dependência financeira da ANPD em relação ao orçamento da União é um fator que prejudica sua autonomia, tendo em vista o histórico de contingenciamento de recursos das Agências Reguladoras com o formato de autarquias, o que pode restringir a sua atuação em um cenário de crise fiscal.

¹³⁶ GUTIERREZ, Andrei. Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Org.). *Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 403.

¹³⁷ BRASIL. Mensagem nº 288, de 8 de julho de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Msg/VEP/VEP-288.htm>. Acesso em: 08 maio 2020.

As agências reguladoras inicialmente dotadas com recursos da União, foram paulatinamente consagradas com orçamentos próprios, oriundos do recolhimento de taxas decorrentes do exercício da atividade regulatória, devidamente prevista nas respectivas leis de criação.

AGÊNCIAS REGULADORAS	PREVISÃO LEGAL - TAXAS
Agência Nacional de Águas	arts. 20 e 21 da Lei nº 9.984/2000
Agência Nacional de Aviação Civil	art. 31 da Lei nº 11.182/2005
Agência Nacional de Telecomunicações	art. 47 usque 50 da Lei nº 9.472/1997
Agência Nacional do Cinema	art. 11 da Medida Provisória nº 2.228/2001
Agência Nacional de Energia Elétrica	arts. 11 usque 13 da Lei nº 9.427/1996
Agência Nacional de Petróleo	arts. 15, 16 e 45 da Lei nº 9.478/1997
Agência Nacional de Saúde	arts. 17 usque 23 da Lei nº 9.961/2000
Agência Nacional de Transportes Aquaviários	arts. 77 e 78 da Lei nº 10.233/2001
Agência Nacional de Transportes Terrestres	arts. 77 e 78 da Lei nº 10.233/2001
Agência Nacional de Vigilância Sanitária	arts. 22 usque 26 da Lei nº 9.782/1999
Agência Nacional de Mineração	art. 19 da Lei nº 13.575/2017

Fonte: elaboração própria

O Tribunal de Contas da União no Acórdão nº 245/2015 proferido por ocasião da auditoria com o objetivo de avaliar a governança da regulação nos setores de energia, comunicações e transportes, partindo de uma orientação da OCDE no sentido de que os recursos das Agências Reguladoras devem ser estáveis e transparentes para proteger sua autonomia, realizou um diagnóstico das Agências Federais e concluiu que o contingenciamento orçamentário é praxe, não existe autossuficiência orçamentária e quando há os recursos são retidos pelo Executivo para alavancagem de superávit primário, razão pela expediu recomendações a Casa Civil para que envidasse esforços para dotar as Agências de real autonomia financeira.¹³⁸

O fato da LGPD ter competência sancionatória para aplicação de multa (art. 52, I e II) gerou no curso do processo legislativo o receio do setor privado de que tal atribuição estimulasse uma espécie de desvio de finalidade na sua aplicação, caso os recursos

¹³⁸ BRASIL. Tribunal de Contas da União. Acórdão n. 240/2015. Processo 031.996/2013-2. Rel. Ministro Raimundo Carreiro, Segunda Câmara, sessão 11 fev. 2015, ata n. 5/2015.

decorrentes da sanção constituíssem receita da entidade que então se tornaria interessada no proveito econômico decorrente, de tal forma que a LGPD, na redação conferida pela Lei nº 13.853/2019, previu que as receitas da arrecadação de multas não serão destinadas a ANPD mas ao Fundo de Defesa de Direitos Difusos (§ 5º do artigo 52).¹³⁹

No entanto, a possibilidade da cobrança de taxa pelo exercício do poder de polícia que decorre da atividade regulatória da ANPD, seria uma iniciativa adequada a viabilizar sua autonomia financeira, assim como ocorre com as Agência Federais e em relação a outras autoridades nacionais de proteção de dados, como por exemplo a Information Commissioner Office – ICO, especialmente no atual contexto de crise com o comprometimento dos recursos orçamentários do tesouro, tendo em vista que além de pessoal extremamente qualificado, a ANPD vai exigir alto investimento em tecnologia e sua renovação periódica para garantir a eficiência do órgão.¹⁴⁰

Cabe ressaltar, finalmente, que o relatório “A Caminho da Era Digital no Brasil” apresentado às autoridades federais pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), ao pontuar aspectos sensíveis relacionadas ao desenho institucional da ANPD e expedir recomendações visando assegurar sua autonomia, ressaltou a necessidade de garantir um orçamento adequado e previsível à ANPD.¹⁴¹

2.5. Conclusão

A Lei Geral de Proteção de Dados atribuiu a Autoridade Nacional de Proteção de Dados Pessoais um modelo institucional que prejudica a sua autonomia formal, na medida em que sua configuração transitória de órgão integrante da Presidência da República suscita questionamentos acerca da autonomia administrativa, funcional e decisória para atuar como regulador frente aos desafios impostos pela sua regra de competência, dado os reflexos jurídicos decorrentes desta qualificação jurídica, necessariamente subordinada a

¹³⁹ LUCCA, Newton de; LIMA, Cintia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e Privacidade. In: LIMA, Cintia Rosa Pereira de (Coordenação). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020, p. 389.

¹⁴⁰ Idem, p. 390-394.

¹⁴¹ A Caminho da Era Digital no Brasil. *OECD-ilibrary*. Disponível em: <https://www.oecd-ilibrary.org/docserver/45a84b29-pt.pdf?expires=1607261489&id=id&accname=guest&checksum=777E12D39468C4466F5844ACCADE5975>. Acesso em: 05 dez. 2020.

uma autoridade superior pelo vínculo da hierarquia, bem como considerando uma evidente subordinação financeira ao poder central pela inexistência de mecanismos que viabilize sua autossuficiência.

A necessidade de atribuir um modelo institucional que favoreça a autonomia da Autoridade Nacional de Proteção de Dados é questão premente, não só para sua efetiva atuação regulatória, de forma a assegurar a preservação dos direitos da personalidade no tratamento de dados pessoais previsto no artigo 2º da Lei nº 13.709/2018, como também um requisito para a reciprocidade no recebimento de dados de cidadãos europeus em função da condicionante prevista Regulamento Geral de Proteção de Dados Pessoais Europeu nº 679/2016 (GPDR), bem como para o ingresso do Brasil em organizações internacionais, a exemplo da OCDE, de tal maneira que não basta existir uma lei sobre o tema da proteção de dados, mas deve ser estabelecidos mecanismos para viabilizar a atuação eficiente e autônoma da ANPD.

3. Hipóteses de não aplicação da LGPD em relação à Administração Pública

O artigo 3º da LGPD determina sua aplicação tanto aos atores do mercado quanto ao Poder Público, nas situações previstas nos seus incisos I a III, no entanto, a própria lei exclui sua incidência nas hipóteses enumeradas no seu artigo 4º:¹⁴²

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Verifica-se que as exceções à aplicação da LGPD previstas no artigo 4º, privilegiam hipóteses em que o tratamento de dados é realizado sob o fundamento de um relevante direito fundamental (no caso da atividade jornalística, por exemplo, a liberdade da informação), ou um interesse público relevante, evidenciado nas exceções à incidência da lei referentes ao tratamento de dados para o fim de segurança pública, defesa nacional, segurança do Estado ou no exercício de atividades de investigação e repressão de infrações penais.¹⁴³

A LGPD não confere uma prerrogativa ilimitada para o Poder Público realizar o tratamento de dados, nas hipóteses em que incidente o interesse público a excepcionar a aplicação da lei, na medida em que o artigo 4º, §1º da LGPD prevê que a operação de tratamento nestas hipótese deve respeitar a legislação específica aplicável, bem como os

¹⁴² “Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:”

¹⁴³ MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor. São Paulo: Ed. Revista dos Tribunais, nov.-dez. 2018, vol. 120, p. 469-483.

princípios da proteção de dados e os direitos do seu titular previstos na lei de proteção de dados.

Neste capítulo do estudo, cujo fio condutor é a proteção dos dados pessoais no âmbito da Administração Pública, serão analisadas as exceções à aplicação da LGPD à Administração Pública, quando incidente interesse público relevante, excluídas as demais hipóteses de tratamento de dados previstas na lei (por pessoa natural para fins não econômicos, atividade jornalística, artística e acadêmica).

3.1. Interesse público x interesse privado: a compatibilização de direitos na LGPD

As exceções à aplicação da LGPD previstas no artigo 4º, III da LGPD, notadamente o tratamento de dados realizado pelo Poder Público para o fim de segurança pública, defesa nacional, segurança do estado ou no exercício de atividades de investigação e repressão de infrações penais, é efetivado no exercício de denominado poder de polícia que, segundo Celso Antônio Bandeira de Mello, constitui manifestação da “atividade estatal de condicionar a liberdade e a propriedade ajustando-as aos interesse coletivos”.¹⁴⁴ Nessa ordem, o “fundamento do poder de polícia é princípio da supremacia do interesse público sobre o particular, que dá à Administração posição de supremacia sobre os administrados”.¹⁴⁵

Em relação ao princípio da supremacia do interesse público sobre o particular que, por sua vez, fundamenta as restrições impostas aos particulares com base no chamado poder de polícia, cabe considerar que a par das discussões acerca do mesmo, sua aplicação é reivindicada nas hipóteses em que um interesse da coletividade deva ser amplificado em detrimento de direitos individuais, quando premente um fundamento de ordem constitucional apto a determinar essa relação de superioridade, de forma proporcional e nos limites da lei.

Autores como Daniel Sarmiento rejeitam o princípio da supremacia do interesse público sobre o particular no ordenamento jurídico brasileiro, tendo em vista que na visão do mencionado autor haveria uma superioridade a priori independentemente da situação posta em conflito, com o sacrifício automático do interesse particular, postulado que seria

¹⁴⁴ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 851.

¹⁴⁵ PIETRO, Maria Sylvania Zanella Di. *Direito Administrativo*. 23. ed. São Paulo: Editora Atlas, 2009. p. 115.

incompatível com o princípio da proporcionalidade que obriga o intérprete a harmonizar tanto quanto possível os interesses em conflito.¹⁴⁶

Gustavo Binimbojm, alinhado com o entendimento acima mencionado, considera que o princípio da proporcionalidade impõe um ponto de otimização entre os interesses conflitantes, mediante um processo de construção da opção do intérprete pela ponderação, não possuindo fundamento constitucional uma opção de prevalência do interesse público, por se tratar de conceito indeterminado que deve ser concretizado após juízo de ponderação a luz das circunstâncias concretas.¹⁴⁷

Humberto Ávila, por sua vez, entende não existir uma norma-princípio de supremacia do interesse público sobre o particular no Direito brasileiro, sendo que a única possibilidade que considera possível para compor a relação entre interesses públicos e privados decorre da ponderação entre tais interesses reciprocamente considerados, com fundamento na sistematização das normas constitucionais.¹⁴⁸

Em relação às posições mencionadas acerca da existência e aplicação do princípio da supremacia do interesse público, Maria Sylvia Zanella Di Pietro registra partirem de premissas equivocadas, a saber: (i) atribuem ao princípio uma generalidade inexistente, pois é evidente a impossibilidade dele prevalecer a priori em qualquer situação de conflito, o que representaria uma negação a existência dos direitos individuais; (ii) olvidam de institutos de direito administrativo, a exemplo da desapropriação, a regulação, dentre outros inerentes ao poder de polícia que o próprio ordenamento constitucional atribuir essa posição de superioridade; (iii) o princípio em questão não materializa a negação dos direitos individuais, pois, de acordo com a autora durante o Estado Social, na busca do interesse da coletividade, houve um incremento dos direitos individuais; (iv) representa em verdade uma proteção aos interesses individuais, na medida em que a dignidade humana respalda não só interesses individuais, como também coletivos e, finalmente; (v) ignora o binômio autoridade e liberdade que representa o contomo

¹⁴⁶ SARMENTO, Daniel. Interesses Públicos vs. Interesses Privados na Perspectiva da Teoria e da Filosofia Constitucional. In: SARMENTO, Daniel (Org.). *Interesses Públicos versus Interesses Privados: Desconstruindo o Princípio da Supremacia do Interesse Público*. 2.ed. Rio de Janeiro: Lumen Juris, 2007. p. 100.

¹⁴⁷ BINENBOJM, Gustavo. Da Supremacia do Interesse Público ao Dever de Proporcionalidade: Um Novo Paradigma para o Direito Administrativo. In: SARMENTO, Daniel (Org.). *Interesses Públicos versus Interesses Privados: Desconstruindo o Princípio da Supremacia do Interesse Público*. 2. ed. Rio de Janeiro: Lumen Juris, 2007. p. 164-167.

¹⁴⁸ AVILA, Humberto. Repensando o 'Princípio da Supremacia do Interesse Público sobre o Particular'. In: SARMENTO, Daniel (Org.). *Interesses Públicos versus Interesses Privados: Desconstruindo o Princípio da Supremacia do Interesse Público*. 2. ed. Rio de Janeiro: Lumen Juris, 2007. p. 214.

histórico do direito administrativo, e que se compatibilizam mutuamente para garantia das funções administrativas essenciais e das liberdades individuais¹⁴⁹.

Sobre o tema, Celso Antonio Bandeira de Mello considera ser o princípio da supremacia do interesse público um princípio geral de Direito, pressuposto do convívio social, com aplicações concretas no texto constitucional, a exemplo do instituto da desapropriação, representando a possibilidade do Poder Público constituir restrições a terceiros nos termos da lei, fundado em uma lógica de dever, como o meio indispensável a realização da finalidade determinada pelo exercício da função pública delimitada pela Constituição. Dessa forma, age o Poder Público no exercício do princípio da supremacia do interesse público em nome da coletividade e não da entidade governamental em si (interesse público primário), o qual deve se concretizar “na extensão e na intensidade proporcionais ao que seja irrecusavelmente requerido para o atendimento do escopo legal a que estão vinculados”.¹⁵⁰

Segundo Tércio Sampaio Ferraz Júnior “como se subentende que as relações privadas sejam utilitárias num sentido estrito e as públicas abrangentes e neutras, visando ao bem de todos, dir-se-á que o interesse público prevalece sobre o privado”.¹⁵¹

A LGPD ao excepcionar a aplicação da lei às hipóteses onde presente o poder de polícia no seu sentido amplo, representando a atividade estatal condicionante da liberdade individual, o fez sob fundamento da supremacia da interesse público representado nas atividades afetas a defesa nacional e segurança pública, com assento constitucional nos artigos art. 4º, I, 21, III, e 144 da CF.¹⁵²

É importante registrar que não houve a concretização legislativa a priori de um interesse público de forma excludente, mas a devida compatibilização com os direitos inerentes à privacidade com assento constitucional no artigo 5º, X da CF, pois, a par do artigo 4º, III prever a não aplicação da LGPD no tratamento de dados realizados ao Poder Público para as finalidades mencionadas, limitou essa prerrogativa às regras aplicáveis, ao princípio constitucional do devido processo legal e aos princípios gerais de proteção de dados previstos na LGPD (artigo 4º, §1º), além de ter imposto restrição ao tratamento

¹⁴⁹ PIETRO, Maria Sylvania Zanella Di. *Transformações do Direito Administrativo*. Revista de Direito da Administração Pública, v. 1, n. 2, jun/dez 2016, p. 197.

¹⁵⁰ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 99-102.

¹⁵¹ FERRAZ JÚNIOR, Tércio Sampaio Ferraz. *Introdução ao Estudo do Direito*. São Paulo: Atlas, 1994. p. 137.

¹⁵² MELLO, Celso Antônio Bandeira de, op. cit., p. 851.

por pessoas jurídicas de direito privado (artigo 4º, §§2º e 4º da LGPD) e fixado competência fiscalizatória à Autoridade Nacional de Dados Pessoais (ANDP).

3.2. Da garantia de aplicação da legislação específica e dos princípios da proteção de dados

O artigo 4º, §1º da LGPD prevê que as hipóteses de tratamento de dados pelo Poder Público, onde a lei excepciona sua aplicação (art. 4º, III), “será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.”

Vale ressaltar acerca da necessidade de uma legislação específica para o tratamento de dados realizados pelo Poder Público, no exercício de atividades relacionadas a Defesa Nacional e Segurança Pública, no entanto, não se deve olvidar de diplomas legais existentes que impõem restrições em relação ao tratamento de dados pelo Poder Público, em respeito a transparência e às liberdades individuais, a exemplo do artigo 31 da Lei 12.527/2011 (Lei de Acesso à Informação):

A despeito da importância de uma regulamentação específica, a Lei de Acesso à Informação (LAI) – Lei 12.527/2011 – e o respectivo regulamento, Decreto 7.724/2012, aplicam-se ao tratamento de dados pelo Poder Público quando age nas hipóteses do art. 4º, inciso III da LGPD. Apenas pelo teor do art. 31 da LAI já se estabelece o princípio da transparência e o respeito às liberdades individuais e garantias individuais dos titulares de tratamento, lançando balizas que limitarão eventuais abusos.¹⁵³

A inaplicabilidade da LGPD as matérias previstas no artigo 4º, III não é absoluta, pois, de acordo com seu artigo 4º, §1º, continuam sendo aplicados os princípios da proteção de dados, “sejam eles: finalidade; adequação; necessidade; transparência e não discriminação. O titular de dados também terá como invocar o direito de acesso, a correção, anonimização e eliminação de informações inadequadas”.¹⁵⁴

Dessa forma, a exceção à incidência da LGPD as operações de tratamento de dados pessoais pelo Poder Público, em atividades afetas a Defesa Nacional e Segurança Pública

¹⁵³ MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a proteção de dados não se aplica. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 188.

¹⁵⁴ Idem, p. 187.

(art. 4º, III), não está imune de restrições, pois, o artigo 4º, §1º da LGPD prevê a aplicação nessa hipótese da legislação específica, do princípio constitucional da ampla defesa e dos princípios da proteção de dados pessoais.

3.3. O Poder Público no exercício de tratamento de dados para fins de segurança pública e defesa nacional: há competência sancionatória por parte da ANPD?

O artigo 4º, §3º da LGPD prevê que, nas hipóteses de tratamentos realizado pela Administração Pública, onde é restringida a aplicação da lei (art. 4º, III), a Autoridade Nacional de Proteção de Dados tem o papel de emitir recomendações, opiniões técnicas e solicitar relatórios de impacto a proteção de dados pessoais.¹⁵⁵

A par da competência prevista no artigo 4º, §3º da LGPD, dúvidas poderão surgir acerca da extensão da competência fiscalizatória e sancionatória da ANPD em relação à Administração Pública, quando no exercício das atividades previstas no artigo 4º, III onde é excepcionada, em parte, a aplicação da lei.

Explica-se: o artigo 52 da LGPD prevê que o agente de tratamento de dados fica sujeitos as sanções administrativas aplicáveis pela ANPD, em função de infrações cometidas às “normas” previstas na lei.¹⁵⁶ Por outro lado, como visto, a inaplicabilidade da LGPD em relação ao Poder Público no exercício previstas no artigo 4º, III não é absoluta, pois, de acordo com seu artigo 4º, §1º, continuam sendo aplicados os princípios da proteção de dados. Se considerarmos os princípios da proteção de dados como “normas”, a violação pelo Poder Público de um dado princípio no exercício das atividades previstas no artigo 4º, III arrogará a competência sancionatória da ANPD.

Isso porque os princípios de proteção de dados não deixam de ser normas devidamente positivadas no artigo 6º da LGPD, possuindo conteúdo aberto, as quais “indicam o fundamento a ser utilizado pelo aplicador para futuramente encontrar a regra para o caso concreto”, aplicável de modo gradual, onde o relacionamento entre ambos é solucionável mediante ponderação, de tal forma que o artigo 52 da LGPD ao fazer

¹⁵⁵ § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

¹⁵⁶ Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

referência a competência da ANPD nas situações em que se verificar violação a “normas”, certamente não excluiu da sua aplicação a violação aos princípios da proteção de dados.¹⁵⁷

Sobre a qualificação de princípios como normas jurídicas, Josef Esser (apud Ávila) considera que princípios são normas que estabelecem fundamentos para que determinado mandamento seja encontrado, diferenciando das regras por exercer o princípio a função de fundamento normativo para a tomada de decisão.¹⁵⁸ Na mesma linha, Karl Larenz (apud Ávila) define princípio como normas de grande relevância para o ordenamento jurídico, estabelecendo os fundamentos normativos para a interpretação e aplicação do direito.¹⁵⁹

Para Ronald Dworkin (apud Ávila), os princípios são normas que contém fundamentos que devem ser conjugados com outros fundamentos de outros princípios, de forma que os princípios ao contrário das regras que se aplicam sob a lógica do tudo ou nada, possuiriam uma dimensão de peso, sobrepondo na hipótese de colisão o princípio classificado como de peso maior.¹⁶⁰

Robert Alexy (apud Ávila), por sua vez, precisou a definição de princípios como sendo uma espécie de normas jurídicas, as quais impõem deveres de otimização aplicáveis em vários graus, sendo que ao contrário de Dworkin, Alexy entende que a colisão entre princípios não se resolve com a prevalência imediata sobre outro (dimensão de peso), mas diante da sua aplicação no caso concreto mediante a ponderação e a criação de uma regra de prevalência (teorema da colisão).¹⁶¹

Voltando à questão da aplicação da competência sancionatória da ANPD ao Poder Público, no exercício das atividades inerentes a defesa nacional e segurança pública (art. 4º, III), considera-se uma situação hipotética: em uma atividade típica de investigação policial, onde a LGPD excepciona sua aplicação, há o tratamento de dados pessoais do suspeito e das pessoas que o cercam. Nessa situação, a LGPD prevê no artigo 4º, § 1º a aplicação dos princípios da proteção de dados, a exemplo do princípio da transparência (art. 6º, VI), do acesso (art. 6º, IV), responsabilização e prestação de contas (art. 6º, X). A eventual negativa de acesso às operações de tratamento dados aos interessados violaria, em tese, tais princípios.

¹⁵⁷ ÁVILA, Humberto. *Teoria dos Princípios*. 4.ed. São Paulo: Malheiros, 2005. p. 30-31.

¹⁵⁸ Idem, p. 27.

¹⁵⁹ Idem, 2005, p. 27.

¹⁶⁰ idem, 2005, p. 28.

¹⁶¹ Idem, 2005, p. 30-31

Nessa hipótese, haveria a competência sancionatória da ANPD para, por exemplo, impor uma advertência ao órgão público e determinar as medidas inerentes ao acesso dessa operação de tratamento de dados aos interessados (art. 31 c/c art. 52, I da LGDP)?

A interpretação sistemática acerca dos dispositivos da LGPD direciona para uma resposta afirmativa, pois, qual o sentido da Administração estar sujeita aos princípios proteção de dados (artigo 4º, §1º), obrigada a apresentar relatórios de impactos à proteção dos dados pessoais à ANPD (art. 4º, § 3º da LGPD) se, ao concluir pela violação dos direitos à privacidade no tratamento de dados realizado com fundamento no artigo 4º, III, não possuir o regulador a competência sancionatória para impor advertência e determinar a cessação de determinada operação de tratamento abusiva (art. 52, I da LGDP). Raciocínio contrário representaria tornar praticamente nula qualquer tipo de atuação da ANPD em relação ao Poder Público, quando este último realizar o tratamento de dados em atividades afetas a defesa nacional e à segurança pública.

A questão se torna mais premente quando se verifica que a LGPD autorizou a possibilidade da realização do tratamento de dados por pessoa jurídica de direito privado, para fins de segurança pública (artigo 4º, §§ 2º e 4º da LGPD). Isso porque, se o tratamento de dados para fins de segurança pública não está sujeito as regras da LGPD e ao poder sancionatório da ANPD, as empresas que vierem a operar tais dados serão fiscalizadas por qual autoridade?¹⁶²

Stefano Rodota defende a sujeição de tais atividades à autoridades criadas para a tutela dos dados pessoais, a exemplo da Autoridade Nacional de Proteção de Dados no Brasil, visando evitar violações de direitos e o “surgimento das zonas francas, livres de qualquer controle”, não só no âmbito nacional, como também internacional, de forma a assegurar o direito à privacidade dos cidadãos, notadamente no que respeita ao direito de acesso a este ao processo de tratamento de dados, bem como para evitar a criação de governos “incontroláveis e irresponsáveis”.¹⁶³

A questão da abrangência da competência sancionatória da ANPD em relação à Administração Pública, quando se tratar de operações de tratamento de dados nas atividades inerentes a Segurança Pública e Defesa Nacional (art. 4º, III) não é algo simples, sendo que tal discussão deverá ser enfrentada em breve. De qualquer maneira,

¹⁶² MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a proteção de dados não se aplica. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 191.

¹⁶³ RODOTA, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 149.

em um Estado Democrático de Direito à luz dos seus fundamentos e objetivos que se extraem dos artigos 1º e 3 da CF de 1988, o dever de transparência e prestação de contas pelo Poder Público não comporta o surgimento de determinados *locus* administrativos infensos à sujeição dos órgãos de controle.

3.4. Tratamento de dados por pessoa jurídica de direito privado sob a tutela do Poder Público

O artigo 4º, §§ 2º e 4º da LGPD prevê a possibilidade do tratamento de dados fundado no artigo 4º, III da lei ser realizado por pessoa jurídica de direito privado, nas seguintes condições: (i) sob a tutela de pessoa jurídica de direito público; (ii) mediante informe específico a Autoridade Nacional de Proteção de Dados e; (iii) desde que não trate da totalidade dos dados, excetuado se se tratar de pessoa jurídica de direito privado com capital integralmente constituído pelo Poder Público. Segundo Márcio Cots e Ricardo Oliveira:

A intenção de não permitir que a pessoa de direito privado trate a totalidade dos dados colhidos pelo Poder Público em determinado banco de dados é justamente mitigar riscos de vazamento, pois a segregação inviabilizaria, em tese, o vazamento, eliminação ou perda completa dos dados de uma única vez.¹⁶⁴

A contratação de pessoas jurídicas de direito privado para atuar em colaboração com a Administração, no exercício do poder de polícia, não uma novidade, devendo ser ressaltado que nestas hipóteses há a realização de “certos atos materiais que precedem atos jurídicos de polícia”, realizados por particulares mediante delegação ou em decorrência de contrato de prestação de serviços, a exemplo dos equipamentos fotossensores que pertencem e são operados por pessoas jurídicas de direito privado contratadas pelo Poder Público.¹⁶⁵

O artigo 4º, §§ 2º e 4º da LGPD revela a cautela do legislador em confiar ao setor privado a custódia de um sistema de vigilância, extremamente invasivo e potencialmente violador do direito à privacidade, idealizado para fins de defesa nacional e de segurança pública com prerrogativas próprias, parcialmente fora do campo de aplicação das regras

¹⁶⁴ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais Comentada*. 3. ed. São Paulo: Revista dos Tribunais, 2019. p. 71.

¹⁶⁵ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo. Editora: Malheiros, 2016. p. 869.

protetivas da LGPD. No entanto, tal cautela não se revela despropositada, considerando situações identificadas no sistema pátrio:

A título de exemplo, cita-se parceria celebrada, no ano de 2019, entre o Estado do Rio de Janeiro e a empresa telefônica Oi, para instalação e monitoramento de algumas câmeras no bairro de Copacabana, visando identificar pessoas procuradas pela Justiça. No ano de 2014, o relatório “Quem Defende seus Dados” publicado anualmente pelo InternetLab, mostrou que essa mesma empresa foi autuada por violar a privacidade de seus consumidores ao monitorar hábitos de navegação. Estaríamos confiando a segurança dos ovos à raposa.¹⁶⁶

Como tratado no capítulo anterior, até o advento de legislação específica para regulação da atividade de tratamento de dados realizado pelo Poder Público com fundamento no artigo 4º, III da LGPD, afigura-se inevitável a controvérsia acerca do alcance da competência da ANPD em relação ao Poder Público, no exercício deste mister e também das pessoas jurídicas de direito privado que realizarem operações de tratamento de tais atividades em colaboração com o setor público.

Dessa forma, o artigo 4º, §§ 2º e 4º da LGPD prevê a possibilidade do tratamento de dados fundado no artigo 4º, III da lei ser realizado por pessoa jurídica de direito privado, sob a tutela do Poder Público e restrita à parcela dos dados, sendo conveniente proposição normativa futura que extirpe de dúvidas a sujeição destas pessoas jurídicas de direito privado, no exercício de tais atividades, à regulação exercida pela Autoridade Nacional de Proteção de Dados.

3.5. Experiência internacional – modelo adotado pela GPDR

O Regulamento Geral de Proteção de Dados Pessoais Europeu nº 679, aprovado em 27 de abril de 2016 (GPDR), diploma legal que regulamenta a proteção de dados nos países integrantes da União Europeia, prevê no seu artigo 2º, *d* que o regulamento não se aplica ao tratamento de dados pessoais “Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infração penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.”

¹⁶⁶ MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a proteção de dados não se aplica. In: TEPELINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 190.

Segundo Rony Vainzof, a LGPD contempla previsão semelhante ao GPDR no seu artigo 4º, III, com a diferença de que de que a União Europeia editou de forma concomitante à GPDR a Diretiva 2016/680 que trata do tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.¹⁶⁷

Cabe ressaltar que o artigo 45, 1 do Regulamento 679/2016 (GPDR) condiciona a transferência de dados pessoais de cidadãos europeus para países não integrantes do bloco, a um nível de proteção compatível com o padrão europeu.¹⁶⁸

Sobre essa questão, de rigor mencionar que o acordo de privacidade denominado *privacy shield* firmado entre EUA e UE em 12 de julho de 2016, para transferência para os Estados Unidos de dados de cidadãos europeus para fins comerciais, foi anulado pelo Tribunal de Justiça da União Europeia em decisão proferida em 16 de julho de 2020, sob o entendimento de que os requisitos de acesso a tais dados pelas autoridades americanas não tinham o mesmo nível de proteção previsto na União Europeia. Tal decisão dificulta o envio de dados de cidadãos europeus a empresas americanas e demonstra uma postura da União Europeia de exigir um alto nível de proteção aos dados pessoais, para manutenção de relações comerciais com os demais países.¹⁶⁹¹⁷⁰

Dessa forma, para assegurar um nível compatível de proteção de dados pessoais com o padrão adotado pela União Europeia, conforme exige o artigo 45, 1 do Regulamento 679/2016 (GPDR), seria oportuna a edição de uma legislação específica para tratamento de dados pelo Poder Público nas hipóteses previstas no artigo 4º, III, da LGPD, conforme prevê seu artigo 4, § 1º, sob pena dos diversos sistemas internacionais, a exemplo da União Europeia, entender que o Brasil não possui um modelo adequado de proteção dados, o que prejudicaria o envio de dados por estes países às empresas brasileiras.

¹⁶⁷ VAINZOF, Rony. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 72.

¹⁶⁸ O artigo 45, 1 do Regulamento 679/2016 (GPDR) prevê: “Pode ser realizada uma transferência de dados para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção a dequado. Esta transferência não exige autorização específica.”

¹⁶⁹ Commercial sector: EU-US Privacy Shield. *European Commission*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en. Acesso em: 20 jul. 2020.

¹⁷⁰ Impactos da decisão da Corte de Justiça da União Europeia sobre transferência de dados pessoais. *Lexlatin*, 17 jul. 2020. Disponível em: <https://br.lexlatin.com/opiniao/impactos-da-decisao-da-corte-de-justica-da-uniao-europeia-sobre-transferencia-de-dados> Acesso em: 20 jul. 2020.

3.6. Defesa Nacional e Segurança do Estado

As competências administrativas da União encontram-se previstas no artigo 21, I a XXV, da CF de 1988, dentre as quais destaca-se a “manutenção de relações com Estados estrangeiros (inciso I), declarar a guerra e celebrar a paz (inciso II), assegurar a defesa nacional (inciso III), decretar Estado de Sítio, Estado de Defesa e a Intervenção Federal (inciso V).”¹⁷¹

No que respeita ao conceito de defesa nacional, o Decreto nº 5.484, de 30 de junho de 2005, que aprovou a Política de Defesa Nacional, conceitua o instituto como sendo o “conjunto de medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas” (1.4, II).

O mencionado ato normativo conceituou defesa nacional como sendo o conjunto de medidas visando assegurar a independência nacional, prevista no artigo 4º, I, da CF de 1988, a qual nas lições de Ingo Wolfgang Sarlet assume uma dimensão de defesa externa da soberania:

A independência nacional (art. 4º, I, da CF) guarda relação direta com a própria noção de soberania, que, por sua vez, assume a função de fundamento do Estado Democrático de Direito brasileiro e simultaneamente opera como princípio fundamental (art. 1º, I), de tal sorte que a independência há de ser compreendida nessa perspectiva, como dimensão externa (internacional) da soberania. Não se trata, contudo, de uma soberania excludente e arrogante, portanto, mas, sim, de uma noção de independência voltada à integração na comunidade internacional, baseada no respeito, igualdade e reciprocidade, tal como evidenciam outros dispositivos constitucionais. O próprio art. 4º contempla, em seus incisos, a prevalência dos direitos humanos (II), a autodeterminação dos povos (III), o princípio da não intervenção (IV), a igualdade entre os Estados (V), a defesa da paz, a solução pacífica dos conflitos e o repúdio ao terrorismo (VI, VII e VIII), cooperação entre os povos (IX) e a busca da integração latino-americana (parágrafo único).¹⁷²

Dessa forma, por defesa nacional tem-se os atos de competência da União (art. 21, III, da CF de 1988) que visam assegurar a independência nacional, assim entendida como a soberania em relação à sua política externa, por meio das Forças Armadas, instituição

¹⁷¹ SARLET, Ingo Wolfgang. In: SARLET, Ingo Wolfgang; MITIDIERO, Daniel; MARINONI, Luiz G. (Org.). *Curso de direito constitucional*. 9. ed. São Paulo: Saraiva, 2020. p. 948.

¹⁷² Idem, p. 309.

permanente sob a autoridade a Presidência da República, nos termos do artigo 142 da CF de 1988.

A segurança do Estado pode se concretizar nas medidas que integram a competência da União (art. 21, V da CF de 1988), inerentes “a possibilidade de suspensão do sigilo das comunicações (de correspondência, telefônica etc.) durante a vigência de estado de defesa (art. 136, § 1.º, I, b e c) e de estado de sítio (art. 139, III) sem que se tenha feito qualquer distinção em relação aos meios de comunicação”.¹⁷³

Isso porque na vigência do estado de defesa e estado de sítio, tanto o sigilo de comunicações de dados (informações dinâmicas), que está submetido a reserva de jurisdição conforme preceitua o artigo 5º, XII da CF, quanto o sigilo de dados em si mesmo (informações estáticas) que, nada obstante acobertado pela garantia do sigilo (art. 5º, X), não está sujeito a reserva de jurisdição, estarão submetidos a um regime de excepcional constitucionalidade.

Quando verificadas as situações que impõem um regime de excepcional constitucionalidade, notadamente as medidas inerentes à concretização da defesa nacional e segurança do Estado (Estado de Defesa e Estado de Sítio), evidentemente não se aplica a sistemática de tratamento de dados pessoais levadas a efeito pela LGPD, nada obstante a lei prever que, mesmo nestas situações, deverá ser observada a legislação específica e os princípios aplicáveis à proteção de dados (4º, § 1º da LGDP).¹⁷⁴

3.6.1. Ataques cibernéticos

No campo da defesa nacional, assim entendida como as medidas relacionadas à política externa objetivando assegurar a soberania nacional, há uma recente preocupação em relação aos ataques cibernéticos, onde a chamada “guerra cibernética” pode representar uma real ameaça à segurança nacional, um novo contexto em que é identificada uma crescente tendência à militarização do espaço virtual.

Os ataques cibernéticos muitas vezes ocorrem de forma global, a exemplo do denominado Wanacry ocorrido em 2017, o qual infectou mais de 230.000 PCs Windows

¹⁷³ SARLET, Ingo Wolfgang. In: SARLET, Ingo Wolfgang; MITIDIERO, Daniel; MARINONI, Luiz G. (Org.). *Curso de direito constitucional*. 9 ed. São Paulo: Saraiva, 2020, p. 488.

¹⁷⁴ § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

em 150 países em um dia, muitos dos ataques direcionados a entidades governamentais e hospitais, por meio de um expediente onde os cibercriminosos bloqueavam os arquivos do computador e exigiam o pagamento pelo desbloqueio.¹⁷⁵

Na ocasião, os EUA acusaram os norte-coreanos pelo ataque denominado Wannacry em 2017 e pela investida realizada contra a Sony em 2014.¹⁷⁶ Além destes, apenas a título de exemplo, os EUA acusam os Russos por ataques que teriam sido direcionados ao Estado da Geórgia em 2019, o qual teria prejudicado sites de operações militares do governo da Geórgia e a transmissão de ao menos duas grandes emissoras de televisão.¹⁷⁷ Recentemente, os EUA promoveram ataques cibernéticos contra os sistemas de inteligência do Irã, especificamente o controle de mísseis.¹⁷⁸ Essa nova realidade determinou a criação nos EUA de setores de inteligência na área dos ataques cibernéticos e o direcionamento de investimentos em segurança para redes de infraestrutura.¹⁷⁹

O Brasil não está alheio a esta nova realidade, sendo considerado pela Organização das Nações Unidas (ONU) um dos países mais sujeitos a ataques cibernéticos, sendo que em nota à imprensa o Gabinete de Segurança Institucional da Presidência informou que os ataques considerados mais preocupantes objetivam acesso à informações sigilosas da Administração Pública Federal.¹⁸⁰¹⁸¹ Diante deste cenário, especialistas da ONU e do governo brasileiro têm realizados reuniões visando discutir alternativas contra crimes cibernéticos, inclusive com a formação de um grupo de trabalho para definir medidas de prevenção ao cibercrime.¹⁸²

¹⁷⁵ O que é o WanaCry?. *Avast*. Disponível em: <https://www.avast.com/pt-br/c-wannacry>. Acesso em 14 jul. 2020.

¹⁷⁶ EUA acusam norte coreano por Wannacry e ataques a Sony. *Security Report*. Disponível em: <https://www.securityreport.com.br/overview/eua-acusam-norte-coreano-por-wannacry-e-ataque-contra-sony/#.Xw8TwyhKiMo>. Acesso em: 14 jul. 2020.

¹⁷⁷ EUA e UK acusam Rússia de ataque cibernético à Geórgia. *Ciso Advisor*. Disponível em: <https://www.cisoadvisor.com.br/eua-e-uk-acusam-russia-de-ataque-cibernetico-a-georgia/>. Acesso em: 14 jul. 2020.

¹⁷⁸ EUA lançaram ataques cibernéticos contra sistema de inteligência do Irã. *Veja*. Disponível em: <https://veja.abril.com.br/mundo/eua-lancaram-ataques-ciberneticos-contra-sistemas-de-inteligencia-do-ira/>. Acesso em: 14 jul. 2020.

¹⁷⁹ EUA terão unidade de proteção cibernética para redes de energia elétrica. *Globo.com*. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/eua-terao-unidade-de-protecao-cibernetica-para-redes-de-energia-eletrica.ghtml>. Acesso em: 14 jul. 2020.

¹⁸⁰ Brasil está entre os emergentes que mais sofrem ataques cibernéticos. *Onu News*. Disponível em: <https://news.un.org/pt/tags/ataques-cibernetico>. Acesso em: 14 jul. 2020.

¹⁸¹ Inimigos Invisíveis: a guerra cibernética. *Senado*. Disponível em: <https://www.senado.gov.br/noticias/Jornal/emdiscussao/defesa-nacional/razoes-para-a-implementacao-da-estrategia-nacional-de-defesa/inimigos-invisiveis-a-guerra-cibernetica.aspx>. Acesso em: 14 jul. 2020.

¹⁸² Especialistas da ONU e governo brasileiro discutem ações contra crimes cibernéticos. *Nações Unidas Brasil*. Disponível em: <https://nacoesunidas.org/especialistas-da-onu-e-governo-brasileiro-discutem-acoes-contra-crimes-ciberneticos/>. Acesso em: 14 jul. 2020.

Dentro deste novo cenário de “guerra virtual” marcada pelos denominados ataques cibernéticos, que envolvem a subtração de dados e a invasão de sistemas, colocando em risco a segurança nacional, o qual pode ocorrer por diversos meios, amplia-se ao Poder Público o denominado “estado de vigilância”, excluindo a incidência do regime de tratamento de dados previsto na LGDP, com a possibilidade de maior controle das movimentações e dos dados dos usuários na rede mundial de internet, com fundamento na soberania e na segurança nacional.

Deve-se registrar, por fim, que não é conferida à União uma prerrogativa ilimitada, infensa a restrições, mesmo quando atua no exercício da defesa nacional, pois, nada obstante a exceção à aplicação da política de proteção de dados prevista na LGPD em relação às medidas afetas a temas de segurança do Estado, o tratamento de dados realizado sob tal fundamento deve respeitar legislação própria aplicável à questão e os princípios da proteção de dados (art. 4º, §1º da LGDP), em especial, o princípio que determina que o tratamento deve ser restrito a realização da finalidade que o determinou (princípio da finalidade), bem como a limitação à utilização dos dados estritamente necessários a realização deste fim (princípio da necessidade).

3.6.2. Ameaça terrorista

França, 13 de novembro de 2015: 129 pessoas foram mortas em um ataque terrorista realizado em vários lugares de Paris e de forma simultânea, cuja autoria foi reivindicada pelo grupo radical Estado Islâmico.¹⁸³ O que há de novo no modo operacional que levou ao mencionado ataque terrorista:

Em comum, as investidas ultraviolentas contra alvos civis da sociedade francesa se caracterizam por um novo estilo de organização do terrorismo, em muito creditado à disseminação da internet e das redes sociais. Através deste meio, as cédulas terroristas extremamente organizadas conseguem suprimir as distâncias, convocar e converter cidadãos dos países-alvo ao fundamentalismo, transformando o próprio nativo, por variadas formas de convencimento, em arma poderosa de disseminação de ódio, terror e morte. Servem-se também deste meio para propagar o medo e demonstrar força e poder

¹⁸³ Atentados em Paris: perguntas e respostas sobre os ataques. *Globo.com*. Disponível em: <http://g1.globo.com/mundo/noticia/2015/11/atentados-em-paris-perguntas-e-respostas-sobre-os-ataques.html>. Acesso em: 14 jul. 2020.

nas regiões de seus domínios, constituindo-se como meio ideal de publicidade e propaganda terrorista.¹⁸⁴

Logo após os ataques de 11 de setembro de 2001, os EUA editaram o chamado Usa Patriot Act aproveitando o estado de medo que existia na sociedade americana, para restringir de forma contundente os direitos e garantias individuais, por meio do mencionado ato que, dentre outras medidas, fixava regras de vigilância dos cidadãos, viabilizando a coleta e o rastreamento de dados pessoas tidas como suspeitas de terrorismo, sem a necessidade de intervenção judicial.¹⁸⁵

Anos após os atentados de 11 de setembro 2001, o ex-agente da National Security Agency, Edward Snowden, denunciou um grande sistema de vigilância da população americana utilizando servidores de empresas como Google, Apple e Facebook, evidenciando na ocasião que o sistema de vigilância não se restringia aos suspeitos de terrorismos, mas era realizado de forma massiva em relação não só a população americana mas também em nível global, envolvendo inclusive a espionagem ostensiva de líderes mundiais.¹⁸⁶

Os atentados terroristas ocorridos em Londres em 2005, onde uma série de ataques a bomba nos transportes públicos vitimou 56 pessoas e feriu mais de 700, trouxe como reação imediata a criação de regras de maior vigilância, as quais foram posteriormente invalidadas considerando o nível de restrição à privacidade que representavam¹⁸⁷:

Na Europa, no contexto de combate ao terrorismo, intensificado após os atentados de Londres em 2005, foi editada a Diretiva 2006/24 (Diretiva de Retenção de Dados), obrigando companhias de telecomunicações a manter, por ao menos seis meses, os registros de dados pessoais de seus usuários para sua eventual utilização em investigações. Porém, esse impulso foi contido em razão da violação indiscriminada à privacidade de todos os seus cidadãos que a Diretiva de Retenção de Dados representava¹²¹. Assim, em abril de 2014 a Diretiva foi invalidada pelo Tribunal de Justiça da União Europeia, com fundamento na proteção à privacidade, considerando que a investigação indiscriminada não pode prevalecer, mesmo quando objetiva combater infrações graves como o terrorismo. Ou seja, mesmo a grave ameaça representada pelo

¹⁸⁴ REIS JÚNIOR, Antonio dos. O direito à privacidade na era digital: desafios em face da ameaça terrorista. In: BARBOSA-FOHRMANN, Ana Paula; BARRETO, Gustavo Augusto Ferreira. *A vida dos direitos humanos*. Reflexões sobre questões atuais. Rio de Janeiro: Gramma, 2016. p. 24.

¹⁸⁵ DOYLE, Charles. Senior Specialist, American Division of Law. The USA patriot Act: A Legal Analysis. 15 de abril de 2002. Congressional Research Service. The Library of the Congress. p. 02.

¹⁸⁶ Entenda o caso de Edward Snowden, que revelou espionagem nos EUA. *Globo.com*, 14 fev. 2014. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 23 mar. 2020.

¹⁸⁷ Atentados islâmicos de 07 de julho de 2015 em Londres. *Uol*. Disponível em: <https://noticias.uol.com.br/ultnot/afp/2007/03/22/ult34u177057.jhtm>. Acesso em: 16 jul. 2020.

terrorismo foi insuficiente para justificar uma atuação de vigilância sobre todos os usuários de telecomunicações (*dragnet surveillance*).¹⁸⁸

A observação realizada por Antonio dos Reis Júnior no sentido de que o terrorismo constitui em duplo ataque à dignidade se afigura adequada, pois, há de um lado as vítimas diretas dos atos do terror e, de outro, os que têm sua vida privada invadidas pelos setores de segurança, como decorrência da reação dos governos de instituírem o estado de vigilância devidamente autorizado por uma sociedade assolada pelo medo.¹⁸⁹

A Constituição Federal prevê que o Brasil rege-se nas relações internacionais pelo repúdio ao terrorismo (art. 4º, VIII), contemplado como tipo penal na Lei nº 7.170/1983 (art. 20), de tal forma que apesar de não ser comum a prática de atos de terrorismo no território pátrio, o artigo 4º da LGDP excepciona a aplicação da lei as operações de tratamento de dados visando a defesa nacional (art. 4, III, *b*), o que abrange medidas visando evitar atos de terrorismo, de tal forma que, eventuais atos e diplomas normativos editados sob o mote de combate ao terror, devem obviamente garantir poderes ao Estado para atuar neste mister, no entanto, deve-se buscar a adoção de um modelo equilibrado que não exclua os direitos individuais, considerando o abuso de direito evidenciado na experiência internacional, bem como respeitados os princípios gerais da proteção de dados previstos na LGPD.

3.6.3. Da nova estrutura da ABIN e a ADI nº 6529

O Decreto nº 10.445, de 30 de julho de 2020 aprovou a estrutura regimental e de cargos da Agência Brasileira de Inteligência (ABIN), criada pela Lei nº 9.883/1999, instituindo um órgão denominado Centro de Inteligência Nacional com a competência para: (i) planejar e executar atividades de inteligência destinadas ao enfrentamento de ameaças à segurança e à estabilidade do Estado e da sociedade (art. 15, II, a), mediante “a produção de inteligência corrente e a coleta estruturada de dados” (art. 15, V).

A criação do mencionado órgão com atribuições de produção de inteligência mediante coleta estruturada de dados dos cidadãos brasileiros tem sido alvo de críticas de parlamentares, inclusive o deputado Alessandro Molon (PSB-RJ) foi autor do Projeto de Decreto Legislativo

¹⁸⁸ ABRUSIO, Juliana et al. Dados de Geolocalização e a investigação do caso Marielle. *Conjur*, 07 jul 2020. Disponível em: <https://www.conjur.com.br/2020-jul-07/direito-digital-dados-geolocalizacao-investigacao-marielle?pagina=2>. Acesso em: 16 jul. 2020.

¹⁸⁹ REIS JÚNIOR, Antonio dos. O direito à privacidade na era digital: desafios em face da ameaça terrorista. In: BARBOSA-FOHRMANN, Ana Paula; BARRETO, Gustavo Augusto Ferreira. *A vida dos direitos humanos*. Reflexões sobre questões atuais. Rio de Janeiro: Gramma, 2016. p. 26.

351/20 visando anular os efeitos do Decreto nº 10.445/2020, sob o fundamento de que o ato normativo subverte a lógica institucional da Abin: "a alteração normativa permite transformar a Abin em mera unidade de investigação, em afronta ao seu verdadeiro propósito de produzir inteligência e de auxiliar no processo decisório do Estado".¹⁹⁰

Os partidos Rede Sustentabilidade e Partido Socialista Brasileiro ajuizaram a ADI nº 6529, questionando a constitucionalidade do parágrafo único do artigo 4º da Lei 9.883/1999, que viabiliza o compartilhamento de dados no âmbito do Sistema Brasileiro de Inteligência (Sisbin) para a Agência, compartilhamento que poderia ser realizado de forma abusiva pelo fato do Decreto 10.445/2020 viabilizar tal ato mediante uma simples requisição, na medida em que não restringiu as hipóteses de requisição de informações no âmbito do Sisbin pela Agência.¹⁹¹

Os questionamentos acerca do Decreto 10.445/2020 não são infundados considerando que, no contexto recente à edição do mencionado Decreto, o veículo jornalístico denominado *The Intercept* publicou uma reportagem onde a Abin teria solicitado ao Serviço Federal de Processamento de Dados (SERPRO), os dados de milhões de brasileiros constantes do Banco de Imagens do Registro Nacional de Condutores Habilitados (RENACH), notadamente o nome, filiação, CPF, endereço, telefones, foto, dados dos veículos (nomes de proprietários anteriores, situação e procedência) de todo cidadão que possui habilitação para dirigir, sendo estimados mais de 75 milhões de registros.¹⁹²

Danilo Doneda foi entrevistado pelo *The Intercept* na oportunidade, demonstrando receio de que tais informações estariam sendo utilizados por um sistema massivo de vigilância, a exemplo do realizado pelos EUA por meio da agência de espionagem NSA que implementou um amplo sistema de espionagem dos cidadãos americanos:

Esse caso, pelo volume de informações, chama atenção. Eu me pergunto qual é o interesse estratégico para inteligência nacional você fazer vigilância massiva”, questiona

¹⁹⁰ Projeto anula decreto de Bolsonaro que cria Centro de Inteligência Nacional. *Câmara dos Deputados*. Disponível em: <https://www.camara.leg.br/noticias/682074-projeto-anula-decreto-de-bolsonaro-que-cria-centro-de-inteligencia-nacional/>. Acesso em: 11 ago. 2020.

¹⁹¹ Partidos questionam norma que condiciona fornecimento de dados à Abin a ato presidencial. *Supremo Tribunal Federal*. Disponível em: <http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449429&ori=1>. Acesso em: 15 ago. 2020.

¹⁹² Documentos vazados mostram que ABIN pediu a o SERPRO dados e fotos de todas as CNHs do país. *The Intercept*. Disponível em: <https://theintercept.com/2020/06/06/abin-carteira-motorista-sepro-vigilancia/>. Acesso em: 01 ago. 2020.

o advogado Danilo Doneda, doutor em Direito Civil e membro indicado pela Câmara dos Deputados para o Conselho Nacional de Proteção de Dados e Privacidade. “O que chama a atenção agora é que é um momento de politização exacerbada dos órgãos de estado. Há um receio latente de informações pessoais sendo usadas para fins não republicanos. Acende a luz amarela, no mínimo”.

Para o advogado, o esquema montado pela Abin remete ao escândalo de espionagem da NSA, a agência de segurança digital dos EUA, que usou um sistema massivo de vigilância para fins obscuros e, muitas vezes, privados. O caso foi revelado pelo analista de segurança Edward Snowden.¹⁹³

O Plenário do Supremo Tribunal Federal analisou a medida cautelar requerida na ADI nº 6529, em julgamento realizado em 13 de agosto de 2020, deferindo parcialmente a liminar para conferir interpretação conforme ao parágrafo único do artigo 4º da Lei 9.883/1999, de maneira a estabelecer que os órgãos integrantes do Sistema Brasileiro de Inteligência (Sisbin) somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (Abin) quando for comprovado o interesse público da medida, mediante solicitação devidamente motivada, vedado o compartilhamento de dados sujeitos à reserva de jurisdição, sendo imprescindível a instauração de procedimento formal e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.¹⁹⁴

Cabe ressaltar que a Relatora da ADI nº 6529, Ministra Carmem Lúcia, ressaltou em seu voto que o fornecimento de informações entre órgãos públicos para a defesa das instituições e dos interesses nacionais é legítimo, sendo que “o que é proibido é que se torne subterfúgio para atendimento ou benefício de interesses particulares ou pessoais, especialmente daqueles que têm acesso aos dados, desvirtuando-se competências constitucionalmente definidas e que não podem ser objeto de escolha pessoal”, afirmando também que “Arapongagem’ não é direito, é crime, e, praticado pelo Estado, é ilícito gravíssimo”.¹⁹⁵

¹⁹³ Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHS do país. *The Intercept*. Disponível em: <https://theintercept.com/2020/06/06/abin-carteira-motorista-sepro-vigilancia/>. Acesso em: 01 ago. 2020.

¹⁹⁴ Interesses públicos, e não privados, justificam o repasse de dados à Abin, diz STF. *Conjur*. Disponível em: <https://www.conjur.com.br/2020-ago-13/interesse-publico-necessario-repasse-dados-abin-stf>. Acesso em: 16 ago. 2020.

¹⁹⁵ STF impõe limite ao compartilhamento de dados do sistema Brasileiro de inteligência (Sisbin). *Supremo Tribunal Federal*. Disponível em: <http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449549&ori=1>. Acesso em: 16 ago. 2020.

Como mencionado pelo advogado Danilo Doneda na reportagem acima citada, a experiência internacional, especialmente dos Estados Unidos da América, evidencia que as sociedades organizadas devem efetivamente ser receosas quanto aos sistemas estatais de vigilância instituídos para fins de segurança do estado e defesa nacional, pois, a experiência direciona para uma tendência de violação reiterada de direitos fundamentais, especialmente o direito à privacidade, sendo necessário para tal mister não só a previsão legal impondo ao Estado a observação de princípios próprios da proteção de dados, mas também a submissão de tais atividades ao controle regulatório específico da ANPD que deve, para além emitir opiniões técnicas ou solicitar relatórios de impactos a proteção de dados (art. 4º, §3º da LGDP), ter a possibilidade de impor sanções como advertências e imposição de prazo para adoção de medidas corretivas (art. 52, I da LGPD).

3.7. Segurança pública e atividades de investigação e repressão de infrações penais

O artigo 144 da CF de 1988 traz disposições relativas à segurança pública, exercida com a finalidade de “preservação da ordem pública e da incolumidade das pessoas e do patrimônio”, discriminando a competência das instituições dotadas de poder de polícia penal, com atribuições de apurar atos que atentem contra os mencionados fins assegurados pela segurança pública.

A polícia judiciária é uma competência conferida a Polícia Federal e a Polícia Civil, cuja finalidade é a apuração das infrações penais comuns (artigo 144, §§ 1º e 4º da CF de 1988), sendo exercida pelas autoridades policiais nos termos do artigo 4º do Código de Processo Penal.

Cabe ressaltar que o Supremo Tribunal Federal reconheceu a competência do Ministério Público para a realização de investigações de natureza penal, desde que respeitados os direitos e garantias do investigado, a reserva de jurisdição para os casos em que a Constituição específica e as prerrogativas dos advogados, sem prejuízo do controle jurisdicional dos atos de investigação que deverão ser necessariamente documentados.¹⁹⁶

Dessa forma, quando o Poder Público atua sob o desígnio de assegurar a segurança pública e no exercício de poder de polícia judiciária, visando a apuração de infrações penais, as operações de tratamento de dados pessoais para tal fim não estará sujeita a

¹⁹⁶ BRASIL. Supremo Tribunal Federal. RE nº 593.727, Rel. para o acórdão Ministro Gilmar Mendes, julgamento 14 maio 2015, Tema 184.

política de proteção de dados prevista na LGPD, no entanto, conforme prescreve referida lei, tal situação não exime o Ente Público de observar regras previstas em legislações específicas e os princípios próprios da proteção de dados (art. 4º, §1º da LGPD), de maneira a evitar o uso indiscriminado de dados pessoais para finalidades alheias aos escopos da segurança pública.

Ainda, deve ser consignado que a LGPD assegura a transferência internacional de dados, entre órgãos públicos de inteligência, investigação e persecução, de acordo com os instrumentos de direito internacional.¹⁹⁷

3.7.1. Dos bancos de dados de perfil genético, multibiométrico e de impressões digitais previstos na lei anticrime

A Lei nº 13.964/2019 também conhecida como “Pacote Anticrime” autorizou a criação, no âmbito do Ministério da Justiça, do Banco Nacional Multibiométrico e de impressões digitais, com o objetivo de consolidar dados “biométricos, de impressões digitais e, quando possível, de íris, face e voz, para subsidiar investigações criminais”, a par da existência de um banco de dados de perfis genéticos que já era possível à luz da Lei nº 12.654/2012.

A coleta de dados de perfil genético é possível para fins de identificação criminal e em sede de execução penal por crimes violentos ou crimes hediondos (Art. 9-A da Lei 7.210/84), podendo ser realizado na primeira hipótese para fins de investigação criminal (art. 3º, IV, lei nº 12.654/2012), armazenados em banco de dados específico de caráter sigiloso (art. 5º, § 2º), o qual não poderá em tese revelar traços somáticos ou comportamentais (art. 5º, § 1º), sendo que a exclusão do banco de dados será possível na hipótese de absolvição do acusado (art. 7º, I), ou após 20 anos de cumprimento da pena, na hipótese de condenação (art. 7º, II).

O Banco Nacional Multibiométrico e de impressões digitais, cuja criação foi autorizado pela Lei nº 13.964/2019, tem como objetivo armazenar dados de “registros biométricos, de impressões digitais e, quando possível, de íris, face e voz, para subsidiar investigações criminais federais, estaduais ou distritais.” (art. 7º, § 2º), de caráter sigiloso

¹⁹⁷ “Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
(...)

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;”

(art. 7º, § 8º), colhido em investigações criminais ou por ocasião da identificação criminal (art. 7º, § 3º), podendo atuar de forma interoperável com outros bancos de dados por meio de acordo ou convênio com a unidade gestora (art. 7º, § 7º), sendo vedada sua comercialização (art. 7º, § 10).

O Supremo Tribunal Federal irá analisar a constitucionalidade do art. 9º-A da Lei nº 7.210/1984, na redação conferida pela Lei nº 12.645/2012, o qual prevê o armazenamento de perfis genéticos de condenados por crimes violentos ou hediondos, ante uma suposta violação aos direitos constitucionais da personalidade e da prerrogativa de não incriminação. O v. acórdão que afetou o tema a repercussão geral, abordou de forma elucidativa como a questão tem sido tratada no Tribunal Europeu de Direitos Humanos que, por sua vez, exterioriza o entendimento de que a coleta de dados de condenados e sua manutenção por tempo determinado, seria uma intromissão proporcional ao direito da privacidade:

O Tribunal Europeu dos Direitos Humanos já se debruçou sobre a questão em algumas oportunidades. Em *Van der Velden contra Holanda*, 29514/05, decisão de 7.12.2006, o Tribunal considerou que o método de colheita do material – esfregação de cotonete na parte interna da bochecha – é invasivo à privacidade. Também avaliou como uma intromissão relevante na privacidade a manutenção do material celular e do perfil de DNA. Quanto a esse aspecto, remarcou-se não se tratar de métodos neutros de identificação, na medida em que podem revelar características pessoais do indivíduo. No entanto, a Corte avaliou que a adoção da medida em relação a condenados era uma intromissão proporcional, tendo em vista o objetivo de prevenir e investigar crimes.

No caso *S. e MARPER contra Reino Unido* (decisão de 4.12.2008), o Tribunal afirmou que a manutenção, por prazo indeterminado, dos perfis genéticos de pessoas não condenadas, viola o direito à privacidade, previsto no art. 8º da Convenção Europeia de Direitos Humanos. Por outro lado, no caso *Peruzzo e Martens contra Alemanha* (30562/04 e 30566/04, decisão de 4 de dezembro de 2008), considerou-se manifestamente infundada a alegação de que a manutenção, em bancos de dados estatais, de perfis genéticos de condenados por crimes graves violaria o direito à privacidade.¹⁹⁸

A controvérsia identificada na hipótese de coleta de perfis genéticos e seu armazenamento em banco de dados, diz respeito a eventual afronta aos dispositivos da personalidade, notadamente o direito a dignidade da pessoa humana (art. 1º, III da CF de 1988) e da privacidade (art. 5º, X da CF de 1988), os quais devem encontrar um equilíbrio na sociedade da informação com as iniciativas inerentes a segurança pública que

¹⁹⁸ BRASIL. Supremo Tribunal Federal. RE nº 973837, Rel. Ministro Gilmar Mendes, julgamento 23 jun. 2016, Tema 905.

envolvem a prevenção e a repressão de infrações criminais. Sobre o tema, Stefano Rodotà tece importantes considerações:

Trata-se de imponentes coletâneas de dados. O arquivo *Shengen* já conta com 9 milhões de informações, dos quais seis milhões e meio relacionados a pessoas. Mas são outros os casos que fornecem mais prontamente as dimensões e as perspectivas das coletâneas de informações para finalidades de segurança. Em alguns países europeus já existem bancos de dados contendo o DNA de indivíduos considerados perigosos. Ampliam-se coletas de dados sobre a saúde. Multiplicam-se as formas de controle com câmeras de vídeo, já habituais em setores como bancos, estações e supermercados, e que controlam inteiras zonas urbanas consideradas “de risco”. A Grã-Bretanha é o local onde o controle através de câmeras de vídeo é mais disseminado, contanto com mais de um milhão de câmeras cada vez mais sofisticadas (fala-se de câmeras de vídeo “pensantes”): mas essa é uma tendência que já parece irresistível, comum aos mais diversos países. Em muitos Estados existe uma obrigação de gestores dos serviço telefônicos de conservar por um determinado período os dados relacionados ao tráfico telefônico e de colocá-los à disposição da magistratura e da polícia: na Itália, onde a obrigação de conservação é de cinco anos, isso significa um imenso banco de dados que abrange mais de 100 bilhões de dados, graças aos quais é possível seguir os rastros de todos os telefonemas feitos por uma pessoa, determinando o lugar da chamada, o seu destinatário, duração da conversa. Dois relatórios do Parlamento europeu sobre o sistema Echelon analisaram a capilaridade do sistema mundial de escuta liderado pela National Security Agency americana. Uma rede de malhas finíssimas se estende, desta forma, por toda a sociedade.

Existem evidentemente muitas boas razões que sustentam a necessidade de usar todas as oportunidades oferecidas pelas novas tecnologias para proteger a sociedade de crimes, fomentar a prevenção de doenças, proteger os mais vulneráveis dos riscos sociais. Deve-se buscar um justo equilíbrio entre uma visão individualista da privacidade e a satisfação das exigências sociais, como ressalta o maior teórico do comunitarismo americano, Amitai Etzioni.¹⁹⁹

O artigo 5º, § 1º da Lei nº 12.654/2012 veda o tratamento de dados constante em banco de dados de perfis genéticos, com vistas à obtenção de traços somáticos e comportamentais das pessoas, o que entende-se aplicar também ao banco de dados multibiométrico e de impressões digitais que abrangem informações “biométricas, de impressões digitais e, quando possível, de íris”, porquanto que a finalidade da restrição é impossibilitar a criação via tratamento de dados de padrões físicos e comportamentais que poderiam gerar situações discriminatórias.

Esse é necessariamente um risco que deve ser considerado no procedimento de tratamento de dados, pois, nos EUA um programa de computador chamado COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), analisa a

¹⁹⁹ RODOTA, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 146-147.

probabilidade de reincidência criminal do indivíduo com base em sistema de pontos que considera informações pessoais do acusado, no entanto, muitas questões tem surgido acerca dos critérios utilizados pelos algoritmos, que é gerido por uma empresa privada e cujo acesso aos critérios para definição do sistema de pontuação não é concedido sob o fundamento de sigilo comercial, especialmente diante de acusações de refletir um risco maior de reincidência para negros.²⁰⁰

Vale ressaltar que o tema inerente à premente criação do Banco Nacional de Perfil Genético e do Banco Nacional Multibiométrico, por ocasião da aprovação do pacote anticrime, já encontra ressonância na doutrina, no sentido de que a iniciativa seja delimitada pelo “direito à privacidade (Art. 17, LGPD) e os princípios conexos à proteção de dados devem ser o escudo protetor da pessoa em face do Estado de Vigilância.”²⁰¹

Dessa forma, não se olvida acerca da necessidade das novas tecnologias à disposição do Poder Público para o exercício das políticas públicas inerentes a segurança pública e a repressão criminal, no entanto, há de se ter como fim a compatibilidade dos diversos modelos e tecnologias frente aos direitos individuais, especialmente os inerentes a privacidade e a não discriminação, de maneira que tais aplicações não se convertam em mero instrumento de vigilância com potencialidade de replicar as injustiças já evidenciadas no nosso sistema de justiça criminal.

3.7.2. Investigação com base em dados de geolocalização: *geofencing* ou *busca reversa*

A investigação do notório caso do assassinato da ex-vereadora Marielle Franco e seu motorista Anderson Gomes, em 18/03/2018 na cidade do Rio de Janeiro, trouxe à tona uma discussão a respeito da privacidade de dados nos procedimentos de investigação criminal.

Isso porque o Ministério Público obteve junto a Justiça carioca uma ordem que lhe garantiu a quebra do sigilo telemático de dispositivos determinados por geolocalização, possibilitando o acesso dos investigadores aos dados de quaisquer pessoas, não só as investigadas, que estiveram próximas do local do crime no dia que ocorreu, bem como os

²⁰⁰ Sistema de algoritmo que determina pena de condenados cria polêmica nos EUA. *BBC News*, 31 out. 2016. Disponível em: <https://www.bbc.com/portuguese/brasil-37677421>. Acesso em: 12 jul. 2020.

²⁰¹ MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a proteção de dados não se aplica. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 187-188.

dados das pessoas que tenham, por qualquer motivo, pesquisado o nome da vereadora nos cinco dias que antecederam o crime.²⁰²

O caso chegou ao Superior Tribunal de Justiça em virtude de três recursos em mandado de segurança interpostos pelo Google Brasil, tendo Terceira Seção do Superior Tribunal de Justiça negada provimento aos recursos interpostos, para que a empresa forneça as informações solicitadas no âmbito da investigação criminal do caso Marielle Franco, sob o entendimento de que a medida não impõe restrição desproporcional à privacidade das pessoas.²⁰³

Abrusio *et al* (2020) traz importante contextualização da experiência internacional tanto nos EUA quanto na União Europeia, acerca da prática que recebeu o nome de *geofencing* ou *busca reversa*:

Nos Estados Unidos, havia posicionamento jurisprudencial até 2015, no sentido de “que o usuário não tem uma razoável expectativa de privacidade sobre seus dados de geolocalização” pois carrega seus dispositivos para todo lado e concordou com suas políticas de privacidade.

Porém, esse cenário se alterou diante da adoção da prática de geofencing ou busca reversa por agentes federais americanos, em 2016, na Carolina do Norte e que se espalhou para estados como Califórnia, Flórida, Minnesota e Washington. Um caso específico chamou a atenção da imprensa americana ao cobrir, em dois mandados, uma área de 29.387 metros quadrados, equivalente a 3 hectares, em período de 9 horas, obrigando a empresa a entregar à polícia federal americana dados de 1.500 dispositivos armazenados em um banco de dados chamado Sensor Vault. O tema voltou aos holofotes em casos relevantes como o Cambridge Analytica e em marcos legais recentes o California Consumer Privacy Act.

Diante do espanto que os números de geofencing tem causado, inclusive em membros do Congresso Americano, é possível esperar julgamentos judiciais específicos revisitando o tema da expectativa de privacidade dos usuários diante da nova cultura de privacidade que tem se desenvolvido no país. Nesse sentido, a Suprema Corte decidiu, em 2018, no sentido de que é necessário mandado específico para obtenção de dados de conexão de dispositivos em estações rádio base próximas a cenas de crime por companhias de telecomunicações em *Carpenter v. Estados Unidos*.

²⁰² Dados obtidos pelo MP/RJ: i) de geolocalização dos usuários que estavam na noite de 2 de dezembro de 2018 nos arredores de onde foi visto pela última vez o carro usado pelos atiradores. Devem ser apresentadas informações coletadas em um período de 15 minutos; ii) Buscas no Google por sete palavras-chave ("Marielle Franco", "vereadora Marielle", "agenda Marielle", "agenda vereadora Marielle", "Casa das Pretas", "Rua dos Inválidos 122" e "Rua dos Inválidos") feitas por quaisquer usuários nos cinco dias antes da noite do crime. *UOL*. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/06/12/google-mp-stj-pode-julgar-em-agosto-disputa-pelos-dados-do-caso-marielle.htm> Acesso em: 16 jul. 2020.

²⁰³ Terceira Seção rejeita recurso da Google contra fornecimento de dados no caso Marielle Franco. *Superior Tribunal de Justiça*, 26 ago. 2020. Disponível em: <http://www.stj.jus.br/sites/portals/Paginas/Comunicacao/Noticias/26082020-Terceira-Seca-o-rejeita-recurso-da-Google-contr-fornecimento-de-dados-no-caso-Marielle-Franco.aspx#:~:text=%E2%80%8BPor%20maioria%2C%20a%20Terceira,Franco%20e%20de%20seu%20motorista%2C>. Acesso em: 14 set. 2020.

Na Europa, no contexto de combate ao terrorismo, intensificado após os atentados de Londres em 2005, foi editada a Diretiva 2006/24 (Diretiva de Retenção de Dados), obrigando companhias de telecomunicações a manter, por ao menos seis meses, os registros de dados pessoais de seus usuários para sua eventual utilização em investigações. Porém, esse impulso foi contido em razão da violação indiscriminada à privacidade de todos os seus cidadãos que a Diretiva de Retenção de Dados representava. Assim, em abril de 2014 a Diretiva foi invalidada pelo Tribunal de Justiça da União Europeia, com fundamento na proteção à privacidade, considerando que a investigação indiscriminada não pode prevalecer, mesmo quando objetiva combater infrações graves como o terrorismo. Ou seja, mesmo a grave ameaça representada pelo terrorismo foi insuficiente para justificar uma atuação de vigilância sobre todos os usuários de telecomunicações (*dragnet surveillance*).²⁰⁴

Sobre o tema, Stefano Rodota relaciona tal prática a instalação de chip em um produto, no caso o celular, que permita a localização das pessoas à semelhança de um “guizo eletrônico”, bem como o conflito desse sistema com a dignidade da pessoa, sendo que a conservação dessas informações e sua utilização para fins de segurança pública deve ser necessariamente motivada e circunscrita a determinado período:

O tema da localização e da possibilidade de mapear cada movimento das pessoas aponta assim para uma dimensão na qual a proteção de dados pode se cruzar com outros direitos fundamentais, invioláveis e indisponíveis. Isso quer dizer que nem mesmo o consentimento do interessado pode tornar legítima nem a inserção em seu corpo de um chip que permita seguir os seus movimentos, bem como o recurso a chips que, inseridos em um produto, tornem possível o controle dos comportamentos de quem o utiliza. O guizo eletrônico entra em conflito com a dignidade da pessoa.

A localização através do telefone exige que sejam feitas avaliações que partam destes mesmos princípios. Afastada qualquer utilização lesiva à dignidade ou que interfira flagrantemente na esfera privada alheia e mantidas as regras sobre o consentimento, deve-se ressaltar o reconhecimento do direito de não ser localizado, que permita evitar uma opressora forma de controle social, sem estigmatizações ou discriminações contra quem se utilize concretamente de tal direito.

Além disso, qualquer conservação, por um determinado período, dos dados de tráfego que impliquem na possibilidade de reconstruir os movimentos da pessoa, deve ser necessariamente motivada e circunscrita no tempo, com referências detalhadas às eventuais situações de emergência ou exigências de segurança.²⁰⁵

Cabe ressaltar que, de acordo com Lei nº 12.965/2014 (Marco Civil da Internet), o provedor de aplicações de internet, a exemplo do Google, deverá manter os registros de

²⁰⁴ ABRUSIO, Juliana et al. Dados de Geolocalização e a investigação do caso Marielle. *Conjur*, 07 jul 2020. Disponível em: <https://www.conjur.com.br/2020-jul-07/direito-digital-dados-geolocalizacao-investigacao-marielle?pagina=2>. Acesso em: 16 jul. 2020.

²⁰⁵ RODOTA, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 253.

acesso a aplicações de internet, pelo prazo de 6 (seis) meses (art. 15), no entanto, não traz a lei regras específicas acerca da abrangência do uso estatal, mediante autorização judicial, de tais dados no exercício do poder de polícia judiciária.

Dessa forma, mesmo que a Terceira Seção do Superior Tribunal de Justiça tenha enfrentado a questão do *geofencing* ou *busca reversa*, por ocasião do julgamento dos três recursos mandados de segurança impetrados pelo Google no caso Marielle Franco, é salutar que eventual legislação específica a ser formulada com fundamento no artigo 4º, §1º LGDP, visando regular o exercício de atividade onde a lei não se aplica, a exemplo do tratamento de dados em investigações criminais (artigo 4º, III, d), trate dessa prática de *geofencing* ou busca reversa, onde é realizado o tratamento de dados não só das vítimas do crime e dos investigados, mas também de terceiros de forma ostensiva com base em critérios de geolocalização.

3.7.3. Criptografia: julgamento do caso Whatsapp

O Supremo Tribunal Federal iniciou o julgamento da ADI nº 5527 e da ADPF nº 403, onde será definida a possibilidade de decisões judiciais autorizarem o bloqueio de serviços de mensagens pela internet, como o aplicativo WhatsApp, com fundamento nos artigos 10, § 2º e o art. 12, incisos III e IV da Lei nº 12.965/2014 (Marco Civil da Internet).

Votaram até então a Ministra Rosa Weber (Relatora da ADI nº 5527) e o Ministro Edson Fachin (Relator da ADPF nº 403), sendo o processo retirado de pauta em razão do pedido de vista do Ministro Alexandre de Moraes. Os votos de ambos os Ministros Relatores convergem para o entendimento de afastar interpretação as regras do Marco Civil da Internet que viabilizem o acesso, por determinação judicial, do conteúdo das mensagens protegidos pela criptografia. Nesse sentido, é o trecho abaixo do voto do Ministro Edson Fachin:

Sexta: Na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações. A criptografia, em especial, é um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública.

Sétima: É contraditório que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas.

A criptografia é um modelo que tem como objetivo assegurar o sigilo das comunicações, sendo que a controvérsia acerca desse sistema reside no fato de que pode ser utilizado para o emprego de dificultar o acesso a provas e evidências de crimes. No entanto, conforme assinala Thiago Luís Santos Sombra, é “consenso entre as empresas de tecnologia, representantes da sociedade civil, órgãos públicos e comunidade acadêmica que a criptografia também é responsável por proteger milhões de pessoas contra roubos, fraudes e outros atos criminosos”.²⁰⁶

O julgamento no STF da ADI nº 5527 e da ADPF nº 403 acerca da obrigatoriedade dos aplicativos de mensagens disponibilizarem, mediante ordem judicial, acesso a conteúdo protegido pela criptografia sob pena de bloqueio, apenas se iniciou e há a possibilidade do entendimento manifestado nos votos dos referidos Ministros Relatores serem alterados ao seu final, no entanto, mencionados votos evidenciam uma preocupação com a criptografia das mensagens, sob o fundamento de se tratar de um meio de garantir a segurança na internet, prevalecendo tal interesse em detrimento das atividades de investigação criminal.

3.8. Conclusão

As exceções à aplicação da LGPD à Administração Pública previstas no artigo 4º, III da LGPD, notadamente o tratamento de dados realizado para o fim de segurança pública, defesa nacional, segurança do estado ou em atividades de investigação e repressão de infrações penais, é efetivado no exercício de denominado poder de polícia que, segundo Celso Antônio Bandeira de Mello, constitui manifestação da “atividade estatal de condicionar a liberdade e a propriedade ajustando-as aos interesse coletivos”.

²⁰⁷

Deve ser ressaltado que não houve a concretização legislativa a priori de um interesse público, mas sim a compatibilização com os direitos inerentes à privacidade com assento constitucional no artigo 5º, X da CF, pois, a par do artigo 4º, III prever a não aplicação da LGPD ao Poder Público no tratamento de dados realizados para as

²⁰⁶ SOMBRA, Thiago Luís Santos. *Fundamentos da Regulação da Privacidade e Proteção de Dados Pessoais*. São Paulo: Revista dos Tribunais, 2019, p. 161.

²⁰⁷ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016, p. 851.

finalidades mencionadas, limitou essa prerrogativa às regras aplicáveis, ao princípio constitucional do devido processo legal e aos princípios gerais de proteção de dados previstos na LGPD (artigo 4º, §1º), além de ter imposto restrição ao tratamento por pessoas jurídicas de direito privado (artigo 4º, §§2º e 4º da LGPD) e fixado competência fiscalizatória à Autoridade Nacional de Dados Pessoais (ANDP) no exercício desta atividade pelo Poder Público.

A questão da abrangência da competência fiscalizatória e sancionatória da ANPD em relação à Administração Pública, quando se tratar de operações de tratamento de dados nas atividades inerentes a Segurança Pública e Defesa Nacional (art. 4º, III), certamente vai suscitar questionamentos, no entanto, a sujeição do Estado ao poder sancionatório do regulador, mesmo nas hipóteses descritas, atende aos reclamos do Estado Democrático de Direito à luz dos seus fundamentos e objetivos que se extraem dos artigos 1º e 3 da CF de 1988, quais sejam, o dever de transparência e prestação de contas pelo Poder Público, de forma a evitar violações de direitos e o “surgimento das zonas francas, livres de qualquer controle”.²⁰⁸

²⁰⁸ RODOTA, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 149.

4. Da aplicação da LGPD ao Poder Público

O artigo 23 da LGPD prevê que o tratamento de dados pelo Poder Público é realizado no âmbito das pessoas jurídicas de direito público, previstas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação):

Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

Parágrafo único. Subordinam-se ao regime desta Lei:

I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;

II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Verifica-se que a LGPD se aplica à Administração Pública Direta e Indireta, abrangendo os órgãos integrantes da Administração centralizada, unidas pelo liame da hierarquia, bem como as entidades constituídas e mantidas pelo Poder Público que sobre elas exerce o controle.²⁰⁹ Os diversos órgãos e entidades da Administração mantêm uma série de banco de dados potencialmente sensíveis, os quais se submetem às regras e princípios da LGPD, a exemplo dos programas de Nota Fiscal, Bilhete Único do transporte Público, prontuários médicos do sistema público de saúde.²¹⁰

4.1. Administração Direta

O artigo 1º, parágrafo único, inciso I da Lei 12.527/2011 prevê que a lei se aplica aos “*órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público*”. Desta feita, segundo se verifica do mencionado dispositivo, a LGPD se aplica à Administração Direta em seus diversos níveis.

Segundo prevê o Decreto-Lei nº 200, de 25.02.1967, a Administração Direta é constituída “dos serviços integrados na estrutura administrativa da Presidência da

²⁰⁹ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 154-155.

²¹⁰ TASSO, Fernando Antonio. Lei Geral de Proteção de Dados Comentada. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 72.

República e dos Ministérios” (art. 4º, I), sendo a Administração indireta compreendida pelas “seguintes categorias de entidades dotadas de personalidade jurídica própria: a) Autarquias; b) Empresas Públicas; c) Sociedades de Economia Mista; d) Fundações Públicas (art. 4º, II)”. Segundo Celso Antonio Bandeira de Mello, o critério da classificação levada a efeito pelo mencionado decreto foi o orgânico ou subjetivo, considerando os sujeitos integrantes do aparelho estatal, independente da natureza das atividades e do regime jurídico que lhe corresponda, o que acabou por excluir, por exemplo, os delegados dos ofícios públicos (servidores notariais, registros de nascimento, de óbito e casamentos).²¹¹

O decreto-lei 200/67, embora aplicável a priori à União, contém conceitos princípios que, com ressalvas doutrinárias, se “incorporaram aos Estados e Municípios” que admitem as mesmas entidades como integrantes da Administração Indireta, bem como considerando o tratamento dado ao tema pela CF de 1988.²¹²

O Estado quando desempenha ele próprio as atividades, estará atuando de forma centralizada, repartindo no seu interior os encargos de sua alçada em diferentes órgãos das diversas pessoas políticas do Estado (União, Estados, Distrito Federal e Municípios) que, segundo Celso Antonio Bandeira de Mello, constituem “unidades abstratas que sintetizam os vários círculos de atribuições do Estado”, exercido pelos “agentes investidos dos correspondentes poderes funcionais, a fim de exprimir na qualidade de titulares deles, a vontade estatal”.²¹³

Assim, é de se sentir o impacto da LGPD em relação à Administração Direta, pois, aplicável a todos os entes políticos (União, Estados, Distrito Federal e Municípios) que, em seus diversos órgãos e por meio de seus agentes públicos realizem tratamento de dados pessoais para consecução de suas competências públicas.

4.1.1. Da aplicação aos Poderes Legislativo, Tribunal de Contas, Judiciário, Ministério Público e Defensoria Pública

²¹¹ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 156-159.

²¹² PIETRO, Maria Sylvia Zanella Di. *Direito Administrativo*. 23. ed. São Paulo: Editora Atlas, 2009. p. 58.

²¹³ MELLO, Celso Antônio Bandeira de. *Apontamentos sobre os agentes e órgãos públicos*. 4. ed. São Paulo: Revista dos Tribunais, 1984. p. 69.

A LGPD faz menção ao artigo 1º da Lei 12.527/2011 (Lei de Acesso à Informação) para definir seu campo de aplicação em relação ao Poder Público, sendo que artigo 1º, parágrafo único, inciso I desta lei prevê sua incidência não só aos órgãos públicos integrantes da Administração Direta do Poder Executivo, como também aos órgãos integrantes do “*Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público*”.

Deve ser ressaltado o lapso do legislador ao não incluir a Defensoria Pública no rol das demais instituições permanentes e autônomas, na denominada Lei de Acesso à Informação.

Tal equívoco deve ser creditado ao fato da Lei nº 12.527, de 18 de novembro de 2011 ser anterior a Emenda Constitucional nº 80, de 04 de junho de 2014 que alterou o artigo 133 da CF de 1988 para prever a Defensoria Pública como instituição permanente, sendo-lhe aplicado o mesmo tratamento dispensado ao Poder Judiciário, tanto no que respeita a estrutura da carreira (art. 93), a iniciativa legislativa para tratar de cargos e remunerações (art. 96, II), sendo princípios institucionais a “unidade, a indivisibilidade e a independência funcional”.

Nada obstante o lapso legal, é fora de dúvidas que tanto a LAI quanto a LGPD se aplicam à Defensoria Pública, tendo em vista que eventual exclusão desta instituição da incidência da lei não se coaduna com os princípios republicanos extraídos da Constituição Federal, especialmente o da transparência (inciso XXXIII do art. 5º, inciso II do § 3º do art. 37 e § 2º do art. 216 da Constituição Federal), notadamente se levarmos em conta que esta instituição realiza o tratamento de dados de membros, servidores e usuários do serviço.

4.2. Serviços notariais e de registro

A LGPD previu sua aplicação aos serviços notariais e de registros “exercidos em caráter privado, por delegação do Poder Público”, os quais terão o mesmo tratamento atribuído a Administração Pública²¹⁴.

²¹⁴ Art. 23:

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Os serviços notariais e de registro, exercidos em caráter privado por delegação do Poder Público nos termos do artigo 236 da CF de 1988, a par de não consistir serviço público conforme definido pelo Supremo Tribunal Federal na ADI nº 3.643, Relator Ministro Ayres Britto, constitui “atividades tidas como função pública *lato sensu*, a exemplo das funções de legislação, diplomacia, defesa nacional, segurança pública, trânsito, controle externo e tantos outros cometimentos”, estando sujeito a um regime jurídico de direito público, de tal forma que a LGPD atribuiu aos serviços notariais e de registro o mesmo tratamento conferido as pessoas jurídicas de direito público.²¹⁵

4.3. Administração Indireta

A LGPD consoante, prevê seu artigo 23, se aplica às “as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.”²¹⁶

Maria Sylvia Zanella Di Pietro destaca que a descentralização só ocorre quando o poder público destaca um serviço público que é de sua atribuição, transferindo-o por meio da descentralização a outra entidade com personalidade jurídica própria. Quando a atuação estatal não se restringir a serviços públicos, mas ingressar nas atividades conferidas à iniciativa privada, tal atuação no domínio econômico não se fundamenta no fenômeno da descentralização, mas na atividade de intervenção direta na economia por meio de empresas estatais.²¹⁷

Dessa forma, por Administração Indireta, nos termos do art. 4º do Decreto-Lei nº 200/67, temos o “conjunto de pessoas jurídicas, de direito público ou privado, criadas ou autorizadas por lei, para o desempenho de atividades assumidas pelo Estado, como serviços públicos ou a título de intervenção no domínio econômico”.²¹⁸ Segundo Maria Sylvia Zanella Di Pietro integra a Administração Indireta “as autarquias, as fundações instituídas pelo Poder Público, as sociedades de economia mista, as empresas públicas e os consórcios públicos”.²¹⁹

²¹⁵ BRASIL. Supremo Tribunal Federal. ADI nº 3.643, Rel. Ministro Ayres Britto, julgamento em 08 nov 2006.

²¹⁶ Artigo 1º, parágrafo único, inciso II da Lei 12.527/2011.

²¹⁷ PIETRO, Maria Sylvia Zanella Di. *Direito Administrativo*. 23. ed. São Paulo: Editora Atlas, 2009. p. 418.

²¹⁸ *Idem*, p. 419.

²¹⁹ *Idem*, p. 419.

Deve ser consignado que as Agências Reguladoras são espécies do gênero autarquias, consistindo em autarquias especiais, cuja distinção é materializada em um traço maior de autonomia das Agências em relação ao poder central.²²⁰

Os consórcios públicos, por sua vez, também integram conceito de Administração Indireta, pois, o artigo 6º da Lei nº 11.107/2005 dotou esse acordo de vontade entre os entes políticos de personalidade jurídica, de forma que lhe é aplicável as disposições da LGPD por incidir sobre “entidades controladas diretamente ou indiretamente pela União, Estados, Distrito Federal e Municípios”.

4.3.1. Aplicação da LGPD em relação às empresas estatais

O artigo 24 da LGPD prevê que as empresas estatais (empresa pública e sociedade de economia mista) que integram que atuam em regime de concorrência, nos termos do artigo 173 da CF de 1988, estão sujeitos ao regime jurídico aplicável as empresas integrantes do setor privado, enquanto que o parágrafo único do mencionado dispositivo determina que as empresas estatais que operacionalizam “políticas públicas” terão o mesmo tratamento dispensado pessoas jurídicas de direito público.

Com relação às empresas públicas e as sociedades de economia mista, seus regimes jurídicos diferem pela textura das atividades que são afetadas. Nesse sentido, de rigor a menção à distinção realizada por Celso Antonio Bandeira de Mello acerca da distinção entre as estatais que exploram atividade econômica e que prestam serviços públicos:

No primeiro caso, é compreensível que o regime jurídico de tais pessoas seja o mais próximo possível daquele aplicável à generalidade das Pessoas de Direito Privado. Seja pela natureza do objeto de sua ação, seja para prevenir que desfrutem de situação vantajosa em relação às empresas privadas – às quais cabe a senhoria no campo econômico -, compreende-se que estejam, em suas atuações, submetidas a uma disciplina bastante avizinhada da que regula as entidades particulares de fins empresariais. Daí haver o texto constitucional estabelecido que em tais hipóteses regular-se-ão pelo regime próprio das empresas privadas (art. 173, § 1º).

(...)

No segundo caso, quando concebidas para prestar serviços públicos ou desenvolver quaisquer atividades de índole pública propriamente (como promover a

²²⁰ Lei nº 13.848/2019: Art. 3º A natureza especial conferida à agência reguladora é caracterizada pela ausência de tutela ou de subordinação hierárquica, pela autonomia funcional, decisória, administrativa e financeira e pela investidura a termo de seus dirigentes e estabilidade durante os mandatos, bem como pelas demais disposições constantes desta Lei ou de leis específicas voltadas à sua implementação.

realização de obras públicas), é natural que sofram o influxo mais acentuado de princípios e regras de Direito Público, ajustados, portanto, ao resguardo de interesses desta índole.²²¹

Seguindo a mesma lógica, Maria Sylvia Zanella entende que quando se trata de atividade econômica exercida pelo Estado com fundamento no artigo 173 da CF/88, haverá uma sujeição ao regime de direito privado, enquanto que na hipótese da estatal realizar a gestão privada do serviço público, aplica-se o regime jurídico de Direito Público, ressaltando que outra solução não seria possível, considerando que alguns princípios são inatos à noção de serviço público, tais como predominância do interesse público, igualdade de tratamento entre os usuários e continuidade do serviço público.²²²

O Supremo Tribunal Federal, por sua vez, possui entendimento consolidado no sentido de que as empresas estatais que explorem atividade econômica, nos termos do artigo 173 da CF de 1988, estão sujeitas ao regime jurídico próprio das empresas privadas, não se beneficiando de prerrogativas específicas do regime de Direito Público, a exemplo do regime de precatórios previsto no artigo 100 da CF, de forma que o § 1º do art. 173 se restringe as estatais desenvolvem atividade econômica não se aplicando as prestadoras de serviços públicos ou que exerçam atividades de natureza pública.²²³²²⁴

Dessa forma, a LGPD está alinhada com os ditames da Constituição (art. 173), bem como a posição doutrinária e jurisprudencial, ao prever que a distinção entre os regimes jurídicos de proteção de dados entre as estatais que exploram atividade econômica e as que prestam serviço público.

4.3.2. Especificidades da proteção de dados das estatais que prestam serviço público

O parágrafo único do artigo 24 da LGPD prevê que as empresas públicas e as sociedades de economia mista, “quando estiverem operacionalizando políticas públicas e no âmbito da execução delas”, terão o mesmo tratamento dispensado pela lei às pessoas jurídicas de Direito Público.

²²¹ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 203.

²²² PIETRO, Maria Sylvia Zanella Di. *Direito Administrativo*. 23. ed. São Paulo: Editora Atlas, 2009. p. 418.

²²³ BRASIL. Supremo Tribunal Federal. ADI nº 1.642, Rel. Ministro Eros Grau, julgamento em 03 abr. 2008.

²²⁴ BRASIL. Supremo Tribunal Federal. RE nº 599.628 (Tema 253), Rel. Ministro Ayres Britto, julgamento em 11 mar. 2010.

O mencionado dispositivo da LGPD atribui às estatais o tratamento conferido às pessoas jurídicas de Direito Público, quando estas estiverem atuando sob o enfoque de uma política pública, restringindo tal tratamento aos limites de execução desta atividade.

Cabe registrar que políticas públicas sempre foram vinculadas ao surgimento do Estado social, consistindo em prestações positivas para realização de interesses socioeconômicos que, por sua vez, impôs uma nova ordem de competências ao Estado mediante assunção de funções e finalidades específicas para implementação dos direitos sociais. Segundo Maria Paula Dallari Bucci:

O fundamento mediato das políticas públicas, o que justifica o seu aparecimento, é a própria existência dos direitos sociais – aqueles, dentre o rol de direitos fundamentais do homem, que se concretizam por meio de prestações positivas do Estado. Enquanto os direitos individuais, ditos direitos fundamentais de primeira geração, consistem em liberdades, os direitos sociais, ditos de segunda geração, consistem em poderes, que “só podem ser realizados se for imposto a outros (incluídos aqui os órgãos públicos) um certo número de obrigações positivas.”²²⁵

As políticas públicas são instrumentos de ação dos governos, a expressão dos direitos socioeconômicos, consistindo no modo de agir ordenado do Estado e se aproximando a ideia de plano, programa de ação governamental para realização de objetivos determinados num espaço de tempo certo, um processo político de escolha de prioridades do governo em termos de objetivos e procedimentos, dentro da atividade técnica de planejamento da ação estatal. Nesse sentido:

Veja que políticas públicas não se confunde com o próprio direito social em si. É, na verdade, um programa de governo para se alcançar a efetivação desse direito. Nesse diapasão, a Constituição Federal já fixou as políticas públicas prioritárias que devem ser implementadas pelo Executivo e pelo Legislativo, aos quais resta apenas a discricionariedade de meios.²²⁶

O serviço público é, ao fim e ao cabo, a materialização de uma determinada política pública à coletividade, é o modo como o Poder Público implementa concretamente uma dada utilidade aos administrados, definida previamente por uma política pública espelhada em um programa de ação governamental, criado com o objetivo de garantir

²²⁵ BUCCI, Maria Paula Dallari. *Políticas públicas e direito administrativo*. Revista de informação legislativa, v. 34, n. 133, jan./mar. 1997, p. 90.

²²⁶ BISSOLI, Livia Regina Sa vergnini. Políticas Públicas como Programas e Ações para o Atingimento dos Objetivos Fundamentais do Estado. In: GRINOVER, Ada Pelegrine; WATANABE, Kazuo. *O controle jurisdicional de políticas públicas*. 2. ed. Rio de Janeiro: Forense, 2013.

determinada comodidade aos usuários do serviço. O conceito de serviço público formulado por Celso Antonio Bandeira de Mello se alinha à conclusão levada a efeito:

Serviço Público é toda atividade de oferecimento de utilidade ou comodidade material destinada a satisfação da coletividade em geral, mas fruível singularmente pelos administrados, que o Estado assume como pertinente a seus deveres e presta por si mesmo ou por quem lhe faça as vezes, sob um regime de Direito Público – portanto, consagrador de prerrogativas de supremacia e de restrições especiais - instituído em favor dos interesses definidos no sistema normativo.²²⁷

Dessa forma, quando determinada empresa pública ou sociedade de economia mista “estiverem operacionalizando políticas públicas”, com vistas a prestação de um dado serviço público, receberão o mesmo tratamento dispensado pela LGPD às pessoas jurídicas de Direito Público.

A questão que se coloca é: qual será o regime de tratamento de dados de uma determinada estatal quando realizar ambas as atividades, ou seja, quando sua atividade represente intervenção no domínio econômico e, em algumas situações, a prestação de um serviço público?

Explica-se exemplificando com o caso da Empresa Brasileira de Correios e Telégrafos (ECT): O Supremo Tribunal Federal definiu por ocasião do julgamento da ADPF nº 46 que o monopólio definido pela Lei nº 6.538/76 no que respeita ao envio de carta, o que abrange cartas pessoais e comerciais, cartões-postais, correspondências agrupadas (malotes), consiste em uma prestação de serviço público, sendo que as demais atividades relativas ao envio outros tipos de correspondências e encomendas caracteriza atividade econômica, que pode ser exercida em regime concorrencial com as empresas integrantes do setor privado.

Nessa hipótese, o fato dos Correios prestarem serviço público no que toca apenas a uma parcela de sua atividade, relativa ao envio de cartas, mas possuem para além desta atividade, serviços onde concorre diretamente com a iniciativa privada, a exemplo do serviço de entrega, vai ensejar questionamentos acerca do regime jurídico de dados aplicável a entidade, se o incidente sobre as pessoas jurídicas de direito público ou as aplicáveis ao setor privado.

A incidência linear do regime de proteção de dados aplicável as entidades de Direito Público aos Correios, tanto em relação às atividades que integram a prestação de serviço

²²⁷ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 699.

público (cartas), quanto às que caracterizam atividade econômica (serviço de entrega), poderia ensejar privilégios não extensíveis ao setor privado, a exemplo da dispensa do consentimento do titular de dados para o seu tratamento prevista no artigo 7º, III, da LGPD, o que não se aplica ao setor privado que demanda consentimento do titular para o tratamento de seus dados (art. 7º, I), o que representaria, em tese, uma violação ao artigo 173 da Constituição Federal, tendo em vista prejudicar a livre concorrência.

A solução preconizada por autores como Fernando Antonio Tasso, Marcio Cots e Ricardo Oliveira nessa hipótese, seria o mapeamento e a segregação da base de dados, dispensando o tratamento jurídico aplicável a entidade de Direito Público àquela que realiza o tratamento correspondente a prestação de serviços, bem como o tratamento aplicável ao setor privado a base de dados correspondentes às atividades que consistam em intervenção na atividade econômica.²²⁸²²⁹

Dessa forma, o regime jurídico aplicável a LGPD as empresas públicas e sociedades de economia mista está condicionado a atividade à qual está afetada determinada entidade, sendo que a incidência das regras inerentes às pessoas jurídicas de Direito Público ocorrerá sob a fórmula de “se e quando” estas “estiverem operacionalizando políticas públicas”, posto se tratar de um regime com privilégios específicos não extensíveis ao setor privado.

4.4. Regime jurídico do tratamento dados pelo Poder Público

4.4.1 Prerrogativa: desnecessidade de obtenção do consentimento do titular para o tratamento de dados

O Poder Público no atual momento histórico é responsável pela gestão de uma série de banco de dados, sendo que o tratamento de dados para fins de políticas públicas é realizado massivamente em programas de governos, como o Bolsa Família, Bilhete Único de transporte público, o próprio recenseamento, sendo que a operação de tratamento de dados pelo Poder Público, o que conforme o artigo 5º, X da LGPD abrange a coleta e a

²²⁸ TASSO, Fernando Antonio. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 269.

²²⁹ COTS, Marcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais Comentada*. 3. ed. São Paulo: Revista dos Tribunais, 2019. p. 71.

classificação destes dados, que é feito em escala, recebeu da lei uma sistematização própria.²³⁰²³¹

O regime jurídico do tratamento de dados conferido pela LGPD ao setor público, o que como visto abrange a Administração direta e indireta, esta última restrita às estatais prestadoras de serviço público, bem como os serviços notariais e de registro, possui privilégios específicos, especialmente a dispensa do consentimento do seu titular, lógica que se aplica não só em relação aos dados pessoais (art. 7º, II), como também em relação aos dados sensíveis (art. 11, II, b) dos administrados, sendo que estes últimos correspondem a uma espécie de dados que gozam de especial proteção por dizer respeito a aspectos específicos da privacidade do seu titular (art. 5º, II).²³²

Na hipótese de tratamento de dados pela Administração, o que supõe ser realizado no contexto específico da realização de uma política pública por prescindir de consentimento do titular, havia a contrapartida materializada no § 1º do artigo 7º da LGPD da Administração informar ao titular as hipóteses em que ocorre o tratamento de seus dados, cuja forma de disponibilização de tais informações poderiam ser especificadas pela ANPD (§2º do artigo 7º). Ocorre que tais dispositivos foram revogados pela MP nº 860/2018, convertida na Lei nº 13.853/2019.

Dessa forma, o tratamento de dados pela Administração, tanto os pessoais quanto os sensíveis, não está condicionado a obtenção do consentimento do titular, ao contrário da regra aplicável ao setor privado, nada obstante assegurados os demais direitos do titular, como o direito de acesso ao processo de tratamento e correção dos dados previsto nos artigos 9º e 18 da LGPD.

De qualquer forma, não é pouco o privilégio de isentar a Administração da necessidade de obter o consentimento do titular para operações de tratamento de seus dados, pois, o instituto do consentimento integra o conceito da autodeterminação informativa que é um dos objetivos da LGPD, cuja finalidade é permitir ao titular um

²³⁰ Art. 5º. X - tratamento: 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;

²³¹ TASSO, Fernando Antonio. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais. 2019. p 269.

²³² Dado pessoal sensível: Art. 5º. II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

poder real de controle acerca dos seus dados.²³³ Sobre o direito da autodeterminação informativa:

O notório conceito do “direito de estar só”, o direito à vida privada atribuído à elaboração de Warren e Brandeis (mas na verdade, adverte o autor, concebido por Robert Kerr quarenta anos antes), é qualitativamente diferente da privacidade como “direito à determinação informativa”, o qual concede a cada um de nós um real poder sobre nossas próprias informações, nossos próprios dados”. Percebe-se aqui, segundo Rodotà, um ponto de chegada na longa evolução do conceito de privacidade, da originária definição – *the right to be alone* – ao direito de manter o controle sobre as informações e de determinar as modalidades de construção da própria esfera privada. Visto desta maneira, configura-se o direito à privacidade como um instrumento fundamental contra a discriminação, a favor da igualdade e da liberdade. De fato, nas sociedades da informação, como são as sociedades em que vivemos, pode-se dizer que “nós somos as nossas informações”, pois que elas nos definem, nos classificam, nos etiquetam; portanto, ter como controlar a circulação e saber quem as usa significa adquirir, concretamente, um poder sobre si mesmo.²³⁴

Assim, a LGPD assegura à Administração Pública a prerrogativa de proceder ao tratamento de dados dos administrados, tanto os pessoais quanto os sensíveis, sem a necessidade de obtenção de prévio consentimento do titular, fundado na circunstância do Poder Público gerir dados em escala nos diversos programas governamentais. No entanto, tal prerrogativa não afasta os demais direitos do titular dos dados, como o acesso ao processo de tratamento e a correção dos dados previsto nos artigos 9º e 18 da LGPD.

4.4.2. Condicionamentos: cumprimento dos pressupostos previstos na LGPD

4.4.3. A busca do interesse público no tratamento de dados pelo Poder Público

O artigo 23 da LGPD prevê alguns pressupostos para o tratamento de dados pelo Poder Público, de forma que possa usufruir das prerrogativas tratadas anteriormente, notadamente “o atendimento de sua finalidade pública, na persecução do interesse

²³³ Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa.

²³⁴ BODIN, Maria Cecília. Apresentação do autor e da obra. In: RODOTA, Stefano. *A vida na sociedade da vigilância* - a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.07.

público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”.²³⁵

O mencionado dispositivo condiciona o tratamento de dados pelo Poder Público, ao atingimento do “interesse público” que determinou tal operação de coleta e classificação dos dados, dentro de uma política pública que lhe dê suporte. Nesse ponto, retorna-se à discussão recente e que está longe de ser definida acerca do sentido e alcance da expressão que corresponde a um princípio do Direito Público.

Autores como Daniel Sarmiento, Gustavo Binbenbajt, Humberto Ávila rejeitam a ideia de supremacia do interesse público qualificado como um princípio, sob uma suposta ausência de normatividade e elevado grau de indeterminação, bem como sua hipotética posição de supremacia a priori em relação a outros princípios igualmente importantes que consagrariam direitos fundamentais e que, numa relação de conflito, seriam automaticamente sacrificados sem levar em conta os interesses levados a efeito por estes últimos. Dentro dessa lógica, a alternativa dos mencionados autores seriam a ponderação entre interesses públicos e privados, com fundamento no princípio da proporcionalidade e na sistematização das normas constitucionais.²³⁶

Apesar do esforço dos mencionados autores, deve ser respeitado o posicionamento de Celso Antonio Bandeira de Mello que considera ser o princípio da supremacia do interesse público um princípio geral de Direito, pressuposto do convívio social, com aplicações concretas no texto constitucional, a exemplo do instituto da desapropriação, representando a possibilidade do Poder Público constituir restrições a terceiros nos termos da lei, fundado em uma lógica de dever, como o meio indispensável a realização da finalidade determinada pelo exercício da função pública delimitada pela Constituição. Assim, age o Poder Público sob o influxo do interesse público em nome da coletividade e não da entidade governamental em si (interesse público primário), o qual deve se concretizar “na extensão e na intensidade proporcionais ao que seja irrecusavelmente requerido para o atendimento do escopo legal a que estão vinculados”.²³⁷

²³⁵ Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

²³⁶ SARMENTO, Daniel. Interesses Públicos vs. Interesses Privados na Perspectiva da Teoria e da Filosofia Constitucional. In: SARMENTO, Daniel (Org.). *Interesses Públicos versus Interesses Privados: Desconstruindo o Princípio da Supremacia do Interesse Público*. 2.ed. Rio de Janeiro: Lumen Juris, 2007.

²³⁷ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p. 99-102.

No caso em questão, não identifica-se o interesse público como um princípio prevalente a priori, mas na intensidade proporcional que a lei lhe atribuiu nas mais diversas situações, como efetivamente verifica-se na LGDP que, a par de prever uma prerrogativa a Administração de tratar dados sem a necessidade de autorização de seus titulares, com fundamento na supremacia do interesse público, limitou ou restringiu tal prerrogativa ao tratamento de dados necessários ao atingimento dos interesses públicos qualificados pela política pública que dê suporte a essa operação de tratamento.

Assim, ao atribuir à Administração a prerrogativa de realizar operações de coleta e classificação de dados (tratamento de dados), sem o consentimento de seus titulares, para sua utilização em bancos de dados públicos dentro de políticas públicas governamentais, a exemplo da assistência social (Bolsa Família) e dos transportes (Bilhete Único), visou o legislador o interesse público qualificado como um interesse da coletividade, objetivando *a contrario sensu* que o tratamento de dados pela Administração não seja realizado em desvio de finalidade, seja para fins contrários a lei ou para obtenção de vantagens privadas pelo gestor público.

4.4.4. Dever de informação e prestação de contas

Além de prever que a operação de tratamento de dados pelo Poder Público deve observar o interesse público, qualificado pela política pública que lhe dê suporte, determinou o artigo 23: (i) a obrigação da Administração informar as hipóteses em que realiza tratamento de dados; bem como (ii) a indicação de um encarregado pelo tratamento.²³⁸

Quanto à obrigação da Administração informar as hipóteses em que realiza tratamento de dados, já foi mencionado que a MP nº 860/2018 convertida na Lei nº 13.853/2019, revogou o §1º do artigo 7º da LGPD que previu a obrigação do Poder Público informar ao titular as hipóteses em que ocorre o tratamento de seus dados. Dessa

²³⁸ Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e

forma, segundo previsto no artigo 23, §1º da LGPD, a Administração não está obrigada a informar ao titular, de forma individual, acerca da operação de tratamento realizados pontualmente, mas tem o dever de informar, de forma geral, as hipóteses em que realiza o tratamento, com informações claras acerca da previsão legal, finalidade e procedimentos, em veículo de fácil acesso.

Cabe ressaltar que compete à ANPD dispor sobre as formas de publicidade das operações de tratamento pela Administração Pública.

Prevê a lei, também, como um pressuposto a operação de tratamento de dados, a indicação de um encarregado de dados (artigo 23, III), figura que a lei atribui a responsabilidade de atuar como canal de comunicação entre o agente de tratamentos (Poder Público), os titulares dos dados e ANPD (art. 5º, VIII), com a atribuição de receber reclamações, prestar esclarecimentos, orientar servidores a respeito de práticas a serem adotadas em relação à proteção dos dados pessoais (art. 41), obrigação que pode ser dispensada pela ANPD considerando o porte da entidade e o volume de tratamento de dados realizado (3º do artigo 41).

A LGPD prevê, assim, condições para o tratamento de dados como a obrigação de informar as hipóteses em que este é realizado, em nome do princípio da transparência, bem como a necessidade de indicar um encarregado de dados com a função de prestar contas a ANPD e aos titulares acerca dos dados objeto tratamento, com vistas a assegurar a concretização do interesse público que determinou sua realização, sendo que, para além destes pressupostos, deve a Administração observar a legislação esparsa, os princípios aplicáveis à Administração Pública e os princípios setoriais da proteção de dados.

4.5. Diplomas legais e Princípios aplicáveis ao Poder Público

A LGPD condiciona o tratamento de dados pelo Poder Público a (i) observância do interesse público subjacente a política pública que determinou sua coleta e classificação; (ii) informar ostensivamente as hipóteses em que os dados são tratados; e (iii) indicar um encarregado para prestação de contas a coletividade e à ANPD.

A par destas condições impostas pela LGPD, está a Administração sujeita também as legislações que a antecederam e que tem repercussão na proteção de dados pessoais, conforme previsto no § 3º do seu artigo 23 que, de forma exemplificativa, cita a Lei do Habeas Data, Lei do Processo Administrativo federal, e Lei de Acesso à Informação. Além das mencionadas legislações, cita-se também, conforme verificado em capítulo

próprio deste estudo, a Lei dos Arquivos Públicos, o Marco Civil da Internet, a Lei Geral de Telecomunicações, Lei de Interceptações Telefônicas e Lei das Organizações Criminosas, considerando trazer aplicações relacionadas a dados pessoais e o seu tratamento pelo Poder Público.

A Administração deve, para além e inclusive no exercício das atividades relacionadas ao tratamento de dados pessoais, obedecer aos princípios constitucionais que vinculam sua atuação, notadamente os previstos no artigo 37 da CF de 1988, saber: legalidade, impessoalidade, moralidade, publicidade e eficiência, além dos princípios implícitos da supremacia do interesse público, finalidade, razoabilidade, proporcionalidade, motivação, devido processo legal e ampla defesa, da responsabilidade por atos administrativos, boa administração e, finalmente, da segurança jurídica.²³⁹

Por fim, adicionalmente aos princípios constitucionais que direcionam a atuação administrativa de uma forma geral, no exercício de atividades de tratamento de dados, o Poder Público deve observar os princípios setoriais aplicáveis à proteção de dados previstos no artigo 6º da LGPD, notadamente: os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Assim, a prerrogativa atribuída à Administração para tratar dados pessoais e sensíveis sem a necessidade de autorização prévia do seu titular (artigos 7º, III e 11, II, b), é delimitada pela atribuição de encargos correspondentes, com vistas a concretização do interesse público com a máxima realização dos direitos individuais, manifestada nas seguintes condicionantes: (i) exercer tal mister nos limites do interesse público que determinou o tratamento de dados; (ii) informar ostensivamente as hipóteses em que os dados são tratados; (iii) indicar um encarregado para prestação de contas a coletividade e à ANPD; (iv) cumprir as legislações setoriais aplicáveis; (v) observar os princípios constitucionais que vinculam sua atuação e; (vi) os princípios da proteção dos dados pessoais previstos no artigo 6º da LGPD.

4.5.1. Lei de acesso à informação e eventual conflito com a LGPD

A Lei nº 12.527/2011 conhecida como Lei de Acesso à Informação, foi editada com a finalidade de garantir o direito fundamental de acesso à informação deduzido no inciso

²³⁹ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016. p.98-128.

XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

A Lei de Acesso à Informação disciplina: seu âmbito de aplicação (parágrafo único do artigo 1º); diretrizes do direito de acesso à informação, a conceituação de institutos dentre os quais se destaca o tratamento de informações (art. 4º, V); aspectos procedimentais como a gratuidade do procedimento e os recursos cabíveis (arts. 12 e 15); as regras inerentes ao sigilo da informação, com a classificação dos graus de sigilo e seus prazos máximos (art. 24); tratamento de informações sigilosas por particulares (art. 26, parágrafo único); regras relacionadas as informações pessoais e exceções para o seu tratamento pelo Poder Público (art. 31); e responsabilidades dos agentes públicos e privados pela inobservância da lei (arts. 32 e 33).

Destaca-se na Lei de Acesso à Informação o artigo 3º, I que prevê a transparência das informações como regra e o sigilo como exceção, com o objetivo de promover o controle social da Administração Pública, em linha com os comandos constitucionais mencionados anteriormente e que fundamentam sua criação.

O sigilo levado a efeito na Lei de Acesso à Informação se restringe as informações pertinentes à segurança da sociedade ou do Estado (art. 23), bem como as informações pessoais previstas no artigo 31 que prevê que o “tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.”

No que respeita as informações pessoais, a Lei de Acesso à Informação tratou o tema genericamente, sem apresentar uma distinção criteriosa no sentido de especificar quais dados pessoais estariam especialmente abrangidos, circunstância que trouxe dificuldades aos agentes públicos na compreensão do que efetivamente caracteriza dados pessoais, conforme verifica-se no acórdão 2906-2016 TCU:

274. Um deles se refere ao marco regulatório de dados abertos no Brasil. A Ausência de definição de licença de uso de dados pode trazer limitações à sua utilização por potenciais consumidores. Além disso, a falta de legislação específica sobre o que deveria ser considerado dado pessoal pelo Poder Público pode causar insegurança nos gestores quando da abertura de determinados conjuntos de dados. Dessa forma, apesar dos avanços normativos promovidos pelo recém-editado Decreto 8.777/2016, as citadas deficiências no arcabouço jurídico que regulamenta a abertura de dados no país podem tornar menos efetiva a política de dados abertos do Poder Executivo Federal. (Achado 1, Seção 3.1).²⁴⁰

²⁴⁰ MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA,

A Lei 13.709/2019 (LGPD) definiu no seu artigo 5º, I dados pessoais como “informação relacionada a uma pessoa natural identificada ou identificável”, bem como conceituou no artigo 5, II os dados de caráter pessoal considerados sensíveis²⁴¹.

Dessa forma, a LGPD teve o mérito de dar uma definição acerca do que seriam os dados pessoais, como a informação relacionada a pessoa natural identificada ou identificável, definindo da mesma forma dados pessoais de caráter sensível, cujo tratamento deve ser atribuído um maior cuidado, integrando o conceito de dados pessoais cuja definição aberta conferida pela lei de acesso à informação trazia dúvidas aos agentes públicos acerca do que seriam dados pessoais, cujo acesso ao público era objeto de restrição.

A controvérsia que certamente irá surgir diz respeito à conjugação de ambos os diplomas legais, pois, a lei de acesso à informação impõe a transparência como regra (art. 3º, I), excepcionando o sigilo em relação aos dados pessoais que, por sua vez, pode ser contornado pelo consentimento do titular (art. 31, § 1º, II) ou nas situações previstas no artigo 31, § 3º que, dentre outras hipóteses, prevê a possibilidade de divulgação de informação pessoal para a “proteção do interesse público e geral e preponderante”.

Cabe aqui ressaltar que a LGPD não possui disposição semelhante no que respeita a divulgação de dado pessoal e sensível pela Administração, mas apenas e tão somente as hipóteses em que o tratamento de dados pessoais e sensíveis pela Administração dispensam o consentimento do seu titular (artigo 7, IIIº e 11, II, c), no entanto, o tratamento de dados pessoais e sensíveis pela Administração conceituado no artigo 5, X da LGPD não pressupõe no seu conceito, mesmo que reconhecidamente abrangente, a possibilidade de ampla divulgação desta espécie de dados.²⁴²

Dessa maneira, considerando que o artigo 31, § 3º da lei de acesso à informação prevê a possibilidade de divulgação de informação pessoal, independente do consentimento do seu titular, para a “proteção do interesse público e geral e

Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 205-206.

²⁴¹ Art. 5º Para os fins desta Lei, considera-se:

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

²⁴² Art. 5º Para os fins desta Lei, considera-se:

X - tratamento: 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;

preponderante”, certo é que dúvidas irão surgir acerca do que se considera interesse público para o fim de divulgação de dados pessoais, considerando a fluidez do conceito e o histórico embate doutrinário acerca da sua extensão.

A questão já está levantando discussões doutrinárias acerca do premente conflito que será enfrentado pela Administração, em questões onde estarão em jogo ambos os interesses constitucionais de acesso à informação e o direito a intimidade, com os limites ponderativos para otimização de ambos os postulados, como é o caso dos dados cadastrais.

Os dados cadastrais a luz do artigo 5, I da LGPD são dados pessoais, no entanto, haverá situações onde o interesse público determinará a possibilidade de divulgação sem o consentimento do seu titular, nos termos do artigo 31, § 3º da Lei de Acesso à Informação, como na hipótese de identificação de quem integra a Administração ou com ela celebra negócios, é inegável o controle social por meio de acesso à informação, no entanto, surgirá discussões acerca de quais informações dos dados cadastrais são de interesse público ou de caráter eminentemente privado, por exemplo, os dados relativos a residência dessas pessoas constitui um espaço de privacidade que não pode ser exposto sem autorização do titular, por não constituir, a priori, uma informação de interesse geral.²⁴³

Assim, a Lei de Acesso à Informação representou um inegável avanço na realização do direito de acesso à informação previsto no artigo inciso II do § 3º do art. 37 da CF, no entanto, o advento da LGPD com vistas a assegurar a proteção do direito à privacidade de estatura igualmente constitucional (artigo 5º, X da CF), vai determinar uma remodelação necessária acerca das informações pessoais de posse da Administração, cujo restrição de acesso são necessárias a assegurar um espaço de privacidade onde não incide qualquer interesse público no seu controle social.

4.5.2. Do tratamento de dados no âmbito das políticas públicas de enfrentamento do COVID-19

²⁴³ MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 209.

As iniciativas governamentais nas diversas esferas de governo para o enfrentamento da pandemia do COVID-19, evidenciaram a importância dos dados pessoais no atual contexto da sociedade da informação, notadamente porque muitas políticas para enfrentamento da crise sanitária passaram pelo tratamento de dados dos cidadãos, na maioria dos casos em parceria com a iniciativa privada na cessão destes dados para uso pelo Poder Público, o que gerou controvérsia acerca do limite dessas iniciativas considerando aspectos relacionados ao direito à privacidade.

No âmbito do Governo Federal, foi editada a Medida Provisória nº 954, de 17 de abril de 2020, a qual previu que as empresas de telecomunicação deverão compartilhar com a Fundação IBGE, “a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas” (art. 2º), para a “produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares”. (art. 2º, § 1º).

Foram ajuizadas 5 (cinco) ações diretas de inconstitucionalidade contra os dispositivos da MP nº 954/2020, sendo concedida a liminar em ambas as ações pela Relator Ministra Rosa Weber sob o entendimento de que o ato normativo viola o direito à privacidade, na medida em que não definiu qual o tipo de estatística oficial pretende produzir com os dados pessoais que serão utilizados, não estando evidenciado no caso o interesse público da medida, tendo em vista os postulados da necessidade, adequação e proporcionalidade, além de não viabilizar meios técnicos e administrativos para assegurar o sigilo das informações obtidas, o que possibilitaria o vazamento de informações e o uso indevido.²⁴⁴²⁴⁵

Além da iniciativa levada a efeito na MP nº 954/2020, verifica-se que as diversas instâncias políticas adotaram outros meios, também baseado no tratamento de dados pessoais, para enfrentamento da pandemia do COVID-19, como acordos com as operadoras de telecomunicação para acesso a dados anonimizados de geolocalização de celulares, a fim de ter acesso à localização do usuário e adotar políticas visando evitar

²⁴⁴ BRASIL. Supremo Tribunal Federal. ADI nº 6.387, Rel. Ministra Rosa Weber, decisão proferida em 24 abr 2020.

²⁴⁵ Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE. Supremo Tribunal Federal. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442823>. Acesso em: 20 ago. 2020.

aglomerações. Essa política foi adotada pelo Governo Federal e pelo Governo do Estado de São Paulo.²⁴⁶²⁴⁷

O Sistema de Monitoramento Inteligente de São Paulo (SIMI-SP), fruto do acordo com entre o Instituto de Pesquisa Tecnológicas (IPT) e as operadoras de telefonia, com a finalidade de obter os dados e monitorar a localização dos usuários, foi questionado judicialmente por meio do Mandado de Segurança nº 2073723-23.2020.8.26.0000, sendo que o Órgão Especial do Tribunal de Justiça do Estado de São Paulo, por maioria de votos, entendeu que o referido acordo seria legal, na medida em que não violaria a intimidade dos indivíduos, tendo em vista que os dados seriam anonimizados e agregados, sem a possibilidade de identificação do titular.²⁴⁸

Assim, a pandemia do COVID-19 evidenciou uma tendência à crescente utilização de dados pessoais em políticas públicas pelo Estado, no entanto, o contexto sanitário em questão não deixa de ser um laboratório para a definição dos limites ao tratamento de dados pelo Poder Público, tendo em vista a judicialização verificada no período, cujo pano de fundo é a necessidade de que estes dados sejam utilizados observando os princípios da proteção de dados, especialmente da necessidade, adequação e proporcionalidade, de forma a impossibilitar o uso indevido ou abusivo pelo Poder Público.

4.5.3. Do tratamento de dados pessoais sensíveis pelo Poder Público

O art. 5º, II da LGPD conceitua o dado pessoal sensível como:

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

²⁴⁶ Governo vai monitorar celular para controlar aglomeração na pandemia. *UOL*. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/04/02/para-combater-a-covid-19-o-governo-federal-va-monitorar-o-seu-celular.htm>. Acesso em: 20 ago. 2020.

²⁴⁷ Governo de SP apresenta Sistema de Monitoramento Inteligente contra Coronavírus. *saopaulo.sp.gov.br*. Disponível em: <https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus/>. Acesso em: 20 ago. 2020.

²⁴⁸ BRASIL. Tribunal de Justiça de São Paulo. MS nº 2073723-23.2020.8.26.0000, Rel. Des. Antonio Carlos Malheiros, julgamento realizado em 04 jun. 2020.

A situação de pandemia determinada pelo Covid-19 não evidenciou apenas a crescente necessidade de acesso pelos órgãos públicos aos dados pessoais, para a formulação de políticas públicas, mas também a necessidade de atribuir segurança aos dados constantes em bancos de dados dos diversos órgãos públicos, pois, houve notícias de casos onde os dados pessoais de pessoas infectadas foi objeto de vazamento, dado sensível que deveria ter uma maior governança em relação ao acesso, com rígidas políticas de segurança.²⁴⁹

4.6. Regime jurídico do compartilhamento de dados pelo Poder Público

4.6.1. Interoperabilidade como garantia do compartilhamento de dados

O artigo 25 da LGPD prevê que os dados deverão ser mantidos em formato interoperável e estruturado para seu uso compartilhado, com vistas “à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.”²⁵⁰

Convém ressaltar, inicialmente, que assim como a operação de tratamento de dados, o compartilhamento de dados pessoais entre órgãos e entidades do Poder Público pode ser realizada sem a necessidade do consentimento do titular dos dados pessoais, conforme se depreende do artigo 7º, III da LGPD.²⁵¹

O uso compartilhado de dados entre órgãos e entidades públicas pressupõe, logicamente, que tal operação é realizada para “o cumprimento de suas competências legais”, nos limites do conceito de compartilhamento previsto 5º da LGPD, conjugado com o previsto no artigo 25 da lei, que delimita esta competência à execução de políticas

²⁴⁹ Lista de pessoas infectadas com o novo coronavírus foi divulgada na internet. *Globo.com*, 12 jul. 2020. Disponível em: <https://g1.globo.com/pr/norte-noroeste/noticia/2020/07/12/lista-de-pessoas-infectados-com-o-novo-coronavirus-em-arapongas-foi-divulgada-na-internet.ghtml>. Acesso em: 15 jul. 2020. Vazamento de senha do Ministério da Saúde expõe dados de 16 milhões de pacientes de covid. *Estado de São Paulo*. Disponível em: <https://saude.estadao.com.br/noticias/geral,vazamento-de-senha-do-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid,70003528583>. Acesso em: 05 dez. 2020

²⁵⁰ Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

²⁵¹ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

públicas, prestação de serviços, descentralização da atividade pública e disseminação de informações ao público.

Fato é que a Administração Pública, no exercício da atividade administrativa, promove o compartilhamento de dados pessoais de servidores e dos administrados para diversos fins. Um exemplo do compartilhamento de dados de servidores é o realizado com instituições financeiras para o processamento da folha, o que inclusive motivou o veto ao inciso II do § 1º do artigo 26 da LGPD.

O compartilhamento de dados dos administrados também é uma praxe dentro de políticas sociais, como a previdência e assistência social cujos bancos de dados acerca dos beneficiários é alimentado por meio de compartilhamento de dados de outras bases públicas, a exemplo dos cartórios de registros civis de pessoas naturais que possuem a obrigação de informar óbitos ao INSS (art. 68 da Lei nº 8.212/91). Deve ser ressaltado que o compartilhamento de dados entre o Poder Público era vedado pelo artigo 23, II da LGPD, o qual foi vetado sob o fundamento de inviabilizar o compartilhamento para a realização de políticas públicas.²⁵²

O uso compartilhado de dados pela Administração Pública pressupõe a “capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais troquem dados”, ou seja, a chamada interoperabilidade desses diversos sistemas e bancos de dados.²⁵³ Tal previsão já constava do artigo 24, III e IV do Marco Civil da Internet (Lei nº 12.965/2014).

Nesse sentido, para viabilizar a interoperabilidade dos sistemas, os dados pessoais e sensíveis devem estar armazenados em formato ou padrão aberto, a exemplo das extensões PDF, TXT, HTML, arquivos em áudio no formato OGG e FLAC e imagens em PNG ou SVG, tendo em vista que um arquivo em formato fechado ou proprietário é

²⁵² Inciso II do art. 23

“II - sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado;”

Razões do veto

“O dispositivo veda o compartilhamento de dados pessoais no âmbito do Poder Público e com pessoas jurídicas de direito privado. Ocorre que o compartilhamento de informações relacionadas à pessoa natural identificada ou identificável é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas. É o caso, por exemplo, do banco de dados da Previdência Social e do Cadastro Nacional de Informações Sociais, cujas informações são utilizadas para o reconhecimento do direito de seus beneficiários e alimentados a partir do compartilhamento de diversas bases de dados administrados por outros órgãos públicos. Ademais, algumas atividades afetas ao poder de polícia administrativa poderiam ser inviabilizadas, a exemplo de investigações no âmbito do Sistema Financeiro Nacional, dentre outras.”

²⁵³ Artigo 2º, XVIII do Decreto Federal nº 10.046, de 09 de outubro de 2019, o qual dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

codificado de tal forma que somente o órgão público detentor daquele banco possa acessá-lo, inviabilizando seu compartilhamento com outras bases.²⁵⁴

O Poder Judiciário e órgãos integrantes do sistema de justiça, a exemplo da AGU (Termo de Acordo e Cooperação Técnica nº 058/2009) e Ministério Público (Resolução Conjunta nº 03/2013), adotaram o Modelo Nacional de Interoperabilidade – MNI, com vistas a adoção de um padrão nacional de sistemas de processo eletrônico utilizando a tecnologia “WebService” (clausula primeira do Termo de Acordo e Cooperação Técnica nº 058/2009), integrando a base de dados de informações processuais entre as instituições, viabilizando, por exemplo, dentro dos órgãos do Poder Judiciários que um recurso originário do Tribunal Regional Federal da 1ª Região seja encaminhado ao Superior Tribunal de Justiça pelo próprio sistema.

Deve ser ressaltado que o Modelo Nacional de Interoperabilidade (MNI) adotado pelo Conselho Nacional de Justiça tem, para além da finalidade de interoperar os diversos sistemas do judiciário, “a função primordial de interligar o sistema do poder judiciário com sistemas externos”, a exemplo dos sistemas de polícia judiciária, com a integração do inquérito ao processo criminal.²⁵⁵

O Tribunal de Contas da União em auditoria realizada com o objetivo de avaliar a implementação e o funcionamento da informatização dos processos judiciais (TC nº 008.903/2018-2), consolidada no Acórdão nº 1.534/2009, identificou as seguintes deficiências ao Modelo Nacional de Interoperabilidade (MNI) a ao sistema PJe adotado pelo CNJ

DEFICIÊNCIAS APONTADAS PELO TCU	
a) atraso na implementação do PJe e do Modelo Nacional de Interoperabilidade	“o sistema único ainda não é uma realidade. Em pesquisa com usuários de sistemas do Poder Judiciário realizada pelo CJF em março de 2018, foram observados diversos sistemas: PJe, e-SAJ, e-Proc, Projudi, e-STF, e-STJ e outros. 12. As dificuldades operacionais para a plena implementação do PJe e do MNI pode sem ser justificadas, em princípio, pela dimensão do desafio: 92 tribunais, 18.168 magistrados, 272.093 servidores, 13.087 membros do MP, 6.059 defensores públicos e 1.107.481 advogados, além das autoridades policiais,

²⁵⁴ TASSO, Fernando Antonio. Lei Geral de Proteção de Dados Comentada. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coordenação). 2. ed. São Paulo: Revista dos Tribunais. p. 271.

²⁵⁵ BRASIL. Afirmação realizada pela Administração do CNJ no TC nº 008.903/2018-2. Acórdão nº 1.534. Rel. Ministro Raimundo Carreiro, Plenário, sessão 03 jul. 2019, ata nº 24/2019.

	estagiários, juristas, cidadãos com interesse em determinados processos.”
b) dificuldades operacionais na busca de informações confiáveis	“103. Da análise das informações enviadas pela AGU, observa-se que, do total de operações realizadas com o Poder Judiciário, cerca de 25% resultaram em erro. As falhas concentram-se na operação “recuperação de documento”, bem como em operações realizadas entre a AGU e o TRF3, tribunal com jurisdição no Estado de São Paulo, com grande volume de ações previdenciárias”.
c) fragmentação do sistema PJe-Nacional e não implementação do MNI	“A unidade técnica também pontua a fragmentação do sistema PJe-Nacional, com “sistemas variantes” e “partes que sequer aderiram ao PJe”, e, ainda, que “o MNI não foi efetivamente implementado, de modo que os vários sistemas possuem dificuldades de interoperabilidade”
d) Governança	“há indicadores de progressiva redução das atividades do Comitê Gestor Nacional do PJe (CGN-PJe)”, demonstrados nos gráficos produzidos pela equipe de auditora (§§ 153 a 156, do relatório de auditoria);”
e) Participação das partes interessadas	“o processo de elaboração da Resolução-CNJ 185/2013 desconsiderou mais de 80% das contribuições apresentadas em sede de consulta pública, sem evidenciação das causas destas desconsiderações. (§158 do relatório de auditoria);”
f) Definição de metas e indicadores	“ausência ou insuficiência de “metas e indicadores que permitam identificar e avaliar a efetividade ou o impacto da política pública de informatização do processo judicial sobre os macro-objetivos esperados, a exemplo da ausência de avaliação de impacto das ações sobre a celeridade processual, a acessibilidade à Justiça pelos cidadãos e a redução de custos do Poder Judiciário (§§162 a 167, idem);”

Fonte: elaboração própria com base no Acórdão nº 1.534/2019²⁵⁶

Apesar das deficiências apontadas pelo TCU na auditoria levada a efeito no Acórdão nº1.534/2019, os Ministros enfatizaram os esforços e os avanços do Poder Judiciários no aprimoramento do Processo Eletrônico Judicial (PJe) e do Modelo Nacional de Interoperabilidade do Poder Judiciário e do Ministério Público (MNI), ressaltando que a auditoria teria como fim estimular a intensificação das ações, pois, a

²⁵⁶ BRASIL. Tribunal de Contas da União. Acórdão n. 1.534. Processo TC n ° 008.903/2018-2. Rel. Ministro Raimundo Carreiro, Plenário, sessão 03 jul. 2019, ata n. 24/2019.

interoperabilidade entre os sistemas viabilizaria ganhos de eficiência, redução de custos e aumento de celeridade processual com a maximização do compartilhamento de dados, sendo “extremamente útil para a eficácia e a eficiência dos controles de prevenção, litispendência e coisa julgada”.²⁵⁷

Destaca-se, ainda, o Cadastro Base do Cidadão instituído pelo Decreto Federal nº 10.046, de 09 de outubro de 2019, uma plataforma de integração e interoperação de dados na Administração Pública Federal, congregando dados pessoais e sensíveis dos cidadãos, com o objetivo de compartilhamento entre órgãos e entidades do Governo Federal para fins de implementação de políticas públicas.

Dessa forma, a interoperabilidade entre os sistemas da Administração é condição para o efetivo compartilhamento de dados, sendo que, a par das dificuldades técnicas e orçamentárias para a integração dos diversos sistemas, como verificada no exemplo relacionado ao sistema de justiça, a integração deve ser buscada pelos órgãos e entidades da Administração na medida em que o compartilhamento de dados estruturados, organizados, garantem ganhos de eficiência na gestão de políticas públicas, compartilhamento que terá como critérios de contenção os princípios da proteção de dados previstos no artigo 6º da LGPD, especialmente os princípios da finalidade e necessidade.

4.6.2. Extensão do compartilhamento de dados: das políticas públicas ao poder de polícia

O artigo 25 da LGPD prevê que o compartilhamento de dados entre órgãos e entidades públicas, será realizado com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública, acesso à informação ao público, sendo que o artigo 26 determina que compartilhamento deve atender a finalidades específicas de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitados o princípios da proteção de dados.

Como tratado em capítulo próprio, políticas públicas são instrumentos de ação dos governos, a expressão dos direitos socioeconômicos, consistindo no modo de agir ordenado do Estado, sendo o serviço público a forma como o Estado operacionaliza uma determinada política pública à coletividade. O compartilhamento de dados, no âmbito nas

²⁵⁷ BRASIL. Tribunal de Contas da União. Acórdão n. 1.534. Processo TC n ° 008.903/2018-2. Rel. Ministro Raimundo Carreiro, Plenário, sessão 03 jul. 2019, ata n. 24/2019.

políticas públicas destinadas a efetivação de direitos sociais como previdência e assistencial social, mas não só, é uma realidade.

O compartilhamento de dados no âmbito estatal, no entanto, não se restringe às hipóteses onde o Estado se posiciona como prestador de serviços, oferecendo utilidades à sociedade, mas ocorre também quando o Poder Público atua no exercício de poder de polícia que, segundo Celso Antônio Bandeira de Mello, constitui manifestação da “atividade estatal de condicionar a liberdade e a propriedade ajustando-as aos interesse coletivos”.²⁵⁸

Já foi tratado em capítulo a atuação estatal no exercício de poder de polícia judiciária, a qual se qualifica por tratar de atividades regidas “pelo direito processual penal, incidindo sobre pessoas”, a qual não se submete à aplicação da LGPD nos termos do seu artigo 4º, III, nada obstante aplicável a tais atividades os princípios da proteção e dados pessoais (artigo 4º, § 1º).²⁵⁹

Ocorre que é inerente à atividade estatal, em nome do interesse público, o exercício do poder de polícia administrativa que se conforma na execução de leis administrativas, se repartindo pelos diversos órgãos da Administração, e se manifesta nos “vários órgãos de fiscalização aos quais a lei atribua esse mister, como os que atuam na área da saúde, educação, trabalho, previdência e assistência social”.²⁶⁰

A LC nº 105/2000 prevê no seu artigo 1º, como regra, que as instituições financeiras “conservarão sigilo em suas operações ativas e passivas e serviços prestados”, no entanto, excetua o mencionado sigilo para fins de realização de poder de polícia pelos órgãos de fiscalização tributária (art. 6º), norma declarada constitucional pelo Supremo Tribunal Federal por ocasião do julgamento do RE nº 601.314.²⁶¹ O Decreto nº 10.209, de 22 de janeiro de 2020, por sua vez, viabiliza o compartilhamento dos dados protegidos por sigilo fiscal aos órgãos de controle interno (Controladoria-Geral da União) e externo (Tribunal de Contas da União).

O Supremo Tribunal Federal definiu por ocasião do julgamento do RE nº 1.055.941/SP, julgado na sistemática da repercussão geral (Tema 990), acerca da

²⁵⁸ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33.ed. São Paulo: Malheiros, 2016, p. 851.

²⁵⁹ PIETRO, Maria Sylvia Zanella Di. *Direito Administrativo*. 23. ed. São Paulo: Editora Atlas, 2009. p. 118.

²⁶⁰ *Idem*, p. 118.

²⁶¹ BRASIL. Supremo Tribunal Federal. RE nº 601.314. Ministro Edson Fachin, julgamento em 24 fev. 2016. Tese fixada: “O art. 6º da Lei Complementar 105/01 não ofende o direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o traslado do dever de sigilo da esfera bancária para a fiscal”.

possibilidade do compartilhamento de dados bancários e fiscais obtidos pelo Fisco com o Ministério Público para fins penais, sem a necessidade de interveniência do Judiciário.

O compartilhamento de dados entre os mais diversos órgãos da Administração, para o exercício de polícia administrativa e judiciária, é uma realidade e há uma tendência que tal prática se intensifique, pois, o acesso facilitado a informações estruturadas em um determinado banco de dados permite inegáveis ganhos de eficiência.

A LGPD, por sua vez, viabiliza o compartilhamento para esse fim ao destacar tal possibilidade não só para a realização de políticas públicas, como também para a execução de atividades necessárias à efetivação “da atribuição legal pelos órgãos e entidades públicas” (artigo 26).

Dessa forma, a autorização legal prevista nos artigos 25 e 26 da LGPD para o compartilhamento de dados pela Administração, sem a necessidade do consentimento do titular (art. 7º, III da LGPD), não se restringe às operações necessárias à execução de políticas públicas, se estendendo para o exercício do poder de polícia administrativa e judiciária, no entanto, o compartilhamento em ambas as hipóteses deve respeitar os princípios que norteiam a proteção de dados (art. 6º), com destaque aos princípios da finalidade e necessidade, de tal forma que o compartilhamento esteja adstrito a finalidade que o determinou e seja restrito ao mínimo necessário para realização deste fim.

4.6.3. Do compartilhamento de dados no âmbito do MPF na operação Lava Jato. O compartilhamento como política do controle de operações de tratamento de dados

Órgãos públicos “são unidades abstratas que sintetizam os vários círculos de atribuições do Estado”, materializadas por meio de seus agentes, de tal forma que os órgãos constituem partições internas que não possuem personalidade jurídica e cujas atribuições são exercidas pelos agentes constituídos.²⁶²

O Ministério Público constitui órgão essencial à função jurisdicional do Estado, com a incumbência constitucional de assegurar a “defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis” (art. 127 da CF de 1988), possuindo como princípios institucionais a “unidade, a indivisibilidade e a independência funcional” (§1º, art. 127 da CF de 1988).

²⁶² MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33.ed. São Paulo: Malheiros, 2016, p. 144.

A operação Lava Jato, por sua vez, constitui uma iniciativa do Ministério Público Federal criado sob o enfoque de combate à corrupção, congregando membros da carreira em integração com a Polícia Federal e utilizando uma grande base de dados para as atividades de investigação criminal, a qual abrange informações fiscais da Receita Federal, do Conselho de Controle das Atividades Financeiras (COAF), Conselho Administrativo de Defesa Econômica (CADE) e a Controladoria-Geral União (CGU).²⁶³

O Procurador-Geral da República, Augusto Aras, afirmou em entrevista transmitida pela internet dia 28 de julho de 2020 que “Não se pode imaginar que uma unidade institucional se faça com segredos, com caixas de segredos. Todo o MPF, em seu sistema único, tem 40 terabytes. A força-tarefa da lava jato em Curitiba tem 350 terabytes e 38 mil pessoas com seus dados depositados. Ninguém sabe como [esse nomes] foram escolhidos, quais foram os critérios”.²⁶⁴

Na ocasião, iniciou-se uma controvérsia pelo compartilhamento desses dados dentro da própria estrutura do órgão. Os membros integrantes da Lava Jato de Curitiba negaram o compartilhamento dos dados com a instância superior do Ministério Público Federal, sob o fundamento de inexistir fundamento legal para o compartilhamento.²⁶⁵ Diante da negativa, a Procuradoria-Geral da República ingressou com a Reclamação nº 42.050 junto ao Supremo Tribunal Federal.

O Ministro Dias Toffoli, então presidente do Supremo Tribunal Federal, deferiu a liminar na RCL nº 42.050 para o que os integrantes da Lava Jato disponibilizem os dados estruturados e não estruturados ao Procurador-Geral da República, colhidos em investigações das chamadas forças tarefas nos Estados do Rio de Janeiro, São Paulo e Paraná, sob o fundamento de que a negativa ao compartilhamento de tais dados constituía transgressão ao princípio da unidade do Ministério Público (§1º, art. 127 da CF de 1988) e a ADPF nº 482, bem como trazia a possibilidade de ter no bojo dessas investigações autoridades com prerrogativa de foro.²⁶⁶

A decisão em questão na RCL nº 42.050 foi posteriormente reformada pelo Ministro Edson Fachin, juiz natural do processo, sob o entendimento de que não ser, em

²⁶³ Entenda o caso da Lava Jato. *Ministério Público Federal*. Disponível em: <http://www.mpf.mp.br/grandes-casos/lava-jato/entenda-o-caso>. Acesso em: 11 ago. 2020.

²⁶⁴ “Lava jato” em Curitiba tem dados de 38 mil pessoas. *Conjur*. Disponível em: <https://www.conjur.com.br/2020-jul-29/lava-jato-curitiba-dados-38-mil-pessoas-aras>. Acesso em: 11 ago. 2020.

²⁶⁵ Compartilhamento da “lava jato” com a PGR foi decidido em 2015. *Conjur*. Disponível em: <https://www.conjur.com.br/2020-jun-30/compartilhamento-lava-jato-pgr-foi-decidido-2015>. Acesso em: 11 ago. 2020.

²⁶⁶ BRASIL. Supremo Tribunal Federal. RCL nº 42.050. Ministro Dias Toffoli, julgamento em 08 jul. 2020.

princípio, cabível a reclamação pela inexistência de aderência com a ADPF nº 482.²⁶⁷ A questão será definida pelo Plenário do Supremo Tribunal Federal.

O ponto que se pretende ressaltar é que, para além do compartilhamento de dados entre órgãos para a viabilização de políticas e exercício de poder de polícia, o compartilhamento de dados dentro do próprio órgão, como no caso citado do Ministério Público Federal, ou para órgãos diversos, pode ter a finalidade de controle acerca da regularidade das operações de tratamento de dados realizados no âmbito das mais diversas instâncias administrativas.

No caso em apreço, o Procurador-Geral da República apontou um suposto uso abusivo de dados pessoais no âmbito da chamada força tarefa da Lava Jato, sendo que, se tal afirmação for realmente crível, estar-se-á diante de um verdadeiro estado de vigilância onde os dados de milhares de cidadãos são coletados e tratados de forma abusiva em expedientes investigatórios, sem critérios claros, em manifesta violação a princípios da proteção de dados previstos no artigo 6º da LGPD, notadamente os princípios da finalidade e da necessidade, os quais determinam que o tratamento de dados deve se dar para uma finalidade específica e adstrito ao mínimo possível de informações para se atingir este fim.

O exemplo ilustra uma situação, portanto, onde o compartilhamento de dados dentro de, bem como entre órgãos da Administração Pública não se restringiria à implementação de políticas públicas, ou mesmo ao exercício do poder de polícia, mas sim para aferição e controle de regularidade de operações de tratamento de dados realizado para tais fins, o que não só se afigura desejável do ponto de vista do controle, como alinhado com os reclamos do Estado Democrático de Direito à luz dos seus fundamentos e objetivos que se extraem dos artigos 1º e 3 da CF de 1988, quais sejam, o dever de transparência e prestação de contas pelo Poder Público.

4.6.4. Necessidade de estabelecimento de regras de governança para o compartilhamento de dados pelo Poder Público. Casos SERPRO e ABIN

O artigo 26 da LGPD prevê que o compartilhamento de dados deve respeitar os princípios da proteção de dados previsto no artigo 6º da lei. O artigo 30 da LGPD, por sua vez, consigna que a ANPD “poderá estabelecer normas complementares para as

²⁶⁷ BRASIL. Supremo Tribunal Federal. RCL nº 42.050. Ministro Edson Fachin, julgamento em 03 ago. 2020.

atividades de comunicação e de uso compartilhado de dados pessoais”, a qual também tem a competência de solicitar relatórios de impacto à proteção de dados de sugerir a “adoção de padrões e boas práticas” à Administração (art. 32).

Deve ser ressaltado que a LGDP prevê um capítulo específico (VII) acerca da segurança e boas práticas relacionadas à proteção de dados, atribuindo tanto a ANPD (art. 46, §1º), quanto aos agentes de tratamento de dados (art. 50, §1º), dispor de padrões técnicos para a realização de regras de governança de dados, o que abrange inclusive políticas para o compartilhamento.

A Administração Pública Federal editou o Decreto nº 10.046, de 09 de outubro de 2019, com a finalidade de dispor sobre a governança no compartilhamento de dados no âmbito da Administração Federal, com a criação do Cadastro Base do Cidadão e do Comitê Central de Governança de Dados. O mencionado decreto se aplica apenas às operações de compartilhamento dentro da Administração Pública (art. 1º, §1º), não abrange os dados protegidos por sigilo fiscal (art. 1º, §1º) e tem o objetivo de otimizar, avaliar e monitorar políticas públicas, simplificar a oferta de serviços públicos, qualificar os dados e obter ganhos de eficiência nos trâmites internos (art. 1º, I, II, III).

O mencionado decreto estabeleceu uma categorização em três níveis de compartilhamento baseado no grau de confidencialidade dos dados, que vai do amplo que não está sujeito a nenhuma restrição, ao compartilhamento restrito e específico que são dados protegidos por sigilo (art. 4º).²⁶⁸ A qualificação de um dado como amplo ou restrito, no entanto, não foi objeto de pré-qualificação pelo ato normativo que, apesar de conceituar os vários tipos de dados no artigo 2º, a exemplo do dados inerentes a atributos biográficos, biométricos, genéticos e cadastrais, deixou a critério do gestor dos dados sua categorização em um determinado nível de sigilo (art. 4º, §1º).

O Decreto nº 10.046, de 09 de outubro de 2019 instituiu o Comitê Central de Governança de Dados, com a finalidade de fixar diretrizes para a categorização do sigilo

²⁶⁸ Art. 4 O compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º é categorizado em três níveis, de acordo com sua confidencialidade:

I - compartilhamento amplo, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;

II - compartilhamento restrito, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; e

III - compartilhamento específico, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados.

dos dados (art. 21, I), definir controvérsias acerca do compartilhamento de dados entre órgãos e entidades públicas (art. 26).

O Comitê Central de Governança de Dados, por sua vez, editou: (i) a Resolução nº 02, de 16 de março de 2020, que estabelece diretrizes para a categorização do compartilhamento de dados; bem como a (ii) a Resolução nº 04, de 14 abril de 2020, a qual disponibilizou um guia de boas práticas para a implementação da LGPD na Administração Federal.

A Resolução nº 02, de 16 de março de 2020 prevê orientações e as diretrizes para a categorização de compartilhamento de dados, ressaltando a necessidade de atualização do documento em observância de normativos a serem expedidos pela ANPD (art. art. 1º, §2º), bem como traça aspectos procedimentais para a categorização do dado em um determinado nível de sigilo.

A par de toda a regulação mencionada, o veículo jornalístico denominado *The Intercept* publicou recentemente uma reportagem onde a Agência Brasileira de Inteligência (ABIN), teria solicitado ao Serviço Federal de Processamento de Dados (SERPRO), os dados de milhões de brasileiros constantes do Banco de Imagens do Registro Nacional de Condutores Habilitados (RENACH), notadamente o nome, filiação, CPF, endereço, telefones, foto, dados dos veículos (nomes de proprietários anteriores, situação e procedência) de todo cidadão que possui habilitação para dirigir, sendo estimados mais de 75 milhões de registros.²⁶⁹

Questionado pelo veículo de imprensa acerca da legalidade do pedido, a ABIN por meio do Gabinete de Segurança Institucional informou que o compartilhamento de dados no caso “obedece ao Decreto 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal”.²⁷⁰ O veículo de imprensa, na ocasião, questionou a ABIN acerca do fato do

²⁶⁹ Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHS do país. *The Intercept*. Disponível em: <https://theintercept.com/2020/06/06/abin-carreira-motorista-serpro-vigilancia/>. Acesso em: 01 ago. 2020.

²⁷⁰ Resposta da ABIN e GSI: A obtenção, a integração e o compartilhamento de bases de dados são essenciais para o funcionamento da Atividade de Inteligência.

A utilização dos dados por parte da Agência se dá em conformidade com os objetivos estratégicos e as orientações constantes da Estratégia Nacional de Inteligência, instituída por Decreto em 15 de dezembro de 2017.

O compartilhamento de dados obedece ao Decreto 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e estabelece as normas e as diretrizes para o compartilhamento de dados, de forma legal, entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União.

mencionado decreto não abranger o serviço de inteligência, posto que direcionado a formatação de políticas públicas, mas não obteve resposta.²⁷¹

Danilo Doneda foi entrevistado pelo *The Intercept* na oportunidade, demonstrando receio de que tais informações estariam sendo utilizados por um sistema massivo de vigilância, a exemplo do realizado pelos EUA por meio da agência de espionagem NSA que implementou um amplo sistema de espionagem dos cidadãos americanos:

Esse caso, pelo volume de informações, chama atenção. Eu me pergunto qual é o interesse estratégico para inteligência nacional você fazer vigilância massiva”, questiona o advogado Danilo Doneda, doutor em Direito Civil e membro indicado pela Câmara dos Deputados para o Conselho Nacional de Proteção de Dados e Privacidade. “O que chama a atenção agora é que é um momento de politização exacerbada dos órgãos de estado. Há um receio latente de informações pessoais sendo usadas para fins não republicanos. Acende a luz amarela, no mínimo”.

Para o advogado, o esquema montado pela Abin remete ao escândalo de espionagem da NSA, a agência de segurança digital dos EUA, que usou um sistema massivo de vigilância para fins obscuros e, muitas vezes, privados. O caso foi revelado pelo analista de segurança Edward Snowden.²⁷²

O Decreto 10.046, de 9 de outubro de 2019 não tem a extensão considerada pela ABIN, no que respeita a ações de inteligência, posto ter a finalidade de otimizar, avaliar e monitorar políticas públicas, simplificar a oferta de serviços públicos, qualificar os dados e obter ganhos de eficiência nos trâmites internos (art. 1º, I, II, III).

Cabe fazer uma ressalva, nesse ponto, que para além do compartilhamento de dados de brasileiros com a ABIN, o Serviço Federal de Processamento de Dados (SERPRO), empresa pública federal, vem sendo objeto de investigação por parte do Ministério Público Federal por realizar o compartilhar de dados de brasileiros não só com a própria Administração Federal, como também com o setor privado, utilizando a base de dados da Receita Federal.²⁷³

Outra questão recente envolvendo a ABIN, diz respeito ao compartilhamento de dados à Agência viabilizado pelo Decreto 10.445/2020, o qual alterou sua estrutura. Os

²⁷¹ Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHS do país. *The Intercept*. Disponível em: <https://theintercept.com/2020/06/06/abin-carteira-motorista-sepro-vigilancia/>. Acesso em: 01 ago. 2020.

²⁷² Idem.

²⁷³ MP-DF acusa empresa pública de vender dados pessoais de brasileiros. *Conjur*. Disponível em: <https://www.conjur.com.br/2018-mai-31/mp-df-acusa-empresa-publica-vender-dados-brasileiros>. Acesso em: 01 ago. 2020.

partidos Rede Sustentabilidade e Partido Socialista Brasileiro ajuizaram a ADI nº 6529, questionando a constitucionalidade do parágrafo único do artigo 4º da lei de criação da ABIN (Lei 9.883/1999), o qual viabiliza o compartilhamento de dados no âmbito do Sistema Brasileiro de Inteligência (Sisbin) para a Agência, compartilhamento que poderia ser realizado de forma abusiva pelo fato do Decreto 10.445/2020 viabilizar tal ato mediante uma simples requisição, na medida em que o mencionado ato não restringiu as hipóteses de requisição de informações no âmbito do Sisbin pela Agência.²⁷⁴

O Plenário do Supremo Tribunal Federal analisou a medida cautelar requerida na ADI nº 6529, em julgamento realizado em 13 de agosto de 2020, deferindo parcialmente a liminar para conferir interpretação conforme ao parágrafo único do artigo 4º da Lei 9.883/1999, de maneira a estabelecer que os órgãos integrantes do Sistema Brasileiro de Inteligência (Sisbin) somente podem fornecer dados e conhecimentos específicos à Agência Brasileira de Inteligência (Abin) quando for comprovado o interesse público da medida, mediante solicitação devidamente motivada, vedado o compartilhamento de dados sujeitos à reserva de jurisdição, sendo imprescindível a instauração de procedimento formal e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.²⁷⁵

Cabe ressaltar que a Relatora da ADI nº 6529, Ministra Carmem Lúcia, ressaltou em seu voto que o fornecimento de informações entre órgãos públicos para a defesa das instituições e dos interesses nacionais é legítimo, sendo que “o que é proibido é que se torne subterfúgio para atendimento ou benefício de interesses particulares ou pessoais, especialmente daqueles que têm acesso aos dados, desvirtuando-se competências constitucionalmente definidas e que não podem ser objeto de escolha pessoal”, afirmando também que “‘Arapongagem’ não é direito, é crime, e, praticado pelo Estado, é ilícito gravíssimo”.²⁷⁶

²⁷⁴ Partidos questionam noma que condiciona fornecimento de dados à Abin a ato presidencial. *Supremo Tribunal Federal*. Disponível em: <http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449429&ori=1>. Acesso em: 15 ago. 2020.

²⁷⁵ Interesses públicos, e não privados, justificam o repasse de dados à Abin, diz STF. *Conjur*. Disponível em: <https://www.conjur.com.br/2020-ago-13/interesse-publico-necessario-repasse-dados-abin-stf>. Acesso em: 16 ago 2020.

²⁷⁶ STF impõe limite ao compartilhamento de dados do sistema Brasileiro de inteligência (Sisbin). *Supremo Tribunal Federal*. Disponível em: <http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=449549&ori=1>. Acesso em: 16 ago. 2020.

Os casos citados do SERPRO e ABIN tem a objetivo de evidenciar a necessidade de aperfeiçoar as regras e práticas de governança no compartilhamento de dados na Administração Pública, o que deve ser objeto de regras editadas pela própria Administração (art. 50, §1º), como também e especialmente pela Autoridade Nacional de Proteção de Dados (art. 46, §1º), tanto para fins de políticas públicas, quanto para o exercício de poder de polícia, administrativa e judiciária, e também para fins de Defesa Nacional, nos termos do artigo 4º, § 3º da LGPD, de forma a evitar o denominado estado de vigilância verificado nos EUA após os atentados de 11 de setembro que, em um contexto de polarização política, pode determinar utilização destes dados de forma desvirtuada da finalidade institucional destes órgãos.

Nesse sentido, deve ser ressaltada a necessidade de se atribuir a Autoridade Nacional de Proteção de Dados (ANPD) uma necessária autonomia institucional em relação ao poder central, posto que a regulação incide inclusive em relação a este último, autonomia institucional atualmente prejudicada pela configuração de órgão atribuído ao regulador pelo artigo 55-A da LGPD, conforme tratado neste estudo em capítulo próprio.

4.6.5. Conclusão

O regime jurídico do tratamento e compartilhamento de dados conferido pela LGPD ao setor público, o que como visto abrange a Administração direta e indireta, esta última restrita às estatais prestadoras de serviço público, bem como os serviços notariais e de registro, possui privilégios específicos, especialmente a dispensa do consentimento do seu titular, lógica que se aplica não só em relação aos dados pessoais (art. 7º, II), como também em relação aos dados sensíveis (art. 11, II, b) dos administrados, sendo que estes últimos correspondem a uma espécie de dados que gozam de especial proteção por dizer respeito a aspectos específicos da privacidade do seu titular (art. 5º, II).²⁷⁷

A prerrogativa atribuída à Administração para tratar dados pessoais e sensíveis sem a necessidade de autorização prévia do seu titular (artigos 7º, III e 11, II, b), é delimitada pela atribuição de encargos correspondentes, com vistas a concretização do interesse público com a máxima realização dos direitos individuais, manifestada nas seguintes

²⁷⁷ Dado pessoal sensível: Art. 5º. II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

condicionantes: (i) exercer tal mister nos limites do interesse público que determinou o tratamento de dados; (ii) informar ostensivamente as hipóteses em que os dados são tratados; (iii) indicar um encarregado para prestação de contas a coletividade e à ANPD; (iv) cumprir as legislações setoriais aplicáveis; (v) observar os princípios constitucionais que vinculam sua atuação e; (vi) os princípios da proteção dos dados pessoais previstos no artigo 6º da LGPD.

Da mesma forma, a autorização legal prevista nos artigos 25 e 26 da LGPD para o compartilhamento de dados pela Administração, sem a necessidade do consentimento do titular (art. 7º, III da LGPD), não se restringe às operações necessárias à execução de políticas públicas, se estendendo para o exercício do poder de polícia administrativa e judiciária, no entanto, o compartilhamento em ambas as hipóteses deve respeitar os princípios que norteiam a proteção de dados (art. 6º), com destaque aos princípios da finalidade e necessidade, de tal forma que esteja adstrito a finalidade que o determinou e seja restrito ao mínimo necessário para realização deste fim.

Referências bibliográficas

ABRUSIO, Juliana et al. Dados de Geolocalização e a investigação do caso Marielle. *Conjur*, 07 jul. 2020. Disponível em: <https://www.conjur.com.br/2020-jul-07/direito-digital-dados-geolocalizacao-investigacao-marielle?pagina=2>.

ARAGÃO, Alexandre Santos de. *Agências Reguladoras e a evolução do Direito Administrativo Econômico*. Rio de Janeiro: Forense, 2002.

_____. Atividades Privadas Regulamentadas. In: ARAGÃO, Alexandre Santos de (Org.). *O Poder Normativo das Agências Reguladoras*. 2. edição. Rio de Janeiro: Forense, 2011.

AVILA, Humberto. Repensando o ‘Princípio da Supremacia do Interesse Público sobre o Particular’. In: SARMENTO, Daniel (Org.). *Interesses Públicos versus Interesses Privados: Desconstruindo o Princípio da Supremacia do Interesse Público*. 2. ed. Rio de Janeiro: Lumen Juris, 2007.

_____. *Teoria dos Princípios*. 4.ed. São Paulo: Malheiros, 2005.

BARROSO, Luis Roberto. Apontamentos sobre as agências reguladoras. In: MORAES, Alexandre. (Org) et allí. *Agências reguladoras*. São Paulo: Atlas, 2002.

BAUMAN, Zygmunt. *Modernidade líquida*. Trad. Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

BINENBOJM, Gustavo. Da Supremacia do Interesse Público ao Dever de Proporcionalidade: Um Novo Paradigma para o Direito Administrativo. In: SARMENTO, Daniel (Org.). *Interesses Públicos versus Interesses Privados: Desconstruindo o Princípio da Supremacia do Interesse Público*. 2. ed. Rio de Janeiro: Lumen Juris, 2007.

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

BISSOLI, Livia Regina Savergnini. Políticas Públicas como Programas e Ações para o Atingimento dos Objetivos Fundamentais do Estado. In: GRINOVER, Ada Pelegrine; WATANABE, Kazuo. *O controle jurisdicional de políticas públicas*. 2. ed. Rio de Janeiro: Forense, 2013.

BLANCHET, Luiz Alberto, BUBNIAK, Priscila Lais Ton. *Análise de Impacto Regulatório: uma ferramenta e um procedimento para a melhoria da regulação*. Pensar, Fortaleza, v. 22, n. 3, set/dez. 2017.

BODIN, Maria Cecilia. Apresentação do autor e da obra. In: RODOTA, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

BRASIL. Justificativa constante do texto inicial do PLS 52/2013. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/111048>>.

BRASIL. Mensagem nº 288, de 8 de julho de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Msg/VEP/VEP-288.htm>.

BRASIL. PEC 17/2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>.

BRASIL. Plano Diretor da Reforma do Aparelho do Estado. Brasília: Presidência da República, 1995. Disponível em: <<http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/plano-diretor-da-reforma-do-aparelho-do-estado-1995.pdf>>.

BRASIL. PL nº 6212/2019. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/139980>>.

BRASIL. Requerimento nº 123, 2020. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=8073590&ts=1585142422472&disposition=inline>>.

BRASIL. Superior Tribunal de Justiça. HD 147-DF, Rel. Ministro Arnaldo Esteves Lima, julgamento em 14 jun. 2007.

BRASIL. Superior Tribunal de Justiça. HC nº 135041. Rel. Min. Rosa Weber. Julgamento em 25 set. 2019.

BRASIL. Superior Tribunal de Justiça. REsp nº 1348532. Rel. Ministro Luis Felipe Salomão, julgamento em 10 de out. 2017.

BRASIL. Supremo Tribunal Federal. ADI nº 6387, Rel. Ministra Rosa Weber, julgamento 07 maio 2020.

BRASIL. Supremo Tribunal Federal. ADPF nº 403, Rel. Ministra Edson Fachin, julgamento 28 maio 2020.

BRASIL. Supremo Tribunal Federal. RE nº 593.727, Rel. para o acórdão Ministro Gilmar Mendes, julgamento 14 maio 2015, Tema 184.

BRASIL. Supremo Tribunal Federal. RE nº 973837, Rel. Ministro Gilmar Mendes, julgamento 23 jun. 2016, Tema 905.

BRASIL. Tribunal de Contas da União. Acórdão n. 825/2015. Processo 021.643/2014-8. Rel. Ministro José Múcio Monteiro, Plenário, sessão 15 abr. 2015, ata n. 13/2015.

BRASIL. Tribunal de Contas da União. Acórdão n. 240/2015. Processo 031.996/2013-2. Rel. Ministro Raimundo Carreiro, Segunda Câmara, sessão 11 fev. 2015, ata n. 5/2015.

BRASIL. Supremo Tribunal Federal. ADI nº 3.643, Rel. Ministro Ayres Britto, julgamento em 08 nov 2006.

BRASIL. Supremo Tribunal Federal. ADI nº 1.642, Rel. Ministro Eros Grau, julgamento em 03 abr. 2008.

BRASIL. Supremo Tribunal Federal. RE nº 599.628 (Tema 253), Rel. Ministro Ayres Britto, julgamento em 11 mar. 2010.

BRASIL. Supremo Tribunal Federal. ADI nº 6.387, Rel. Ministra Rosa Weber, decisão proferida em 24 abr 2020.

BRASIL. Tribunal de Justiça de São Paulo. MS nº 2073723-23.2020.8.26.0000, Rel. Des. Antonio Carlos Malheiros, julgamento realizado em 04 jun. 2020.

BRASIL. Tribunal de Contas da União. Acórdão n. 1.534. Processo TC nº 008.903/2018-2. Rel. Ministro Raimundo Carreiro, Plenário, sessão 03 jul. 2019, ata n. 24/2019.

BRASIL. Supremo Tribunal Federal. RE nº 601.314. Ministro Edson Fachin, julgamento em 24 fev. 2016.

BRASIL. Supremo Tribunal Federal. RCL nº 42.050. Ministro Dias Toffoli, julgamento em 08 jul. 2020.

BUCCI, Maria Paula Dallari. *Políticas públicas e direito administrativo*. Revista de informação legislativa, v. 34, n. 133, jan./mar. 1997.

CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf>.

COELHO, Fábio Ulhoa. Reforma do Estado e Direito Concorrencial. In: SUNDFELD, Carlos Ari. *Direito Administrativo Econômico* (Org.). São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000.

CORREA, P. et al. Regulatory governance in infrastructure industries: assessment and measurement of Brazilian regulators. Washington: World Bank, World Bank Publications, 2006.

COTS, Marcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais Comentada*. 3. ed. São Paulo: Revista dos Tribunais, 2019.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DOYLE, Charles. Senior Specialist, American Division of Law. The USA patriot Act: A Legal Analysis. 15 de abril de 2002. Congressional Research Service. The Library of the Congress.

DURAN, Camila Villard. Fragilidades jurídicas na relação BC – bancos públicos. *Jota*, 10 maio 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/fragilidades-juridicas-na-relacao-bc-bancos-publicos-10052017>.

FERRAZ JÚNIOR, Tércio Sampaio Ferraz. *Introdução ao Estudo do Direito*. São Paulo: Atlas, 1994.

FERRAZ JÚNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. In: PIZOLIO, Reinaldo. GAVALDÃO JR., Jayr (Org.). *Sigilo Fiscal e Bancário*. São Paulo: Quartier Latin, 2005.

FILHO, Carlos Edison do Rêgo Monteiro; CASTRO, Diana Paiva de. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Coordenação). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019.

FILHO, José dos Santos Carvalho. O Poder Normativo das Agências Reguladoras. In: ARAGÃO, Alexandre Santos de (Org.). *O Poder Normativo das Agências Reguladoras*. 2. edição. Rio de Janeiro: Forense, 2011.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Weverton Gabriel Gomes. Princípios que regem o tratamento de dados no Brasil. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020.

FRAZÃO, Ana. Fundamentos da Proteção dos Dados Pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019.

GARNICA, Vitor Gabriel; KEMPFER, Marlene. *O fenômeno da captura e a independência das Agências Reguladoras no Brasil*. Revista Brasileira de Filosofia do Direito. Belém, v. 5, n. 2, Jul/Dez 2019.

GILARDI, F. The Formal Independence of Regulators: a comparison of 17 countries and 7 sectors. *Swiss Political Science Review*, v. 11, n. 4, p. 139-167, 2005. GUTIERREZ, L. Regulatory Governance in the Latin American Telecommunications Sector. *Utilities Policy*, n. 11, 2003. GHEVENTER, A. *Autonomia versus controle: origens do novo marco regulatório antitruste na América Latina e seus desafios sobre a democracia*. Belo Horizonte: Editora da UFMG, 2005.

GUTIERREZ, Andrei. Da Autoridade Nacional de Proteção de Dados (ANDP) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Org.). *Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Revista dos Tribunais, 2019.

GUTIERREZ, L. Regulatory Governance in the Latin American Telecommunications Sector. *Utilities Policy*, n. 11, 2003.

KUN, Thomas S. *A estrutura das revoluções científicas*. São Paulo: Editora Perspectiva S.A., 1998.

LUCCA, Newton de; LIMA, Cintia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e Privacidade. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020.

MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019.

MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*. 33. ed. São Paulo: Malheiros, 2016.

_____. *Apontamentos sobre os agentes e órgãos públicos*. 4. ed. São Paulo: Revista dos Tribunais, 1984.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a proteção de dados não se aplica. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019.

MENDES, Conrado Hubner. Reforma do Estado e Agências Reguladoras: Estabelecendo os Parâmetros de Discussão. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000.

MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor. São Paulo: Ed. Revista dos Tribunais, nov.-dez. 2018, vol. 120.

NETO, Benedicto Porto. A Agência Nacional de Telecomunicações. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000.

NETO, Floriano de Azevedo Marques. A Nova Regulação Estatal e as Agências Independentes. In: SUNDFELD, Carlos Ari. *Direito Administrativo Econômico* (Org.). São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000.

_____. Agências Reguladoras. Instrumentos do fortalecimento do Estado. *Associação Brasileira de Agências de Regulação*, 20 jan. 2019. Disponível em: <http://abar.org.br/mdocs-posts/agencias-reguladoras-instrumentos-do-fortalecimento-do-estado/>.

_____. *Regulação Econômica e suas modulações*. Revista de Direito Público da Economia, Belo Horizonte, ano 7, n. 28, out./dez. 2009.

NUSDEO, Ana Maria de Oliveira. Agências Reguladoras e Concorrência. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000.

OLIVEIRA, Gisele; SALOMÃO, Alexa. Como o governo usou o BC para pagar as pedaladas. *O Estado de S. Paulo*, São Paulo, 06 fev. 2016. Disponível em: <https://www.estadao.com.br/infograficos/economia,como-o-governo-usou-o-bc-para-pagar-as-pedaladas,541349>.

OLIVEIRA, José Roberto Pimenta. Reforma do Estado e Direito Concorrencial. In: SUNDFELD, Carlos Ari (Org.). *Direito Administrativo Econômico*. São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000.

PEREIRA, Flávio Henrique Unes; CRUVINEL, Renan. A correção na Lei Geral de Proteção de Dados. *O Estado de São Paulo*, São Paulo, 03 dez. 2019. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/a-corregulacao-na-lei-geral-de-protecao-de-dados/>.

PEREZ, Marcos Augusto. *As Agências Reguladoras no Direito brasileiro: origem, natureza e funções*. Revista de Direito Administrativo e Constitucional. Curitiba, ano 2, n. 5 (2000).

PIETRO, Maria Sylvia Zanella Di. *Direito Administrativo*. 23. ed. São Paulo: Editora Atlas, 2009.

_____. *Transformações do Direito Administrativo*. Revista de Direito da Administração Pública, v. 1, n. 2, jun/dez 2016.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD)*. São Paulo: Saraiva, 2018.

REIS JÚNIOR, Antonio dos. O direito à privacidade na era digital: desafios em face da ameaça terrorista. In: BARBOSA-FOHRMANN, Ana Paula; BARRETO, Gustavo Augusto Ferreira. *A vida dos direitos humanos*. Reflexões sobre questões atuais. Rio de Janeiro: Gramma, 2016.

RODOTA, Stefano. *A vida na sociedade da vigilância - a privacidade hoje*. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SALINAS, Natasha Schmitt Caccia. *A intervenção do Congresso Nacional na Autonomia das Agências Reguladoras*. Revista Estudos Institucionais. Rio de Janeiro, v. 5, n.2, maio/dez. 2019.

SANTANNA, Luciano Portal. *Autorregulação supervisionada pelo Estado: desenvolvimento de um sistema de correção para o mercado de corretagem de seguros, resseguros, capitalização e previdência complementar aberta*. Revista de Direito Administrativo, Rio de Janeiro, v. 257, p. 183-211, mai. 2011. ISSN 2238-5177. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/8591/7327>.

SARLET, Ingo Wolfgang. In: SARLET, Ingo Wolfgang; MITIDIERO, Daniel; MARINONI, Luiz G. (Org.). *Curso de direito constitucional*. 9. ed. São Paulo: Saraiva, 2020.

SARMENTO, Daniel. Interesses Públicos vs. Interesses Privados na Perspectiva da Teoria e da Filosofia Constitucional. In: SARMENTO, Daniel (Org.). *Interesses Públicos versus Interesses Privados: Desconstruindo o Princípio da Supremacia do Interesse Público*. 2.ed. Rio de Janeiro: Lumen Juris, 2007.

SILVA, Carlos Bruno Ferreira da. *Proteção de Dados e Cooperação Transacional. Teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 26. ed. São Paulo: Malheiros, 2006.

SILVA, Mariana Batista da. *Independência após a delegação? Uma análise exploratória da interferência política nas Agências Regulatórias Brasileiras*. 2010. Dissertação (Mestrado em Ciência Política). Universidade Federal de Pernambuco, Recife, 2010.

SUNDFELD, Carlos Ari. Introdução as Agências Reguladoras. In: SUNDFELD, Carlos Ari. *Direito Administrativo Econômico* (Org.). São Paulo: Sociedade Brasileira de Direito Público, Malheiros, 2000.

SOMBRA, Thiago Luís Santos. *Fundamentos da Regulação da Privacidade e Proteção de Dados Pessoais*. São Paulo: Revista dos Tribunais, 2019.

TASSO, Fernando Antonio. Lei Geral de Proteção de Dados Comentada. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: um cotejamento com o CDC. In: LIMA, Cintia Rosa Pereira de (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2019.

VAINZOF, Rony. *Lei Geral de Proteção de Dados Comentada*. In: MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Org.). 2. ed. São Paulo: Revista dos Tribunais, 2019.

VASCONCELOS, Beto; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; SILVA, Milena Donato da (Org.). *Lei Geral de Proteção de Dados Pessoais no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019.

ZOCKUN, Maurício; ZOCKUN, Carolina Zancaner. *A relação de sujeição especial no direito brasileiro*. Revista de Direito Administrativo e Constitucional. Curitiba, n. 77, jul./set. 2019.

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 04 abr. 2015, p. 85. Disponível em: <<https://cryptome.org/2015/07/big-other.pdf>>.