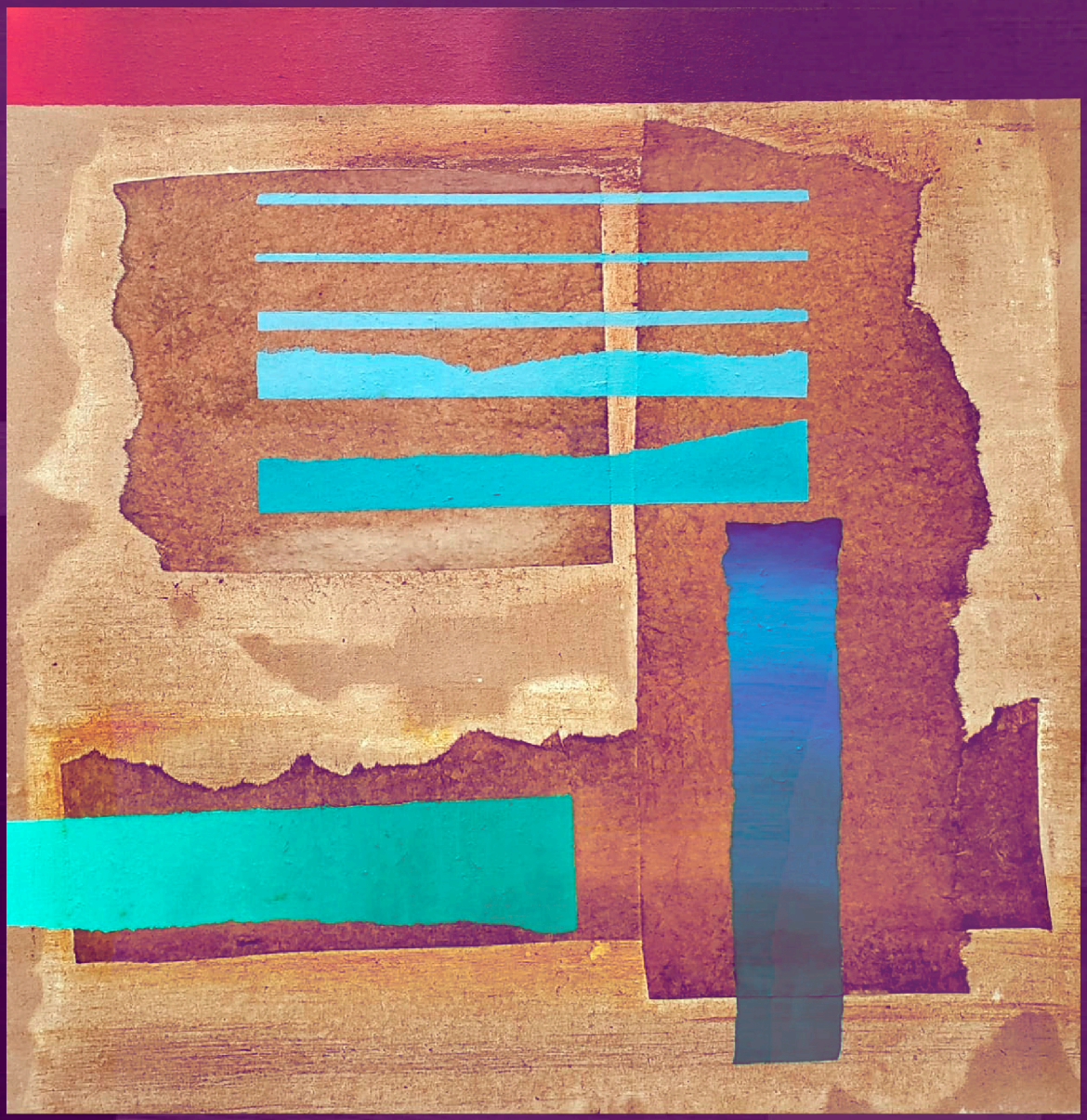
TRIBUNAL DE CONTAS DO ESTADO
DO RIO GRANDE DO SUL

# LEI GERAL DE PROTEÇÃO DE DADOS E O PODER PÚBLICO

ORGANIZADORES
DANIELA COPETTI CRAVO
DANIELA ZAGO GONÇALVES DA CUNDA
RAFAEL RAMOS



OVERTURE - LISIANNE ZAGO GONÇALVES

2021

CEDIM
CENTRO DE ESTUDOS EM DIREITO MUNICIPAL

prefeitura de PORTO ALEGRE
PROCURADORIA-GERAL DO MUNICÍPIO

Daniela Copetti Cravo
Daniela Zago Gonçalves da Cunda
Rafael Ramos
(Organizadores)

# LEI GERAL DE PROTEÇÃO DE DADOS E O PODER PÚBLICO

Tribunal de Contas do Estado do RS
Prefeitura de Porto Alegre
Porto Alegre
2021

L525

Lei Geral de Proteção de Dados e o poder público / organizadores: Daniela Copetti Cravo ; Daniela Zago Gonçalves da Cunda ; Rafael Ramos. – Porto Alegre : Escola Superior de Gestão e Controle Francisco Juruena ; Centro de Estudos de Direito Municipal, 2021.
223 p.

ISBN 978-65-81347-02-0.

1. Direito Público. 2. Direito Constitucional. 3. Lei Geral de Proteção de Dados. I. Cravo, Daniela Copetti. II. Cunda, Daniela Zago Gonçalves da. III. Ramos, Rafael. IV. Rio Grande do Sul. *Tribunal de Contas do Estado. Escola Superior de Gestão e Controle Francisco Juruena.* V. Porto Alegre. *Procuradoria-Geral do Município. Centro de Estudos de Direito Municipal.*

CDDir 341.27

Catalogação na Publicação: Liziane Ungaretti Minuzzo - CRB 10/1643

# APRESENTAÇÃO

A obra, ora apresentada ao público, reúne artigos de um seleto grupo de estudiosos a respeito do tema da proteção de dados pessoais. Tal temática já apresentava indiscutível relevância no ordenamento pátrio, seja pela previsão constitucional de direitos, como a inviolabilidade da vida privada e da intimidade (artigo 5º, inciso X), a garantia do *Habeas Data* (artigo 5º, inciso LXXII), a proibição da invasão de domicílio (artigo 5º, inciso XI) e o sigilo de correspondência (artigo 5º, inciso XII), seja pela existência de normas infraconstitucionais setoriais sobre o tema.

No entanto, tal proteção não era suficiente nem adequada à realidade tecnológica e digital, nomeadamente pela incontestável percepção de que não há dados insignificantes. Mesmo meros fragmentos de dados, se conjugados e utilizados de maneira inadequada, podem gerar prejuízos ao livre desenvolvimento da personalidade dos indivíduos.

Da mesma forma, a existência de legislações setoriais também não era suficiente para uma tutela adequada, justamente pelo problema da fragmentação e do constante fluxo de dados entre diferentes esferas e setores (cita-se, por exemplo, o compartilhamento de dados entre entes privados e públicos).

Em razão disso, a doutrina brasileira sempre defendeu a necessidade de se reconhecer a proteção de dados pessoais como um direito fundamental autônomo, indo além da tutela da intimidade e da privacidade. Ainda, a doutrina, inspirada na experiência internacional, buscou que a proteção desse direito fosse sistematizada em uma legislação contemporânea, uniforme e geral sobre o tema.

À luz dos acontecimentos dos últimos anos, no Brasil, pode-se afirmar que tais anseios e expectativas da doutrina acabaram sendo consagrados. A esse respeito, veja a edição da LGPD (Lei Geral de Proteção de Dados), em 2018; a Proposta de Emenda à Constituição (PEC) nº 17, em 2019; e o julgamento da Medida Cautelar da ADI 6387, pelo Supremo Tribunal Federal (STF), em 2020.

Tais acontecimentos, que cumularam com a recente entrada em vigor da LGPD, despertaram o interesse no desenvolvimento da presente publicação. Muitas obras já foram publicadas com tal escopo, é bem verdade. Contudo, o grande diferencial do presente livro é seu enfoque na aplicação da LGPD, nas relações em que a Administração Pública figura num dos polos da relação jurídica. Tal destaque assume elevada importância, na medida em que a LGPD dedica um capítulo específico sobre o "tratamento de dados pessoais pelo poder público". De outro lado, a fim de dar amplo conhecimento ao público interessado e na linha do papel pedagógico dos Tribunais de Contas, a obra é publicada em formato E-book.

Ademais, a obra é fruto de um exitoso diálogo institucional entre o Centro de Estudos de Direito Municipal (CEDIM) da Procuradoria-Geral do Município de Porto Alegre e a Escola Superior de Gestão e Controle Francisco Juruena do Tribunal de Contas do Estado do Rio Grande do Sul (TCE-RS), assim como as Comissões de Sustentabilidade e LGPD do TCE/RS. Referidos órgãos, desde a publicação da LGPD, têm trabalhado intensamente para realizar as necessárias adequações, assim como disseminar a cultura da proteção de dados pessoais entre servidores e a população em geral, através da organização de palestras, seminários e cursos[1].

O CEDIM, por exemplo, ainda em 2019, organizou evento sobre a LGPD, com a participação de dois professores da Faculdade de Direito da UFRGS (Fabiano Menke e Rafael Dresch da Silveira) e, em 2020, organizou curso para servidores com foco específico na aplicação da lei na Administração Pública, coordenado pela procuradora municipal, Daniela Copetti Cravo. Finalmente, em parceria com o TCE-RS, foi organizado o seminário Lei Geral de Proteção de Dados e o Poder Público, com algumas das maiores autoridades do tema, no país: Danilo Doneda, Ingo Wolfgang Sarlet, Têmis Limberger, Regina Ruaro, Fabiano Menke, entre outros.

O Tribunal de Contas do Estado do Rio Grande do Sul, além dos eventos realizados junto à Escola de Gestão, por sua vez, instituiu Comissão de Estudos sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), designada pela Portaria nº 679/2020, sob a Coordenação do Conselheiro Substituto, Roberto Loureiro, que apresentou Relatório Final (no início de dezembro/2020), especificando temáticas

[1] TCE/RS - Webconferência: Lei Geral de Proteção de Dados e o Poder Público – Mesa, disponível em <https://www.youtube.com/watch?v=z3xCD-rK0tE>; TCE/RS - Webconferência: Lei Geral de Proteção de Dados e o Poder Público - Mesa 2, disponível em <https://www.youtube.com/watch?v=Bn_0f4DgyMs>; e Webinário TCE-RS - Lei Geral de Proteção de Dados (LGPD), disponível em https://www.youtube.com/watch?v=HPVP3QjCDuY.

atinentes ao tratamento de dados pessoais pelo Poder Público; etapas de adequação; necessidade de estrutura permanente de gestão, com considerações sobre o controlador, operador e encarregado, comitê permanente de gestão; considerações sobre a nova política de proteção de dados pessoais, detalhando sua abrangência, publicidade, necessidade de revisão da política de segurança da informação, inventário de dados pessoais e, também, sobre a importância de material de apoio, assim como a divulgação de estudos aos órgãos e entes fiscalizados. Conjuntamente, a proteção e a responsável transparência de dados, de maneira a viabilizar o controle social, são temáticas desenvolvidas pela Comissão de Sustentabilidade do TCE/RS.

Enfim, a presente obra é o coroamento dessa exitosa parceria entre dois órgãos preocupados com o aperfeiçoamento da atividade administrativa brasileira e com a proteção e promoção, do recém-reconhecido, pelo Supremo Tribunal Federal, direito fundamental à proteção de dados pessoais (ADI 6.387).

Daniela Copetti Cravo
Daniela Zago Gonçalves da Cunda
Rafael Ramos

# PREFÁCIO

A proteção dos dados pessoais alcançou uma dimensão sem precedentes, no âmbito da assim chamada sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática e da ampla digitalização que já assumiu um caráter onipresente e afeta todas as esferas da vida social, econômica, política e cultural contemporânea, no Mundo, fenômeno comumente designado de "*Ubiquituous Computing*"[2].

O Direito, portanto, como estrutura organizacional e normativa regulatória de tais esferas e respectivas relações, não poderia deixar de ser convocado a lidar com o fenômeno, cuja dinamicidade e complexidade, contudo, colocam cada vez mais à prova a própria capacidade das ordens jurídicas convencionais (aqui compreendidas em sentido amplo, internacional e nacional) de alcançar resultados satisfatórios, particularmente quando se trata de assegurar um mínimo de proteção efetiva aos direitos humanos e fundamentais afetados.

É por tais razões que se pode acompanhar o entendimento de Carlos Alberto Molinaro e Gabrielle Bezerra S. Sarlet, de que a proteção de dados pessoais - e o reconhecimento de um direito fundamental correspondente -, de certo modo, "confere um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes"[3].

Assim, à vista de tal cenário, embora mais do que sabido que a proteção dos dados pessoais alcançou uma dimensão sem precedentes, no âmbito da assim chamada sociedade tecnológica, notadamente, a partir da introdução do uso da tecnologia da informática e da ampla digitalização, que já assumiu um caráter onipresente - global - e afeta todas as esferas da vida social, econômica, política e

---

[2] Cf., por todos, KÜHLING, Jürgen. Datenschutz und die Rolle des Rechts. *In*: STIFTUNG FÜR DATENSCHUTZ (Ed). **Die Zukunft der informationellen Selbstbestimmung**. Berlin: Erich Schmidt Verlag, 2016. p. 49.

[3] MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. **Direitos Fundamentais & Justiça**, a. 13, n. 41, p. 183-212, jul./dez. 2019.

cultural contemporânea no Mundo, o reconhecimento de um direito humano e de um direito fundamental à proteção de dados pessoais ainda não está totalmente consolidado.

Nesse sentido, note-se que, mesmo já no limiar da terceira Década do Século XXI, ainda existem Estados constitucionais, onde um direito fundamental à proteção de dados não é reconhecido, pelo menos na condição de direito expressamente positivado na Constituição, muito embora tal direito seja, em vários casos, tido como implicitamente positivado, sem prejuízo de uma mais ou menos ampla regulação legislativa e administrativa, ademais de significativo desenvolvimento na esfera jurisprudencial.

No caso do Brasil, inexiste, por ora, previsão expressa de direito fundamental autônomo à proteção de dados pessoais na CF88, embora tramite, no Congresso Nacional, a PEC nº 17/19 que tem, por escopo, a inserção de tal direito no inciso XII do artigo 5º da CF, ao lado dos direitos à inviolabilidade da comunicação de dados, correspondência e das comunicações telefônicas.

No campo doutrinário e jurisprudencial, contudo, os avanços têm sido expressivos, culminando no reconhecimento de um direito fundamental autônomo e implicitamente positivado pelo STF, em paradigmática decisão proferida pelo Plenário, chancelando provimento monocrático, em sede de liminar, da Ministra Rosa Weber, no bojo da ADI 6387 MC-Ref/DF, julgada em 06 e 07.05.20.

A justificação de um direito fundamental à proteção de dados pessoais, na condição de direito implícito, tem sido construída mediante uma interpretação sistemático-evolutiva do texto constitucional, a partir de um conjunto de princípios e direitos fundamentais, mas também de outros direitos não expressamente referidos na CF88.

Embora a CF88 faça referência, no art. 5.º, XII, ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas) e, no artigo 5º, LXXII, tenha instituído na ordem jurídica pátria a figura do *habeas data*, ação constitucional, com *status* de verdadeira garantia procedimental do exercício da autodeterminação informacional[4], tais preceitos - embora relevantes para a proteção de dados pessoais - não substituem nem a sua consagração textual como direito fundamental autônomo expressamente positivado,

[4] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, p. 185-216, jul./dez. 2018.

nem, por si só, constituem fundamento para o seu reconhecimento como direito implícito.

À míngua, portanto, de expressa previsão de tal direito, pelo menos na condição de direito fundamental explicitamente autônomo, no texto da CF88, e a exemplo do que ocorreu em outras ordens constitucionais, o direito à proteção dos dados pessoais pode (e mesmo deve!) ser associado e reconduzido - exatamente como o fez o STF - a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam - aqui nos termos da CF - os direitos à privacidade e à intimidade[5], e um direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa[6].

À vista do exposto, há como aderir ao entendimento - hoje consagrado na literatura jurídica brasileira - de que, mediante uma leitura harmônica e sistemática do texto constitucional, a CF consagrou um direito fundamental implicitamente positivado à proteção de dados pessoais[7].

É de se sublinhar que, a exemplo do que se deu em outras ordens jurídicas, o reconhecimento de um direito fundamental à proteção de dados, no plano constitucional, foi precedido e sucedido, na esfera infraconstitucional, por uma série de diplomas legais e atos normativos, ademais de decisões judiciais, regulando a proteção de dados e dando-lhe expressão concreta.

Tal normativa é de grande relevância, não apenas para a compreensão do conteúdo e alcance do direito fundamental à proteção de dados na CF88, mas, também, para efeitos de seu diálogo com a legislação, jurisprudência e, mesmo,

---

[5] Cf. por todos DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.
[6] MOTA PINTO, Paulo**. Direitos de Personalidade e Direitos Fundamentais**: Estudos, *op. cit.*, p. 642 e ss.
[7] Cf., em especial, o já referido DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**, *op. cit.*, mas também, na sequência, entre outros, LIMBERGER, Têmis. **O Direito à Intimidade na Era da Informática**. Porto Alegre: Livraria do Advogado, 2007; RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade de informação. **Direito, Estado Sociedade**, n. 36, jan/jun. 2010, MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**. São Paulo: Saraiva, 2013, BIONI, Bruno Ricardo. **Proteção de Dados Pessoais***:* A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019. p. 90 e ss. Por último, v. SARLET, Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988, **Direitos Fundamentais & Justiça.** Belo Horizonte, ano 14, n. 42, p. 175-214, jan./jun. 2020.

doutrina sobre o tema, importa sublinhar que diversos diplomas legais em vigor já dispõem sobre aspectos relevantes da proteção de dados, destacando-se, aqui, a Lei de Acesso à Informação (Lei nº 12.527/2011) e o, assim chamado, Marco Civil da Internet (Lei nº 12.965/2014) e o respectivo Decreto que o regulamentou (Decreto nº 8.771/2016), mas, especialmente, a nova Lei Geral de Proteção de Dados - LGPD, que, finalmente, entrou em vigor em Setembro de 2020 -, destacando-se que a sua parte sancionatória só entrará em vigor em 2021 e a Autoridade Nacional de Proteção de Dados ainda não foi implementada e não iniciou, de fato, as suas atividades.

Assim, uma compreensão/interpretação/aplicação constitucionalmente adequada do direito fundamental à proteção de dados deverá, sempre, ser pautada por uma perspectiva sistemática, que, a despeito do caráter autônomo (sempre parcial), desse direito, não pode prescindir do diálogo e da interação (por vezes marcada por concorrências, tensões e colisões) com outros princípios e direitos fundamentais, que, dentre outros pontos a considerar, auxiliam a determinar o seu âmbito de proteção, inclusive mediante o estabelecimento de limites diretos e indiretos.

De particular relevância, no caso brasileiro - justamente pela existência, além da nova LGPD e de outras leis que versam sobre o tema -, é ter sempre presente que, independentemente de sua inclusão no texto da CF88, impõe-se, ao Estado, por força de seus deveres de proteção, não apenas zelar pela consistência constitucional do marco normativo infraconstitucional (inclusive da LGPD), no tocante aos diplomas legais isoladamente considerados, mas, também, de promover sua integração e harmonização produtiva, de modo a superar eventuais contradições e assegurar, ao direito fundamental à proteção de dados, sua máxima eficácia e efetividade.

Os deveres de proteção estatais, decorrentes da assim chamada dimensão objetiva do direito fundamental à proteção de dados pessoais e dos demais direitos fundamentais relevantes no contexto, vinculam, de modo direto e transversal, todos os poderes, funções, atos e agentes do poder público. Tal vinculação se dá em dois planos principais, o primeiro, impondo a proteção pelo poder público dos dados pessoais de pessoas naturais, em face de outros atores privados, incluindo aqui as pessoas jurídicas; ao passo que, no segundo nível, trata-se de o poder público

assegurar tal proteção na sua esfera interna de atuação, portanto, de eventuais violações decorrentes de ações e/ou omissões do próprio poder público.

Além do mais, cuida-se - também - de uma autovinculação, no sentido de o poder público, independentemente da existência de sanções específicas (como as previstas na LGPD), ou de uma autoridade independente de monitoramento e fiscalização, dar efetividade ao direito fundamental à proteção de dados pessoais, como, aliás, já está a ocorrer, gradualmente, em todos os níveis da Federação e em órgãos vinculados aos três poderes estatais.

É por tais razões, aqui sumariamente esboçadas, que recebemos com entusiasmo e, mesmo, alegria o convite formulado para prefaciar a obra que ora é publicada, versando sobre a Lei Geral de Proteção de Dados e o Poder Público, coordenada por DANIELA COPETTI CRAVO, DANIELA ZAGO GONÇALVES DA CUNDA e RAFAEL RAMOS.

A obra reúne contribuições de autores com expertise na área e explora - basta aqui lançar o olhar sobre o sumário - alguns dos principais temas que dizem respeito à aplicação da LGPD no e pelo poder público, assegurando tanto uma boa base teórica quanto oferecendo o instrumental para uma boa prática, de tal sorte que o leitor nela encontrará importantes subsídios, que, de resto, não se limitam ao setor público.

Assim, para não distanciarmos, demasiadamente, o leitor do conteúdo da obra, é o caso de parabenizar coordenadores e autores, desejando que a obra encontre a merecida receptividade, seja pelo jurista, seja por todos os que, no cotidiano, lidam com os inúmeros e muitas vezes nada simples problemas e desafios que dizem respeito à proteção dos dados pessoais e, com isso, à proteção e promoção de tantos outros princípios e direitos fundamentais.

Porto Alegre, 07 de dezembro de 2020.

**Ingo Wolfgang Sarlet**[8]

[8] Professor Titular e Coordenador do PPGD da Escola de Direito da PUCRS. Desembargador aposentado do TJRS. Advogado e parecerista. TCE/RS - **Webconferência**: Lei Geral de Proteção de Dados e o Poder Público - Mesa 1. Disponível em <https://www.youtube.com/watch?v=z3xCD-rK0tE>.

**SUMÁRIO**

**APRESENTAÇÃO** ____ **3**

**PREFÁCIO** ____ **6**

**PROTEÇÃO DE DADOS PESSOAIS E O PODER PÚBLICO: NOÇÕES ESSENCIAIS.**
***Marcelo Crespo*** ____ **16**

1 UMA BREVE VISÃO SOBRE A LGPD ____ 16

2 POR QUE FALAR DE PROTEÇÃO DE DADOS PESSOAIS NO PODER PÚBLICO? ____ 19

3 A LGPD E O TRATAMENTO DE DADOS PELO PODER PÚBLICO: ASPECTOS GERAIS ____ 22

4 CONSIDERAÇÕES FINAIS ____ 27

REFERÊNCIAS ____ 28

**PERSPECTIVAS GERAIS SOBRE OS DIREITOS DO TITULAR DOS DADOS NO PODER PÚBLICO**
***Daniela Copetti Cravo*** ____ **29**

1 INTRODUÇÃO ____ 29

2 PODER PÚBLICO COMO CONTROLADOR ____ 30

3 PECULIARIDADES DO PODER PÚBLICO ____ 32

4 INTERFACE ENTRE LAI E LGPD ____ 34

5 SEGREDOS COMERCIAL E INDUSTRIAL ____ 37

6 CONSIDERAÇÕES FINAIS ____ 41

REFERÊNCIAS ____ **42**

**OS DADOS NÃO PESSOAIS E A UTILIZAÇÃO DE TÉCNICAS DE ANONIMIZAÇÃO NO CONTEXTO DA PANDEMIA DE CORONAVÍRUS**
***Sérgio Marcos Carvalho de Ávila Negri***
***Carolina Fiorini Ramos Giovanini*** **45**

1 INTRODUÇÃO 45

2 DADOS PESSOAIS E DADOS NÃO PESSOAIS: CONCEITUAÇÃO A PARTIR DO MODELO EXPANSIONISTA 46

3 ANONIMIZAÇÃO: TRATAMENTO JURÍDICO E TÉCNICAS 48

4 OS RISCOS NA UTILIZAÇÃO RETÓRICA DA ANONIMIZAÇÃO E O USO DE CARTOGRAFIA DURANTE A PANDEMIA DE CORONAVÍRUS 50

5 CONCLUSÃO 54

REFERÊNCIAS 55

**DECISÕES AUTOMATIZADAS PELA ADMINISTRAÇÃO PÚBLICA: DIÁLOGOS ENTRE *LEADING CASES* E CRITÉRIOS PARA SUA IMPLEMENTAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**
***Cristiano Colombo*** **57**

1 INTRODUÇÃO 57

2 DECISÕES AUTOMATIZADAS PELA ADMINISTRAÇÃO PÚBLICA 57

3 DIÁLOGOS ENTRE *LEADING CASES* E CRITÉRIOS PARA IMPLEMENTAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS 60

4 CONSIDERAÇÕES FINAIS 65

REFERÊNCIAS 65

**A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E A LEI DE ACESSO À INFORMAÇÃO (LAI): UMA PROPOSTA DE INTERPRETAÇÃO SISTEMÁTICA**
***Têmis Limberger*** **67**

1 INTRODUÇÃO 67

2 ADMINISTRAÇÃO PÚBLICA EM REDE 68

3 DAS PREVISÕES NORMATIVAS BRASILEIRAS COM TEMÁTICA CONEXA 70

4 A TRANSPARÊNCIA E A ADMINISTRAÇÃO PÚBLICA 73

4.1 AMPLIAÇÃO DA TRANSPARÊNCIA E DESENVOLVIMENTO HUMANO GLOBAL E MUNICIPAL 74

4.2 CIBERTRANSPARÊNCIA: A CONSTRUÇÃO DE UM CONCEITO 75

5 PROTEÇÃO DOS DADOS PESSOAIS 78

6 CONSIDERAÇÕES FINAIS 81

REFERÊNCIAS 82

**A NECESSÁRIA RELAÇÃO ENTRE INTEROPERABILIDADE E COMPARTILHAMENTO DE DADOS, TRANSPARÊNCIA ADMINISTRATIVA E PRIVACIDADE: UMA ANÁLISE DO COMPORTAMENTO DA ADMINISTRAÇÃO PÚBLICA A PARTIR DA LGPD**
***Gustavo da Silva Santanna*** **85**

1 INTRODUÇÃO 85

2 A INTEROPERABILIDADE COMO PREMISSA PARA O ADEQUADO COMPARTILHAMENTO DE DADOS PELA ADMINISTRAÇÃO PÚBLICA 87

3 A TRANSPARÊNCIA ADMINISTRATIVA COMO CONDIÇÃO PARA O RESPEITO À PRIVACIDADE 92

4 CONSIDERAÇÕES FINAIS 99

REFERÊNCIAS 100

**TRÊS FUNDAMENTOS À CIDADE INTELIGENTE: A TÔNICA DA PROTEÇÃO DE DADOS NO PODER PÚBLICO**
***Isadora Formenton Vargas*** **103**

1 INTRODUÇÃO 103

2 PRIMEIRO FUNDAMENTO: AMPLO ESPECTRO CONCEITUAL 104

3 SEGUNDO FUNDAMENTO: ESTADO DA ARTE DA GOVERNANÇA DIGITAL NO BRASIL 106

4 TERCEIRO FUNDAMENTO: A TÔNICA DA PROTEÇÃO DE DADOS NO PODER PÚBLICO 108

5 CONSIDERAÇÕES FINAIS 111

REFERÊNCIAS 113

**GOVERNANÇA DE DADOS E O PODER PÚBLICO: PERSPECTIVAS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**
***José Luiz de Moura Faleiros Júnior*** **115**

1 INTRODUÇÃO 115

2 A POLÍTICA DE GOVERNANÇA DA ADMINISTRAÇÃO PÚBLICA FEDERAL DIRETA, AUTÁRQUICA E FUNDACIONAL (DECRETO Nº 9.203/2017) 116

3 INICIATIVAS BRASILEIRAS PARA A GOVERNANÇA DE DADOS 123

3.1 A GOVERNANÇA DE DADOS NO ÂMBITO FEDERAL (DECRETOS Nº 10.046/2019 E Nº 10.047/2019) 124

3.2 O EXEMPLO DO ESTADO DE PERNAMBUCO (DECRETO ESTADUAL Nº 49.265/2020) 129

3.3 O EXEMPLO DO MUNICÍPIO DE SÃO PAULO (DECRETO Nº 59.767/2020) 131

4 CONSIDERAÇÕES FINAIS 133

REFERÊNCIAS **134**

**O RECONHECIMENTO FACIAL NO SETOR PÚBLICO E A PROTEÇÃO DE DADOS PESSOAIS**

***Fabiano Menke***
***Sílvia Levenfus*** **138**

1 INTRODUÇÃO 138

2 O RECONHECIMENTO FACIAL E O SEU ENQUADRAMENTO NA LGPD 141

2.1 DELINEAMENTOS CONCEITUAIS ACERCA DO RECONHECIMENTO FACIAL 142

2.2 ENQUADRAMENTO NA LGPD 145

3 IMPLEMENTAÇÃO DO RECONHECIMENTO FACIAL NO PODER PÚBLICO BRASILEIRO 147

3.1 UTILIZAÇÃO NA SEGURANÇA PÚBLICA E NO CONTROLE DOS ADMINISTRADOS 149

3.2 DESAFIOS E RISCOS 152

4 CONCLUSÃO 155

REFERÊNCIAS 157

**A LGPD E O COMBATE AO CORONAVÍRUS**
***Guilherme Bier Barcelos*** **161**

1 INTRODUÇÃO 161

2 TRATAMENTO DE DADOS PESSOAIS E HIPÓTESES AUTORIZATIVAS 163

3 O CASO INLOCO 166

4 CONSIDERAÇÕES FINAIS 169

REFERÊNCIAS 170

**O DESAFIO DA LGPD PARA AS DEFENSORIAS PÚBLICAS NO BRASIL**
***Rafael A. F. Zanatta***
***Marina S. Kitayama*** **171**

1 INTRODUÇÃO 171

2 O ESCOPO DE APLICAÇÃO DA LGPD PARA AS DEFENSORIAS PÚBLICAS 173

3 DO ATENDIMENTO AOS DADOS SENSÍVEIS: PREOCUPAÇÕES COM ATIVIDADE-MEIO DAS DEFENSORIAS PÚBLICAS 174

4 LITÍGIOS ESTRATÉGICOS E ATUAÇÃO DADOCÊNTRICA: ATIVIDADES-FIM DAS DEFENSORIAS PÚBLICAS 177

5 CONSIDERAÇÕES FINAIS 182

REFERÊNCIAS 183

**A ATUAÇÃO DA ADMINISTRAÇÃO PÚBLICA NO PROCESSAMENTO DE DADOS PESSOAIS NOS TRANSPORTES PÚBLICOS**
***Gabriel Araújo Souto***
***Luísa Campos Faria***
***Samanta Barbosa Tiveron*** **185**

1 INTRODUÇÃO 185

2 OS PRINCÍPIOS DA LGPD APLICADOS À ADMINISTRAÇÃO PÚBLICA 186

3 HIPÓTESES DE PROCESSAMENTO DE DADOS PELA ADMINISTRAÇÃO PÚBLICA 189

4 A UTILIZAÇÃO PRÁTICA DE DADOS SENSÍVEIS EM TRANSPORTES PÚBLICOS 191

5 CONSIDERAÇÕES FINAIS 193

REFERÊNCIAS 194

**A PROTEÇÃO E A TRANSPARÊNCIA DE DADOS SOB A PERSPECTIVA DOS CONTROLES EXTERNO E SOCIAL E A GOVERNANÇA DIGITAL**
***Daniela Zago Gonçalves da Cunda***
***Letícia Ayres Ramos***
***Roberto Debacco Loureiro***
***Denizar Simioni*** **196**

1 CONSIDERAÇÕES INICIAIS 196

2 CONTEXTUALIZAÇÃO DO "MICROSSISTEMA DE PROTEÇÃO E DE TRANSPARÊNCIA DE DADOS" E O GOVERNO DIGITAL 201

3 IMPLEMENTAÇÃO DA LGPD NO TCE/RS COMO UMA ESTRUTURA PERMANENTE 206

3.1 DO CONTROLADOR, DO OPERADOR E DO ENCARREGADO 206

3.2 DO GRUPO PERMANENTE DE GESTÃO 209

3.3 DA REGULAMENTAÇÃO DE NOVA POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS 210

3.4 DA REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 210

3.5 DO INVENTÁRIO DE DADOS PESSOAIS 211

3.6 DA PUBLICAÇÃO DAS HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS 212

4 A NECESSÁRIA COMUNICAÇÃO DA LGPD COM OS NORMATIVOS QUE TUTELAM A TRANSPARÊNCIA DE DADOS E O CONTROLE SOCIAL 213

5 CONSIDERAÇÕES FINAIS 219

REFERÊNCIAS 220

# PROTEÇÃO DE DADOS PESSOAIS E O PODER PÚBLICO: NOÇÕES ESSENCIAIS

Marcelo Crespo[9]

## 1 UMA BREVE VISÃO SOBRE A LGPD

O surgimento da LGPD promoveu significativos movimentos corporativos na busca da adequação. As instituições têm buscado consultorias ou, por si mesmas, feito ajustes com vistas a conquistarem um programa de *privacy compliance*.

Para entender esse cenário, é importante notar que a LGPD não impede o tratamento de dados pessoais. Todavia, a legislação busca conscientizar que as instituições formulem programas de boa governança sobre dados pessoais, visando protegê-los.

Com vistas a compreender o seu escopo, confira-se a sua estrutura:

a) Capítulo I – Disposições preliminares (arts. 1 a 6).

b) Capítulo II – Do tratamento de dados pessoais (arts. 7 a 15)

c) Capítulo III – Dos direitos do titular (arts.16 a 22)

[9] Especialista em Direito Digital, Proteção de Dados, Direito Penal e *Compliance*. É Doutor (2012) e Mestre (2008) em Direito Penal pela USP e possui especialização, também em Direito Penal pela Universidade de Salamanca, na Espanha. É *Certified Compliance and Ethics Professional – International* (CCEP-I) pela *Society of Corporate Compliance and Ethics* (SCCE). Possui diversos cursos de extensão como o curso jurídico da Escola de Governança da Internet – EGI (2016) e a *International School of Law and Technology* (2017 e 2018). Possui extensa e demonstrada experiência no atendimento a empresas nacionais e multinacionais em demandas que envolvam Direito Digital, Penal e *Compliance*, tendo atuado em demandas consultivas e contenciosas (remoção de conteúdo, investigações, concorrências desleais, disputas contratuais), participando de gabinetes de gestão de crises, elaborando *risk assessments*, elaborando e revisando documentos e implementando programas de *Privacy Compliance*. Atualmente, é o gestor dos projetos de mapeamento de conformidade com a LGPD no PG Advogados. É o pioneiro no uso da expressão "Compliance Digital", além de ser entusiasta e evangelista dos pilares de um programa de *compliance* aliados a aspectos tecnológicos. Participou de audiência pública no Senado no âmbito de criação da LGPD (2018), na Câmara dos Deputados sobre o PL 2.630 ("fake news") e da CPI das Fake News (2020) da Assembleia Legislativa do Estado de São Paulo (2020). É autor dos livros Crimes digitais (Saraiva – 2011), Advocacia Digital 3.0 (Thomson Reuters – 2018), Advocacia Digital 4.0 (Thomson Reuters – 2020) e Compliance no Direito Digital (Thomson Reuters – 2020), além de possuir artigos publicados no exterior. Também assina artigos publicados em websites, revistas e periódicos. É palestrante, nacional e internacional, sobre temas relacionados ao Direito Digital e *Compliance*. Coordena e leciona na maior pós-graduação em Direito Digital e *Compliance* do país (Damásio Educacional) desde 2015 e é frequentemente convidado para ministrar aulas em diversos cursos de extensão e pós-graduação (FIA, PUC Campinas, INFI/FEBRABAN, Instituto ARC, ESENI).

d) Capítulo IV – Do tratamento de dados pessoais pelo Poder Público (arts. 23 a 36)
e) Capítulo V – Da transferência internacional de dados (arts. 37 a 45).
f) Capítulo VI – Dos agentes de tratamento de dados pessoais (arts. 46 a 51).
g) Capítulo VII – Da segurança e das boas práticas (arts 52 a 54).
h) Capítulo VIII – Da fiscalização (arts. 55 a 57).
i) Capítulo IX – Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (arts. 58 a 59).
j) Capítulo X – Disposições finais e transitórias (arts. 60 a 65).

Vale ressaltar que a LGPD se trata de uma lei principiológica, não sendo minuciosa a respeito das atividades que as instituições precisam providenciar para atingir a conformidade. Assim, observa-se que o art. 2º dispõe sobre os fundamentos[10] da proteção de dados pessoais e o art. 6º discorre sobre os princípios[11] a serem observados nas atividades de tratamento de dados pessoais. Verifica-se que são normas de direcionamento e não processos que devem ser implementados pelas pessoas físicas ou jurídicas.

Prosseguindo, o art. 7º define quais são as hipóteses legais[12] de tratamento dos dados pessoais, enquanto o art. 11 estabelece as hipóteses para o tratamento dos dados sensíveis[13]. As bases legais preconizadas pela LGPD para o tratamento

[10] São fundamentos o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
[11] São princípios a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.
[12] São hipóteses legais que são o consentimento do titular, a execução de obrigação legal ou regulatória pelo controlador, a execução de políticas públicas pela Administração Pública, a realização de estudos por órgão de pesquisa, a execução de contrato ou procedimentos preliminares, o exercício regular de direitos em processos judiciais, administrativos ou arbitrais, a proteção da vida ou incolumidade física de alguém, para a tutela da saúde, para atender interesses legítimos do controlador ou de terceiro e, por fim, para a proteção do crédito.
[13] São eles o consentimento, o cumprimento de obrigação legal ou regulatória, a pesquisa realizada por órgãos de pesquisa, a proteção da vida ou incolumidade física do titular ou terceiro, a tutela da saúde, o exercício regular de direitos inclusive em contratos ou processos administrativos, judiciais ou arbitrais, bem como o tratamento compartilhado de dados pela Administração Pública para a execução de políticas públicas e, por fim, a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

dos dados pessoais nada mais são que fundamentos legais que devem respaldar cada fluxo de dados pessoais.

Como visto e, em resumo, os fundamentos, princípios e hipóteses legais de tratamento de dados não estabelecem concretamente os processos que devem ser adotados pelas instituições para atingirem a conformidade. No entanto, na prática, são amplos direcionamentos que, unidos, constituem proteções e limitações para o tratamento de dados pessoais.

Outras disposições que direcionam ações que as instituições precisam providenciar são as referentes ao atendimento dos direitos dos titulares, com especial atenção aos que estão previstos no art. 18. Referidos direitos são os relativos à confirmação da existência, ao acesso aos dados, à correção, à anonimização, à portabilidade, à eliminação, à informação das entidades com as quais há tratamento compartilhado, à informação sobre a possibilidade de não fornecer o consentimento e as consequências disso, além da evidente possibilidade de revogação do consentimento. Ressalte-se, todavia, que as instituições são livres para determinar como serão acolhidos estes direitos, haja vista que podem ser atendidos por plataforma online, número telefônico exclusivo ou compartilhado com outras funções, e-mail, atendimento pessoal, softwares de automatização e quaisquer outras possibilidades.

Observa-se, ainda, que, mesmo quando a lei fala em medidas técnicas de proteção aos dados pessoais, a legislação não é específica. Veja-se que, no art. 46, a LGPD determina que os "agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Em outras palavras, a legislação não menciona quais são as ferramentas técnicas adequadas.

No que concerne ao programa de *privacy compliance*, o art. 50 da LGPD estabelece normas a seu respeito. Embora a redação não preveja, expressamente, a obrigatoriedade da implementação desse programa - já que apenas expõe que é uma possibilidade -, a legislação aponta os elementos mínimos[14] do programa de *compliance*.

[14] São eles: a demonstração do comprometimento do controlador em adotar processos e políticas que assegurem o cumprimento das normas e boas práticas de proteção de dados pessoais, a aplicação

Observada a estrutura geral da LGPD, serão tratados, nos capítulos abaixo, conceitos fundamentais e aspectos gerais sobre a proteção de dados pessoais no âmbito do Poder Público.

## 2 POR QUE FALAR DE PROTEÇÃO DE DADOS PESSOAIS NO PODER PÚBLICO?

O uso massivo de dados pessoais, nos mais diversos aspectos das nossas vidas, impõe que a atividade normativa destinada à proteção de dados seja incrementada. Nesse sentido, mais de cem países já instituíram leis de proteção de dados pessoais.

Com efeito, uma lei de proteção de dados pessoais, em regra, constitui um marco regulatório que estabelece direitos para o cidadão sobre seus dados, independente de quem realize o tratamento deles. Esses direitos visam proteger o cidadão, disponibilizando ferramentas que o garantam exercer, efetivamente, o controle sobre os seus dados pessoais. O grande desafio, no entanto, trata-se em conciliar a persecução dos objetivos consagrados em tais legislações, sem que se impeça a inovação.

A LGPD cumpre, exatamente, esse propósito, sendo aplicável tanto para a esfera privada quanto para a pública. Se, no âmbito da iniciativa privada, deseja-se não impedir a inovação e desenvolvimento econômico, no que diz respeito ao setor público o desafio é estabelecer um equilíbrio entre a proteção dos dados dos cidadãos e o tratamento desses dados para a elaboração e execução de políticas públicas. O Poder Público, no âmbito das suas competências e responsabilidade, realiza o tratamento de dados pessoas para as mais variadas finalidades, inclusive na prestação de serviços.

Evidentemente, nosso sistema jurídico fornece elementos para a proteção dos dados pessoais, visando evitar que sejam utilizados de forma irregular pelo Poder Público. Um exemplo é a garantia da inviolabilidade do sigilo financeiro e fiscal dos cidadãos, os quais somente podem ser acessados por ordem judicial ou pelas

---

do programa a todo o conjunto de dados pessoais que estejam sob seu controle, a adaptação à estrutura, escala e ao volume das operações e sensibilidade dos dados, o estabelecimento de políticas e salvaguardas baseados em avaliação sistemática de risco, a busca pelo estabelecimento de relação de confiança com o titular dos dados, a integração com a estrutura geral de governança com mecanismos de supervisão internos e externos, a existência de plano de resposta a incidente e remediação e, ainda, que seja atualizado constantemente.

autoridades autorizadas por lei, como é o caso do Conselho de Controle de Atividades de Financeiras (COAF). No entanto, ainda há muitos dados pessoais que são compartilhados com o Poder Público. Como exemplo, o Cadastro de Pessoas Físicas (CPF), Cadastro de Imóveis Rurais (Cafir), Certidão de Registro de Imóveis Urbanos, Nota Fiscal Eletrônica (NF-e), sistema de emissão de Certidão de Regularidade Fiscal perante a Fazenda Nacional, entre outros.

A LGPD não é, propriamente, um tema novo quando pensamos nas adequações que as instituições privadas necessitarão providenciar. Mas, um ponto ainda não muito explorado é o do tratamento de dados no âmbito do setor público. Vale, então, ressaltar, que a LGPD se aplica a qualquer órgão ou entidade pública, bem como a empresas públicas e sociedades de economia mista, conforme se extrai da leitura do seu art. 3º.

Nos termos do art. 4º, a legislação indicou quais tratamentos de dados não estão sujeitos à lei, sendo: os realizados para fins exclusivamente jornalísticos e artísticos; acadêmicos; fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.[15] Também não se aplica a LGPD aos casos de tratamentos de dados provenientes de fora do território nacional, os quais 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 à LGPD.

É importante, ainda, ressaltar alguns conceitos:

a) Considera-se titular de dados pessoais não só o cidadão contribuinte, mas os servidores, empregados públicos, gestores públicos, pessoas físicas com as quais o órgão ou entidade pública possua alguma relação contratual;

[15] A LGPD impõe limitações ao tratamento de dados para essas finalidades, o que se encontra nos parágrafos do art. 4º, que diz que "Esses tratamentos de dados serão regidos 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; Só será admitido o tratamento de dados para tais finalidades por pessoa jurídica de direito privado em procedimentos sob a tutela de pessoa jurídica de direito público, sendo certo que os dados pessoais constantes de bancos de dados constituídos para tais finalidades não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, exceção feita às controladas pelo Poder Público".

b) Considera-se controlador a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. No âmbito público, figura-se como controlador os órgãos públicos, entidades públicas, empresas públicas ou sociedades de economia mista que decidem sobre o tratamento de dados pessoais.
c) Considera-se operador, a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
d) Considera-se encarregado, a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.
e) O uso compartilhado de dados, a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
f) São órgãos de pesquisa, as entidades da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituídas sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Universidades públicas e entidades de pesquisa pública, como a Fundação Oswaldo Cruz, se enquadram nesta definição.

O princípio da transparência figura como requisito fundamental da sociedade contemporânea, conforme amplamente defendido pela doutrina e pela sua positivação na Constituição Federal de 1988. No âmbito infraconstitucional, destaca-se o surgimento da Lei de Acesso à Informação - LAI (Lei nº 12.527 de 2011), a qual é considerada como um marco importante para integrar-se ao tema da proteção de dados pessoais. Nesse sentido, o Grupo de Trabalho do Artigo 29 (WP29), no âmbito da União Europeia, em um parecer sobre dados abertos, afirmou que o propósito de

garntir o acesso à informação dos órgãos públicos consiste em permitir que haja transparência e controle sobre tais entidades. Para o WP29 "os objetivos primários de direitos de acesso à informação têm a ver com a salvaguarda da transparência dos agentes públicos, com o reforço dos controles democráticos". Inclusive, esse é o objetivo do art. 31 da LAI, qual seja, o equilíbrio de interesses entre o princípio da transparência *versus* a proteção de dados. Assim, constata-se que o gestor público deve conferir proteção para ambos os direitos.

A respeito do regramento instituído pela LGPD, quanto ao tratamento de dados pessoais pelo Poder Público no Capítulo IV, verifica-se a conexão da legislação com a LAI. Observam-se, ainda, diversas regras regulamentando o compartilhamento dos dados pessoais, a transparência e as bases legais. A LGPD, inclusive, estipulou disposições normativas específicas para as empresas públicas e sociedades de economia mista que, ora atuam como empresas privadas, ora como gestoras ou executoras de políticas públicas.

## 3 A LGPD E O TRATAMENTO DE DADOS PELO PODER PÚBLICO: ASPECTOS GERAIS

Muito se fala da repercussão da Lei Geral de Proteção de Dados (LGPD) sob a perspectiva da iniciativa privada. Contudo, devido à transversalidade inerente à própria lei em questão, não se deve perder de vista que sua aplicabilidade se estende a qualquer tipo de "tratamento de dados pessoais" e alcança também o Poder Público, que deve se adequar para cumprir as obrigações ali impostas[16].

A relevância do tema "proteção de dados" pelo Poder Público pode ser percebida pela dedicação do Capítulo IV ao tema.

Observa-se que o Poder Público detém prerrogativas e atribuições para alcançar finalidades públicas, havendo uma assimetria de informação na relação entre o detentor do dado e o Poder Público. Nesse sentido, os órgãos públicos obtêm massivas quantidades de dados pessoais e dados pessoais sensíveis, em virtude da obrigatoriedade da entrega dessas informações pelos cidadãos. Afinal de contas, não é possível adquirir um imóvel ou veículo automotor, ser atendido em hospitais, emitir a Carteira Nacional de Habilitação e o Título de Eleitor, entre outras

[16] PINHEIRO, Patricia PECK. **Proteção de Dados Pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2.ed. São Paulo: Saraiva Educação, 2020.

tantas hipóteses, sem que concedamos nossos dados pessoais. Deveria, assim, haver maior transparência nesses tratamentos, considerando a dicotomia “compulsoriedade” e “atendimento de políticas públicas”.

Há, todavia, hipóteses claramente excepcionais de tratamento de dados pessoais pelo Poder Público sem que haja a incidência da LGPD. Referimo-nos ao inciso III do art. 4º, o qual prescreve que a LGPD não se aplica ao “tratamento de dados pessoais, realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais”.

Sujeitam-se à aplicação da LGPD, portanto, os órgãos públicos da administração direta dos Poderes Executivo, o Poder Legislativo, o Poder Judiciário, os Tribunais de Contas e o Ministério Público, bem como as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas, direta ou indiretamente, pela União, Estados, Distrito Federal e Municípios (art. 1º, parágrafo único da Lei nº 12.527/2011). Além disso, os serviços notariais e de registro, exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público.

Os entes públicos possuem legitimidade para realizar o tratamento de dados pessoais visando ao atendimento de finalidades públicas, na persecução do interesse público, para que sejam executadas competências ou atribuições legais, conforme expõe o art. 23 da LGPD. Contudo, necessita-se que sejam transmitidas informações claras e precisas sobre a previsão legal, finalidade, procedimentos e práticas para a execução dessas atividades em canais de acesso facilitado, além de terem que indicar um encarregado de proteção de dados pessoais.

Com vistas a otimizar o processo de indicação de escolha do encarregado, no Poder Público, a Secretaria de Governo Digital do Ministério da Economia publicou, no dia 22 de outubro de 2020, a Instrução Normativa DEGDI nº 100, de 19 de outubro de 2020, definindo, entre outras questões, o perfil do encarregado que deve ser indicado pelos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP. Compõem o SISP os órgãos da administração direta, autárquica e fundacional do Poder Executivo Federal.

Segundo estabelecem os incisos do §1º do artigo 1º da referida Instrução, o encarregado deve possuir como requisitos mínimos: a) experiência na análise e

elaboração de respostas de pedido(s) de acesso à informação pelo Serviço de Informação ao Cidadão e/ou Ouvidoria; b) conhecimentos multidisciplinares essenciais à sua atribuição, incluindo as áreas de gestão, segurança da informação, gestão de riscos, tecnologia da informação, proteção da privacidade e governança de dados; e c) conclusão dos cursos de Proteção de Dados no Setor Público e Governança de Dados ou equivalente, quando disponíveis na Escola Virtual de Governo.

Na esfera municipal, ressaltam-se as iniciativas elaboradas pelas prefeituras municipais de São Paulo e Porto Alegre, quanto à necessidade de conformidade com a legislação de proteção de dados. O município de São Paulo elaborou o Decreto nº 59.767, de 15 de setembro de 2020, regulamentando a LGPD no âmbito administração direta e indireta municipal. Preconiza o art. 5 do referido decreto que o controlador-geral do município assumirá a posição de encarregado pelo tratamento de dados pessoais. Já, em Porto Alegre, instaurou-se um Comitê Gestor de Proteção de Dados, por meio do Decreto nº 20.777, de 28 de outubro de 2020, visando a definir e formular estratégias, diretrizes e procedimentos para adequação com a LGPD.

No que concerne às hipóteses legais de tratamento de dados, pelo Poder Público, verifica-se que estas decorrem de interpretação sistemática do art. 7º complementado pelo disposto no art. 23 da legislação de proteção de dados. Devemos lembrar, ainda, que há entes públicos que não executam políticas públicas, mas cumprem atribuição ou competência constitucional, como é o caso do Poder Judiciário, do Poder Legislativo, do Ministério Público e Defensoria Pública. Nem por isso deixam de ter legitimidade para tratar dados pessoais.

Já não fossem suficientes os princípios previstos no art. 37 da CF88[17], os entes públicos também devem zelar pelo cumprimento dos princípios expostos no art. 6º[18] da LGPD. Com isso, temos uma excelente combinação de princípios que, sendo respeitados, darão maior garantia da proteção de dados pessoais.

No art. 24, da LGDP, verifica-se que as empresas públicas e as sociedades de economia mista, que atuarem em regime de concorrência, nos termos do art. 173 da CF, deverão receber o mesmo tratamento dado às pessoas jurídicas de direito

[17] São eles: legalidade, impessoalidade, moralidade, publicidade e eficiência.
[18] São eles: adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

privado não públicas. Quando as empresas públicas e as sociedades de economia mista estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão tratamento igual ao conferido aos órgãos e às entidades do Poder Público.

Como exemplo, podemos mencionar uma instituição financeira pública, que estará sujeita ao mesmo tratamento como se fosse privada, quando tratar dados dos correntistas. No entanto, na operacionalização de políticas públicas, será conferido, às instituições, o mesmo tratamento dedicado pela LGPD aos órgãos e às entidades do Poder Público. É o caso do tratamento dos dados pessoais para fins do FGTS, do Programa de Integração Social (PIS) ou do Seguro-Desemprego.

O art. 26 da LGPD também estabelece que o compartilhamento de dados pessoais deva atender finalidades específicas relacionadas à execução de políticas públicas, respeitando os princípios expostos pela lei (art. 6). Uma clara hipótese de uso compartilhado de dados pela Administração Pública é a regulada pela Portaria nº 1.384/16 da Receita Federal que “disciplina a disponibilização, pela Secretaria da Receita Federal do Brasil, de dados não protegidos por sigilo fiscal a órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional”.

Além disso, a Receita Federal, em processo de adequação às disposições normativas da LGPD, recentemente, publicou a Portaria nº 4.255, de 27 de agosto de 2020 e revogou o processo imediato de disponibilização a terceiros de dados constantes em Notas Fiscais Eletrônicas (NF-e). Segundo dispõe o §4º do art. 1 desse novo ato normativo, para que haja o compartilhamento dos dados da NF-e, necessária se faz a prévia avaliação e identificação de risco institucional ou risco ao sigilo individual da pessoa física ou jurídica.

Ressalta-se, ademais, que o Poder Executivo Federal, em atenção à LGPD, editou o Decreto nº 10.046, de 9 de outubro de 2019, mediante o qual estabeleceu diretrizes e normas para o compartilhamento de dados na administração pública federal e instituiu o Cadastro Base do Cidadão e o Comitê Central de Governança dos Dados. Assim, o compartilhamento de dados será possível dentro dos limites especificados por três níveis diversos de confidencialidade, conforme se observa da leitura do art. 4° do citado decreto.

Por outro lado, o art. 26 da LGPD prescreve, como regra geral, a vedação da transferência de dados pessoais para entidades privadas. Excepcionalmente poderá haver a transferência quando houver: execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado,

observado o disposto na LAI; a indicação de um encarregado para as operações de tratamento de dados pessoais; previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (que deverão ser comunicados à autoridade nacional). Busca-se, com esses requisitos, prevenir fraudes e irregularidades, bem como proteger e resguardar a segurança e a integridade do titular dos dados, nos casos em que os dados forem acessíveis publicamente.

Nesse sentido, um ponto sensível será a discussão quanto à aceitabilidade, a partir da vigência da LGPD, dos acordos celebrados entre o Poder Público e as instituições financeiras, para disponibilização da base de dados pessoais dos seus servidores, mediante contraprestação pecuniária em favor da própria Administração Pública, como acontece com as chamadas "vendas de folha de pagamento" ou oferecimento dos conhecidos "empréstimos consignados". Isso porque, como as instituições financeiras utilizarão esses dados apenas para potencializar a oferta de seus produtos financeiros aos servidores, torna-se realmente muito discutível e polêmica a manutenção desta prática frente aos fundamentos e princípios da LGPD, sobretudo, ao se analisar a finalidade do tratamento dos dados pessoais em tais contratos.

Outro aspecto a ser analisado refere-se à violação da LGPD pelos órgãos públicos.

Prescreve o art. 31 que a ANPD poderá enviar informe com medidas cabíveis para fazer a cessação desta violação. A ANPD poderá, também, solicitar, nos termos do art. 32, que os agentes do Poder Público apresentem relatórios de impacto à proteção de dados pessoais e, diante disso, sugerir a adoção de padrões e boas práticas para o saneamento de inconformidades.

Ademais, vale ressaltar que as empresas públicas e sociedades de economia mista que, conforme art. 24 da LGPD, exerçam políticas públicas (envolvendo ou não a prestação de serviço público, nos termos do art. 175, CF), também estão sujeitas ao regime da LGPD, todavia com os temperamentos prescritos no Capítulo IV (arts. 31 e 32), em especial quanto ao tratamento de dados a ser realizado para estas finalidades[19]. No entanto, as pessoas jurídicas da Administração Indireta que prestam atividade econômica *stricto sensu* (nos moldes do art. 173, CF) estão

[19] CARVALHO, André Castro; CONTI, José Maurício; BLUM, Rita Peixoto Ferreira. **Aplicação da LGPD ao Setor Público: aspectos relevantes** *In* MONACO, Gustavo Ferraz de Campos; MARTINS, Amanda Cunha e Mello Smith; CAMARGO, Solano de (Orgs.). **Lei Geral de Proteção de Dados**: ensaios e controvérsias da Lei 13.709/18. São Paulo: Quartier Latin, 2020.

sujeitos ao regramento geral da LGPD, prescrito no Capítulo VIII. Assim, respeita-se o princípio da igualdade de tratamento concorrencial.

Nesse particular, uma atenção maior haverá de se ter no campo das instituições financeiras, a exemplo do Banco do Brasil e Caixa Econômica Federal, que possuem uma atuação híbrida, ou seja, de um lado concorrem com outros players do mercado bancário de varejo e, de outro, são utilizados como braço operacional de diversas políticas públicas (celebração de convênios, contratos de financiamento de habitação popular, programas de transferência de renda e auxílio financeiro).

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados, exclusivamente, dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico. A legislação recomenda, sempre que possível, a anonimização ou pseudonimização dos dados, bem como que sejam considerados os devidos padrões éticos relacionados aos estudos e às pesquisas.

A LGPD, ademais, trouxe outras regras protetivas para essa hipótese, como: a divulgação dos resultados ou excertos do estudo ou pesquisa não poderá revelar dados pessoais, o órgão de pesquisa será responsável pela segurança da informação e não poderá – em hipótese alguma – transferir os dados a terceiros; o acesso aos dados pessoais pelos órgãos de pesquisa para fins de realização de estudos em saúde pública será objeto de regulamentação pela ANPD e pelas autoridades da área de saúde e sanitárias, no âmbito de suas competências.

## 4 CONSIDERAÇÕES FINAIS

Diante do exposto, verificou-se que, a despeito do regramento diferenciado disposto na LGPD, o Poder Público, em todas as suas esferas, deve impulsionar medidas que estimulem a conformidade com a LGPD. Conforme se expôs, os órgãos públicos, diariamente, coletam e armazenam dados pessoais dos cidadãos, seja por obrigação legal, seja para fins de pesquisa, seja para execução de política pública, sempre perseguindo o interesse público.

Percebeu-se, ainda, quão importante deve o Poder Público ter atenção e observar as disposições normativas da Lei de Acesso à Informação e da LGPD. É que a transparência e a proteção de dados devem ser sopesadas em qualquer movimento ou decisão de compartilhamento de dados que possa ferir direito fundamental à privacidade de pessoa física ou jurídica. Analisaram-se, também, os aspectos gerais e controversos sobre o tratamento de dados pessoais pelo Poder Público e iniciativas dos órgãos públicos quanto à adequação com a LGPD.

Conclui-se, evidentemente, que ainda há muitos temas sensíveis e polêmicos a serem avaliados e solucionados, uma vez que o Brasil ainda é pouco familiarizado com a cultura da proteção de dados e privacidade, como é o caso da União Europeia. É natural que haja pontos nebulosos na aplicação da lei, sobretudo no âmbito do Poder Público. Atingir a conformidade com a LGPD, portanto, também depende de mudança cultural, sobretudo no setor público.

A consolidação da efetividade da ANPD, de forma preventiva ou repressiva, poderá realmente ser um instrumento de transformação qualitativa da sociedade brasileira, no campo da proteção de dados no âmbito setor público, todavia os recursos humanos, ou seja, a conscientização dos gestores e servidores será fundamental para que a promoção destas boas práticas e diretrizes aconteça de forma mais célere e duradoura.

## REFERÊNCIAS

CARVALHO, André Castro; CONTI, José Maurício; BLUM, Rita Peixoto Ferreira. Aplicação da LGPD ao Setor Público: aspectos relevantes**.** *In* MONACO, Gustavo Ferraz de Campos; MARTINS, Amanda Cunha e Mello Smith; CAMARGO, Solano de (Orgs.). **Lei Geral de Proteção de Dados**: ensaios e controvérsias da Lei 13.709/18. São Paulo: Quartier Latin, 2020.

CRESPO, Marcelo Xavier de Freitas; PINTO, Daniel Rodrigues; STADLER, Bianca Bona; SCAPINELLI JUNIOR, Marcelo Jesus Ferrari. Adequação e bases legais: o dilema do enquadramento legal das atividades de tratamento de dados pessoais. In CRESPO, Marcelo. **Compliance no Direito Digital**. Thomson Reuters: São Paulo, 2020.

PALHARES, Felipe. As funções do DPO no GDPR e do encarregado na LGPD. In CRESPO, Marcelo. **Compliance no Direito Digital**. Thomson Reuters: São Paulo, 2020.

PINHEIRO, Patrícia PECK. **Proteção de Dados Pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

# PERSPECTIVAS GERAIS SOBRE OS DIREITOS DO TITULAR DOS DADOS NO PODER PÚBLICO

Daniela Copetti Cravo[1]

## 1 INTRODUÇÃO

O Brasil acabou de dar um passo importante no tema da proteção de dados pessoais. Após aproximadamente 10 anos de debate e maturação do tema, entrou em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD): uma lei uniforme, transversal e apropriada à realidade digital.

No entanto, mesmo com a entrada em vigor da LGPD, muitos desafios terão de ser enfrentados na busca de uma tutela efetiva, em termos de dados pessoais. Em especial, cita-se a necessária definição de certos preceitos normativos a respeito do tratamento de dados pelo poder público.

No que toca aos direitos do titular dos dados, a LGPD trouxe um catálogo específico para esses, no seu Capítulo III. Se é bem verdade que alguns direitos já existiam no nosso ordenamento, outros são verdadeiras novidades. Dentro dessas novidades, há alguns direitos que se destacam pela sua modernidade e sofisticação, dando um passo além na tentativa de efetivação da autodeterminação informativa.

Tais direitos recaem sobre o tratamento de dados pessoais, nas hipóteses previstas na LGPD. Entende-se que o tratamento abrangido é tanto o digital, quanto também o físico, à luz do previsto no artigo 1º da LGPD.

O titular dos dados, ou seu representante, poderá exercer esses direitos perante o controlador[2]. Esse é o responsável por atender às requisições do titular, muito embora possa pedir auxilio ou colaboração do operador[3]. E o controlador

---

[1] Procuradora do Município de Porto Alegre. Doutora em Direito pela UFRGS. TCE/RS - Webconferência: Lei Geral de Proteção de Dados e o Poder Público - Mesa 2. Disponível em <https://www.youtube.com/watch?v=Bn_0f4DgyMs>.

[2] O *caput* do artigo 18 da LGPD estabelece o controlador como o responsável pela promoção dos direitos dos titulares. A respeito do atendimento por parte do controlador da pretensão endereçada pelo titular, ver: MALDONADO, Viviane Nóbrega. Capítulo III - Dos Direitos do Titular. In MALDONADO, Viviane Nóbrega; ÓPICE BLUM, Renato. **LGPD Lei Geral de Proteção de Dados**, p. 221, São Paulo: RT, 2. ed., 2019.

[3] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Disponível em: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf>. Acesso em 2 de novembro de 2020, p. 36.

poderá ser pessoa física ou jurídica, de direito privado ou público, enquadrando-se, pois, a administração pública nessa figura.

Desta feita, a proposta do artigo em tela é justamente verificar alguns pontos e perspectivas importantes no exercício desses direitos na administração pública, na figura de controladora. Para tanto, foram selecionados alguns temas dentre aqueles que vêm gerando discussões não só teóricas, mas principalmente práticas quando da execução do grande desafio que é a adequação do poder público à LGPD. Em especial, serão abordados os seguintes temas: (i) a interface entre proteção de dados pessoais e transparência e (ii) a harmonização dos direitos dos titulares com o segredo de empresa (comercial ou industrial), o qual o poder público pode ter a obrigação de guardo decorrente da lei ou de contrato.

## 2 PODER PÚBLICO COMO CONTROLADOR

A LGPD, no afã de uniformização do tratamento de dados pessoais, conjugou, em apenas um diploma, as normas pertinentes ao tema, tratando como controlador tanto o poder público como o privado[4]. Essa simetria entre público e privado no tocante ao uso de dados pessoais é, inclusive, uma tendência global e pode ser observada nas diretrizes da OCDE sobre proteção da privacidade e fluxos transfronteiriços de dados pessoais e na Convenção para a Proteção dos Indivíduos com Respeito ao Processamento Automático de Dados Pessoais.[5]

Com algumas exceções de não incidência da lei (a exemplo do artigo 4º), a LGPD tenta combater a fragmentação e aplica-se independentemente se o dado foi originário de uma relação de consumo, tributária, de direito administrativo, de saúde,

[4] Há autores que tecem críticas a essa disciplina trazida pela LGPD, pois entendem que a regulamentação do acesso administrativo a dados privados diz respeito ao direito administrativo, isto é, ao exercício da função administrativa. E tal matéria seria competência de cada ente federativo. Nesse sentido: "A Lei 13.709/2018, contudo, disciplina o assunto como se ignorasse esse fato. O Legislador Federal arvora-se no direito de disciplinar o acesso a dados privados para a Administração estadual e municipal sem qualquer constrangimento" (MARTINS, Ricardo Marcondes. Lei Geral de Proteção de Dados Pessoais e direito administrativo: questões polêmicas. In DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e Administração Pública**, p. 19-34, São Paulo: RT, 2020.).

[5] WIMMER, Miriam. Cidadania, Tecnologia e Governo Digital: Proteção de Dados Pessoais no Estado Movido a Dados. In: Alexandre F. Barbosa. (Org.). **TIC Governo Eletrônico 2019**. Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. 1 ed.São Paulo: Comitê Gestor da Internet no Brasil, 2020, v. 1, p. 30.

entre outras complexas relações que o indivíduo atualmente desempenha na pós-modernidade.

Apesar dessa busca por uniformidade no trato dos dados pessoais, a LGPD destinou um capítulo próprio ao poder público (arts. 23 a 30). Mas afinal, quem é poder público para fins de aplicação das disposições específicas nesse capítulo?

Segundo o artigo 24 da LGPD, considera-se poder público a administração direta e indireta, exceto as empresas públicas e sociedades de economia mista que atuem em regime de concorrência[6]. Para essas pessoas jurídicas que atuem em regime de concorrência, será dispensado o mesmo tratamento das pessoas jurídicas de direito privado particulares.

Porém, se essas Empresas Públicas e Sociedades de Economia Mista também operacionalizem políticas públicas, no âmbito da execução dessas, o tratamento passa a ser o mesmo das entidades do poder público, de acordo com o parágrafo único do artigo 24 da LGPD.

Assim, nessas instituições atuantes em livre concorrência, caso também prestem políticas públicas, haverá uma clivagem. Um possível exemplo seria um banco público que, além de atuar no setor financeiro, também operacionaliza uma política habitacional.

Um possível efeito prático dessa diferenciação feita pela LGPD, no que toca às Empresas Públicas e Sociedades de Economia Mista, diz respeito à sanção de multa. Para as empresas da administração indireta, que atuem em regime de concorrência, entende-se que é possível a aplicação das sanções previstas nos incisos II e III do artigo 52 (multa simples e multa diária).

Pois bem, não há dúvidas de que entidades que integram o conceito de poder público podem ser enquadradas como controlador e, pois, serem demandadas pelos titulares quando esses estiverem no exercício dos seus direitos. Cabe pontuar que, na prática, tem-se verificado grandes dificuldades das entidades do poder público de reconhecer e estruturar, na adequação da LGPD, as figuras do controlador, operador e do próprio encarregado.

Apesar de todas as controvérsias, entende-se que controlador é a pessoa a quem compete as decisões referentes ao tratamento de dados pessoais, sendo,

[6] Nas lições de Eros Grau, quando o estado atua na atividade econômica em sentido estrito, ele pode operar em regime de monopólio ou competição, isto é, em livre concorrência (GRAU, Eros. **A Ordem Econômica na Constituição de 1988**. São Paulo: Malheiros, p.119.).

portanto, o responsável pelo tratamento. As decisões do controlador são tomadas pelo seu representante legal, o qual pode delegá-las, por exemplo, pra um Comitê Gestor de proteção de dados pessoais.

Já o operador é a pessoa externa que realiza o tratamento de dados pessoais em nome e por ordem do controlador. A título de exemplo, operadores são os fornecedores contratados pelo poder público que venham a tratar os dados do cidadão na execução do contrato.

Por fim, o encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). No âmbito a União Europeia, garante-se que o encarregado seja membro do quadro pessoal, mediante a preservação dos deveres de sigilo e confidencialidade e mandato fixo e renovável[7] .

## 3 PECULIARIDADES DO PODER PÚBLICO

Apesar da louvável tentativa de uniformização da proteção de dados pessoais inaugurada pela LGPD, não se pode descurar que a relação entre poder público e administrado é diferente da relação poder privado e indivíduos. Na maioria das vezes, o tratamento de dados, feito pelo poder público, decorre do cumprimento de seus deveres constitucionais e legais[8] , ou seja, situações que, como regra, não são embasadas no consentimento.

Considerando que as relações entabuladas entre poder público e cidadão, em regra, não são simétricas, seria bastante contestável a utilização do consentimento. Muitas vezes os titulares dos dados poderiam ter dúvidas ou receio quanto à

[7] ALVES. Fabrício da Mota. Estruturação do Cargo de DPO em entes públicos. In VAINZOF, R.; BLUM, R. M. S. O. (Org.); FABRETTI, H. (Org.). **Data Protection Officer***:* Teoria e Prática de Acordo com a LGPD e o GDPR. 1. ed. São Paulo: Revista dos Tribunais, 2020. v. 1., p. 540.

[8] Acerca dessa base legal, observam Chiara de Teffé e Mario Viola: “Há, entretanto, autores que defendem a existência de outra base legal para o tratamento de dados pessoais no Art. 23 da LGPD para o exercício geral das competências ou o cumprimento de atribuições legais da Administração Pública. Contudo, entendemos que o tratamento de dados pessoais para tais atividades já estaria contemplado nas hipóteses relativas ao cumprimento de uma obrigação legal (Art. 7º, II, e Art. 11, II, 'a'), já que a atuação da Administração Pública decorreria de um mandamento legal, e ao tratamento e uso compartilhado de dados necessários à execução de políticas públicas (Art. 7º, III, e Art. 11, II, 'b')” (TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com - Revista Eletrônica de Direito Civil**, v. 9, p. 4, 2020.).

possibilidade da não concessão do consentimento, razão pela qual se entende que o uso dessa base legal na esfera pública é limitada[9].

Lado outro, a existência de outras bases legais diferentes do consentimento para o poder público também se faz necessária para evitar o abuso de direito pelo titular (exercício inadmissível de posição jurídica), que inviabilizaria as atividades públicas. A título de exemplo, imaginem se o poder público precisasse do consentimento para tratar dados pessoais para fins de cobranças fiscais ou para exercer o poder polícia?

Diante dessas peculiaridades, é válida a reflexão acerca dos direitos dos titulares, previstos nos artigos do Capítulo III, e se esses devem se aplicar indistintamente aos controladores, como previsto na sua redação, independente de serem entes públicos ou privados. Nessa senda, indaga-se: será que o cidadão poderia se opor ao tratamento? Existe limite ao solicitar que seus dados sejam eliminados de algum cadastro público?

Aqui cabe fazer menção a um interessante caso julgado pelo Tribunal de Justiça da União Europeia (TJUE), o caso C-398/15, julgado pelo TJUE[10], enquanto ainda vigente a Diretiva 95/46/CE. A análise versou sobre a possibilidade ou não da eliminação de dados pessoais de um registro público de empresas mercantis. Na oportunidade, a Corte, apesar de concluir que não havia direito à eliminação, entendeu pertinente que o Estado-Membro, no caso a Itália, analisasse a possibilidade de restringir o acesso de terceiros a tais informações, após o transcurso de um razoável período de tempo.

Evidente que há ponderações a serem feitas no que toca ao exercício dos direitos dos titulares no poder público, até mesmo para adequar a realidade das atribuições e deveres desse. A propósito, o §3º do artigo 23 da LGPD expressamente determina que os procedimentos e prazos para exercício dos direitos

---

[9] SWEDISH DATA PROTECTION AUTHORITY. Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students. Disponível em: < https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf>. Acesso em: 6 nov. de 2020, p. 4. O Considerando 43 do RGPD bem reforça esse entendimento: “A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa”.

[10] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Caso C-398/15. Disponível em: <http://curia.europa.eu/juris/liste.jsf?num=C-398/15&language=PT> Acesso em: 2 nov. de 2020.

do titular, perante o Poder Público, observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Aqui, cabe ponderar que o termo "em especial" traz uma abertura normativa para que outras leis também possam ser utilizadas para reger os procedimentos e prazos de exercício. Um exemplo seria o uso do Código de Defesa dos Usuários de Serviços Públicos (Lei n° 13.460/2017)[11]. A vantagem do uso de tal legislação seria a existência de prazos e procedimentos padronizados e coordenados. Ademais, tal lei tem abrangência nacional, diferentemente do que ocorre com a Lei do Processo Administrativo Federal, já que cada ente de federativo tem competência para legislar em matéria de processo administrativo[12].

Atenção especial deve ser dada à interface entre a Lei de Acesso à Informação (LAI) e a LGPD. Como a própria LGPD dispõe, os direitos nela previstos observarão os prazos e procedimentos previstos na LAI, entre outras legislações. Mas será que essas leis são totalmente harmonizáveis? Há possibilidade de conflito? Vejamos, então, tais questões no próximo capítulo.

## 4 INTERFACE ENTRE LAI E LGPD

Fazendo um cotejo entre LAI e LGPD é possível apontar duas facetas: (i) uma que indica os preceitos normativos dessas legislações que estão em consonância; e (ii) outra em que o cotejo pode apresentar antinomias aparentes, porém possíveis de superação e harmonização[13]. Na verdade, a LGPD vem a complementar as disposições previstas na LAI.

---

[11] GOV.BR. **Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD).** Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>. Acesso em: 2 nov. de 2020.

[12] MAFFINI, Rafael. **Elementos de Direito Administrativo**. Porto Alegre: Livraria do Advogado, 2016, p. 29.

[13] Lembra-se que, tanto a proteção aos dados pessoais (STF. Medida Cautelar em Ação Direta de Inconstitucionalidade n. 6.387/DF. Plenário, maio de 2020.), quanto o acesso à informação (SARLET, Ingo Wolfgang. **Direitos Fundamentais e Pandemia V – O STF e o acesso à informação,** disponível em: <https://www.conjur.com.br/2020-jul-03/direitos-fundamentais-direitos-fundamentais-pandemia-stf-acesso-informacao> Acesso em: 2 nov. de 2020.) são considerados direitos fundamentais, razão pela qual se faz necessária uma ponderação no caso concreto. Como bem destaca Fernando Canhadas, a LAI traz ao operador do direito diversos elementos que devem ser

Quanto aos pontos em consonância, dessas duas legislações, as disposições da LAI reforçam os direitos dos titulares previstos na LGPD, no que toca ao acesso e à transparência. Assim, os titulares poderão acessar os dados pertinentes à sua pessoa, bem como todas as informações relacionadas ao tratamento dos seus dados, numa espécie de "prestação de contas" ou *accountability*[14].

Aqui, as disposições já inauguradas pela LAI, no que toca à transparência, serão utilizadas igualmente para reforçar os direitos dos titulares dos dados no poder público. Lembre-se que a transparência é fundamento ontológico do direito de acesso e desponta como base para outros direitos[15], como o de retificação ou eliminação.

Como a LGPD diz que o exercício dos direitos, no poder público, observará lei específica (art. 23, §3º, da LGPD), no caso do exercício pelo titular do seu direito de acesso, o prazo e procedimento a ser observado será o da LAI[16]. No âmbito federal, o Guia de Boas Práticas menciona, inclusive, que o requerimento do direito de acesso, com base na LGPD, será recebido por meio do Serviço de Informação ao Cidadão[17].

A outra faceta na interface entre LAI e LGPD diz respeito ao cuidado especial que a administração pública deverá observar ao promover a transparência passiva ou ativa. Considerando que não há mais dados insignificantes[18] diante da evolução tecnologia e da existência de ferramentas computacionais avançadas, talvez aquela

---

utilizados na aplicação de mecanismos de ponderação, sempre que houver conflito entre o direito de acesso à informação, detida pelo poder público, e uma hipótese legal de restrição a esse, como é o caso das informações pessoais (CANHADAS, Fernando. A Lei de Acesso à Informação e a Lei Geral de Proteção de Dados: a transparência proibida. *In* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e Administração Pública**, p. 425, São Paulo: RT, 2020).

[14] BIONI, Bruno; LUCIANO, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: Seriam as Leis de Proteção de Dados o seu Portal de Entrada?. In: FRAZÃO, Ana; MULHOLLAND, Caitlin. (Org**.). Inteligência Artificial e Direito -** Ética, Regulação e Responsabilidade. 1. ed. São Paulo: Thomson Reuters, 2019, v., p. 217. O princípio da *accountability* exige explicitamente dos controladores de dados a implementação de medidas apropriadas e efetivas para botar em prática os princípios e obrigações previstos na norma de proteção de dados, bem como a demonstração dessa implementação caso assim requeira o titular (*ARTICLE 29 DATA PROTECTION WORKING PARTY*. *Opinion 3/2010 on the principle of accountability*. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf> Acesso em: 1º nov. de 2020, p.3.).

[15] BIONI; LUCIANO, *op. cit.* 2019, p. 217.

[16] GOV.BR. **Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD).** Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf> Acesso em: 2 nov.de 2020, p. 17.

[17] *Idem Ibidem*.

[18] MENDES, Laura Schertel. A encruzilhada da Proteção de Dados no Brasil e o Caso do IBGE. **Jota.info,** 2020. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020> Acesso em: 1º nov. de 2020.

proteção da LAI, apenas a dados relacionados à privacidade ou intimidade, não seja mais uma proteção suficiente. E aqui haveria uma antinomia aparente entre a LAI e a LGPD.

Segundo o art. 31 da LAI, não é toda e qualquer informação pessoal que goza de um regime específico de proteção. Apenas aquela com potencial de vulnerar os direitos de personalidade, tais como definidos no art. 5º, X (intimidade, vida privada, honra e imagem) da Constituição Federal de 1988, estaria sob uma proteção especial.

Assim, a partir de uma leitura isolada da LAI seria possível dizer, por exemplo, que dados cadastrais não estariam englobados na proteção às informações pessoais. No entanto, à luz da LGPD, tais dados são enquadrados como dados pessoais, o que pode gerar o entendimento de que devem ser protegidos e tratados de acordo com as suas normas.

Tendo em vista uma possível harmonização da LAI e da LGPD, é cabível afirmar que essa suposta antinomia entre dados pessoais a serem protegidos na LAI com aqueles na LGPD é meramente aparente. É possível a harmonização, de maneira que o tratamento já dispensado na LAI às informações pessoais deve continuar a ser observado. No entanto, o conceito de informações pessoais deve ser atualizado, para fins de abarcar também aqueles dados que se enquadram no conceito previsto no artigo 5º, inciso I, da LGPD.

Nesse sentido, assim apontou o Guia de Boas Práticas do Gov.br[19]:

> Diferentemente da LAI, no entanto, os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação. Ou seja, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais.

Veja-se, assim, que não se trata de um conflito entre as legislações. A LGPD apenas dá um passo adiante à proteção então já existente na LAI às informações pessoais[20]. Por tais razões, é cabível sustentar que as decisões do STF, com

[19] GOV.BR, *op. cit*, 2020, p. 19.

[20] Sobre esse dever já existente na LAI, de guarda das informações pessoais, cita-se a seguinte reflexão: "Certo é que no direito brasileiro existe um dever constitucional do Estado em assegurar a gestão transparente da informação, para tanto o Estado está obrigado na proteção da informação, garantindo sua disponibilidade à cidadania, ademais de proteger de igual modo a informação sigilosa e a informação pessoal" (SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. Direito à informação e

relação à divulgação dos salários dos servidores, podem vir a ser revisitadas[21], não para impedir a transparência, mas, talvez, para adotar medidas de mitigação de exposição dos dados pessoais.

Outro ponto de harmonização é que a administração pública, ao concretizar o princípio da transparência, deve buscar formas alternativas de dar publicidade aos dados, sem divulgar aqueles que são pessoais e sejam desnecessários[22]. Além disso, é possível buscar soluções inovadoras[23] que possibilitem o controle democrático, mas que, ao mesmo tempo, também observem as normas de proteção de dados, seja por meio da anonimização, seja por meio da aplicação do princípio da minimização[24].

## 5 SEGREDOS COMERCIAL E INDUSTRIAL

Um limite aos direitos dos titulares pode ser decorrente da observância do segredo de empresa (segredos comercial e industrial)[25]. É possível que a

---

direito de acesso à informação como direitos fundamentais na Constituição brasileira. **Revista da AGU**, Brasília-DF, ano XIII, n. 42, p. 38, out./dez. 2014.).

[22] A respeito ver: STF. ARE 652777. Relator Ministro Teori Zavascki, divulgado em 30/06/2015. Ainda, na Ação Originária 2.367, assim restou na ementa: "Não há violação à intimidade ou à vida privada na divulgação nominal e pormenorizada da remuneração de magistrados". STF. Ação Originária 2.367, Relator Ministro Roberto Barroso, julgado em 23 de agosto de 2018. Percebe-se, ademais, que a proteção de dados, muito embora herdeira da tutela da privacidade, é mais ampla que essa e apresenta características próprias (DONEDA, Danilo. A proteção de dados com um direito fundamental. **R. Espaço Jurídico.** Joaçaba, v. 12, n. 2, p. 95, jul./dez. 2011). Por isso, deve ser reconhecida como um direito autônomo. A proteção de dados, segundo Ruaro, Rodriguez e Finger, para além da defesa da privacidade, protege e regula o direito de acesso e o poder de controle das informações pessoais (RUARO, Regina; RODRIGUEZ, Daniel Piñeiro ; FINGER, Brunize. **O Direito à Proteção de Dados Pessoais e à Privacidade Revista da Faculdade de Direito (UFPR),** v. 53, p. 64, 2012.).

[23] A esse respeito, Têmis Limberger menciona o seguinte: "Se por um lado tem-se a administração com a necessidade de transparência, por outro tem-se o limite da proteção dos dados pessoais. Partindo-se da ideia já conhecida de que não há direitos absolutos, todos eles encontram um limite, tem-se que o nome integra os direitos de personalidade e deve ser preservado. Assim, não é possível sua exposição indevida, pois esta identifica mais facilmente a pessoa. Pode, ainda, comprometer a segurança do indivíduo, principalmente, em países com desigualdades econômicas muito grandes" (LIMBERGER, Têmis. Cibertransparência: informação pública em rede e a intimidade como um dos limites constitucionais – uma abordagem a partir do tema 483 da Repercussão Geral examinada pelo STF **R. de Dir. Adm. Const**., Belo Horizonte, ano 16, n. 65, p. 209, jul./set. 2016.).

[24] Uma alternativa é tarjar os documentos para não expor dados pessoais desnecessários. Na Espanha, "uma normativa afirma que apenas nome, sobrenome e 4 (quatro) números aleatórios do documento de identificação podem ser disponibilizados" (PEDROSO, Lucas. Tratamento de dados pessoais pelo Poder Público: o que esperar segundo a experiência europeia? In DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes**. LGPD e Administração Pública**, p. 335, São Paulo: RT, 2020).

[25] Existe uma multiplicidade de vocábulos usados no país para designar os dados confidenciais das empresas que são merecedores de proteção legal (FEKETE, Elisabeth Kasznar. **O regime jurídico do segredo de indústria e comércio no Direito Brasileiro**. Forense: Rio de Janeiro, 2003, p. 17).

contratação de ferramentas computacionais ou de inteligência artificial, pelo poder público, implique o cuidado e guarda do segredo de empresa[26].

Além disso, é inegável que durante o exercício das suas atividades a administração pública acaba tendo posse de documentos e informações sensíveis para as empresas, que mereceriam ser protegias pelo segredo. Ocorre que tais documentos também podem envolver dados pessoais, o que pode gerar um conflito entre esses interesses quando o titular estiver exercendo os seus direitos[27].

Por tal razão, é importante que seja, desde já, delimitada a extensão do segredo de empresa. Ainda, a construção de alguns vetores interpretativos de como os direitos do titular devem se harmonizar com o segredo de empresa é fundamental, seja para os entes privados, que desejam proteger suas informações, seja pelo poder público, quando se torna guardião de informações importantes das empresas.

No texto da LGPD, podemos encontrar em torno de treze disposições sobre a necessária observância do segredo de empresa[28]. Em que pese a grande

---

Tendo em vista que a expressão "segredo de empresa" é um gênero que acaba abarcando as demais espécies, como os segredos comercial e industrial (BARBOSA, Denis Borges. **Tratado de Propriedade Intelectual**. Tomo I. Rio de Janeiro: Editora Lumen Juris, 2013,p. 124), optou-se por utilizar o gênero "segredo de empresa", no presente artigo.

[26] Apesar dessa possibilidade, é importante destacar que há a defesa no sentido de que o uso de algoritmos, pelo poder público, implica em transparência e publicidade, o que, em certa intensidade, pode até mesmo afetar o segredo de empresa. Sobre iniciativas de transparência, citam-se as iniciativas de Amsterdã e Helsinque, que laçaram registros de Inteligência Artificial para detalhar como cada governo municipal usa algoritmos para fornecer serviços públicos. Nesse registro, são listados os algoritmos usados, bem como os conjuntos de dados usados para treinar um modelo, a descrição de uso do algoritmo, além das possíveis tendências ou riscos. Disponível em <https://www.itu.int/en/myitu/News/2020/09/30/07/41/Helsinki-Amsterdam-AI-registers-city-systems-Cities-Today> Acesso em: 1º nov. de 2020.

[27] Conflito parecido já existia para o poder público, mesmo antes da LGPD. A publicação de dados ou o acesso a informações era limitado pelo dever de guarda do segredo industrial ou comercial, conforme previsão expressa na LAI (Art. 22. O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.). A este respeito, ver os seguintes precedentes da CGU: CGU. Precedente 99926000080201785. Disponível em <http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/99926000080201785_CGU.pdf>. Acesso em: 8 nov. de 2020. E CGU. Precedente 25820006868201747. Disponível em: <http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/25820006868201747_CGU.pdf.>. Acesso em: 8 nov. de 2020.

[43] A esse respeito, citam-se os seguintes dispositivos: Art. 6 º, inciso VI, sobre o princípio da transparência; artigo 9º, inciso II, sobre o direito de acesso; art. 10, § 3º, que trata do relatório de impacto à proteção de dados pessoais; art. 18, inciso V, que traz o direito à portabilidade de dados; art. 19, inciso II, e § 3º (confirmação e acesso a dados pessoais); art. 20, § 1º e 2º, que versa sobre o direito à revisão de decisões automatizadas; art. 38 (relatório de impacto) e art. 48, a respeito da comunicação de incidente de segurança (§ 1º, inciso III). Havia, também, disposições no artigo 56, que restou vetado.

preocupação do legislador com a proteção do conhecimento empresarial no âmbito da proteção dos dados pessoais, esse é um dos temas mais negligenciados e pouco explorados no Brasil[29], não havendo uma definição precisa do seu conteúdo, além de estar condicionado à prática de concorrência desleal[30].

Com efeito, as disposições sobre o segredo de empresa, previstas na LGPD, precisarão ser aplicadas com cautela, seja pela falta de tradição e consenso, no tema, seja pela ausência de vetores interpretativos na própria LGPD, que não define o que pode ser considerado como segredo, nem em que medida ou grau esse interesse deve ser observado.

Em especial, é preciso refletir como deverá ser harmonizado o monopólio da informação intangível protegido genericamente por meio do segredo de empresa com o direito concedido aos titulares dos dados pessoais de controle do acesso, uso e tratamento dos seus dados[31].

Independentemente das escolhas que sejam feitas quanto à intensidade que será dada à proteção do segredo de empresa, especialmente quando esse estiver em conflito com os direitos do titular dos dados[32], deve-se ponderar que, se a proteção do segredo de empresa é condicionada a um ato de concorrência desleal, a simples obtenção de uma cópia dos dados, para uso pessoal, ou o direito de acesso pelo titular não poderão ser negados, *prima facie*, com base no segredo de empresa, já que em regra tal exercício não tem o condão de gerar prejuízos

---

A Medida Provisória (MP) 869/2018 pretendia determinar que a autoridade competente em matéria de proteção de dados fosse responsabilizada caso não zelasse pela preservação do segredo empresarial. Com a apreciação da MP, pelo Poder Legislativo, houve a conversão da MP na Lei 13.853/2019, que não ratificou a hipótese da responsabilização, mas determinou, no artigo 55-J, inciso II e §5º, da LGPD, que a autoridade deverá zelar pela preservação do segredo empresarial e dispor sobre as formas de publicidade, respeitado o segredo de empresa (inciso X). As disposições acerca dos segredos comercial e industrial foram trazidas pela EMP9 recebida em Plenário, durante a apreciação do PL 4060/2012 pela Câmara dos Deputados, estando em apenso à proposição principal o PL 5.276/2016 e o PL 6.291/16.

[29] PELA, Juliana Krueger. The Brazilian Regulation of Trade Secrets. A proposal for its review. **Gewerblicher Rechtsschutz und Urheberrecht - Internationaler Teil,** v. 6, p. 546, 2018.
Na União Europeia, o tema foi objeto da Diretiva 943/2016: tendo em vista que as informações são a moeda da economia do conhecimento e, como tal, uma vez qualificada para proteção de segredos comerciais, merece proteção em termos legais em toda a União Europeia. Tal harmonização serve, ademais, para promover o *Single Market* europeu (FALCE, Valéria. *Trade Secrets – Looking for (Full) Harmonization in the Innovation Union.* ***IIC - International Review of Intellectual Property and Competition Law*****,** v. 46, p. 964, 2015.).

[30] Ver art. 195, incisos XI e XII, da Lei 9.279/1996 (Lei da Propriedade Industrial - LPI).

[31] MALGIERI, Gianclaudio, Trade Secrets v Personal Data: A Possible Solution for Balancing Rights. **International Data Privacy Law**, Vol. 6, Issue 2, p. 102–116,1 May 2016.

[32] Deve ser destacado que o direito à portabilidade de dados é o direito que, dentre os outros da LGPD, mas tem implicações à concorrência desleal, matéria que no nosso ordenamento regula o segredo de empresa.

competitivos de forma desleal à empresa, nem coloca em risco a atividade empresarial[33].

Outro ponto nevrálgico, envolvendo o segredo de empresa, reside nas inferências, que são obtidas por meio do tratamento do dado cru, realizado em geral com inteligência artificial. Essas inferências apontam os gostos, preferências e posições de determinada pessoa. Também se enquadram como inferências a criação de perfis e de sistemas de *rating.*

Será que as inferências poderiam ser protegidas pelo segredo de empresa? Responder essa questão não é tarefa fácil, até mesmo porque seria necessário investigar com profundidade a natureza das inferências, a fim de verificar se essas são consideradas dados pessoais.

De qualquer forma, é possível ponderar que conhecimentos gerados pela utilização de dados que não sejam mais associados ao dado original, de maneira que o titular não possa mais ser identificado, impossibilitando o *backtrace,* podem ser protegidos pelo segredo de empresa[34]. Ademais, as técnicas e os algoritmos utilizados para obtenção de informações e conhecimentos também podem estar abarcados no segredo de empresa[35].

Em última análise, toda vez que o exercício de algum direito do titular dos dados, como é o caso do direito de acesso, vulnere o segredo de empresa, o controlador poderá justificar eventual negativa ou limitação dos direitos do titular, desde que assim proceda de forma transparente e expressa. O poder público deve demonstrar especificamente que assumiu o compromisso de zelar pelo segredo de empresa, quando da contratação de alguma ferramenta computacional ou

---

[33] Critério como regra, utilizado pela CGU em casos de restrição do acesso à informação. Ver: CGU. Precedente 99926000080201785. Disponível em: <http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/99926000080201785_CGU.pdf>. Acesso em 8 de nov. de 2020.

[34] Assunto correlato, diz respeito a certos "*blind spots*" das legislações de proteções de dados. Há situações que não haverá a incidência da LGPD por não se tratar mais de dado pessoal, porém ainda assim é possível que o uso de inteligência artificial gere impactos a grupos ou a indivíduos. Nesse sentido, cita-se o contexto do *deep learning* em que os dados são usados em escala massiva para produzir correlações que podem afetar coletividades (VILLANI, Cédric***. For a Meaningful Artifical Intelligence***. Disponível em: <https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf>. Acesso em: 24 set. de 2020, p. 121.). Veja que, às vezes, tais dados não estarão abarcados em certos direitos das leis de proteção de dados pessoais, pois muitas vezes já não dizem respeito a uma pessoa e sim a grupos. Cabe a reflexão quanto à necessidade de avançarmos em termos de proteção coletiva em matéria de dados.
WACHTER, Sandra; MITTELSTADT, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, 2019, p. 79.

[35] WACHTER, Sandra; MITTELSTADT, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, 2019, p. 79.

inteligência artificial, entre outros, ou que tem o dever de zelar pelo segredo de empresa decorrente das informações contidas em documento que tem posse.

## 6 CONSIDERAÇÕES FINAIS

A LGPD, ao ingressar no ordenamento jurídico, deve dialogar com outros diplomas vigentes. No que toca ao poder público, um dos principais diálogos da LGPD será com a LAI, seja para reforçar a transparência e o *accountability* ao titular-cidadão, seja para que a proteção às informações pessoais da LAI passe a ser compatível com o nível de proteção almejado pela LGPD.

Nessa senda, a administração pública ao concretizar o princípio da transparência, deve buscar formas alternativas de dar publicidade aos seus atos, a fim de evitar a divulgação de dados pessoais que sejam desnecessários. É possível buscar soluções inovadoras que possibilitem o controle democrático, mas que, ao mesmo tempo, também observem as normas de proteção de dados, seja por meio da anonimização, seja por meio da aplicação do princípio da minimização.

Ademais, o próprio exercício dos direitos dos titulares, no poder público, pautar-se-á, em certos casos, nos procedimentos e prazos da LAI. Assim, é indispensável uma harmonização e uma aplicação coordenada entre essas duas legislações.

A par desse diálogo, entre LGPD e transparência, o poder público também terá que balancear outros interesses quando for atender uma pretensão do titular, como é o caso da observância do segredo de empresa (segredos comercial e industrial). É possível que a contratação de ferramentas computacionais ou de inteligência artificial pelo poder público implique o cuidado e guarda do segredo de empresa.

Além disso, é inegável que, durante o exercício das suas atividades, a administração pública acaba tendo posse de documentos e informações sensíveis para as empresas, que mereceriam ser protegidas pelo segredo. Ocorre que tais documentos também podem envolver dados pessoais, o que geraria um conflito entre esses interesses quando o titular estiver exercendo os seus direitos.

Esse dilema não é novo para o poder público, já que, ao promover a transparência, passiva ou ativa, era necessário sopesar o dever de guarda de

informações confidenciais empresariais. No entanto, com a LGPD em vigor, o poder público também terá que sopesar esse dever, quando for responder a um requerimento do titular dos dados.

Para tanto, conclui-se que, toda vez que o exercício de algum direito do titular dos dados, como é o caso do direito de acesso, vulnere o segredo de empresa, o controlador poderá justificar eventual negativa ou limitação dos direitos do titular, desde que assim proceda de forma transparente e expressa. O poder público deve demonstrar, especificamente, que assumiu o compromisso de zelar pelo segredo de empresa, quando da contratação de alguma ferramenta computacional ou inteligência artificial, entre outros, ou que tem o dever de zelar pelo segredo de empresa, decorrente das informações contidas em documento que tem posse. Evidentemente que essa negativa deve ser razoável, até porque não é qualquer situação que irá implicar prejuízos concorrenciais às empresas (elemento necessário para a proteção do segredo) ou risco à atividade empresarial.

## REFERÊNCIAS

ALVES. Fabrício da Mota. Estruturação do Cargo de DPO em entes públicos. In VAINZOF, R.; BLUM, R. M. S. O. (Org.); FABRETTI, H. (Org.). ***Data Protection Officer:*** *Teoria e Prática de Acordo com a LGPD e o GDPR*. 1. ed. São Paulo: Revista dos Tribunais, 2020. v. 1.,.p. 523-544.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 3/2010 on the principle of accountability*. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf>. Acesso em: 1º nov. de 2020.

BARBOSA, Denis Borges. **Tratado de Propriedade Intelectual**. Tomo I. Rio de Janeiro: Editora Lumen Juris, 2013.

BIONI, Bruno; LUCIANO, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: Seriam as Leis de Proteção de Dados o seu Portal de Entrada?. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin. (Org). **Inteligência Artificial e Direito** - Ética, Regulação e Responsabilidade. 1ed. São Paulo: Thomson Reuters, 2019, v. , p. 207-231.

CANHADAS, Fernando. A Lei de Acesso à Informação e a Lei Geral de Proteção de Dados: a transparência proibida. In DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e Administração Pública**, p. 425 - 444, São Paulo: RT, 2020.

CGU. Precedente 99926000080201785. Disponível em: <http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/99926000080201785_CGU.pdf>. Acesso em 8 de nov. de 2020.

CGU. Precedente 25820006868201747. Disponível em: <http://buscaprecedentes.cgu.gov.br/busca/dados/Precedente/25820006868201747_CGU.pdf.>. Acesso em: 8 de nov. de 2020.

DONEDA, Danilo. A proteção de dados com um direito fundamental. **R. Espaço Jurídico.** Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

EDPB. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Disponível em: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf> Acesso em: 2 nov. de 2020, p. 36.

FALCE, Valéria. *Trade Secrets – Looking for (Full) Harmonization in the Innovation Union.* ***IIC - International Review of Intellectual Property and Competition Law***, Volume 46, p. 940-964, 2015.

FEKETE, Elisabeth Kasznar. **O regime jurídico do segredo de indústria e comércio no Direito Brasileiro.** Forense: Rio de Janeiro, 2003.

GOV.BR. **Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD).** Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>. Acesso em: 2 de nov. de 2020.

GRAU, Eros. **A Ordem Econômica na Constituição de 1988**. 3. ed. São Paulo: Malheiros, 1997.

LIMBERGER, Têmis. Cibertransparência: informação pública em rede e a intimidade como um dos limites constitucionais – uma abordagem a partir do tema 483 da Repercussão Geral examinada pelo STF. **R. de Dir. Adm. Const**., Belo Horizonte, ano 16, n. 65, p. 199-217, jul./set. 2016.

MAFFINI, Rafael. **Elementos de Direito Administrativo**. Porto Alegre: Livraria do Advogado, 2016.

MALDONADO, Viviane Nóbrega. Capítulo III- Dos Direitos do Titular. *In* MALDONADO, Viviane Nóbrega; ÓPICE BLUM, Renato (coords.). **LGPD - Lei Geral de Proteção de Dados**, 2. ed., p. 220-242, São Paulo: RT, 2019.

MALGIERI, Gianclaudio, *Trade Secrets v Personal Data: A Possible Solution for Balancing Rights*. ***International Data Privacy Law***, Vol. 6, *Issue* 2, p. 102–116,1 *May* 2016.

MARTINS, Ricardo Marcondes. Lei Geral de Proteção de Dados Pessoais e direito administrativo: questões polêmicas. *In* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e Administração Pública**, p. 19-34, São Paulo: RT, 2020.

MENDES, Laura Schertel. A encruzilhada da Proteção de Dados no Brasil e o Caso do IBGE. **Jota.info**, 2020. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/a-encruzilhada-da-protecao-de-dados-no-brasil-e-o-caso-do-ibge-23042020> Acesso em: 1º nov. de 2020.

PEDROSO, Lucas. Tratamento de dados pessoais pelo Poder Público: o que esperar segundo a experiência europeia? In DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes. **LGPD e Administração Pública**, p. 333-358, São Paulo: RT, 2020.

PELA, Juliana Krueger. *The Brazilian Regulation of Trade Secrets. A proposal for its review.* ***Gewerblicher Rechtsschutz und Urheberrecht - Internationaler Teil, v. 6, 2018.***

RUARO, Regina; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize . O Direito à Proteção de Dados Pessoais e a Privacidade. **R. Revista da Faculdade de Direito (UFPR)**, v. 53, p. 45-66, 2012.

SARLET, Ingo Wolfgang**. Direitos Fundamentais e Pandemia V – O STF e o acesso à informação***.* Disponível em: <https://www.conjur.com.br/2020-jul-03/direitos-fundamentais-direitos-fundamentais-pandemia-stf-acesso-informacao>. Acesso em: 2 nov. de 2020.

SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. Direito à informação e direito de acesso à informação como direitos fundamentais na Constituição brasileira. **Revista da AGU,** Brasília-DF, ano XIII, n. 42, p. 09-38, out./dez. 2014.

STF – Supremo Tribunal Federal. **Ação Originária 2.367**, Relator Ministro Roberto Barroso, julgado em 23 de agosto de 2018.

_____. **ARE 652777**, Relator Ministro Teori Zavascki, divulgado em 30/06/2015.

_____. **Medida Cautelar em Ação Direta de Inconstitucionalidade** n. 6.387/DF. Plenário, maio de 2020.

SWEDISH DATA PROTECTION AUTHORITY. ***Supervision pursuant to the General Data Protection Regulation (EU) 2016/679*** – facial recognition used to monitor the attendance of students. Disponível em: <https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf>. Acesso em 6 de nov. de 2020, p. 4.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. ***Civilistica.com - Revista Eletrônica de Direito Civil***, v. 9, p. 1-38, 2020.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Caso C-398/15**. Disponível em: <http://curia.europa.eu/juris/liste.jsf?num=C-398/15&language=PT>. Acesso em: 2 novembro de 2020.

VILLANI, Cédric. ***For a Meaningful Artifical Intelligence***. Disponível em: <https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf>. Acesso em: 24 set. de 2020.

WACHTER, Sandra; MITTELSTADT, Brent, A. *Right to Reasonable Inferences*: *Re-Thinking Data Protection Law in the Age of Big Data and AI.* ***Columbia Business Law Review***, 2019.

WIMMER, Miriam. Cidadania, Tecnologia e Governo Digital: Proteção de Dados Pessoais no Estado Movido a Dados. *In*: Alexandre F. Barbosa. (Org.). **TIC Governo Eletrônico 2019**. Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. 1ed.São Paulo: Comitê Gestor da Internet no Brasil, 2020, v. 1, p. 27-36.

# OS DADOS NÃO PESSOAIS E A UTILIZAÇÃO DE TÉCNICAS DE ANONIMIZAÇÃO NO CONTEXTO DA PANDEMIA DE CORONAVÍRUS

Sergio Marcos Carvalho de Ávila Negri[1]
Carolina Fiorini Ramos Giovanini[2]

## 1 INTRODUÇÃO

No início da pandemia de coronavírus, verificou-se o surgimento de uma série de iniciativas que utilizavam dados, com o objetivo de conter a disseminação do vírus. No Brasil, ganhou destaque, inicialmente, a utilização de técnicas de cartografia, com a utilização de dados de localização coletados, principalmente, a partir do GPS dos celulares e da triangulação de antenas de telefonia. Foi possível observar que Estados e Prefeituras passaram a se organizar para implementar esse tipo de monitoramento com o objetivo de verificar a adesão, por parte da população, ao isolamento social. Na maior parte dos casos, a anonimização foi apresentada como uma medida técnica de segurança capaz de legitimar o tratamento de dados.

A anonimização pode ser utilizada, contudo, como um instrumento apenas retórico, capaz de afastar a aplicação de um regime mais rigoroso de tutela. Como dados anonimizados não são dados pessoais, o discurso da anonimização pode contribuir com a criação de uma falsa sensação de segurança e, assim, afastar um exame mais cuidadoso em relação aos riscos presentes nas técnicas apresentadas.

A partir de uma abordagem exploratória, o presente trabalho busca analisar o tratamento jurídico, a utilização e os riscos das técnicas de anonimização e verificar se as classificações e conceitos, delineados pela LGPD, são suficientes para incorporar os desafios técnicos da anonimização[3]. A estratégia metodológica utilizada foi o levantamento bibliográfico de trabalhos que apontaram os riscos na utilização dessas variadas técnicas e o acompanhamento das principais iniciativas

[1] Doutor em Direito Civil pela Universidade do Estado do Rio de Janeiro. Professor Adjunto do Departamento de Direito Privado da Faculdade de Direito da Universidade Federal de Juiz de Fora (UFJF) e do Corpo Permanente do Programa de Pós-Graduação em Direito e Inovação da Faculdade de Direito da UFJF. Coordenador do Núcleo de Estudos Avançados em Pessoa, Inovação e Direito (NEAPID), na Universidade Federal de Juiz de Fora (UFJF).
[2] Graduanda em Direito pela Universidade Federal de Juiz de Fora - UFJF.
[3] O tema foi desenvolvido em projeto de pesquisa do Núcleo de Estudos Avançados em Pessoa, Inovação e Direito (NEAPID), na Universidade Federal de Juiz de Fora (UFJF).

de monitoramento do isolamento social a partir de dados, apresentadas no início da pandemia de coronavírus. As disposições da Lei Geral de Proteção de Dados (LGPD), acerca das definições e categorizações de dados pessoais, bem como os dispositivos sobre anonimização, serão igualmente examinados.

## 2 DADOS PESSOAIS E DADOS NÃO PESSOAIS: CONCEITUAÇÃO A PARTIR DO MODELO EXPANSIONISTA

Stefano Rodotà[4] afirma que o direito à privacidade deixa de estar estruturado em torno do eixo "pessoa-informação-segredo" e passa a se fundamentar no eixo "pessoa-circulação-controle", ou seja, a proteção de dados se afasta do próprio discurso abstrato da privacidade. As técnicas de anonimização surgem, assim, como medidas técnicas de segurança, que legitimam a circulação e o tratamento de dados.

A Lei Geral de Proteção de Dados (Lei n° 13.709/2018), abreviada como LGPD, aplica-se ao tratamento de dados pessoais realizado em meio físico ou digital, por isso, a delimitação dos conceitos de dado pessoal e dado não pessoal é de extrema importância, sendo essencial para estabelecer os contornos de aplicação da lei. Nesse sentido, Bruno Bioni[5] esclarece que as expressões empregadas na conceituação podem ser responsáveis por retrair ou expandir a moldura normativa de uma lei de proteção de dados pessoais.

Existem dois modelos de conceituação que podem ser adotados: reducionista e expansionista. Em uma legislação que adota o modelo reducionista, o dado pessoal é definido como informação relacionada à pessoa identificada, ou seja, trata-se de pessoa determinada, evidenciando que o vínculo é imediato, direto, preciso ou exato.

Bioni[6] aponta que, no modelo expansionista, os dados pessoais são conceituados como informações relacionadas à pessoa identificável, ou seja, a pessoa pode ser indeterminada e o vínculo entre esta e a informação é mediato, indireto, impreciso ou inexato. A LGPD, ao estabelecer em seu Art. 5º, Inciso I, que o

---

[4] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.93.
[5] BIONI, Bruno Ricardo. **Proteção de Dados pessoais**: a função e os limites do consentimento. Rio de Janeiro. Forense, 2019, p.68.
[6] *Ibidem*, p.68-69.

dado pessoal é uma *"*informação relacionada a pessoa natural identificada ou identificável*"*, adota o modelo expansionista.

Os dados pessoais podem ser categorizados como dados pessoais sensíveis, ou seja, o dado sensível é um dado pessoal, mas o seu tratamento possui maior potencial de causar discriminação, o que justifica maior proteção[7] . O Art. 5º, inciso II, da LGPD estabelece que dados pessoais 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, são dados sensíveis.

Os dados pessoais poderão ser tratados nas hipóteses previstas no Art. 7º da LGPD, ao passo que dados pessoais sensíveis somente poderão ser tratados nas hipóteses previstas no Art. 11 da referida lei, as quais são mais restritas e exigem que o consentimento seja mais qualificado. Destaca-se que, caso o tratamento de dados pessoais revele informações pessoais sensíveis e possa causar danos ao titular, é possível estender o regime jurídico dos dados pessoais sensíveis, conforme Art. 11, § 1º, da LGPD.

Por outro lado, a conceituação do dado não pessoal também se mostra necessária. É importante ressaltar que não se trata de simples construção teórica. Na verdade, a delimitação do que vem a ser um dado não pessoal possui importância prática para definição do regime jurídico de qualquer tratamento. O dado não pessoal é aquele que não possui associação com pessoa identificada ou identificável, de forma permanente e irreversível, desde a origem ou após tratamento.

Conforme evidenciado anteriormente, a LGPD aplica-se ao tratamento de dados pessoais e, portanto, os não pessoais estão fora do escopo de proteção da lei. Em 2018, a União Europeia publicou o Regulamento (EU) 2018/1807, que trata do fluxo livre de dados eletrônicos não pessoais. No Brasil, ainda não há uma norma que trate especificamente dos não pessoais.

[7] O tratamento de dados pessoais que não sejam dados sensíveis também pode gerar discriminação, por isso, a LGPD determina que as atividades de tratamento de dados pessoais deverão observar o princípio da não discriminação (artigo 6º, IX), que estabelece a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

A Comissão Europeia[8], classifica os dados não pessoais por origem: (i) dados que originalmente não estavam relacionados a uma pessoa natural identificada ou identificável, como dados climáticos ou dados de produção agrícola; e (ii) dados que inicialmente eram dados pessoais, mas que, posteriormente, foram anonimizados.

O dado anonimizado é definido pela LGPD como "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (Art. 5º, III). O Art. 12 da referida lei determina que os dados anonimizados não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

A distinção prática entre dados pessoais e dados não pessoais poderá se revelar difícil, pois, conforme argumentam Graef, Gellert e Husovec[9], os bancos de dados geralmente são mistos, isto é, contêm dados pessoais e não pessoais. Contudo, a compreensão da utilização das técnicas de anonimização é essencial para estabelecer se os regimes jurídicos apresentados pela LGPD serão aplicados ou não ao tratamento em questão.

## 3 ANONIMIZAÇÃO: TRATAMENTO JURÍDICO E TÉCNICAS

As técnicas de anonimização podem ser classificadas em dois tipos gerais de abordagem: aleatorização e generalização. O conjunto de técnicas baseadas em aleatorização busca alterar a veracidade dos dados para que a ligação entre os dados e a pessoa seja eliminada. A técnica de adição de ruídos altera atributos no conjunto de dados para que estes se tornem menos precisos, enquanto se mantém a distribuição global; e a técnica de permutação mistura, aleatoriamente, os valores dos atributos numa tabela, de modo que alguns destes sejam ligados artificialmente a titulares de dados diferentes.

---

[8] EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament and the Council:** Guidence on the Regulation on a framework for the free flow of non-personal data in the European Union. Bruxelas: [s.n.], 2019, p.7. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/guidance-regulation-framework-free-flow-non-personal-data-european-union> Acesso em: 8 nov. de 2020.

[9] GRAEF, Inge; GELLERT, Raphael; HUSOVEC, Martin. **Towards a Holistic Regulatory Approach for the European Data Economy**: why the illusive notion of non-personal data is counterproductive to data innovation. Tilec Discussion Paper, Tilburgo, v. 29, p. 1-18, 28 set. 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256189##> Acesso em: 7 nov. de 2020.

Na família de técnicas de generalização observa-se que a abordagem consiste em generalizar ou diluir os atributos dos titulares dos dados, através da alteração da escala ou ordem de grandeza. Trabalha-se, por exemplo, com uma "região" em vez de uma "cidade", um "mês" em vez de uma "semana". São técnicas desse tipo de abordagem: agregação, k-anonimato, l-diversidade e t-proximidade.

O Grupo de Trabalho do Artigo 29[10], em parecer acerca da utilização de técnicas de anonimização, concluiu que nenhuma das técnicas apresentadas está imune a três riscos: (i) identificação: possibilidade de isolar alguns ou todos os registros que identifiquem uma pessoa num conjunto de dados; (ii) possibilidade de ligação: capacidade de ligar pelo menos dois registros sobre a mesma pessoa; e (iii) inferência: possibilidade de deduzir, com uma probabilidade significativa, o valor de um atributo a partir dos valores de um conjunto de outros atributos.

Conforme já abordado, o dado anonimizado é definido como aquele relativo a titular que não possa ser identificado, tendo em vista a utilização de *"*meios técnicos razoáveis e disponíveis na ocasião de seu tratamento*".* Nesse sentido, faz-se necessário observar que a determinação da razoabilidade da técnica de anonimização utilizada precisa ser fundamentada em fatores objetivos, como custo e tempo necessários para reverter o processo de anonimização empregado, de acordo com as tecnologias disponíveis e a utilização exclusiva de meios próprios (art. 12, §1º, da LGPD)[11].

Para Bioni[12] existem dois eixos de análise da razoabilidade. O primeiro eixo é objetivo e leva em consideração o estado da arte da tecnologia, sendo necessário analisar os recursos e o tempo necessários para reverter a anonimização. O segundo eixo é subjetivo e consiste na análise de quem é o agente de tratamento de dados e se ele possui "meios próprios" para realizar a reversão.

No que diz respeito ao eixo subjetivo, Fink e Pallas[13] evidenciam a figura do "intruso motivado" formulada em abordagem do *Information Commissioner's Office* –

---

[10] *ARTICLE 29 DATA PROTECTION WORKING PARTY*. ***Opinion 5/2014 on Anonymisation techniques*.** Bruxelas: [s. n.], 2014, p.11-12. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. Acesso em: 8 nov. de 2020.

[11] Destaca-se que este filtro jurídico também está previsto no Considerando 26 do Regulamento Geral de Proteção dos Dados Pessoais da União Europeia (RGPD), que entrou em vigência em 25 de maio de 2018.

[12] BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, v. 19, n. 53, p. 191-202, jan./mar. 2020. Bimestral.

[13] FINCK, Michèle; PALLAS, Frank. *They who must not be identified: distinguishing personal from non-personal data under the GDPR. **International Data Privacy Law***, Oxford, v. 10, n. 1, p. 11-36, 10 mar. 2020. Disponível em: <https://doi.org/10.1093/idpl/ipz026>. Acesso em: 8 nov. de 2020.

ICO. O “intruso motivado” seria um terceiro “razoavelmente competente”, que possui acesso a recursos como Internet, bibliotecas e documentos públicos, mas não é necessário que ele seja qualificado como um *expert*, que possui conhecimento especializado, habilidades *hackers* ou acesso a equipamentos específicos. Portanto, na análise do eixo subjetivo faz-se necessário levar em consideração o fluxo de dados interno e o fluxo externo, que se projeta para fora do ambiente em que há o tratamento.

A LGPD apresenta, ainda, a pseudonimização como outra medida técnica que garante a segurança dos dados pessoais. Contudo, anonimização e pseudonimização são conceitos distintos: a pseudonimização é definida como o *“*tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro*”* (art. 13, §4º, da LGPD), ou seja, o dado pseudonimizado ainda é um dado pessoal e, por isso, está dentro do escopo de proteção da LGPD.

## 4 OS RISCOS NA UTILIZAÇÃO RETÓRICA DA ANONIMIZAÇÃO E O USO DE CARTOGRAFIA DURANTE A PANDEMIA DE CORONAVÍRUS

Há uma significativa literatura que analisa os riscos presentes nas diferentes técnicas de anonimização, a partir da demonstração de falhas e do desenvolvimento da denominada ciência da reidentificação[14]. Tais falhas desafiam, inclusive, a utilização de expressões como “anonimização”, “dado anônimo” ou “dado anonimizado”, que são alvos de críticas porque criam a ilusão de que os dados

[14] Nesse sentido, é possível citar os seguintes trabalhos: BRICKELL, J., & SHMATIKOV, V. The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing. **Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining**. Las Vegas, Nevada, Estados Unidos. DOI: 10.1145/1401890.1401904. MACHANAVAJJHALA, A. et al. L-diversity: privacy beyond k-anonymity. Acm Transactions On Knowledge Discovery From Data, [s.l.], v. 1, n. 1, p. 3, mar. 2007. **Association for Computing Machinery** (ACM). Disponível em <http://dx.doi.org/10.1145/1217299.1217302>. Acesso em: 8 nov. de 2020. NARAYANAN, A., & SHMATIKOV, V. Robust De-anonymization of Large Sparse Datasets. **EEE Symposium on Security and Privacy**. Oakland, California, Estados Unidos. DOI: 10.1109/SP.2008.33. NARAYANAN, A., & SHMATIKOV, V. Myths and Fallacies of “Personally Identifiable Information”. **Ċommunications of the ACM**, v. 53, n. 06, p. 24, Junho 2010. Disponível em: <www.cs.utexas.edu/~shmat/shmat_cacm10.pdf> Acesso em: 8 nov. de 2020. ROCHER, L. et al. Estimating the success of re-identifications in incomplete datasets using generative models. **Nature Communications** 10, 3069 (2019). Disponível em <https://doi.org/10.1038/s41467-019-10933-3> Acesso em: 8 nov. de 2020.

anonimizados estariam desvinculados da pessoa de forma irreversível e permanente.

É possível que uma base de dados anonimizada seja vinculada a outra base de dados externa, que contém informações auxiliares. A combinação destas duas bases pode gerar conexões entre as informações e, consequentemente, a extração de informações que possibilite identificação de uma pessoa. Por isso, Paul Ohm[15] sugere que a regulação precisa ser baseada em uma avaliação mais realista dos riscos de reidentificação.

No início da pandemia de coronavírus, como já destacado, várias iniciativas procuraram utilizar dados com o objetivo de conter a disseminação do vírus. A Lei Geral de Proteção de Dados entrou em vigência em setembro de 2020, ou seja, não estava vigindo neste momento inicial da crise sanitária. Contudo, ressalta-se que, em tese, a lei não representaria um obstáculo para essas iniciativas, pelo contrário, o uso de dados poderia ter seguido as hipóteses e salvaguardas previstas[16].

Na União Europeia, o contexto de utilização de dados no enfrentamento à pandemia foi mediado pela atuação das agências ou autoridades de proteção de dados, a partir das regras para as situações emergenciais já apresentadas pela própria legislação. O *European Data Protection Board* (EDPB)[17], em diretrizes sobre o uso de dados de localização, durante a pandemia, indica que as autoridades públicas devem priorizar o tratamento de dados de localização de maneira anônima, o que permite uso de cartografia, isto é, relatórios sobre a concentração de dispositivos móveis em um determinado local. Contudo, o EDPB ressalta que as técnicas de anonimização e os ataques de reidentificação são áreas ainda em investigação, por isso, a transparência em relação à metodologia de anonimização é incentivada.

---

[15] OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, n. 57, p. 1701-1777, 2010.

[16] Nesse sentido, Danilo Doneda destaca que a Lei Geral de Proteção de Dados possui elementos para lidar com o tratamento de informações em situações emergenciais, garantindo a segurança jurídica. Ademais, Doneda destaca que a LGPD será um elemento fundamental para a reestruturação que advirá após a crise sanitária. DONEDA, Danilo. A proteção de dados em tempos de coronavírus. **Jota.info**: 25 de março de 2020. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020>. Acesso em: 08 nov. de 2020.

[17] EUROPEAN DATA PROTECTION BOARD. **Guidelines 04/2020 on the use of location data and contact tracing tools in the contexto of the COVID-19 outbreak**. Bruxelas: [s.n.], 2020, p.6-7. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_en>. Acesso em: 9 nov. de 2020.

Em São Paulo, foi criado o SIMI - SP (Sistema de Monitoramento Inteligente de São Paulo), baseada em um acordo de cooperação firmado entre as operadoras de telefonia Vivo, Claro, Oi e TIM e Governo de São Paulo[18]. A Prefeitura do Rio de Janeiro também firmou acordo com a operadora de telefonia TIM, para monitorar a movimentação e aglomeração de pessoas na capital, sendo que, nesse caso, durante os Jogos Olímpicos de 2016 já havia sido firmada uma parceria semelhante[19].

Além das operadoras de telefonia, a empresa In Loco, que oferece serviços baseados em dados de localização, também atuou junto ao poder público, durante a pandemia. A empresa já contava com uma tecnologia que coletava dados de localização de 60 milhões de brasileiros e trabalhou na criação do "Índice de Isolamento Social", além de disponibilizar a tecnologia para prefeituras, governos, secretarias de saúde, universidades e outros interessados. A título de exemplificação, a partir dos dados de localização, a empresa verificou o percentual de isolamento social em bairros do Recife e de São Paulo[20].

As iniciativas que contam com a participação das operadoras de telefonia ou da empresa In Loco se assemelham porque, além de serem baseadas em cartografia, afirmam utilizar dados anonimizados. Por exemplo, o SIMI-SP destaca que utiliza dados anonimizados *"*sem desrespeitar a privacidade de cada usuário" e a empresa In Loco afirma que "para fins da colaboração com o controle da pandemia, a In Loco está utilizando as mais avançadas técnicas de anonimização*".*

Evidentemente, a proteção dos dados pessoais não é um obstáculo à formulação de políticas públicas que buscam tutelar a saúde. Contudo, a possibilidade de reidentificação dos dados anonimizados precisa ser analisada para evitar uma utilização retórica das técnicas de anonimização, verificada quando (i) as iniciativas informam que utilizam dados anonimizados, mas não esclarecem qual a técnica utilizada e quais são os potenciais riscos; (ii) os termos de uso e políticas de privacidade se limitam a reproduzir trechos da lei; ou (iii) fornecer informações vagas e genéricas.

---

[18] Informação disponível em: <https://www.saopaulo.sp.gov.br/spnoticias/isolamento-social-em-sao-paulo-e-de-47-aponta-sistema-de-monitoramento-inteligente-10/>. Acesso em: 7 nov. de 2020.
[19] Informação disponível em: <https://www.uol.com.br/tilt/noticias/reuters/2020/03/23/tim-faz-parceria-com-prefeitura-do-rio-de-janeiro-para-monitorar-cidadaos-durante-epidemia.htm>. Acesso em: 7 nov. de 2020.
[20] Informações disponíveis em: <https://www.inloco.com.br/covid-19> e em <https://content.inloco.com.br/knowledge/covid/sum%C3%A1rio>. Acesso em: 8 nove. de 2020.

Anonimização não deve ser apresentada ao usuário como uma técnica totalmente efetiva, tendo em vista os riscos de reidentificação. No Chile, o jornal *Interferencia*[21] obteve acesso a um banco de dados georreferenciados do Ministério da Saúde e divulgou esses dados na forma de mapas, que permitem a visualização específica dos casos confirmados de coronavírus em pontos de ruas e de bairros. O jornal informou que, cada ponto que indica um caso testado positivo para a COVID-19, teve sua localização original alterada para outro ponto localizado entre 50 e 100 metros do ponto de origem. Contudo, apesar da tentativa de adição de ruído, como forma de anonimização, ainda é possível visualizar blocos, prédios e casas específicas nas quais há casos confirmados e, por conseguinte, é possível identificar um indivíduo supostamente contaminado a partir de seu endereço.

O EDPB[22] destaca que os sinais de mobilidade de um indivíduo são intrinseca e altamente correlacionados, isto é, podem ser submetidos a tentativas de reidentificação. Isso significa que um dado que era considerado, em tese, anonimizado, pode não sê-lo, na prática. Por isso, além de informar qual técnica está sendo utilizada, os riscos técnicos, jurídicos e éticos - intrínsecos ao uso da anonimização - devem ser esclarecidos ao titular de forma clara, acessível e transparente. Nesse processo, a construção e implementação de uma cultura de transparência e proteção de dados é imprescindível.

As normas elaboradas por agentes privados são importantes para estabelecer rotinas e procedimentos que garantem a segurança da informação. O desenvolvimento de medidas técnicas voltadas ao aprimoramento das técnicas de anonimização também deve ser incentivado. Contudo, a atuação de agentes externos fiscalizadores é extremamente importante para verificar se essas garantias, de fato, confirmam-se na atuação prática ou se são utilizadas de forma discursiva, criando apenas uma falsa sensação de segurança.

Quando utilizada discursivamente, a anonimização contribui para a construção de uma reputação institucional que transmite ao público o imaginário de segurança da informação e proteção de dados pessoais. O uso retórico da anonimização pode, ainda, acentuar a assimetria informacional já existente entre

---

[21] HERRERO, Victor. *Exclusivo: Estos son los mapas de contagio de Covid-19 que Mañalich mantiene en secreto*. **Interferencia**: 11 de maio de 2020. Disponível em: <https://interferencia.cl/articulos/exclusivo-estos-son-los-mapas-de-contagio-de-covid-19-que-manalich-mantiene-en-secreto>. Acesso em: 9 nov. de 2020.

[22] EUROPEAN DATA PROTECTION BOARD, *op. cit.*, 2020.

agentes de tratamento e titulares, justificando tratamentos abusivos e desproporcionais. Mesmo em situações emergenciais, como a crise sanitária, causada pela pandemia de coronavírus, é necessário estabelecer modelos transparentes que se traduzam em parâmetros, rotinas e regras efetivas, de modo a gerar confiança e assegurar, principalmente, a legitimidade necessária para o tratamento de dados.

Tendo em vista os riscos que envolvem a utilização das técnicas de anonimização, a governança dos dados não pessoais também assume papel relevante. Não se trata de impedir a utilização de técnicas de anonimização, mas de associá-las a rotinas e procedimentos transparentes, efetivamente implementados, os quais permitam a verificação e divulgação dos riscos técnicos, jurídicos e éticos.

## 5 CONCLUSÃO

A partir do modelo expansionista de conceituação dos dados pessoais, foi possível verificar que a delimitação do conceito de dado não pessoal também é de extrema relevância para estabelecer a moldura normativa da Lei Geral de Proteção de Dados. Nesse sentido, o presente trabalho buscou analisar a utilização de técnicas de anonimização, uma vez que os dados anonimizados, em regra, não serão considerados dados pessoais.

Tendo em vista a utilização de dados anonimizados, no combate à pandemia de coronavírus, procurou-se demonstrar que as técnicas de anonimização podem ser utilizadas de forma retórica, ou seja, podem ser mencionadas em termos de uso e políticas de privacidade, que fazem mera referência aos dispositivos da lei e apresentam informações vagas e genéricas, sem ações concretas de implementação de medidas de segurança. A utilização retórica da anonimização evidencia a importância da construção de uma cultura de proteção de dados pessoais no Brasil. A construção dessa cultura passa, necessariamente, pelo combate a uma retórica vazia e ilusória, dissociada de rotinas e práticas implementadas concretamente.

# REFERÊNCIAS


ARTICLE 29 DATA PROTECTION WORKING PARTY. ***Opinion 5/2014 on Anonymisation techniques***. Bruxelas: [s. n.], 2014, p.11-12. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. Acesso em: 8 nov. de 2020.

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

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, v. 19, n. 53, p. 191-202, jan./mar. 2020. Bimestral.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 8 nov. de 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais***:* elementos da lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. A proteção de dados em tempos de coronavírus. **Jota.info**: 25 de março de 2020. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020>. Acesso em: 8 nov. de 2020.

EUROPEAN COMMISSION. ***Communication from the Commission to the European Parliament and the Council:*** *Guidence on the Regulation on a framework for the free flow of non-personal data in the European Union*. Bruxelas: [s.n.], 2019. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/guidance-regulation-framework-free-flow-non-personal-data-european-union>. Acesso em: 8 nov. de 2020.

EUROPEAN DATA PROTECTION BOARD. ***Guidelines 04/2020 on the use of location data and contact tracing tools in the contexto of the COVID-19 outbreak****.* Bruxelas: [s.n.], 2020, p.7. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_en>. Acesso em: 9 nov. de 2020.

FINCK, Michèle; PALLAS, Frank. *They who must not be identified: distinguishing personal from non-personal data under the GDPR*. ***International Data Privacy Law****,* Oxford, v. 10, n. 1, p. 11-36, 10 mar. 2020. Disponível em: <https://doi.org/10.1093/idpl/ipz026>. Acesso em: 8 nov. de 2020.

GRAEF, Inge; GELLERT, Raphael; HUSOVEC, Martin. *Towards a Holistic Regulatory Approach for the European Data Economy: why the illusive notion of non-personal data is counterproductive to data innovation*. ***Tilec Discussion Paper****,* Tilburgo, v. 29, p. 1-18, 28 set. 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256189##> Acesso em: 7 nov. de 2020.

HERRERO, Victor*.. **Exclusivo:** Estos son los mapas de contagio de Covid-19 que Mañalich mantiene en secreto*. *Interferencia:* 11 de maio de 2020. Disponível em: <https://interferencia.cl/articulos/exclusivo-estos-son-los-mapas-de-contagio-de-covid-19-que-manalich-mantiene-en-secreto>. Acesso em: 9 nov. de 2020.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais***,* v. 19, p. 159-180, 2018.

OHM, Paul. *Broken promises of privacy*: responding to the surprising failure of anonymization. ***UCLA Law Review****,* n. 57, p. 1701-1777, 2010.

RODOTÀ, Stefano. **A vida na sociedade da vigilância***:* a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**: *General Regulation Data Protection* (Regulamento Geral sobre a Proteção de Dados). Bruxelas, 27 abr. 2016. Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em: 8 nov. de 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho sobre um quadro para a livre circulação de dados não pessoais na União Europeia***.* Bruxelas, 14 de nov. 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807>. Acesso em: 8 nov. de 2020.

# DECISÕES AUTOMATIZADAS PELA ADMINISTRAÇÃO PÚBLICA: DIÁLOGOS ENTRE *LEADING CASES* E CRITÉRIOS PARA SUA IMPLEMENTAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Cristiano Colombo[1]

## 1 INTRODUÇÃO

Volta-se o presente artigo às decisões automatizadas tomadas pela administração pública, no que toca à utilização de dados pessoais de seus cidadãos, partindo de dois casos paradigmáticos, que se constituíram em *Leading Cases* acerca do tema: a Reclamação Constitucional contra Ato Normativo sobre a Lei do Censo de 1983, no Tribunal Constitucional Alemão, bem como as Ações Diretas de Inconstitucionalidade (ADI) sob os números 6387 a 6390 e 6393, estas que tramitam no Supremo Tribunal Federal.

No primeiro capítulo, serão apresentadas reflexões históricas e conceituais sobre decisões automatizadas e o *profiling*, aplicados no contexto da administração pública. No segundo capítulo, promover-se-á análise acerca das supramencionadas decisões. Outrossim, buscar-se-á estabelecer critérios, observando boas práticas, pela administração pública, à luz da Lei Geral de Proteção de Dados (LGPD), sob o nº 13.709 de 2018.

A metodologia da pesquisa é teórica, descritiva e exploratória, a partir de procedimentos bibliográficos e análise jurisprudencial.

## 2 DECISÕES AUTOMATIZADAS PELA ADMINISTRAÇÃO PÚBLICA

São historicamente remotos os registros sobre tratamento de dados pessoais pela administração pública. Na Bíblia Sagrada, no Livro de Lucas (Lc 2,1-5), há referência ao “Censo de Quirino”, realizado há mais de dois milênios, aplicado nas

[1] Pós-Doutor em Direito, pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Doutor e Mestre em Direito, pelo Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul (UFRGS). Professor Permanente do Mestrado Profissional em Direito da Empresa e dos Negócios da UNISINOS; Professor de graduação em Direito e Relações Internacionais da UNISINOS; Professor de Graduação em Direito das Faculdades Integradas São Judas Tadeu; e-mail: cristianocolombo@unisinos.br.

províncias romanas da Síria e da Judeia, por meio do Decreto de César Augusto, que ordenou o "recenseamento de toda a terra"[2]. Reportar este episódio histórico não é acidental, já que foi no contexto da judicialização da Lei do Censo de 1983 (*Volkszählungsgesetz)*, no Tribunal Constitucional Alemão, que foram abertas sólidas *guidelines* acerca do tratamento de dados pessoais pelo Poder Público. Na Reclamação Constitucional contra Ato Normativo, BVerfGE 65, 1, de 15 de dezembro de 1983, a Corte Constitucional Alemã apreciou o conteúdo da Lei do Censo, que se voltava à coleta de dados pessoais como endereço, profissão e local de trabalho "para fins estatísticos". O escopo da norma era observar o crescimento e distribuição populacional, bem como questões sociais, demográficas e econômicas, tudo para dar fundamentação às "decisões político-econômicas da União, Estados e municípios"[3]. No entanto, em seu § 9, havia a permissão de "comparação dos dados levantados com os registros públicos" e "transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais" para a "execução administrativa"[4]. Referida lei foi julgada constitucional, contudo, estes dispositivos foram declarados nulos, a partir do "direito à autodeterminação da informação", tendo sido criado um "marco para a teoria de proteção de dados pessoais"[5]. Nesta linha, o titular dos dados pessoais tem o direito de saber com "segurança quais informações sobre sua pessoa são conhecidas em certas áreas de seu meio social", sendo que o "livre desenvolvimento da personalidade" lhe protege "contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais"[6].

Em um olhar mais alentado, sobre o seu conteúdo decisório, percebe-se seu espírito vanguardista, visto que, na década de 80, o Tribunal Constitucional Alemão fez referência, também, à problematização sobre as decisões automatizadas aplicadas à formação de *profiling* pelo Poder Público. Como se pode verificar, em suas razões, houve a combinação das expressões "processamento automático de

---

[2] **Bíblia Sagrada**. São Paulo: Ave Maria, 1995, (Lc 2,1-5). p. 1347. Trata-se de mera indicação do evento, não se propondo o estudo a realizar um apanhado histórico.

[3] **Cinquenta anos de jurisprudência do Tribunal Constitucional alemão**. Berlin: Fundação Konrad-Adenauer, c2005. Disponível em <http://mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf>. Acesso em: 7 nov. de 2020. p. 233-234.

[4] Ibidem.

[5] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 31.

[6] **Cinquenta anos**..., *op. cit.*, p. 233-234.

dados" e, na sequência, "processos decisórios", revelando tocar diretamente no objeto em comento:

> Esse poder necessita, sob as condições atuais e futuras do processamento automático de dados, de uma proteção especialmente intensa. Ele está ameaçado, sobretudo porque em processos decisórios não se precisa mais lançar mão, como antigamente, de fichas e pastas compostas manualmente. Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dados Pessoais) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos[7].

Dando seguimento à fundamentação decisória, é possível, claramente, verificar o conceito de *profiling*, no contexto do julgado, na medida em que assim dispõe: podem ser combinados, sobretudo, na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase [...]. Portanto, além de histórica, a decisão é extremamente atual.

As decisões automatizadas são aquelas em que o processo decisório conta com a colaboração de meios tecnológicos[8]. Podem ser parcialmente automatizadas, com interação entre ser humano e máquina, ou, quando não há qualquer intervenção humana, são classificadas como exclusivamente automatizadas[9]. Neste último caso, opera-se "a resposta ao destinatário, sem a análise ou revisão prévia de uma pessoa natural"[10]. Por sua vez, a técnica do *profiling* assim pode ser conceituada:

> [...] conhecida como *profiling*, pode ser aplicada a indivíduos, bem como estendida a grupos. Com elas, os dados pessoais são tratados com o auxílio de métodos estatístico e técnicas de inteligência artificial, com o fim de se obter uma "metainformação", que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa[11].

---

[7] *Ibidem*, p. 233-234.

[8] **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento** (UE) 2016/679. 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>. Acesso em: 2019.

[9] *Idem Ibidem*.

[10] COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Decisões automatizadas em matéria de perfis e riscos algorítmicos: diálogos entre Brasil e Europa acerca dos direitos das vítimas de dano estético digital. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord). **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco, 2020, p. 163-184, p. 166.

[11] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2019.

Decisões automatizadas podem se operar no âmbito da administração pública, em temas como tributação, saúde, previdência, segurança, enfim, de forma ampla em políticas públicas.

O Comité Europeu de Proteção de Dados da União Europeia, apontando a crescente capacidade de processamento dos dados pessoais, assim denomina o *profiling*:

> A disponibilidade generalizada de dados pessoais na Internet e a partir de dispositivos da Internet das Coisas (IdC), bem como a capacidade para encontrar correlações e criar ligações, podem tornar possível determinar, analisar e prever aspetos que digam respeito à personalidade ou ao comportamento, aos interesses e aos hábitos de uma pessoa[12].

Importa destacar que, em nível legislativo, a Lei Geral de Proteção de Dados Pessoais (LGPD), sob o nº 13.709 de 2018, também consagrou o *profiling*, em seu artigo 12, § 2º, trazendo expressa referência ao "perfil comportamental"[13]. E, portanto, encontrando proteção às violações daí decorrentes. Outrossim, no artigo 20 da LGPD, opera-se o enlace entre as duas temáticas ao tratar sobre o direito de revisão de decisões exclusivamente automatizadas[14].

Verifica-se a atualidade e importância do estudo das decisões automatizadas em matéria de perfis e, neste sentido, passar-se-á a estabelecer pontes entre o julgado do Tribunal Constitucional Alemão e recentes posicionamentos do Supremo Tribunal Federal.

## 3 DIÁLOGOS ENTRE *LEADING CASES* E CRITÉRIOS PARA IMPLEMENTAÇÃO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Como recorte metodológico, passar-se-á a enumerar as contribuições oferecidas por dois célebres *Leading Cases,* sobre o tratamento de dados pessoais

---

[12] Grupo de Trabalho do Art. 29º para proteção de dados. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento** (UE) 2016/679. WP 251 Rev. 1. 3 de Outubro de 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>. Acesso em: 3 jul.de 2020.

[13] Artigo 12, § 2º. Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

[14] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base 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.

pela administração pública, que resultam em critérios de aplicação, buscando estabelecer *guidelines* sobre a matéria em comento. Primeiramente, aprofundar-se-á o rol dos fundamentos dispostos na celebérrima decisão sobre a Lei do Censo de 1983, que é referencial em nível mundial, para, posteriormente, à luz do ordenamento jurídico pátrio, refletir sobre as Ações Diretas de Inconstitucionalidade (ADI) sob os números 6387 a 6390 e 6393, relativamente à Medida Provisória 954, de 2020, esta que determinou a disponibilização à Fundação IBGE, "da relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas".

O julgado do Tribunal Constitucional Alemão estabeleceu que o "direito fundamental garante o poder do indivíduo de decidir, ele mesmo, em princípio, sobre a exibição e o uso de seus dados pessoais"; no entanto, salientou que limitações a este direito podem ocorrer quando houver "interesse predominante da coletividade", à luz do princípio da proporcionalidade[15]. Outrossim, refletiu sobre o que, hoje, se reconhece como riscos algoritmos[16], ao destacar a possibilidade da formação de um "quadro de personalidade [...] sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso", ainda, podendo "atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas"[17].

Em importante distinção, a Corte Alemã divisou os "dados pessoais que são levantados e manipulados individualmente, não anonimamente", daqueles que "são destinados a objetivos estatísticos"[18].

Quanto aos dados pessoais, salientou que, em questões como tributação e concessão de benefícios sociais, o "levantamento obrigatório de dados relativos à pessoa não é admissível de forma irrestrita", ou seja, prevendo "medidas processuais de proteção"[19]. E, na busca em atender ao interesse comum, deve-se levar em conta "dados com significado social", não aqueles que se voltam a "informações íntimas inexigíveis". Para estes dados, a lei deve, sempre, definir qual a "finalidade do uso por área e de forma precisa", voltando-se a dados "adequados e necessários" a este fim. Advertiu o julgado, que as autoridades devem restringir,

---

[15] **Cinquenta anos**..., *op. cit.*, p. 233-234.
[16] COLOMBO; FACCHINI NETO, *op. cit.*, 2020, p. 166.
[17] **Cinquenta anos**..., *op. cit.*, p. 233-234.
[18] *Idem Ibidem*.
[19] *Idem Ibidem*..

valendo-se do “mínimo indispensável para alcançar o seu objetivo”, primando pela transparência[20].

Dessa forma, é possível identificar princípios como da finalidade, adequação, necessidade e da transparência, na linha do que preceitua o artigo 6º, da Lei Geral de Proteção de Dados Pessoais.

No que tange à estatística, em que dados podem “ser utilizados para as tarefas mais diversas”, advertiu a Corte que:

> É necessário criar condições de manipulação claramente definidas que garantam que o indivíduo não se torne um simples objeto de informação, no contexto de um levantamento e manipulação automáticos dos dados relativos à sua pessoa. Ambas as coisas, a falta de vinculação a um propósito definido, reconhecível e compreensível a qualquer momento, e o uso multifuncional dos dados, fortalecem as tendências que devem ser identificadas e restringidas pelas leis de proteção aos dados, que concretizam o direito garantido constitucionalmente à autodeterminação sobre a informação.

E, ainda, salientou, sobre importância da anonimização:

> Mesmo no levantamento de dados individuais que serão utilizados para fins estatísticos, o legislador deve examinar, ao ordenar o dever de informação, se eles podem causar para o cidadão o perigo da discriminação social (p.ex. como viciado em drogas, com antecedentes criminais, doente mental, antissocial) e se o objetivo da pesquisa não pode ser alcançado também com uma averiguação anônima[21].

Nessa linha, oportuno trazer, ao presente estudo, as palavras de Rodotà, que versa sobre o corpo eletrônico, como essa reunião de dados, que não pode ser alvo de uma mineração oportunista e irrestrita, sobretudo, na construção de perfis:

> O corpo eletrônico, um conjunto de informações que constroem a nossa identidade, vem assim reunido ao corpo físico: a dignidade se torna o meio forte de reconstituir a integridade da pessoa (Carta dos Direitos Fundamentais da União Europeia, art. 3), para evitar que a pessoa venha considerada um tipo de mina a céu aberto, onde qualquer um pode acessar qualquer informação e assim constituir perfis individuais, familiar, de grupo, fazendo assim que a pessoa se torne objeto de poder esterno, que possam falsifica-la, construí-la de acordo às necessidades de uma sociedade de vigilância, de seleção social, do cálculo econômico[22].

De tal forma, os critérios devem ser definidos, na linha da decisão objeto de estudo, inclusive, para que se evite o caráter discriminatório, apontando a via da anonimização dos dados como mais adequada.

---

[20] **Cinquenta anos**..., *op. cit.*, p. 233-234.
[21] *Idem Ibidem*.
[22] RODOTÀ, Stefano. ***La rivoluzione della dignità***. Napoli: La Scuola di Pitagora, 2013, p. 33. (tradução livre)

No contexto brasileiro, no julgamento, em caráter liminar, das Ações Diretas de Inconstitucionalidade (ADI) sob os números 6387 a 6390 e 6393, junto ao Supremo Tribunal Federal, depreende-se que a inconstitucionalidade se debruçou ao disposto no artigo 2º, da Medida Provisória 954, que determinou o "compartilhamento de dados por empresas de telecomunicações durante a emergência de saúde pública", mais especificamente, a disponibilização à "Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas"[23].

Atualmente, a cautelar deferida, de Relatoria da Ministra Rosa Weber, foi referendada em 07 de maio de 2020, nos autos da ADI 6389, para "suspender a eficácia da Medida Provisória n. 954/2020, determinando, em consequência, que o Instituto Brasileiro de Geografia e Estatística – IBGE se abstenha de requerer a disponibilização dos dados objeto da referida medida provisória e, caso já o tenha feito, que suste tal pedido". A decisão traz importantes critérios, para a compreensão da utilização de dados pessoais. Ao concluir que a Medida Provisória em análise exorbitou os limites, destaca a Ministra Rosa Weber, que a disponibilização ao IBGE versa sobre dados pessoais, oportunizando "identificação - efetiva ou potencial - de pessoa natural" e, portanto, deve observar os "limites delineados pela proteção constitucional". Nessa linha, ao referir os princípios da privacidade, da autodeterminação informativa, declarou que a Medida Provisória em questão "não delimita o objeto da estatística a ser produzida, nem a finalidade, tampouco a amplitude", bem como "a necessidade de disponibilização dos dados nem como serão efetivamente utilizados".

O julgado brasileiro também ressalva que não há referência ao "mecanismo técnico ou administrativo a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida", tampouco, no caso, "o anonimato dos dados compartilhados".

Cumpre destacar que, por ocasião da sustentação oral, Danilo Doneda assim se manifestou sobre o caso:

> A integralidade da base de dados dos usuários de telefonia fixa e móvel, que, nos termos da MP 954 deve ser transferida ao IBGE, representa volume de dados pessoais imensamente maior do que a amostragem necessária para a realização da PNAD - Pesquisa Nacional por Amostra de Domicílios, que gira em torno de pouco mais de mil respondentes. Esta enorme desproporção representa clara violação ao princípio da proporcionalidade e do princípio da minimização, princípios clássicos de proteção de dados, e ensejam em risco desnecessário para a sociedade.

> Estamos em um momento de construção, em um momento de notável aceleração de processos históricos. [...] Em um momento como este, caso o compartilhamento de dados como o ensejado pela MP 954 seja tornado possível sem a aposição de garantias efetivas sobre a finalidade, transparência, segurança e proporcionalidade e seu devido controle, arrisca-se a consolidação de uma situação irreversível para a garantia dos direitos fundamentais.[23]

De tal arte, a decisão, no contexto nacional, que afastou a possibilidade do compartilhamento, andou nos veios "dos princípios da finalidade, da transparência, da segurança, proporcionalidade e do princípio da minimização.", na linha da decisão do Tribunal Constitucional alemão.[24]

Cumpre destacar, por último, que a Lei Geral de Proteção de Dados Pessoais, em seus artigos 23 a 32, versa, expressamente, sobre o tratamento de dados pela administração pública, estabelecendo regras e a responsabilidade da administração e seus agentes. E, em oportuno "Guia de Boas Práticas Lei Geral de Proteção de Dados Pessoais"[25], expedido pelo Comitê Central de Governança de Dados, do Governo Federal, são indicadas ações concretas, a fim de cumprir o que dispõe a legislação, a saber:

> • informar as hipóteses em que, no exercício de suas competências, o órgão respalda 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 (Art. 23, I);
>
> • indicar encarregado quando realizar operações de tratamento de dados pessoais, nos termos do art. 39 da LGPD (Art. 23, II);
>
> • observar as formas de publicidade das operações de tratamento que poderão ser estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD, Art. 23, § 1º);
>
> • manter os dados 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. (Art. 25); e
>
> • realizar o uso compartilhado de dados pessoais de acordo com as finalidades específicas de execução de políticas públicas e atribuição legal

[23] DONEDA, Danilo. Registro da sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art. 2º, caput e §§ 1º e 3º da MP 954/2020. **Civilistica.com**, v. 9, n. 1, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/519/397>. Acesso em: 24 jun. de 2020.

[24] COLOMBO, Cristiano; ENGELMANN, Wilson. Inteligência artificial em favor da saúde: proteção de dados pessoais e critérios de tratamento em tempos de pandemia. *In*: PINTO, Henrique Alves; GUEDES, Jefferson Carús; CÉSAR, Joaquim Pontes de Cerequeira. (Coord). **Inteligência artificial aplicada ao processo de tomada de decisões**. Belo Horizonte, São Paulo: D'Plácido, 2020. p. 225-246, p. 240.

[25] **GUIA de boas práticas**: lei geral de proteção de dados (LGPD). [Brasília], 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>. Acesso em: 2020.

> do órgão ou entidade, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da LGPD (Art. 26).[26]

Nesse sentido, é que a tensão entre o interesse individual do titular de dados pessoais e o interesse da coletividade devem ser sopesados, observando os princípios da Lei Geral de Proteção de Dados Pessoais, como critérios a serem adotados.

## 4 CONSIDERAÇÕES FINAIS

A partir da análise das decisões judiciais e, à luz da Lei Geral de Proteção de Dados Pessoais, é possível considerar que: a uma, o salto do meio físico para o digital, acelerou a possibilidade de processamento, cruzamento de dados, propulsando a tomadas de decisões automatizadas e a criação de perfis; a duas, na utilização de dados pessoais pelo Poder Público, devem ser observados os princípios da Lei Geral de Proteção de Dados Pessoais, sobretudo, princípios da finalidade, da transparência, da segurança, proporcionalidade e do princípio da minimização; a três, na linha da decisão da ADI 6389, mesmo em se tratando de questões estatísticas, devem ser apontadas as finalidades, delimitando o mecanismo técnico ou administrativo a proteger os dados pessoais, buscando a implementação de boas práticas, pela administração pública.

## REFERÊNCIAS

**Bíblia Sagrada**. São Paulo: Ave Maria, 1995.

BRASIL**. Medida Provisória n° 954**, de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm>. Acesso em: 24 jun. de 2020.

**Cinquenta anos de jurisprudência do Tribunal Constitucional alemão**. Berlin: Fundação Konrad-Adenauer, c2005. Disponível em <http://mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-

[26] **GUIA de boas práticas**: lei geral de proteção de dados (LGPD). [Brasília], 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>. Acesso em: 2020.

jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf>. Acesso em: 7 nov. de 2020.

COLOMBO, Cristiano; ENGELMANN, Wilson. Inteligência artificial em favor da saúde: proteção de dados pessoais e critérios de tratamento em tempos de pandemia. *In*: PINTO, Henrique Alves; GUEDES, Jefferson Carús; CÉSAR, Joaquim Pontes de Cerqueira. (Coord). **Inteligência artificial aplicada ao processo de tomada de decisões**. Belo Horizonte, São Paulo: D'Plácido, 2020. p. 225-246.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Decisões automatizadas em matéria de perfis e riscos algorítmicos: diálogos entre Brasil e Europa acerca dos direitos das vítimas de dano estético digital. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coord). **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco, 2020. p. 163-184.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2019.

_____. Registro da sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art. 2º, caput e §§ 1º e 3º da MP 954/2020. **Civilistica.com**, v. 9, n. 1, 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/519/397>. Acesso em: 24 jun. de 2020.

**Grupo de Trabalho do Art. 29º para proteção de dados**. Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679. WP 251 Rev. 1. 3 de Outubro de 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>. Acesso em 3 jul. de 2020.

**Guia de boas práticas: lei geral de proteção de dados (LGPD)**. [Brasília], 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>. Acesso em: 2020.

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

**Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento** (UE) 2016/679. 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>. Acesso em: 2019.

RODOTÀ, Stefano***. La rivoluzione della dignità***. Napoli: La Scuola di Pitagora, 2013.

# A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E A LEI DE ACESSO À INFORMAÇÃO (LAI): UMA PROPOSTA DE INTERPRETAÇÃO SISTEMÁTICA

Têmis Limberger[1]

> A internet é a nova metáfora da globalização. O mar é a grande metáfora, não a nova. A liberdade dos mares se confronta com o "nomos" da terra, por isso, a ação de quem se movimenta na Internet, fica descrita como navegar.[2]

## 1 INTRODUÇÃO

A sociedade em rede, pela qual se caracteriza a sociedade do século XXI, é uma estrutura ao redor da rede de comunicação digital.[3] É abolida a centralidade da difusão da informação e cada sujeito comunicante se transforma em emissor e receptor de mensagem, rompendo com a barreira passiva, que, até então, existia. Esta é a dinâmica da sociedade em que vivemos, aonde se retoma a ideia de que informação é poder.[4] A economia informacional é global.[5] Uma economia global é uma realidade diferente de uma economia mundial (que é uma experiência que no ocidente existe desde o século XVI, como sendo uma experiência de acumulação de capital que avança pelo mundo).

A sociedade em rede já estava em franca evolução, quando se operou a pandemia da Covid-19, fazendo com que as relações virtuais crescessem em escala exponencial. Como revelou a revista *The Economist*[6] : os dados são a nova riqueza

---

[1] Doutora em Direito Público pela Universidade Pompeu Fabra - UPF de Barcelona. Pós-doutora em Direito pela Universidade de Sevilha. Professora do Programa de Pós-graduação da Universidade do Vale do Rio dos Sinos - UNISINOS. Procuradora de Justiça do Ministério Público do Estado do Rio Grande do Sul. Orientadora de Mestrado e Doutorado. Autora do livro **Cibertransparência** - Informação Pública em Rede - A virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016.
TCE/RS - Webconferência: Lei Geral de Proteção de Dados e o Poder Público - Mesa 2. Disponível em <https://www.youtube.com/watch?v=Bn_0f4DgyMs&ab_channel=tcegaucho>. Acesso em: 20 set. de 2020

[2] RODOTÀ, Stefano***. El derecho a tener derechos***. Madrid: Trotta, 2014, p.31.

[3] CASTELLS, Manuel. ***Comunicación y Poder***. Madri: Alianza Editorial, 2009.

[4] NORA, Simon; MINC, Alain. **Informe Nora-Minc** – La informatización de la sociedad. Madrid: [S.n.], 1982, p. 18 (*Colección popular*).

[5] CASTELLS, Manuel. **A Sociedade em Rede: a era da informação** - economia, sociedade e cultura. 4. ed. Lisboa: Fundação Calouste Gulbenkia. 2011, p. 123-124.

[6] The Economis Review. ***The world's most valuable resource is no longer oil but data***. *May* 6 *th* 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 20 set. de 2020.

do século XXI, suplantando formas até então tradicionais como, por exemplo, o petróleo. Assim, pode não haver uma prestação pecuniária típica, mas os dados possuem valor e são o objeto de troca na sociedade de consumo e que podem trazer impactos nos regimes democráticos.[7]

Neste contexto, a administração pública não poderia ficar imune ao fenômeno informático e legislações foram editadas, visando acompanhar este movimento. A tentativa é difícil, pois a legislação tem uma perspectiva mais morosa em termos de procedimento[8] e o fenômeno informático evolui muito rapidamente, fazendo com que a lei, quando entre em vigor, corra o risco de já não dar conta dos fatos a que pretende regular. Há um evidente descompasso.

Portanto, estudar-se- á a Lei Geral de Proteção de Dados - LGPD e a Lei de Acesso à Informação - LAI, visando verificar se são compatíveis no ordenamento jurídico brasileiro, propondo-se, ao final, uma interpretação sistemática, entre ambas. Tratar-se-á, primeiramente, da LAI, em virtude de a mesma haver tido a primazia do vigor, no ordenamento jurídico brasileiro.

## 2 ADMINISTRAÇÃO PÚBLICA EM REDE

Primeiramente, é importante conceituar “administração em rede”[9]. Para isso, explicar-se-á “rede”, ou ainda, o que é uma “sociedade em rede”. Castells[10] vai elucidar que redes “são estruturas complexas de comunicação, construídas em torno de um conjunto de metas que, simultaneamente, garantem a unidade de propósito e a flexibilidade de execução, em virtude de sua adaptabilidade ao ambiente operacional”. Ensina, o autor, que são programas autoconfiguráveis por atores

[7] ISTOÉ - Revista, 18/04/2018, **Zuckerberg contra a parede**, Tecnologia, p. 66.
[8] PÉREZ LUÑO, Antonio Enrique. El desbordamiento de las fuentes del Derecho. Sevilla: Real **Academia Sevillana de Legislación y Jurisprudencia**, 1993.
[9] LIMBERGER, Têmis; SANTANNA, Gustavo da Silva. **Na sociedade em rede, em que o uso dos recursos digitais foi potencializado pela COVID-19**, qual o papel do direito à proteção dos dados pessoais (sensíveis), interoperabilidade, cooperação e transparência para contribuir à efetivação do direito à saúde (no prelo).
SANTANNA, Gustavo da Silva. **Do patrimonialismo à sociedade da informação**: proposições para a implantação da administração pública eletrônica (e-administração) no Brasil. Tese (Doutorado em Programa de Pós-Graduação em Direito). São Leopoldo: Universidade do Vale do Rio dos Sinos - UNISINOS, 2019.
[10] CASTELLS, Manuel. **O poder da comunicação**. Tradução de Vera Lúcia Mello Joscelyne. Rio de Janeiro: Paz e Terra, 2015, p. 67.

sociais, cuja estrutura, ao mesmo tempo em que evolui, autoconfigura-se “em uma busca permanente por combinações de redes mais eficientes”[11].

As redes sociais, portanto, são estruturas comunicativas nas quais atores sociais promovem seus valores e interagem[12]. Assim, não é correto associar que rede é somente a rede de computadores. Na verdade, a rede de computadores é um (ou o) local em que interagem os atores sociais e em que as mensagens da rede social se processam, não sendo possível afirmar que, antes do século XXI, não existiam redes, pois “onde quer que exista vida, existem redes”[13].

Existem (iam) redes verticais/hierarquizadas, como a organização da Administração Pública, por exemplo, e redes mais modernas, horizontalizadas.[14] Explica Castells[15] que, como as redes são flexíveis, permitem introduzir novos atores e conteúdos, bem como adaptar-se a novas realidades, como as mudanças tecnológicas de comunicação. Ora, mesmo no tempo das ferrovias e telégrafo, já existiam “redes de comunicação”, é claro, muito mais rudimentares do que nos tempos modernos. Naquela época (Primeira e Segunda Revolução Industrial), as organizações eram estruturadas verticalmente e extremamente hierarquizadas. Não se pode imaginar, contudo, em pleno século XXI, na quarta Revolução Industrial[16], que as estruturas sejam, ainda, organizadas da mesma maneira.

Uma “sociedade em rede” é, por sua vez, “uma sociedade cuja estrutura social é construída em torno de redes ativadas por tecnologias de comunicação e de informação processadas digitalmente e baseadas na microeletrônica”.[17] Como a rede digital está mundialmente espalhada, é possível que a sociedade interaja de forma global, ou seja, além das fronteiras territoriais, podendo-se denominar de “sociedade em rede global”.[18] A partir dessa visão horizontalizada de sociedade, podem-se extrair, adequadamente, os escritos de Moreira Neto[19], quando colocou a expressão “da pirâmide à rede”. Para o autor, a “rede informacional” impede que os processos

---

[11] CASTELLS, Manuel, *op. cit.*, 2015, p. 67.
[12] *Idem Ibidem*.
[13] *Idem Ibidem*.
[14] LOUREIRO, João Carlos. Constituição, tecnologia e risco(s): entre medo(s) e esperança(s). *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord.). **Direito, Inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 33-84.
[15] CASTELLS, Manuel, *op. cit.*, 2015, p. 67.
[16] SCHWAB, Klaus. **A quarta revolução industrial**. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.
[17] CASTELLS, *op. cit.*, 2015, p. 70.
[18] *Idem Ibidem*.
[19] MOREIRA NETO, Diogo de Figueiredo. **Quatro paradigmas do direito administrativo pós-moderno**: legitimidade, finalidade, eficiência e resultados. Belo Horizonte: Forum, 2008, p. 53.

sociais fluam de forma hierarquizada, “transmitida sob a forma de pirâmide” típica das sociedades estamentais, em que os detentores de poder ocupavam as altas posições dentro deste cenário piramidal.[20] Na nova configuração social, não existiria mais um centro unitário de poder (o Estado), mas um emaranhado de órgãos e entidades, governamentais ou não, capazes de exercer poder e tomar decisões, em uma perspectiva pluralista, em que existem “plúrimos centros de comando”, passando da ideia de “subordinação” para a “colaboração”.[21] É visível, portanto, o poder não mais limitado ao Estado, mas, de certa forma, compartilhado com ele. Com essas premissas estabelecidas, é possível compreender o que seria uma Administração Pública em rede. Uma administração dialógica, horizontal, que não “dita” as regas, mas que as constrói de forma democrática com a atuação de outros atores.

## 3 DAS PREVISÕES NORMATIVAS BRASILEIRAS COM TEMÁTICA CONEXA

No Brasil, os direitos à intimidade e à privacidade estão referidos no artigo 5º, X, da Constituição Federal – CF88, agasalhando a distinção proveniente da doutrina e jurisprudência alemãs, da teoria das esferas ou dos círculos concêntricos.[22] As esferas da vida privada comportam o grau de interferência que o indivíduo suporta com relação a terceiros. Para tal, leva-se em consideração o grau de reserva do menor para o maior. Assim, no círculo exterior está a privacidade; no intermediário, a intimidade; e, no interior desta, o sigilo. Logo, a proteção legal torna-se mais intensa, à medida que se adentra no interior da última esfera.

No espectro de proteção aos dados pessoais, algumas leis são referências como: o Marco Civil da Internet (Lei nº 12.965/2014), que em seu artigo 3º, III, já previu a proteção dos dados pessoais, na forma da lei, sendo que, somente agora, a lei foi editada. O Marco Civil prevê o consentimento na coleta dos dados (artigo 7º, IX) e o agir de maneira transparente (artigo 9º, II), tal qual acontece na normativa.

---

[20] MOREIRA NETO, *op. cit.*, 2008, p. 53.
[21] *Idem Ibidem*.
[22] COSTA JR., Paulo José da. **O direito a estar só**: tutela penal da intimidade. São Paulo: RT, 1970, p. 31, citando HENKEL, **Der Strafschutz des Privatlebens**. Em sentido contrário, não reconhecendo a Teoria das Esferas, DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. rev. e atual. São Paulo: Thomsom Reuters **Revista dos Tribunais RT**, 2019, p. 105.

Devido ao comando do artigo 5º, XXXIII, da CF88, que dispõe que todos têm direito ao acesso à informação, contida nos órgãos públicos, sendo o interesse particular ou coletivo, foi promulgada a Lei de Acesso à Informação Pública (Lei nº 12.527/2011). Esta lei prevê que os órgãos públicos disponibilizem informação referente a despesas públicas realizadas com vencimentos ou licitações, em que a regra é a publicidade e o sigilo, a exceção. A lei inverteu a orientação que, até então, existia, quando os princípios tinham aplicação contrária. Atualmente, aquele que requer a informação tem que se identificar, pois receberá informação dos órgãos públicos e, pela utilização desta, ficará responsável. Antecedente importante foi a Lei de Responsabilidade Fiscal, Lei Complementar nº 101/2000, com as alterações da Lei Complementar nº 131/2009, que nos artigos 48/49 determinaram a publicação dos gastos públicos pela rede mundial de computadores. Outra vantagem da informação em rede é a possibilidade do compartilhamento, de uma maneira crítica e com baixo custo. Em razão do artigo 5º, XXXII, da CF88, que dispôs a respeito da proteção ao consumidor, foi o Código de Defesa do Consumidor (Lei nº 8.078/1990) legislação pioneira, editada para proteção aos bancos de dados. Em seus artigos 43/44, tutela os bancos de dados de consumidores, prevendo situações de acesso, retificação e cancelamento das informações negativas, operando-se o prazo prescricional, que não podem ficar por mais de cinco anos registradas. Posteriormente, foi editada a lei dos cadastros positivos, Lei nº 12.414/2011, com a promessa de diminuir as taxas de juros aos tomadores de financiamento, dos denominados “bons pagadores”, que são os consumidores que realizam o adimplemento de suas obrigações pontualmente.

Estatuída pelo comando constitucional do artigo 5º, LXXII, que visou assegurar o conhecimento das informações, em nome do cidadão, constantes em banco de dados de entidades governamentais ou de caráter público, bem como a possibilidade de retificá-las. Para tanto foi editada a Lei que disciplinou o *habeas data* (Lei nº 9.507/1997). Esta lei possui uma particularidade, que é a necessidade de esgotamento da via administrativa, antes do ingresso na via judicial. Isso é uma peculiaridade, pois, no Brasil, há a unidade de jurisdição como expressão do artigo 5º, XXXV, da CF88, em que nenhuma lesão a direito pode deixar de ser examinada pelo Poder Judiciário.

A Lei de Acesso à Informação Pública (Lei nº 12.527/2011), no Brasil, surge em um contexto em que mais de 70 países[23] já a possuíam e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) chega, após cinco décadas de vigência normativa em outros países. Este movimento denota uma tendência globalizada da legislação nos Estados. A proteção de dados pessoais está sendo debatida no Congresso Nacional, com a PEC 17/2019, que pretende erigi-lo à condição de um direito fundamental, tal como já existe no artigo 8º da Carta de Direitos da União Europeia.[24] O que se pode apontar como distinto, desde logo, é que os países, primeiro, tiveram uma legislação protetiva dos dados e, somente depois, é que tornaram acessível a informação pública. A experiência brasileira foi no sentido inverso.

Diante da leitura, principalmente, dos dois estatutos normativos: da LAI, que determina a abertura da informação; e da LGPD, que pretende proteger os dados, em um primeiro momento, podem parecer divergentes, mas é função do jurista buscar a interpretação sistemática que permita um diálogo harmonioso entre os dispositivos normativos.

Como fazer a ponte normativa entre as legislações ou utilizando-se da doutrina trazida ao Brasil, do Professor Erik Jayme, pela Professora Cláudia Lima Marques, como promover o diálogo das fontes? Partindo-se da assertiva proposta por Cláudia Lima Marques[25] de que: o aplicador deve visar o diálogo das fontes, de forma a dar efeito útil a um grande número de normas narrativas, os valores constitucionais e, sobretudo, os direitos humanos, porque, segundo Erik Jayme, o fio condutor, o *Leitmotive*[26], do direito na pós-modernidade, do direito do século XXI, serão os direitos humanos. Pode-se dizer que os direitos humanos conferem a integração das distintas normas no ordenamento jurídico.

---

[23] BRASIL. Câmara dos Deputados. **Lei de Acesso à Informação**: um direito do cidadão. (Eduardo Tramarim). Disponível em: <https://www.camara.leg.br/radio/programas/378496-lei-de-acesso-a-informacao-um-direito-do-cidadao/>. Acesso em: 13 out.de 2020.

[24] UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia, de 07 de dezembro de 2000. **Carta de Nice**. Disponível em: <http://www.europarl.europa.eu/charter/default_pt.htm>. Acesso em: 10 out.de 2020.

[25] MARQUES, Cláudia Lima. Contratos no Código de Defesa do Consumidor, 9ª ed., São Paulo: Thomsom Reuters, **Revista dos Tribunais RT**, 2019, p. 587.
Vide também: MARQUES, Cláudia Lima (coordenadora). Diálogo das Fontes: do conflito à coordenação de normas no direito brasileiro. São Paulo: Thomsom Reuters **Revista dos Tribunais RT**, 2012, p.23.

[26] JAYME, Erik. Identité culturelle et intégration: le droit international privé postmoderne. **Recueil des Cours de l'Académie de Droit International de la Haye,** 1995, II, Kluwer, Haia, p. 36 e ss.

Visando promover a interpretação sistemática, invoca-se Canaris[27] com o postulado do sistema jurídico que se justifica a partir de um dos mais elevados valores do Direito, notadamente o princípio da justiça e suas concretizações no princípio da igualdade e a segurança jurídica em suas manifestações, como determinação e previsibilidade do direito, como estabilidade e continuidade da legislação e da jurisprudência ou, simplesmente, como praticabilidade da aplicação do Direito. Assim, o pensamento sistemático radica na ideia de Direito como o conjunto dos valores mais elevados. Ainda que a adequação e a unidade, com frequência, possam realizar-se de modo fragmentado. A fragmentação não nega a possibilidade da interpretação sistemática, apenas torna claro que são postos certos limites à formação plena. O papel do conceito de sistema é o de traduzir e realizar a adequação valorativa e a unidade interior da ordem jurídica. Deste modo, busca-se realizar uma interpretação sistemática da LGPD e da LAI. Assim, uma das primeiras questões postas é no sentido de como conjugá-las, uma vez que uma lei determina a proteção dos dados pessoais e, outra, a publicidade das informações de caráter público. A primeira impressão pode ser no sentido de contradição, mas esta é apenas aparente. Ordenamento jurídico deve ser interpretado de forma sistemática.

O direito comparado aponta no sentido da compatibilidade, menciona-se a legislação espanhola, aonde existe a Lei nº 19/203 de transparência, acesso à informação pública e bom governo; e a Lei nº 3/2018, de proteção de dados pessoais e garantia de direitos digitais, em consonância com o RGPD. No Brasil, a LGPD, em seu artigo 23, também faz um diálogo com a LAI, demonstrando que o intérprete deve buscar a interpretação sistemática de maneira harmoniosa.[28]

## 4 A TRANSPARÊNCIA E A ADMINISTRAÇÃO PÚBLICA

A transparência administrativa é um elemento essencial na estratégia de restabelecer a confiança no sistema democrático e de salvaguardar o Estado de Direito em uma realidade sempre mais complexa, no entendimento de Karl Peter

[27] CANARIS, Wilhelm Claus. **Pensamento sistemático e conceito de sistema na ciência do direito**. Lisboa: Fundação Calouste Gulbekian, 1989, p. 22-23.
[28] LIMBERGER, TÊMIS. **Comentários à LGPD ...** - arts. 23/30 - Ed. FOCO (no prelo)

Sommermann.[29] Por isto, é importante resgatar e atualizar o brocardo romano: *Res publica, salus publica*.

## 4.1 AMPLIAÇÃO DA TRANSPARÊNCIA E DESENVOLVIMENTO HUMANO GLOBAL E MUNICIPAL

É possível relacionar a ampliação da transparência à diminuição da corrupção e à concretização dos direitos sociais, a partir de estudos estatísticos realizados. Veja-se a pesquisa internacionalmente produzida no ano de 2019, por organismo conhecido como *Transparency International - OIT*, apontando que os denominados países escandinavos possuem menor índice de corrupção no mundo. Foram analisados 180 países, classificados numa escala de zero a dez. Quanto menor a nota recebida, maior é o índice de corrupção. Desta forma, Nova Zelândia, Dinamarca e Finlândia figuraram entre os primeiros lugares, respectivamente, com uma pontuação de 8,5.[30] Estes países possuem um Índice de Desenvolvimento Humano - IDH bastante elevado (Ranking IDH 2019 - Dinamarca (11º) 0.937; Finlândia (12º) 0.925; Nova Zelândia (14º) 0.921).[31] Dentre os países latino-americanos, Uruguai e Chile apresentaram a melhor colocação - 21ª com nota 7,1 -, e o Brasil a 106ª colocação, com nota 3,5, sendo que o IDH brasileiro ocupa a 79ª colocação, com índice 0.761, tendo o Uruguai ficado na 57ª colocação, com índice 0.808.[32]

Naqueles países escandinavos, muita informação está disponível na internet. Até mesmo os dados fiscais não são considerados privados, mas de interesse público, assim, é possível a consulta dos dados por todos os cidadãos.[33] Saliente-se que isto é possível nas sociedades Neozelandesa, Dinamarquesa e Finlandesa, pois existe grande homogeneidade cultural e econômica, sendo que a exposição desta informação não gera risco aos cidadãos. Com relação ao vizinho da América do Sul, sabe-se da diferença geográfica, tendo o Uruguai um território pequeno, se

---

[29] SOMMERMANN, Karl-Peter. La exigência de uma administración transparente em la perspectiva de los princípios de democracia y del Estado de Derecho. In **Derecho administrativo de la información y administración transparente**. Ricardo García Macho (ed). Madrid: Marcial Pons, 2010, p. 25.

[30] TRANSPARENCY INTERNATIONAL. ***Corruption Perceptions Index 2019***. Disponível em: <https://www.transparency.org/en/cpi/2019/results>. Acesso em: 20 set. de 2020.

[31] PNUD - Programa das Nações Unidas para o Desenvolvimento. *2019* ***Human Development Index Ranking.*** Disponível em: <http://hdr.undp.org/en/content/2019-human-development-index-ranking> Acesso em: 21 set. de 2020.

[32] *Idem Ibidem*.

[33] SAARENPÄ, Ahti. From de Information Society to the legal Network Society, ID-card and eletronic services. Conferência proferida no dia 7 de novembro, no **X Congreso Ibero-americano de Derecho e Informática**, Santiago do Chile, 6 a 9 de novembro, 2004.

comparado às dimensões continentais do Brasil. Mas, deve-se trabalhar estes números para buscar melhores níveis de transparência que se traduzem em melhor concretização dos direitos sociais.

Procurou-se verificar, em pesquisa realizada, se os indicadores internacionais poderiam ser encontrados, também, no nível municipal. Para tanto, estudou-se os portais das cidades gaúchas e se constatou a relação entre o cumprimento dos direitos sociais (saúde e educação) e os portais de transparência.[34] Assim, os estudos internacionais dialogam simetricamente com os municipais.

## 4.2 CIBERTRANSPARÊNCIA: A CONSTRUÇÃO DE UM CONCEITO

O termo cibertransparência serve para designar as novas relações que se travam em rede, denominadas *ciber*, aglutinadas à ideia de transparência. O fenômeno tecnológico pode servir para potencializar a informação pública.

A expressão *ciber* encontra origem nos trabalhos de Cass Sustein – *República.com;* e de Pérez Luño - *Ciberciudadania o ciudadania.com;* daí o objetivo de cunhar uma expressão que traduza esta nova forma de a administração disponibilizar a informação em rede, para com os administrados, que não é somente a utilização da ferramenta tecnológica, mas uma nova forma de gerenciamento público e das relações democráticas com a sociedade, que daí advenham.

A transparência é uma composição decorrente do princípio da publicidade, do direito à informação, relacionada ao princípio democrático. É a administração agindo em conformidade com o seu dever de tornar público seus atos e o cidadão se informando dos atos praticados pela administração, tudo isto fortalece a cultura democrática.

Nos estados democráticos, a livre discussão é um componente jurídico prévio à tomada de decisão que afeta a coletividade e é imprescindível para sua legitimação. Por isso, para Ignácio Villaverde Menéndez[35] , no Estado Democrático, a informação é credora de uma atenção particular por sua importância na participação do cidadão no controle e na crítica dos assuntos públicos. Não se protege somente a difusão, como sucedia no Estado Liberal, mas se assegura a própria informação, porque o processo de comunicação é essencial à democracia. O

[34] LIMBERGER, Têmis. **Cibertransparência**: informação pública em rede – a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016, p. 94-104.
[35] VILLAVERDE MENÉZES, Ignácio. **Estado democrático e información**: El derecho a ser informado y La Constitución Española de 1978. Oviedo: Junta General Del Principado de Asturias, 1994, p. 33-5.

ordenamento jurídico, no Estado Democrático, assenta-se no princípio geral da publicidade, devendo o sigilo ser excepcional e justificado. Esse preceito é extraído com base no princípio da publicidade e do direito a ser informado do cidadão.

Norberto Bobbio[36], ao tratar das relações da democracia com o poder invisível, estatui que a publicidade seja entendida como uma categoria tipicamente iluminista na medida em que representa um dos aspectos da batalha de quem se considera chamado a derrotar o reino das trevas. Utiliza-se, por isso, a metáfora da luz, do clareamento para contrastar o poder visível do invisível. A visibilidade vai fornecer a acessibilidade e a possibilidade de controle dos atos públicos. Daí se origina a polêmica do iluminismo contra o Estado absoluto, a exigência da publicidade, com relação aos atos do monarca fundados no poder divino. O triunfo dos iluministas tem, como resultado, o art. 15 da Declaração dos Direitos do Homem e do Cidadão[37], que prevê o direito da sociedade de pedir contas a todo o agente público incumbido da administração. Deste modo, a revolução tecnológica

> [...] visa propiciar uma administração mais eficiente e eficaz, mais próxima ao cidadão, mais moderna, mais rápida, que permita oferecer ao cidadão um serviço muito melhor. Exige-se uma administração mais transparente, democrática, mais controlada, mais acessível, mais respeitosa com a privacidade.[38]

A esta assertiva, poder-se-ia acrescentar os direitos humanos, de uma maneira ampla. Nesse sentido, vale referir que, quando o poder estatal faz uso das novas tecnologias para tornar disponível a informação pública, na internet, permite a participação do cidadão nos assuntos públicos, propicia o controle social e, consequentemente, a fiscalização do gasto estatal; a isto se denomina cibertransparência.[39] A Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação Pública – LAI, busca difundir a Informação Pública na Internet, sendo um espectro importante, pois significa um avanço em matéria de transparência; no entanto, suscita algumas questões para reflexão. Impõe o dever dos entes da administração de tornarem públicos dados, que se forem colocados, efetivamente, em rede e tiverem uma correta utilização, podem contribuir ao debate democrático e ao controle social.

---

[36] BOBBIO, Norberto. **O futuro da democracia**. 7. ed., São Paulo: Paz e Terra, 2000, p. 103.
[37] RIALS, Stéphane. **Que sais-je?** Textes constitutionnels français. 11. ed. Paris: Presses Universitaires de France, 1995, p. 5.
[38] PIÑAR MAÑAS, José Luis. ***Administración Electrónica y Ciudadanos***. Pamplona: Thomson Reuters – Civitas, Aranzadi ed, 2011, p. 30.
[39] LIMBERGER, *op. cit.*, 2016.

Buscando-se a etimologia da palavra informação, tem-se o compromisso com a formação da cidadania, assim, visa a contribuir ao debate na esfera pública.[40] Não é qualquer comunicação[41], na rede, que tem este compromisso. Pois, em época de grande quantidade de circulação de conteúdo[42], em que qualquer indivíduo pode produzir e colocar materiais na rede, perde-se em qualidade, e nem tudo é veraz. Por isso, a informação proveniente do poder público deve ter esta qualificação, no sentido de incrementar a cidadania na esfera pública e contribuir à democracia.

A informação pública deve ser disponibilizada de uma maneira padronizada, sempre que possível. Imagine-se um país, com as dimensões continentais do Brasil; se cada um dos 5.570 municípios e dos 26 estados da Federação lançar o dado de uma maneira, dificultará, em muito, o acesso pelo cidadão. Os portais de transparência, com informações facilitadas, auxiliam a acessibilidade daqueles que buscam os dados. No Brasil, por ora, o debate ainda está restrito, por vezes, à informação dos vencimentos dos servidores públicos[43] , sem que se tenha conferido a atenção necessária às licitações e outros repasses estatais a grupos privados. Sabe-se que há constitucionalização do privado e a privatização do público[44] , mas, nesta análise, sopesa-se[45] a predominância do público (agente público, recursos públicos, interesse público) ou do privado (relativos aos direitos fundamentais), na divulgação da informação. Transparência e proteção de dados são valores básicos do Estado Democrático de Direito e há que se buscar o equilíbrio, a partir da construção de critérios jurisprudenciais.

---

[40] HABERMAS, Jürgen. **Mudança estrutural da esfera pública**. São Paulo: Unesp, 2014.

[41] TABORDA, Máren. Porque os que têm armas dão poder para quem não as tem? Discussão sobre a atuação da Justiça Constitucional na concreção ao direito à comunicação social no Brasil.(no prelo) Palestra realizada por ocasião do **IV Congresso Mundial de Justiça Constitucional**, Porto Alegre/RS, Brasil, 2019. Aonde a autora assevera: Informar significa "formar", quando vem do interior, quando é expressada, exteriorizada e compartilhada, tem-se a comunicação.

[42] LLOSA, Mario Vargas. **A civilização do espetáculo**: uma radiografia do nosso tempo e da nossa cultura. Rio de Janeiro: Objetiva, 2013; DEBORD, Guy. **A sociedade do espetáculo**. Rio de Janeiro: Contraponto, 1997.

[43] Tema 483 da repercussão geral, no Agravo 652.777-SP, Rel. Min. Ayres. Entendendo que a matrícula seria suficiente, sem exposição do nome do servidor, veja-se LIMBERGER, *op. cit.*, 2016, p.54/8.

[44] CANOTILHO, José Joaquim Gomes. Civilização do direito constitucional ou constitucionalização do direito civil? A eficácia dos direitos fundamentais na ordem jurídico-civil. *In:* GRAU, Eros Roberto; GUERRA FILHO, Willis Santiago (Org). **Direito Constitucional**: estudos em homenagem a Paulo Bonavides. São Paulo: Malheiros, 2001, p.108-115.

[45] LIMBERGER, Têmis. **O Direito à intimidade na era da informática:** o desafio da proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007, p. 127-137. A respeito dos critérios de interpretação do Tribunal Constitucional Espanhol, nesta matéria.

Importante consagração em prol da transparência foi conferido pelo julgamento no Supremo Tribunal Federal da ADPF nº 690/DF[46], constituindo-se em um marco importante.

## 5 PROTEÇÃO DOS DADOS PESSOAIS

A mais recente novidade, na Europa, é o Regulamento Geral de Proteção de Dados – RGPD nº 679/2016, que surge após cinco décadas de evolução legislativa, em três fases: a) primeiras leis, na Alemanha, em 1970 (Land de Hesse), b) França – instituiu a Agência de Proteção de Dados, em 1978, c) Legislação Unificada com a DC 46/95 (antes já existia o Convênio 108/81 – que já previa a livre circulação dos dados com a devida proteção legal), que, após evolução normativa, vai culminar com a previsão de um direito autônomo na Carta Europeia e, posteriormente, com o Regulamento Europeu 2016/679 que unifica ainda mais as regras em matéria de proteção de dados. O Regulamento traz novidades[47], ao tratar do consentimento, do direito ao esquecimento, do direito à portabilidade, o princípio de *accountability* ou responsabilidade proativa, imposição de pesadas multas, etc.

Diante de um cenário de crise sanitária, o direito à proteção de dados pessoais e o direito à saúde entraram em conflito, no Brasil, em virtude da Medida Provisória - MP nº 954, de 17 de abril de 2020, que dispôs sobre

> o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação do Instituto Brasileiro de Geografia e Estatística - IBGE, para fins de suporte à produção estatística oficial, durante a situação de emergência de saúde pública de importância internacional decorrente da Covid-19, de que trata a Lei nº 13.979, de 6 de fevereiro de 2020 (MP nº 954/2020).

O Supremo Tribunal Federal[48], em julgamento plenário, suspendeu a eficácia da Medida Provisória nº 954/2020, que prevê o compartilhamento de dados dos usuários de telecomunicações, com o IBGE, para a produção de estatística oficial durante a pandemia da Covid-19. Assim, firmou o entendimento de que o compartilhamento de dados, previsto na Medida Provisória, viola o direito

[46] BRASIL. Supremo Tribunal Federal. **Partidos contestam atos que restringem publicidade dos dados relativos à Covid-19**. 08/06/2020. Disponível em: <http://stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=445045>. Acesso em: 25 set. de 2020.
[47] PIÑAR MAÑAS, José Luis. **Regulamento general de protección de datos**: hacia um nuevo modelo de privacidade (Director). Madrid: Reus, 2016, p. 19.
[48] ADI 6387, ADI 6388, ADI 6389, ADI 6390 e ADI 6393.

constitucional à intimidade, à vida privada e ao sigilo de dados. Reconhecida, assim, a importância do direito à proteção dos dados pessoais. Neste cenário, é fundamental esclarecer que a Administração Pública e(m) rede é uma via de mão dupla, pois, ao mesmo tempo em que capta dados dos cidadãos, respeitando direitos fundamentais, reverte-se em transparência. Portanto, a falta de transparência, por si só, já se apresenta como uma barreira ao acesso aos dados dos cidadãos, como aponta a decisão.

A pouca, ou nenhuma, cooperação entre os órgãos públicos e entre estes e a iniciativa privada, bem como a falta de interoperabilidade são mais dois elementos que apontam para o desrespeito do Estado/Administração à proteção de dados, uma vez que muitos dos dados, possivelmente requeridos pelo IBGE, certamente já estão de posse do Estado, mas de forma desestruturada, fragmentada.

A Lei nº 13.709/2018 versa a respeito da proteção dos dados pessoais, com a vigência ocorrida em agosto de 2020. Existe o projeto que visa tornar a proteção de dados pessoais um direito fundamental pelo Projeto de Emenda Constitucional nº 17/2019, acrescentando, ao artigo 5º da Constituição Federal de 1988, o inciso XII-A e, ao artigo 22, o inciso XXX, tornando competência privativa de a União legislar sobre a matéria., tal como existe na Carta dos Direitos Fundamentais da União Europeia[49] , que prevê o direito fundamental à proteção dos dados pessoais (art. 8º), como um direito distinto da privacidade (art. 7º), acabando com a discussão, por muitos anos travada[50] , no sentido de ser autônomo ou simples faceta do direito à privacidade. A Legislação Brasileira nasce com uma debilidade, ao não prever uma Agência de Proteção de Dados Pessoais, de maneira independente ou autônoma. Pela arquitetura criada pela lei, a Agência incumbida de velar pelos dados ficará dentro da seara do Poder Executivo (Lei nº 13.853/2019 e Decreto nº 10.474/2020). Porém, isso ocorre com as demais Agências Reguladoras do modelo brasileiro, que são autarquias em regime especial.

Os dados pessoais sempre merecem uma proteção, mas, em se tratando de dados sensíveis, há que se aumentar este cuidado, visto que podem causar uma situação de discriminação, caso sejam de conhecimento ou manipulados por outrem, que não o destinatário ao qual se consentiu a guarda do dado, com uma finalidade

[49] UNIÃO EUROPEIA, Carta dos Direitos Fundamentais..., *op. cit.*, 2020.
[50] LIMBERGER, *op. cit.*, 2007, p. 103-115.

específica, comprometendo o princípio constitucional da igualdade.[51] Daí a importância da interoperabilidade e da cooperação entre os entes, como forma de garantia de mínima intervenção aos dados sensíveis.

Os dados sensíveis ficam mais sujeitos a que se processem discriminações algorítmicas[52] , fazendo-se necessárias a transparência e a fiscalização, bem como a incidência de valores que orientam o ordenamento jurídico. Daí porque a diminuição da privacidade somente se justifica com o aumento da transparência da administração.[53] Assim como o Tribunal Constitucional Alemão proclamou o direito à proteção dos dados pessoais[54] , por considerar indevidas as intromissões causadas pela lei do censo, com fundamento no livre desenvolvimento, artigo 2.1; e da dignidade da pessoa humana, artigo 1.1, ambos da Lei fundamental; no Brasil, o STF proclamou a proteção dos dados pessoais, em geral, e dos sensíveis como da saúde, em particular, neste episódio da Covid-19, relativo aos dados que seriam repassados pelas empresas de telefonia, ao IBGE, uma vez que não tinham o cuidado adequado, a respeito do fluxo dos dados, já que ainda era inexistente a Agência de Proteção de Dados.

No cenário jurídico brasileiro, revelam-se alguns "aparentes paradoxos"[55] , a partir de um marco jurídico estruturado desde a privacidade, tornando-se necessário promover a transparência, que ganha cada vez mais protagonismo. Deste modo, uma nova leitura se impõe. A LGPD, em seus artigos 23 a 30, dispõe a respeito da proteção de dados no âmbito do poder público e determina, expressamente, que haverá a incidência da LAI, com o objetivo de atender o interesse público e seus desdobramentos. Assim, é necessário promover-se uma interpretação sistemática.

Vale, por isso, referir a decisão do TJUE[56] , quando decidiu: *el derecho a la protección de los datos de carácter personal no constituye una prerrogativa absoluta*,

---

[51] LIMBERGER, Têmis, *op. cit.*, 2007, p. 60-62.
[52] MENDES, Laura Schertel; MATIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público**. Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias. v. 16, n. 90, p. 39-64, 2019.
[53] RODOTÁ, Stefano. **A vida na sociedade de vigilância***:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 36-37.
[54] A Sentença do Tribunal Constitucional Alemão, de 15/12/1983, no **Boletim de Jurisprudência Constitucional n. 33**, consolidou a existência de um "direito à autodeterminação informativa" (informationelle selbstestimmung), que consistia no direito de um indivíduo controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos à sua pessoa.
[55] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da LGPD, 2. ed, São Paulo: Thomson Reuters RT, 2020, p. 325.
[56] PIÑAR MAÑAS, José Luis y RECIO GAYO, Miguel. El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea. Madrid: Wolters kluwer, 2018, p. 29.

*sino que debe ser considerado en relación com su función en la sociedade*. Daí se pode extrair a lição de que os direitos fundamentais podem ser submetidos a restrições da esfera pública[57] e privada e o direito à proteção de dados pessoais não pode fugir a este postulado.

## 6 CONSIDERAÇÕES FINAIS

A legislação brasileira de proteção de dados pessoais surge após a lei de acesso à informação pública e inverte a sistemática de entrada em vigor, existente no direito comparado. A lei protetiva dos dados pessoais surge, no cenário brasileiro, clamando que se instaure uma cultura de 'valor aos dados', que foi construída nos países europeus ao longo de cinco décadas.

Diante deste contexto, volta-se à questão inicialmente formulada de apontar se é possível promover um diálogo entre a LGPD e a LAI. O STF realizou julgamentos importantes em prol da proteção de dados e da transparência (ADPF nº 690/DF e ADI 6387 e outros). No direito comparado, especificamente na Espanha, tem-se a demonstração de que é possível a interpretação sistemática, no sentido de proteger-se os dados dos cidadãos e tornar acessível a informação em harmonia com a legislação nacional e comunitária RGPD. Apesar de parecer que há uma contradição, quando a última pretende a proteção dos dados e, a outra, a informação, ambas dialogam em uma ação coordenada pelos valores constitucionais (princípio da publicidade, direito à informação e proteção de dados pessoais).

Quando a administração opera de forma transparente, concretiza-se o princípio da publicidade e o direito a ser informado do cidadão, porém há de se proteger o cidadão e o servidor público, no que concerne aos seus dados pessoais lançados, que dizem respeito a questões privadas.

Assim, disponibilizam-se os vencimentos do servidor público, mas há de se proteger as informações referentes ao desconto de pensão alimentícia, plano médico e prestação imobiliária, por exemplo.

A informação em rede possui a vantagem de possibilidade do compartilhamento, de uma maneira crítica e com baixo custo. A informação pública

[57] HABERMAS, Jürgen. **Mudança estrutural da esfera pública**. São Paulo: Unesp, 2014. Utiliza-se público e privado como um contraponto clássico, não se desconsiderando a tendência contemporânea de publicização do privado e privatização do público.

visa contribuir ao debate democrático e promover a formação da cidadania, estimulando-a a participar nos assuntos da esfera pública e realizar o controle social dos atos administrativos, ou provocar as Instituições públicas que podem fazê-lo, tais como Tribunal de Contas e Ministério Público. A transparência contribui para a concretização dos direitos sociais.

O poder público tem um compromisso maior com a divulgação da informação (principalmente em tempos de *fake news*) já que lhe incumbe o cumprimento do binômio: divulgação da informação pública em rede com transparência e a proteção de dados pessoais, que são compatíveis, na maioria das vezes, a fim de contribuir ao debate democrático.

## REFERÊNCIAS


BOBBIO, Norberto. **O futuro da democracia**. 7. ed., São Paulo: Paz e Terra, 2000.

BRASIL. Câmara dos Deputados. **Lei de Acesso à Informação**: um direito do cidadão. (Eduardo Tramarim). Disponível em: <https://www.camara.leg.br/radio/programas/378496-lei-de-acesso-a-informacao-um-direito-do-cidadao/>. Acesso em: 13 out. de 2020.

_____. Supremo Tribunal Federal. **Partidos contestam atos que restringem publicidade dos dados relativos à Covid-19**. 08/06/2020. Disponível em: <http://stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=445045>. Acesso em: 25 set. de 2020.

_____. _____. **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE**. 07/05/2020. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902#:~:text=O%20Plen%C3%A1rio%20do%20Supremo%20Tribunal,a%20pandemia%20do%20novo%20coronav%C3%ADrus.>. Aceso em: 25 set. de 2020.

CANARIS, Wilhelm Claus. **Pensamento sistemático e conceito de sistema na ciência do direito**. Lisboa: Fundação Calouste Gulbekian, 1989.

CANOTILHO, José Joaquim Gomes. Civilização do direito constitucional ou constitucionalização do direito civil? A eficácia dos direitos fundamentais na ordem jurídico-civil. *In*: GRAU, Eros Roberto; GUERRA FILHO, Willis Santiago (Org). **Direito Constitucional**: estudos em homenagem a Paulo Bonavides. São Paulo: Malheiros, 2001.

CASTELLS, Manuel. **O poder da comunicação**. Tradução de Vera Lúcia Mello Joscelyne. Rio de Janeiro: Paz e Terra, 2015.

_____. **A Sociedade em Rede**: a era da informação - economia, sociedade e cultura. 4. ed. Lisboa: Fundação Calouste Gulbenkian, 2011.

_____. ***Comunicación y Poder***. Madrid: Alianza Editorial, 2009.

COSTA JR., Paulo José da. **O direito a estar só:** tutela penal da intimidade. São Paulo: RT, 1970.

DEBORD, Guy. **A sociedade do espetáculo**. Rio de Janeiro: Contraponto, 1997.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais***:* fundamentos da LGPD, 2. ed., São Paulo: Thomson Reuters RT, 2019/2020.

HABERMAS, Jürgen. **Mudança estrutural da esfera pública**. São Paulo: Unesp, 2014.

JAYME, Erik**.** *Identité culturelle et intégration: le droit international privé postmoderne*. ***Recueil des Cours de l'Académie de Droit International de la Haye***. Haia: Kluwer, 1995.

LIMBERGER, TÊMIS. **Comentários à LGPD** – arts. 23/30 – Ed. FOCO (no prelo).

_____. **Cibertransparência:** informação pública em rede – a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016.

_____. **O Direito à intimidade na era da informática**: o desafio da proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LIMBERGER, Têmis; SANTANNA, Gustavo da Silva. **Na sociedade em rede, em que o uso dos recursos digitais foi potencializado pela COVID-19**, qual o papel do direito à proteção dos dados pessoais (sensíveis), interoperabilidade, cooperação e transparência para contribuir à efetivação do direito à saúde. (no prelo)

LOUREIRO, João Carlos. Constituição, tecnologia e risco(s): entre medo(s) e esperança(s). *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord.). **Direito, Inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 33-84.

LLOSA, Mario Vargas. **A civilização do espetáculo**: uma radiografia do nosso tempo e da nossa cultura. Rio de Janeiro: Objetiva, 2013.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor**, 9. ed., São Paulo: Thomsom Reuters - RT, 2019.

_____. (coord.) **Diálogo das Fontes**: do conflito à coordenação de normas no direito brasileiro. São Paulo: Thomsom Reuters - RT, 2012.

MENDES, Laura Schertel; MATIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista Direito Público**. Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias. v. 16, n. 90, p. 39-64, 2019.

MOREIRA NETO, Diogo de Figueiredo. **Quatro paradigmas do direito administrativo pós-moderno**: legitimidade, finalidade, eficiência e resultados. Belo Horizonte: Forum, 2008.

NORA, Simon; MINC, Alain. ***Informe Nora-Minc*** *– La informatización de la sociedad*. Madrid: [S.n.], 1982 (Colección popular).

PÉREZ LUÑO, Antonio Enrique. ***El desbordamiento de las fuentes del Derecho***. Sevilha: Real Academia *Sevillana* de *Legislación y Jurisprudencia*, 1993.

PIÑAR MAÑAS, José Luis. ***Reglamento general de protección de datos****: hacia un nuevo modelo de privacidad* (Director). Madrid: Reus, 2016.

_____. ***Administración Electrónica y Ciudadanos***. Pamplona: Thomson Reuters – Civitas, Aranzadi Ed, 2011.

PIÑAR MAÑAS, José Luis y RECIO GAYO, Miguel. ***El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea***. Madrid: Wolters Kluwer, 2018.

PNUD - Programa das Nações Unidas para o Desenvolvimento. ***2019 Human Development Index Ranking***. Disponível em: <http://hdr.undp.org/en/content/2019-human-development-index-ranking> Acesso em: 21 set. de 2020.

ISTOÉ, Revista. ***Zuckerberg contra a parede***. Tecnologia. 18/04, 2018, p. 66.

RIALS, Stéphane. ***Que sais-je?*** *Textes constitutionnels français*. 11. ed. Paris: *Presses Universitaires de France*, 1995.

RODOTÀ, Stefano. ***El derecho a tener derechos***. Madrid: Trotta, 2014.

_____. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SAARENPÄ, Ahti. *From de Information Society to the legal Network Society, ID-card and electronic services*. Conferência proferida no dia 7 de novembro, no ***X Congresso Ibero-americano de Derecho e Informática***. Santiago do Chile, 6 a 9 de novembro, 2004.

SANTANNA, Gustavo da Silva. **Do patrimonialismo à sociedade da informação: proposições para a implantação da administração pública eletrônica (e-administração) no Brasil**. Tese (Doutorado em Programa de Pós-Graduação em Direito). Orientador: Têmis Limberger. São Leopoldo: Universidade do Vale do Rio dos Sinos - UNISINOS, 2019.

SCHWAB, Klaus**. A quarta revolução industrial.** Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SOMMERMANN, Karl-Peter. *La exigência de uma administración transparente em la perspectiva de los princípios de democracia y del Estado de Derecho*. *In* ***Derecho administrativo de la información y administración transparente.*** Ricardo García Macho (ed). Madrid: Marcial Pons, 2010.

THE ECONOMIST REVIEW. ***The world's most valuable resource is no longer oil but data***. May 6 *th* 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 20 set. de 2020.

TRANSPARENCY INTERNATIONAL. ***Corruption Perceptions Index 2019***. Disponível em: <https://www.transparency.org/en/cpi/2019/results>. Acesso em: 20 set. de 2020.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia, de 07 de dezembro de 2000. **Carta de Nice**. Disponível em: <http://www.europarl.europa.eu/charter/default_pt.htm>. Acesso em: 10 out. de 2020.

VILLAVERDE MENÉZES, Ignácio. ***Estado democrático e información****: El derecho a ser informado y La Constitución Española de 1978.* Junta General del Principado de Astúrias: Oviedo, 1994.

# A NECESSÁRIA RELAÇÃO ENTRE INTEROPERABILIDADE E COMPARTILHAMENTO DE DADOS, TRANSPARÊNCIA ADMINISTRATIVA E PRIVACIDADE: UMA ANÁLISE DO COMPORTAMENTO DA ADMINISTRAÇÃO PÚBLICA A PARTIR DA LGPD

Gustavo da Silva Santanna[1]

## 1 INTRODUÇÃO

A Lei Geral de Proteção de Dados dá início a uma nova realidade. Não só pelo objetivo de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[2], mas, principalmente, porque impõe uma mudança de comportamento nas pessoas e no Estado.

Nesse breve estudo, o eixo será, exclusivamente, a Administração Pública e algumas normas serão trabalhadas de forma mais detalhada. Um dos princípios que o tratamento de dados pessoais deve seguir é o da transparência, a respeito da qual o artigo 6º da Lei nº 13.709[3] , de 14 de agosto de 2018, aufere que é a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial." Aliás, o controlador deve, inclusive, adotar medidas que garantam essa transparência (artigo 10, §2º).

Outra regra estabelecida para o tratamento de dados, pela Administração Pública, é que o uso e o compartilhamento destes somente serão admitidos para a execução de políticas públicas (artigo 7º). É no mesmo sentido que o artigo 11 da Lei estudada repete que o tratamento de dados pessoais, agora "sensíveis", somente poderá ocorrer, mesmo sem fornecimento de consentimento do titular, nas

[1] Possui graduação em Ciências Jurídicas e Sociais (2002), mestrado em Direito (2011) e doutorado em Direito pela Universidade do Vale do Rio dos Sinos (2019). Atualmente, é professor de graduação do Complexo de Ensino Superior Meridional (IMED), professor da especialização em Direito do Estado da Universidade Federal do Rio Grande do Sul (UFRGS), professor da especialização em Direito Digital, Gestão da Inovação e Propriedade Intelectual da Pontifícia Universidade Católica de Minas Gerais (PUC-MG), professor da Fundação Escola Superior da Defensoria Pública do Rio Grande do Sul (FESDEP/RS), revisor técnico da SAGAH Educação S.A. e Procurador do Município de Alvorada/RS.

[2] BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em:<http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 10 out. de 2020.

[3] *Idem Ibidem*.

hipóteses em que for indispensável, para tratamento compartilhado de dados necessários à execução, pela administração pública de políticas públicas previstas em leis ou regulamentos. O artigo 26 reforça esse pensamento ao reportar que "o uso compartilhado de dados pessoais, pelo Poder Público, deve atender a finalidades específicas de execução de políticas públicas"[4], devendo respeitar a proteção de dados pessoais.

Além da transparência e da possibilidade de compartilhamento de dados, outra regra que se impõe à Administração Pública é a de mantê-los (os dados) em formato interoperável, "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" (artigo 25 da LGPD[5]). Inclusive, o artigo 40[6] da norma autoriza a autoridade nacional a "dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência".

Mas, será possível que haja transparência administrativa, respeito à privacidade e compartilhamento de dados se os sistemas não forem, antes de tudo, interoperáveis? Esse questionamento pode também ser colocado da seguinte forma: é possível garantir um efetivo compartilhamento de dados pela Administração Pública se os sistemas não forem interoperáveis? Seria aceitável restringir a privacidade do cidadão sem, em troca, ou antes de tudo, garantir a transparência administrativa?

Perceber-se-á, ao fim, que a interoperabilidade é o pressuposto básico para o compartilhamento e tratamento de dados no âmbito da Administração Pública. Além disso, também restará demonstrado que não se permite deixar mais opaca a privacidade do cidadão sem que, antes, a Administração Pública seja efetivamente transparente.

---

[4] BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 10 out. de 2020.

[5] *Idem Ibidem*.

[6] *Idem Ibidem*.

## 2 A INTEROPERABILIDADE COMO PREMISSA PARA O ADEQUADO COMPARTILHAMENTO DE DADOS PELA ADMINISTRAÇÃO PÚBLICA

A (falta de) interoperabilidade é uma das mais delicadas, e problemáticas, temáticas dentro da estrutura administrativa brasileira. Segundo o Marco Civil da Internet[7] , por exemplo, o uso da rede, no Brasil, tem, por objetivo, a promoção "da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados". No artigo 24, ao disciplinar a atuação do poder público, uma das diretrizes no desenvolvimento da internet no Brasil é (III) a promoção da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, como forma de permitir o intercâmbio de informações e a celeridade de procedimentos, bem como (IV) a promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade.[8] Vislumbra-se, pois, que, mesmo antes da publicação da Lei Geral de Proteção de Dados, a interoperabilidade já estava presente na legislação brasileira. Contudo, até hoje, não existe um programa ou uma política pública para pôr em prática essa premissa que, indiscutivelmente, é o "vértice" de uma Administração que se propõe a respeitar a LGPD.

Essa matéria, inclusive, já foi objeto de debate em, pelo menos, três oportunidades no Supremo Tribunal Federal. A primeira delas, em 2016, julgada no Recurso Extraordinário nº 601.314 (tema 225),[9] e nas Ações Diretas de Inconstitucionalidade nº 2.390[10] e 2.859[11] , em que a Corte entendeu não ofender o sigilo bancário a possibilidade de requisição de dados/informações pela Receita

---

[7] *Id*. **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 09 jul. de 2020.

[8] BRASIL. **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 09 jul. de 2020.

[9] *Id*. Supremo Tribunal Federal. **Recurso Extraordinário 601.314** São Paulo. Relator: Min. Edson Fachin. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11668355>. Acesso em: 10 out. de 2020.

[10] *Id*. **Ação Direta de Inconstitucionalidade 2.390** Distrito Federal. Relator: Min. Dias Toffoli. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI2390.pdf>. Acesso em: 10 out. de 2020.

[11] *Id*. **Ação Direta de Inconstitucionalidade 2.859** Distrito Federal**.** Relator: Min. Dias Toffoli. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11899965>. Acesso em: 10 out. de 2020.

Federal às instituições financeiras, considerando constitucional o artigo 6º da Lei Complementar nº 105/2001. Em um segundo momento, agora em 2019, no Recurso Extraordinário nº 1.055.941[12] (tema 990), o STF decidiu ser possível o compartilhamento "dos relatórios" (leia-se dados/informações) da Unidade de Inteligência Financeira (UIF/COAF) e da Receita Federal, com órgãos de persecução penal, como o Ministério Público, por exemplo. Não foi, no mesmo sentido, o julgamento da Medida Cautelar da ADI nº 6.387[13], que julgou inconstitucional o artigo 2º da Medida Provisória nº 954/2020, na qual as empresas de telecomunicações deveriam disponibilizar, ao IBGE, a relação de nomes, números de telefone e endereços de seus consumidores para produção estatística oficial, a fim de realizar entrevistas não presenciais. Em suas considerações, a Ministra Relatora Rosa Weber entendeu que o cumprimento do referido artigo ofenderia a privacidade, a autodeterminação informativa e, consequentemente, a proteção de dados pessoais. Percebe-se, portanto, que, entre os órgãos estatais, já existe certa tendência, no Supremo Tribunal Federal, a permitir o compartilhamento de dados, mesmo não estando "estruturada" a Administração Pública para as demais obrigações como (ciber) segurança e interoperabilidade. Veja-se, também, que as decisões são pontuais e não estabelecem um padrão ou política (e nem deveriam) de como deve ocorrer o compartilhamento de dados, quais princípios deve seguir ou qual medida deve ser adotada, no caso de uso indevido desse compartilhamento. Portanto, a carência de uma norma regulamentadora é facilmente perceptível.

Na União Europeia, a interoperabilidade aparece como um princípio explicitado na *Decisión* 2004/387/CE *del Parlamento Europeo y del Consejo*[14], sendo conceituado como "*capacidad de los sistemas de tecnologías de la información y las comunicaciones (TIC), y de los procesos empresariales a los que apoyan, de intercambiar datos y posibilitar la puesta en común de información y*

---

[12] *Id*. **Recurso Extraordinário 1.055.941** São Paulo**.** Min. Dias Toffoli. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754018828>. Acesso em: 10 out. de 2020.

[13] *Id*. **Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387** Distrito Federal. Relatora: Min. Rosa Weber. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em: 10 out.de 2020.

[14] UNIÓN EUROPEA. **Decisión 2004/387/CE del parlamento europeo y del consejo de 21 de abril de 2004.** Relativa à la prestación interoperable de servicios pan-europeus de administración electrónica al sector público, las empresas y los ciudad. Disponível em: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32004D0387R(01)&from=GA>. Acesso em: 10 out. de 2020.

*conocimientos*". Coloca Gutiérrez[15] que a interoperabilidade tem, como objetivo, garantir a "conectividade" entre as diversas estruturas administrativas, de modo a possibilitar o fluxo das informações, ou seja, a possibilidade de um programa de informática compartilhar informação com outros programas e sistemas, estabelecendo-se uma comunicação, entre eles, refletindo, diretamente, nos resultados e acabando com as "ilhas" de sistemas[16], ilhas estas que acabam beneficiando a corrupção, desvios e ilícitos de uma forma geral.

De fato, é impensável uma Administração Pública contemporânea que não tenha, por premissa, a colaboração/inter-relação administrativa entre suas estruturas, de forma a facilitar o compartilhamento de informações. Veja-se, portanto, que a interoperabilidade está direcionada, neste primeiro momento, ao campo interno da Administração.

Conforme a relação com outras entidades vai-se estreitando, seja para fins sociais (como a escolaridade, declaração de Imposto de Renda ou endereço), ou públicos (como concessionárias ou organizações sociais, por exemplo), seja para fins econômicos ou arrecadatórios (como a nota fiscal eletrônica), mais difícil fica a possibilidade de se cometerem ilícitos (sejam civis ou penais), ou mais fáceis de serem identificados. Como bem adverte Gutiérrez[17], a interoperabilidade "*no puede encontrarse únicamente limitada a la dimensión interna y será necesario incorporar en el concepto de interoperabilidad la referida dimensión externa del fenómeno de la Administración electrónica*." Assim é que, quanto mais desenvolvida a interoperabilidade entre os sistemas, maior será a quantidade de tempo, dinheiro e força humana, economizados pelas Administrações e pelos cidadãos.

A Lei nº 11 de junho de 2007[18] - *Ley de acceso electrónico de los ciudadanos a los Servicios Públicos* – LAECSP – em seu anexo, letra "o", conceituava a interoperabilidade como a "*capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos*." Atualmente, a Lei Espanhola

---

[15] GUTIÉRREZ, Rubén Martínez. *Administración pública electrónica.* Pamplona: Thomson Reuters, 2009.
[16] CASADO, Eduardo Gamero. Interoperabilidad y administración electrónica: conéctense, por favor. *Revista de Administración Pública*. Madri, n. 179, p. 291-332, maio/ago. 2009.
[17] GUTIÉRREZ, Rubén Martínez. *Administración pública electrónica*. Pamplona: Thomson Reuters, 2009. p. 271.
[18] *ESPANHA. Ley 11, de 22 de junio de 2007*. Acceso electrónico de los ciudadanos a los Servicios Públicos. Disponível em: **https://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf**. Acesso em: 10 out 2020.

nº 40, de 2015[19], em seu artigo 3º, coloca interoperabilidade junto à proteção de dados, como se esta fosse diretamente dependente daquela:

> *Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados*.

Sendo assim, para que a interoperabilidade seja posta em prática, faz-se necessária uma "estandartização" da base tecnológica utilizada pela Administração, em todos os níveis, resolvendo os problemas de compatibilidade técnica. Como bem destaca Reilly[20], não é incomum as Administrações solicitarem, diversas vezes, a mesma informação do cidadão (algumas, por razões de privacidade ou segurança, o que daí se justifica). Deveria, sim, segue o autor, o Estado buscar as informações em seus próprios sistemas (se fossem interoperáveis), deixando um "rastro digital" daqueles que as buscaram, de forma a garantir a necessária transparência e eventual responsabilização pelo mau uso do dado consultado.

Casado[21] cita quatro dimensões da interoperabilidade, todas entrelaçadas e que se impulsionam simultaneamente. A primeira, organizativa, é relativa à capacidade das entidades e dos processos de compartilharem êxitos relativos aos serviços que prestam, incluindo, nesse universo, sujeitos, órgãos e entidades que exercem atividades públicas ou de interesse público, sendo, ao fim, "*un objetivo a escala mundial*." A interoperabilidade semântica refere-se à informação disponibilizada de forma automatizada e reutilizável por sujeitos, órgãos e entidades que não intervieram na sua disponibilização. Tangenciando-se com a cooperação, essa dimensão da interoperabilidade encontra grande dificuldade na diversidade de linguagens de programas informáticos.

A terceira dimensão da interoperabilidade é a técnica:

> *Determinada por la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como los interfaces, la presentación*

---

[19] *Id.* ***Ley 40, de 1 de octubre de 2015***. *De Régimen Jurídico del Sector Público*. Disponível em: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566>. Acesso em: 10 out. de 2020.

[20] REILLY, Marcelo Bauzá. La Administración electrónica a la luz de los principios. In: HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). **Administración electrónica**: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España. Valencia: Tirant do Blanch, 2010. p. 47-66.

[21] CASADO, Eduardo Gamero. Interoperabilidad y administración electrónica: conéctense, por favor. **Revista de Administración Pública**. Madri, n. 179, p. 291-332, maio/ago. 2009. p. 295-296.

> *de la información, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad*.[22]

Essa dimensão leva muito, em consideração, o usuário dos serviços, uma vez que se preocupa com a interface, a forma com que a informação é apresentada, a acessibilidade (pensa-se na quantidade de cliques que o cidadão necessita dar para alcançar a informação desejada) e a segurança no acesso. A última dimensão da interoperabilidade é a legal ou jurídica. Muito mais direcionada para uma realidade europeia, a partir dela deve haver harmonia entre as diversas legislações (dos diversos países que integram a União Europeia), uma convergência normativa, que possibilite a utilização de um mesmo certificado (ou assinatura) eletrônico, em qualquer país, por exemplo. É do somatório dessas dimensões que se extrai a "cadeia de interoperabilidade".[23]

Ainda que o artigo 25 da Lei Geral de Proteção de Dados[24] tenha definido que 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, a situação brasileira é emblematicamente negativa. Levando-se em consideração somente a União, excluindo-se, portanto, estados-membros e municípios, diversos são os *softwares* e programas utilizados, sem a devida atenção, tanto aos demais entes políticos, quanto aos próprios órgãos. A partir da implementação da interoperabilidade, competirá à Administração a busca pelos dados já existentes (*Big Data*), mesmo que em outros órgãos ou entidades, e não mais ao cidadão o novo fornecimento da informação. Destaca-se, mais uma vez, que essa utilização, a partir de uma base de dados (*Big Data*) somente se vislumbra lícita se for possível verificar quem efetuou a consulta ("rastro digital"). Caso contrário, restaria inválida essa utilização, por falta de transparência, outra diretriz a ser seguida pela Administração Pública.

A interoperabilidade parte de uma Administração Pública horizontal, em rede, não cabendo a uma estrutura impor o "seu" sistema frente aos demais. Ao fim, o que de fato se pretende é um compartilhamento das informações e não de sistemas (este um meio para aquele). Logo, essa possibilidade de comunicação entre os

---

[22] CASADO, *op. cit.*, 2009, p. 297.
[23] *Idem*, p. 299.
[24] BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 10 out. de 2020.

sistemas somente é possível a partir de diálogo entre todas as esferas administrativas, havendo, sobretudo, uma colaboração entre elas, espírito esse percebível no artigo 26 da Lei nº 13.709[25], ao propiciar o uso compartilhado de dados pessoais, atendendo a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais.

Ademais, a "cooperação" (ainda que tratada como "instrumento"), para fins tecnológicos, já está prevista na Constituição Federal de 1988, desde 2015, com a inserção do artigo 219-A, em que os entes federativos poderão (o correto deveria ser "deverão") cooperar entre si, ou com entidades privadas para a execução de projetos de pesquisa, de desenvolvimento científico e tecnológico e de inovação, mediante contrapartida financeira, ou não financeira, assumida pelo ente beneficiário. Portanto, tal compartilhamento somente se apresenta viável se os sistemas forem interoperáveis e a transparência efetiva.

## 3 A TRANSPARÊNCIA ADMINISTRATIVA COMO CONDIÇÃO PARA O RESPEITO À PRIVACIDADE

Os dados podem traduzir aspectos de personalidade, comportamento e preferências[26], que podem ser úteis, não somente na esfera privada, mas, também, na estatal, na confecção de políticas públicas e, ainda, que tenham grande valor econômico, quando coletados pelo Estado/Administração; devem-se traduzir em políticas de inclusão social, de correção de distorções, de aplicação da igualdade. O fato é que, junto à coleta de dados, a proteção à privacidade torna-se uma preocupação meditada. Ademais, com o aumento da troca de dados entre pessoas e coisas e entre coisas e coisas, as informações extraíveis também tomaram proporções exponenciais.

Aliás, a proteção dos dados, como bem afirma Rodotà[27], está vinculada à proteção da personalidade e não à propriedade, razão pela qual, ainda que possam

[25] BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 10 out. de 2020.
[26] LIMBERGER, Têmis. **O direito à intimidade na era da informática***:* a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.
[27] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

adquirir valor, algumas categorias, como natureza médica ou genética, não poderiam ser utilizadas de maneira negocial. Define, assim, Reina[28], que dados pessoais são todas as informações "nominativas" de qualquer gênero ("que permitem identificar uma pessoa de maneira direta")[29], e a omissão do nome é o que permitiria, inclusive, uma real participação anônima nas atividades públicas, possibilitando o controle efetivo (democrático) da atividade da Administração.

O artigo 12 da Declaração Universal dos Direitos Humanos[30] assegura que ninguém será sujeito à interferência, em sua vida privada, em sua família, em seu lar ou em sua correspondência, portanto, garante a privacidade do cidadão. Na mesma linha, é a redação do artigo 5º da Constituição da República de 1988[31], ao estabelecer a inviolabilidade da "vida privada, a honra e a imagem" (inciso X), da "casa" (inciso XI) e da "correspondência" (inciso XII)[32]. O Marco Civil da Internet, em seu artigo 3º, II e III, respectivamente, estabelece como princípios a proteção da privacidade e dos dados pessoais, bem como, o direito de inviolabilidade da intimidade e da vida privada (artigo 7º, I)[33]. Há, inclusive, em tramitação no Senado Federal, uma Proposta de Emenda Constitucional nº 17, que incluirá a proteção de dados pessoais entre os direitos e garantias fundamentais do cidadão[34]. Como bem salienta Doneda[35], após a Segunda Guerra Mundial, a privacidade ganhou especial

---

[28] "Todo dato referido a una persona identificada o identificable entra en el manto de protección del derecho fundamental a la protección de datos, de modo que cualquier injerencia en el mismo (y la publicidad inconsentida lo es) debe tener un fundamento constitucional" (REINA, Emilio Guichot. La comunicación de datos personales en poder de la Administración. Aspectos generales y especialidades derivadas de la comunicación por vía telemática. In: HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). **Administración electrónica**: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España. Valencia: Tirant, 2010. p. 765-806. p. 787.

[29] LIMBERGER, *op. cit.*, 2007, p. 61.

[30] NAÇÕES UNIDAS DO BRASIL. **Declaração Universal dos Direitos Humanos**. Disponível em: <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em: 10 out.de 2020.

[31] *Idem Ibidem*.

[32] BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 out.de 2020.

[33] O artigo 10 segue no mesmo sentido, ao afirmar que: "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas". *Id*. **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 out. de 2020.

[34] *Id.* BRASIL. Senado Federal. **Proposta de Emenda à Constituição n° 17, de 2019**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 10 out. de 2020.

[35] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

proteção no plano internacional e, posteriormente, no plano nacional, consagrada como verdadeiro direito fundamental.

Não resta dúvida, portanto, de que a privacidade é direito humano e fundamental, de eficácia horizontal[36], explicitamente reconhecida, razão pela qual seu afastamento ou abrandamento necessita da devida justificativa, também, constitucional. Não é por outra razão que o respeito à privacidade consta como fundamento na Lei Geral de Proteção de Dados Pessoais. Não hão de ser limitadas tais proteções apenas à esfera física/analógica, mas estendendo-se, também e obrigatoriamente, ao âmbito digital/eletrônico. Por óbvio, todos os mecanismos, ou "coisas" aptas a viabilizarem o tratamento dos dados de qualquer cidadão estão, sim, expondo a sua privacidade.

Alerta, mais uma vez, Rodotà[37], que as "novas dimensões da coleta e do tratamento de informações" forçaram uma nova (re) configuração de determinados conceitos, dentre eles, o da privacidade. Veja-se que não se está tratando, aqui, somente do preenchimento de algum cadastro ou ingresso em alguma rede social, mas também, de "coisas", como um celular ligado ou um veículo em movimento, que, simplesmente, por estarem nessas condições, são aptos a captar dados e enviá-los a uma central (no caso, pública). É claro que, para tanto, deve haver uma aceitação explícita do cidadão para o envio desses dados, e aqui há um obstáculo a ser superado: a desconfiança do cidadão em relação à Administração. Isso porque, como bem destaca o autor italiano, a defesa da privacidade ou a coleta de dados pode adotar sentidos distintos "dependendo de qual seja o objetivo perseguido através da coleta das informações"[38], e boa parte do debate, quanto à privacidade e a coleta de dados, diz respeito à "resistência em fornecer à autoridade pública (local, estatal ou federal) informações relevantes para a elaboração de programas sociais".[39]

> Tal comportamento verifica-se, sobretudo, nas classes médias e se define, desta maneira, em oposição a uma política de intervenção pública com finalidades sociais. [...]. Nesse caso, por trás da defesa da privacidade se esconde a hostilidade em relação a uma pressão fiscal mais acentuada e a uma política de diminuição da diferença social, na qual a classe média, seria a primeira a ser atingida. [...]. Tem significado inverso a reação contra a

[36] Têmis Limberger escreve, nesse sentido, em relação à intimidade, que certamente possui idêntica aplicação com relação à privacidade. (LIMBERGER, *op. cit.*, 2007, p. 38.)
[37] RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 23.
[38] *Idem*, p. 29.
[39] *Idem Ibidem*.

> coleta de informações com finalidade de controle do comportamento político.[40]

Logo, são as motivações que modificam a "evocação" do direito à privacidade, no primeiro caso, para consolidar os privilégios de um grupo; no segundo, para banir o autoritarismo. Não é à toa que a maior resistência de acesso aos dados diz respeito às informações econômico-financeiras.[41] Portanto, a falta de confiança dos cidadãos passa a ser uma barreira a ser superada pela Administração Pública. Estar-se-ia, assim, em uma encruzilhada, pois se, por um lado, para que a Administração Pública inserida no século XXI funcione adequadamente, necessita dispor de dados suficientes e atualizados dos cidadãos/usuários; por outro lado, a cedência desses dados gera certa inquietude, pois as pessoas (sejam físicas ou jurídicas) temem, não só a falta de segurança, como a má utilização deles.[42]

Batalla[43] vai escrever que os cidadãos e empresas deveriam observar, primeiramente, que o acesso aos dados, pela Administração Pública, importa em benefícios reais, melhorando a qualidade de vida de todos e eventuais dúvidas que se colocariam acerca do efetivo respeito à privacidade deveriam ser superadas pela transparência administrativa. Percebe-se, pois, que a falta de confiança no Estado é um fator determinante e é a desconfiança, também, que obriga o Estado a adotar medidas de controle e segurança adequados para assegurar o respeito à privacidade. Deve-se ter presente que não são as novas tecnologias, em si, que causam risco ou insegurança, mas o mau uso dos dados/informações coletados[44].

Assim, a coleta de dados deve deixar claro, ao cidadão, os objetivos de sua utilização, uma vez que, diante dessa informação, caberá a ele (indivíduo) escolher se abre ou não mão de sua privacidade. Em termos de gestão pública, o objetivo dessa captação de dados deve se direcionar para a construção de políticas públicas, buscando diminuir o distanciamento entre classes sociais e, assim, a realização da igualdade. Afinal, quanto mais acurado for o conhecimento de sua população, mais

---

[40] RODOTÀ, o. cit., 2008. p. 29.
[41] *Idem Ibidem*.
[42] BATALLA, Antoni Roig. Intimidad y administración electrónica. In: HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). **Administración electrónica**: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España. Valencia: Tirant do Blanch, 2010. p. 729-748.
[43] *Idem Ibidem*.
[44] LÓPEZ, Ramón Mirales. Modelos de evaluación del impacto sobre la privacidad (PIA, "Privacy Impact Assessments) y el artículo 34 de la Ley 11/2007. In: HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). **Administración electrónica**: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España. Valencia: Tirant, 2010. p. 749-764.

eficiente tornar-se-á a administração pública.[45] Contudo, qualquer dado/informação, ainda que anônimo, utilizado fora desse objetivo, deve ser imediatamente eliminado (apagado), e os responsáveis pela sua manipulação punidos, afinal: "*la implantación de las mejoras electrónicas, que suponen una mejora en la eficacia administrativa, no pueden significar a la vez un perjuicio para los usuarios en cuanto a las garantías*".[46]

Na Alemanha, essa aceitação, que envolve diretamente elementos da personalidade, denomina-se: direito à "autodeterminação informativa" ou "autoapresentação" que consiste no direito de o próprio indivíduo decidir acerca da divulgação e utilização de seus dados pessoais, possibilitando, inclusive, que o indivíduo "se insurja contra as falsas, não autorizadas, degradantes ou deturpadas representações de sua pessoa, bem como o protege das observações secretas e indesejadas de sua personalidade".[47] Diferencia-se da "autodeterminação", que trata do direito de o indivíduo determinar/definir sua identidade, desde a origem biológica até a orientação sexual. Também se distingue da "autopreservação", que consiste na garantia de o indivíduo recolher-se para si, de ficar só, abrangendo o sigilo a diários pessoais, boletins médicos e materiais biológicos.[48] Essa preocupação se deve, principalmente, em razão da utilização que pode ser dada aos dados dos indivíduos, uma vez que estes podem ser manipulados por instituições (públicas ou privadas) sem que o indivíduo saiba disso.[49] É exatamente no combate à manipulação dos dados e à discriminação que pode ser gerada, em razão das informações, que o respeito à privacidade se impõem.

Rodotà[50], inclusive, chega a sugerir que, se fosse possível redefinir uma classificação acerca da privacidade, o grau máximo de opacidade seria dado àquelas que pudessem gerar práticas discriminatórias, sendo de grau "máximo de transparência aquelas que, referindo-se à esfera econômica dos sujeitos, concorrem

---

[45] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.
[46] BATALLA, Antoni Roig. Intimidad y administración electrónica. In: HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). **Administración electrónica:** la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España. Valencia: Tirant do Blanch, 2010. p. 729-748. p. 730.
[47] MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnicos-informacionais no direito alemão. *In:* MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 205-230. p. 210.
[48] *Idem Ibidem*.
[49] MENKE *In* MENDES *et al.,* 2015, *op. cit.*, p. 205-230.
[50] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

para embasar decisões de relevância coletiva". Logo, a privacidade não possui caráter absoluto[51] e sua limitação deve estar condicionada a determinadas circunstâncias, como a exigência legal de seu abrandamento, para evitar eventuais "intromissões ilegítimas".[52] Da mesma maneira, os dados coletados deveriam ser mínimos, "*no sólo para preservar el derecho a la protección de datos, sino también para darles mayor efectividad*".[53] Há de se ter presente, também, que a entrega de dados a uma Administração local ou federal, por exemplo, não a impede de compartilhar (com o intuito da cooperação) com a outra, desde que não haja restrição a algum dado especialmente protegido. É visando a esse compartilhamento que a interoperabilidade ganha importância. Ou seja, podem existir casos em que um órgão administrativo tenha o dever de pôr à disposição a qualquer outro órgão, sem a necessidade de um pedido "formal", a informação que detém, para que outro órgão "solicitante" possa exercer suas competências, sem que, para isso, haja um consentimento expresso do cidadão[54], "*dicho flujo inconsentido es pensable tanto dentro de una misma Administración como entre Administraciones Públicas*"[55] , tendo sempre, em conta, o princípio da finalidade. O fornecimento de dados a outra Administração (outro município, ou estado-membro) justifica-se, em razão da "colaboração interadministrativa", e pode ser formalizado mediante convênio.[56]

O uso dos dados "adquiridos" pode ou não exigir consentimento do cidadão, dependendo da finalidade para a qual os dados foram coletados. Quando os dados compartilhados possuem emprego/finalidade idênticos ou semelhantes, não seria necessário o consentimento do interessado. Contrário senso, se os dados forem utilizados para finalidade distinta daquela na qual foram coletados e tratados, seria necessária uma previsão legal específica de "cessão de dados", mas, ainda assim,

---

[51] Na mesma direção: "el derecho a la protección de datos es un derecho que trata de garantizar, no la reserva absoluta de los mismos, sino, precisamente, las facultades de disposición y control de los ciudadanos sobre sus datos". (BATALLA, Antoni Roig. Intimidad y administración electrónica. In: HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). **Administración electrónica**: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España. Valencia: Tirant do Blanch, 2010. p. 729-748. p. 767.)

[52] LIMBERGER, Têmis**. O direito à intimidade na era da informática***:* a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007. p. 127-130.

[53] BATALLA, *op. cit.*, 2010, p. 735.

[54] REINA, Emilio Guichot. La comunicación de datos personales en poder de la Administración. Aspectos generales y especialidades derivadas de la comunicación por vía telemática. In: HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). **Administración electrónica**: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España. Valencia: Tirant, 2010. p. 765-806.

[55] BATALLA, *op. cit.*, 2010, p. 769.

[56] REINA, *op. cit.*, 2010. p. 765-806.

sem o consentimento do interessado. Parte-se, não obstante, da premissa de que as finalidades são legítimas, específicas e conhecidas pelo titular (que podem ser compartilhadas).[57] Com isso, um banco de dados pode ter mais de uma finalidade, não necessitando o cidadão, constantemente, fornecer as mesmas informações que o Estado já possui.[58] Ainda assim, a solicitação de acesso deveria ser motivada, explicitando a impossibilidade de ter acesso àqueles dados de outra forma. Para tanto, deve haver controle frente a eventuais abusos, principalmente se os dados forem utilizados para fins distintos dos coletados. Assim é que:

> *El derecho de acceso, el derecho a la protección de datos y el derecho a la intimidad son derechos constitucionales que deben ser compatibilizados entre sí y con los demás derechos e intereses públicos con reconocimiento constitucional, alcanzando la solución que en cada caso entrañe el menor sacrificio posible*.[59]

Por essa razão, seria fundamental a existência de um órgão de natureza administrativa, porém, independente e capaz de controlar o compartilhamento desses dados, o que não se observa na Autoridade Nacional de Proteção de Dados (ANPD), por ser órgão integrante da Presidência da República e, portanto, subordinado ao Chefe do Executivo Federal.[60] Por isso, é que Rodotà[61] vai exigir especial atenção à "minimização da coleta de dados", na qual nenhum dado pessoal deve ser colacionado se a finalidade puder ser alcançada de outra forma (quer dizer, sem o tratamento de dados pessoais). É por todas essas razões que o direito à privacidade, inicialmente atrelado à noção inicial de garantia de ser deixado só, evoluiu até alcançar a gestão das informações, criadas a partir da coleta de dados. O Estado/Administração deve surgir como um protetor da vida privada, inclusive dos dados pessoais, pois "o direito de proteger a privacidade combinado com o dever de proteção dos dados é o supremo direito humano internacional".[62]

---

[57] BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.
[58] REINA, *op. cit.*, 2010, p. 765-806.
[59] *Idem*, p. 781.
[60] BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 10 out. de 2020.
[61] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 20.
[62] BECK, Ulrich. **A metamorfose do mundo**: novos conceitos para uma nova realidade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2018. p. 187.

# 4 CONSIDERAÇÕES FINAIS

A presente pesquisa buscou trazer, ao debate, algumas questões que precisam ser abertamente enfrentadas pela Administração Pública, de forma a alcançar os reais objetivos da Lei Geral de Proteção de Dados. Dentro deste debate, destacaram-se duas temáticas, estudadas conjuntamente a mais duas, quais sejam: a interoperabilidade e o compartilhamento de dados, bem como, a transparência e o respeito à privacidade.

Entendeu-se, por interoperabilidade, a possibilidade de vários sistemas (públicos) se interconectarem, objetivando, assim, o compartilhamento de informações, que chegam por meio dos dados fornecidos ou coletados do cidadão. O que se constata, até hoje, contudo, é que nem mesmo internamente os entes federativos alcançam esta interconexão. Como consequência dessa falta de comunicação, há uma Administração apresentando-se morosa e ineficiente, exigindo, constantemente, dados que já são de seu conhecimento. Em verdade, se ampliado, ainda mais, o espectro, incluindo Estados e Municípios, esse anacronismo é ainda mais assustador.

Deve-se deixar claro que o fornecimento/coleta de dados dos cidadãos, pelo Estado, para a implantação de políticas públicas, não são interesses antagônicos. Não é por outra razão que a incorporação de novas tecnologias, na estrutura da Administração Pública, somente se torna viável e segura se inserida junto a uma série de outros instrumentos como a própria transparência administrativa.

Neste contexto, a diminuição da privacidade somente se justifica com o aumento da transparência da administração. As informações constantes nos dados coletados (ou seja, o abrir mão da privacidade), que devem ser direcionadas e capazes de viabilizar programas sociais, também permitem “novas concentrações de poder”, razão pela qual “os cidadãos têm o direito de pretender exercer controle direto” sobre os sujeitos possuidores dessas informações, e isso somente se dá a partir da transparência.[63] O controle viabilizado por meio da transparência possibilitaria, não apenas verificar-se a exatidão ou o uso correto das informações

[63] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 36-37.

coletadas, mas, também, serviria como um “instrumento de equilíbrio na nova distribuição de poder”.[64]

A transparência surge, portanto, como uma consequência da implantação da Administração Pública que atenda a LGPD, que, para tratar dos dados dos cidadãos, deve, em troca, mostrar-se de forma cristalina. Ao se inserir em (na) rede, a Administração Pública deve voltar sua atenção para o respeito à privacidade do cidadão, bem como, à proteção (ou “cibersegurança”) dos dados de sua posse, visto que está sujeita aos mesmos infortúnios de qualquer cidadão que está conectado à internet.

## REFERÊNCIAS


BATALLA, Antoni Roig. *Intimidad y administración electrónica*. *In:* HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). ***Administración electrónica***: *la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*. Valencia: Tirant do Blanch, 2010. p. 729-748.

BECK, Ulrich. **A metamorfose do mundo**: novos conceitos para uma nova realidade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2018.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade***:* do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 out. de 2020.

_____. Senado Federal. **Proposta de Emenda à Constituição n° 17, de 2019**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 10 out. de2020.

_____. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 10 out. de 2020.

_____. **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 09 jul. de 2020.

_____. Supremo Tribunal Federal. **Recurso Extraordinário 601.314 São Paulo.** Relator: Min. Edson Fachin. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11668355>. Acesso em: 10 out. de 2020.


[64] RODOTÀ, *op. cit.*, 2010, p. 37.

_____. _____. **Ação Direta de Inconstitucionalidade 2.390 Distrito Federal.** Relator: Min. Dias Toffoli. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI2390.pdf>. Acesso em: 10 out. de 2020.

_____. _____. **Ação Direta de Inconstitucionalidade 2.859 Distrito Federal.** Relator: Min. Dias Toffoli. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11899965>. Acesso em: 10 out. de 2020.

_____. _____. **Recurso Extraordinário 1.055.941 São Paulo.** Min. Dias Toffoli. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754018828>. Acesso em: 10 out. de 2020.

_____. _____. **Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Relatora: Min. Rosa Weber. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em: 10 out. de 2020.

CASADO, Eduardo Gamero. Interoperabilidad y administración electrónica: conéctense, por favor. **Revista de Administración Pública**. Madri, n. 179, p. 291-332, maio/ago. 2009.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

ESPANHA. ***Ley 11, de 22 de junio de 2007.*** *Acceso electrónico de los ciudadanos a los Servicios Públicos.* Disponível em: <https://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf>. Acesso em: 10 out de 2020.

_____. ***Ley 40, de 1 de octubre de 2015****. De Régimen Jurídico del Sector Público*. Disponível em: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566>. Acesso em: 10 out. de 2020.

GUTIÉRREZ, Rubén Martínez. ***Administración pública electrónica***. Pamplona: Thomson Reuters, 2009.

LIMBERGER, Têmis. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LÓPEZ, Ramón Mirales. *Modelos de evaluación del impacto sobre la privacidad (PIA, "Privacy Impact Assessments) y el artículo 34 de la Ley 11/2007*. *In:* HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). ***Administración electrónica****: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*. Valencia: Tirant, 2010. p. 749-764.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnicos-informacionais no direito alemão. *In:* MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 205-230.

NAÇÕES UNIDAS. Brasil. **Declaração Universal dos Direitos Humanos**. Disponível em: <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em: 10 out. de 2020.

REILLY, Marcelo Bauzá. *La Administración electrónica a la luz de los principios*. *In:* HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). ***Administración electrónica****: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*. Valencia: Tirant do Blanch, 2010. p. 47-66.

REINA, Emilio Guichot. *La comunicación de datos personales en poder de la Administración. Aspectos generales y especialidades derivadas de la comunicación por vía telemática*. *In:* HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero. (coord.). ***Administración electrónica****: la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*. Valencia: Tirant, 2010. p. 765-806.

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

UNIÓN EUROPEA. ***Decisión 2004/387/CE del parlamento europeo y del consejo de 21 de abril de 2004****. Relativa a la prestación interoperable de servicios pan-europeus de administración electrónica al sector público, las empresas y los ciudad*. Disponível em: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32004D0387R(01)&from=GA>. Acesso em: 10 out. de 2020.

# TRÊS FUNDAMENTOS À CIDADE INTELIGENTE: A TÔNICA DA PROTEÇÃO DE DADOS NO PODER PÚBLICO

Isadora Formenton Vargas[1]

## 1 INTRODUÇÃO

A configuração de uma cidade é um conceito aberto. Das zonas industriais periféricas ao *home office,* na atualidade, a cidade precisa acompanhar as mudanças sociais, econômicas, políticas e tecnológicas, sem perder, entretanto, a identidade da comunidade. É o abrigo das manifestações populares, das relações interpessoais, a despeito da constante intensificação das relações virtuais. É na cidade, enquanto espaço físico ou, inclusive, digital, que se encontra a esfera pública, bem como as esferas reservadas às atuações sociais e privadas.

Surgem alguns questionamentos, em torno das contratações que visam à implementação de cidades inteligentes *(smart cities)*. Neste artigo, busca-se conferir enfoque a três fundamentos norteadores da discussão, como pontos de partida à compreensão do tema.

O primeiro, quanto à prévia compreensão acerca do conceito de cidade inteligente, sobre o qual, embora não haja consenso, permite que sejam identificadas prioridades de atuação pelo Poder Público, mesmo no exercício da discricionariedade.

O segundo, quanto ao estado da arte no Brasil em termos operacionais e legais, no âmbito das tecnologias de informação e comunicação (TICs), necessárias à governança digital, dentro da qual se insere a viabilidade prática de uma cidade inteligente.

O terceiro fundamento, não menos importante, envolve o dever-se que orienta o Poder Público à garantia das liberdades civis e, no caso das cidades inteligentes, mecanismos de *accountability,* prestação de contas, dando enfoque, tanto aos

[1] Mestranda e graduada em Direito pela Universidade Federal do Rio Grande do Sul. Mestre em Argumentação Jurídica pela Universidad de Alicante (ESP) e Università degli Studi di Palermo (ITA). Assessora do Procurador-Geral do Ministério Público de Contas junto ao Tribunal de Contas do Estado do Rio Grande do Sul. Associada ao Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC).

princípios que orientam a Administração Pública (transparência e publicidade, por exemplo), quanto à necessária observância às boas práticas de governança em relação ao tratamento de dados pessoais.

A opção pela temática das cidades inteligentes consiste no fato de que guardam, em si, diversas funções inseridas no contexto da governança digital, viabilizando sua análise sob diferentes perspectivas, além de ser assunto atual em agendas políticas.

## 2 PRIMEIRO FUNDAMENTO: AMPLO ESPECTRO CONCEITUAL

De acordo com a União Internacional de Telecomunicações (UIT), existem, pelo menos, 116 definições de cidade inteligente[2], diluídas em aproximadamente trinta dimensões, dentre elas: acessibilidade, segurança, economia, educação, transporte e mobilidade, telecomunicações, abastecimento elétrico e hidráulico, governança, cidadãos, saúde. No Relatório da UIT, a necessidade de uma compreensão acerca da definição do conceito é fundamental para direcionar a tecnologia da informação, especialmente quanto a políticas relacionadas à segurança de dados.[3]

Em análise final, com a conjugação dos conceitos e dimensões, a Agência da Organização das Nações Unidas concluiu que cidade inteligente sustentável é aquela que se vale das tecnologias de informação e comunicação (TICs), entre outras, à promoção de qualidade de vida, eficiência urbana em operações e serviços, competitividade, garantindo que sejam atendidas as necessidades das gerações presentes e futuras com respeito aos aspectos econômicos, sociais e ambientais.[4] Por isso, fala-se em “cidade ecológica”, pois é ideia de “todo” e de conexão entre organismos, como em um ecossistema, que reproduz a interação entre as tecnologias da informação em um ambiente caracterizado pelo fluxo informacional[5], denominado infosfera.[6]

---

[2] INTERNATIONAL TELECOMMUNICATION UNION. **Smart Sustainable Cities:** An Analysis of Definitions. ITU-T Focus Group on Smart Sustainable Cities, Telecommunication Standardization Sector of the International Telecommunication Union, 2014, p. 09.
[3] *Idem*, p. 12.
[4] *Idem,* p. 09.
[5] BIONI, Bruno. Ecologia: uma narrativa inteligente para a Proteção de Dados Pessoais nas Cidades Inteligentes. In: TIC GOVERNO ELETRÔNICO. **Pesquisa Sobre o Uso das Tecnologias de**

No Relatório da UIT, também, são referidas ocorrências bibliográficas em porcentagem, a fim de identificar a maior incidência de expressões apresentadas na literatura à definição de cidade inteligente. A partir do agrupamento das ocorrências, partiu-se à minimização da subjetividade das definições, com o aprofundamento, por exemplo, sobre o que se entende a respeito de "qualidade de vida e estilo de vida", "infraestrutura e serviços", "TIC, comunicação, inteligência, informação", "governança e administração"; "pessoas, cidadãos, sociedade".

Nesse sentido, quanto à ocorrência "pessoas, cidadãos, sociedade", relaciona-se à necessidade de ferramentas à elevação da educação, ao aumento do tempo de aprendizado e à integração social em termos de capital humano.[7] Isso é relevante, uma vez que a manutenção e aprimoramento de uma cidade inteligente se encontra diretamente proporcional à capacitação humana em termos de educação e de recursos. Se carentes de formação técnica, no âmbito da tecnologia da informação, bem como de formação em ciências humanas à condução ética das propostas, corre-se o risco - apenas a título exemplificativo, sob um aspecto utilitarista - de desperdício de recursos à implementação da tecnologia.

Quanto à escolha política acerca de determinada concepção de cidade inteligente, um Gestor pode entender que a prioridade reside na eficientização do trânsito e, assim, otimizar o transporte público, investindo em ciclovias e em acessibilidade, por exemplo. Outro Gestor pode entender que a otimização do trânsito depende de câmeras de vigilância, as quais também servem ao aumento da segurança pública e, por meio dos dados captados, novas estratégias de eficientização de rotas e serviços (abastecimento, saneamento, iluminação pública) poderão ser desenvolvidas. Ainda, algum Gestor pode optar pela destinação de prédios abandonados e antigas construções fabris em desuso a atividades culturais, artísticas e educacionais, como é o caso de Barcelona.

A breve menção a alguns exemplos serve para contextualizar o leitor a respeito das inúmeras possibilidades que residem nas propostas de cidades inteligentes. Verifica-se que o enfoque a ser conferido depende das prioridades que o Poder Público elege à eficientização de determinado serviço ou uso de bem

---

**Informação e Comunicação no Setor Público Brasileiro**. São Paulo: Comitê Gestor da Internet no Brasil, 2018, p. 54.

[6] FLORIDI, Luciano. ***The 4th revolution:*** *How the infosphere is reshaping human reality*. Oxford: Oxford University Press, 2014, p. 25.

[7] INTERNATIONAL TELECOMMUNICATION UNION. *op. cit.*, 2014, p. 18.

público ou da existência de prévia condução a uma via específica de implementação de cidades inteligentes, no âmbito da Administração Pública.

## 3 SEGUNDO FUNDAMENTO: ESTADO DA ARTE DA GOVERNANÇA DIGITAL NO BRASIL

Em recente estudo, elaborado pela Comissão Europeia sobre Inteligência Artificial no Poder Público, faz-se referência à necessidade de reforma da Administração Pública para conduzir à inovação possibilitada pelas tecnologias da informação e da comunicação (TICs).[8] Nesse mesmo sentido, como refere José Faleiros Jr., inexistindo adequação das políticas de gestão, diante do fluxo incessante e massivo de dados, "não haverá alternativa capaz de sustentar um modelo de atuação pública consentâneo com os desafios que se apresentam nesta nova realidade informacional"[9].

Quanto às cidades inteligentes, no Brasil, importa referir que vem sendo elaborada a Carta Brasileira para Cidades Inteligentes, de iniciativa da Secretaria Nacional de Mobilidade e Desenvolvimento Regional e Urbano do Ministério do Desenvolvimento regional (SMDRU/MDR), em diálogo com a Política Nacional de Desenvolvimento Urbano.[10]

A Carta já possui nove objetivos, em sua agenda, quais sejam: (i) transformação digital é parte do desenvolvimento urbano; (ii) a conectividade deve ser para todos os municípios e inclusão digital dos cidadãos; (iii) a transformação digital propicia novas formas de governança urbana; (iv) o protagonismo local usa de forma inteligente a transformação digital na diversidade territorial; (v) municípios, cidadãos, empresas e academia produzem e usam dados de maneira responsável; (vi) os impactos sistêmicos da transformação digital são continuamente compreendidos e avaliados; (vii) o Poder Público é um facilitador de impactos positivos da transformação digital, na redução das desigualdades e aumento da qualidade de vida nas cidades; (viii) as oportunidades da transformação digital são

[8] MISURACA, Gianluca; VAN NOORDT, Colin. ***Overview of the use and impact of AI in public services in the EU***. Luxembourg: Publications Office of the European Union, 2020, p. 69.
[9] FALEIROS JÚNIOR, José Luiz de Moura. **Administração Pública Digital**: proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. Indaiatuba: Editora Foco, 2020, p. 154.
[10] GOVERNO FEDERAL. Ministério do Desenvolvimento Regional. **Carta Brasileira para Cidades Inteligentes.** 23 ago. 2019. Disponível em: <https://bityli.com/aAaHA>. Acesso em: 21 out. de 2020.

aproveitadas para a criação de empregos e renda locais, manutenção da inteligência local e promoção de sistemas econômicos locais justos e sustentáveis; (ix) capacitação, educação e comunicação são instrumentos de produção de uma transformação digital, que reduz desigualdades e aumenta a qualidade de vida.

Dos objetivos acima expostos, é possível identificar direcionamentos importantes do Governo Federal ao que se compreende por cidade inteligente, com foco no aumento da qualidade de vida, na geração de empregos e priorizando a capacitação e educação à transformação digital, além de um constante acompanhamento dos impactos gerados. Aqui, possivelmente, verifica-se a necessidade de prestação de contas e de fiscalização, seja pelo controle interno, seja pelo controle externo, bem como pela própria sociedade, em posição ativa.

Além da referida Carta, verifica-se que o Poder Público vem se preparando, com o estabelecimento de planos e diretrizes, à transformação digital, de acordo com instrumentos legislativos e também técnicos sobre a temática.

Em 2015, Relatório do Tribunal de Contas da União (TCU) identificou desafios da inclusão digital, no Brasil, contemplando ações realizadas nos últimos 15 anos. Ao destacar quatro eixos da inclusão digital, refere, no terceiro, o Programa Cidades Digitais, caracterizado pela implantação de redes metropolitanas de alta velocidade, em prefeituras, fornecimento de aplicativos de governo eletrônico e disponibilização de pontos de acesso à internet, para uso livre e gratuito em espaços públicos.[11]

Já o Decreto nº 8.777/2016, que institui a Política de Dados Abertos do Poder Executivo Federal, prevê, dentre alguns objetivos, nos incisos do art. 1º, a promoção do desenvolvimento tecnológico e a inovação nos setores público e privado e fomentar novos negócios; o compartilhamento de recursos de tecnologia da informação, de maneira a evitar a duplicidade de ações e o desperdício de recursos na disseminação de dados e informações; e a oferta de serviços públicos digitais de forma integrada. Esses objetivos da Política de Dados Abertos estão intrinsecamente relacionados aos requisitos à implementação de uma cidade inteligente, a qual requer, como já visto, a aplicação de TICs.

O Brasil também conta com o Decreto nº 99.319/2018, o qual instituiu o sistema nacional para a Transformação Digital e estabeleceu a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação

[11] TRIBUNAL DE CONTAS DA UNIÃO**. Política pública de inclusão digital.** Brasília: Seinfra Aero Telecom, 2015, p. 28.

Digital. Atualmente, o Decreto nº 10.332/2020 volta-se à Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal.

De acordo com o documento elaborado à apresentação do plano de Estratégia Brasileira para a Transformação Digital (E-Digital), encontra-se a ação estratégica para "fornecimento de Internet das Coisas em elos da cadeia de valor de cada uma das quatro verticais definidas como prioritárias: Saúde, Agropecuária, Indústria e Cidades Inteligente"[12]. Verifica-se, assim, a prioridade das cidades inteligentes na agenda política de transformação digital. No mesmo documento, faz-se, também, referência ao modelo de armazenamento para dados em nuvem, ampliando a inteligência e cruzamento de bases de dados.[13]

Relevante decreto que não pode passar despercebido é o Decreto nº 10.046/2019, que 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. Trata-se do instrumento ao *Big Data* nacional, uma vez que, dentre os elementos da governança, reside a gestão de dados e de sistemas de informação. Disso decorre a importância de análise quanto às implicações que envolvem segurança de dados e de informação.

Os estudos e instrumentos legislativos, além de algumas TICs apresentadas (serviços de nuvem, internet das coisas, por exemplo) permitem que se identifique a tônica que permeia os fundamentos à implementação das cidades inteligentes, apresentados neste estudo: a proteção de dados no Poder Público, objeto do próximo tópico.

## 4 TERCEIRO FUNDAMENTO: A TÔNICA DA PROTEÇÃO DE DADOS NO PODER PÚBLICO

Acompanhada da cidade inteligente, a governança digital também busca a redução da burocracia das atividades estatais. Interessante, porque a primeira geração de leis de proteção de dados buscava justamente proteger os dados

[12] GOVERNO FEDERAL. **Estratégia brasileira para a transformação digital**. 2018. Disponível em: <https://bit.ly/3d1SXjG>. Acesso em: 21 out. de 2020.
[13] *Idem*, p. 108. E, também, VARGAS, Isadora Formenton; BASSANI, Matheus Linck Bassani. Standards mínimos à contratação de cloud service pelo poder público: estudos preliminares. In: I Congresso Internacional de Direito e Inteligência Artificial, 2020, Virtual. **Governança sustentável**. Belo Horizonte - MG: Skema Business School, 2020. v. II. p. 119-126.

pessoais utilizados a serviço da burocracia governamental[14], vindo a consolidar bancos de dados descentralizados do governo ao aprimoramento das finalidades estatais: previdência, tributação, saúde, por exemplo.

Esse cenário instaurou a preocupação com a tutela da privacidade informacional, passando a importar o consentimento do titular dos dados.[15] Identifica-se, assim, que a proteção de dados surge no contexto público, a partir da relação entre Estado e cidadãos.

No Poder Público, a Lei de Acesso à Informação (LAI) nº 12.527/2011, conjugada com os princípios constitucionais que norteiam o agir da Administração Pública[16], demonstra que a regra geral é a transparência e a publicidade das informações, sem descuidar, entretanto, da necessidade de proteção das informações (art. 6º, incisos). Inclusive, o *caput* do art. 31, indica 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".

Atualmente, com a vigência da Lei Geral de Proteção de Dados (LGPD) nº 13.709/2018, o diploma técnico específico de tutela da autodeterminação informativa e dos instrumentos disponíveis à segurança da informação (art. 46), a boas práticas e da governança (art. 50), além dos princípios que promovem o dever-se em matéria de proteção de dados (art. 6º), recaem, também, sobre o Poder Público.

Assim, a transparência que preconiza a LAI, sobre o tratamento das informações, aparece na LGPD, dentre seus princípios, no inciso X do art. 6º, quanto à responsabilização e prestação de contas, bem como no art. 50 que trata das boas práticas e governança. Ao operar e tratar dados, o Poder Público, diante do acesso massivo e relevante, em termos políticos e sociais, além de econômicos - uma vez que dados são, também, ativos e matéria-prima a novas formas de consumo -

---

[14] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor***:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 34.

[15] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais***.* Rio de Janeiro: Renovar, 2006, p. 372.

[16] Ver, também: "A legalidade não é suficiente para caracterizar a moralidade de um ato administrativo, requer-se muito além da lei uma observância à juridicidade administrativa, em uma concepção ampla de adequação ao direito (MELLO, 2013). No caso da proteção de dados, a boa-fé objetiva relaciona-se, não só à expectativa legítima como, também, à segurança". VARGAS, Isadora Formenton; JOELSON, Marcela; PAGANELLA, Victoria Dickow. Proteção de dados pessoais e COVID-19: promoção da segurança jurídica a partir da eficácia dos princípios. *In*: SQUEFF, Tatiana Cardoso; D'AQUINO, Lúcia Souza; MUCELIN, Guilherme. **O Direito em tempos de crise***:* impactos da COVID-19 nas relações sociojurídicas. Curitiba: Editora CRV, 2020, p. 373.

possui papel fundamental à garantia de segurança dessas informações, mesmo quando adquire tecnologia à implementação das cidades inteligentes, por meio de parcerias e contratos com entidades privadas.

Dessa forma, surge preocupação quanto aos limites ao compartilhamento de dados. Isso porque, caso se reconheça a possibilidade de estender a entidades privadas o diploma de proteção de dados, disponível ao Poder Público, quando a relação jurídica representa uma extensão da atuação da administração, há vulnerabilidades significativas à garantia de que serão preservadas as finalidades das operações de dados pessoais, dado o amplo espectro de aplicações. Assim, há um dever de prestação de contas, em via de mão dupla: das entidades privadas, responsáveis pela tecnologia ao Poder Público, e do Poder Público, aos cidadãos.

Essa relação de compartilhamento e disponibilização de dados ficou bastante conhecida no caso da Medida Provisória nº 954/2020, no contexto da pandemia gerada pela COVID-19, a partir da qual seria possível que empresas de telecomunicação, prestadoras de serviços de telefonia fixa e móvel pessoal no país, devessem disponibilizar, à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas. O Supremo Tribunal Federal, ao referendar a medida cautelar na Ação Direta de Inconstitucionalidade nº 6.389/DF, consolidou importante marco jurisprudencial à tutela da autodeterminação informativa no Brasil, mesmo anterior à vigência da LGPD, com atenção à limitação da finalidade, da minimização e, se possível, da anonimização.

Todas essas nuances, já verificadas em casos atuais, durante a pandemia, dada a necessidade de adoção de estratégias em saúde pública, para as quais se faz, inevitavelmente, necessária a operação de dados, demonstram que muitos mecanismos à implementação de cidades inteligentes, mesmo não concernentes à temática específica, já são objeto de controvérsia jurídica, condição que deve ser levada em consideração pela atuação do Poder Público diante da gestão de dados.

No que se refere ao exercício das liberdades, sejam negativas (contra intervenções arbitrárias), sejam positivas, a Governança Digital deve ocorrer em conformidade às melhores práticas à garantia dos direitos fundamentais e da proteção dados. Assim, busca-se preservar, tanto o Poder Público, de, eventualmente, operar, tratar e compartilhar dados de forma ilícita ou ilegal, quanto

cidadãos, uma vez que desenvolvem sua personalidade no espaço público, que só existe, porque, também, há um espaço aos resguardos da esfera privada.

A viabilidade das cidades inteligentes implica a comunicação entre grandes bancos de dados (*Big Data*), aplicação de heurísticas de inteligência artificial, reconhecimento facial e a Internet das Coisas, na governança digital, promovendo o aperfeiçoamento de inúmeros serviços públicos, além de tornar o Estado mais eficiente, dinâmico e competitivo. No entanto, essas novas tecnologias de informação e comunicação (NTICs) podem resultar em discriminações arbitrárias e nos chamados algoritmos *black boxes*[17] (caixas-pretas), isto é, processos decisórios cujas premissas vão de encontro ao dever de transparência, no âmbito do Poder Público. Por isso, necessário que se atente à tônica da proteção de dados, como fundamento à implementação das idades inteligentes.

## 5 CONSIDERAÇÕES FINAIS

Os três fundamentos apresentados, neste breve estudo, possuem o condão de atentar a quem possa o tema interessar, sobre as bases necessárias, os pontos de partida fundamentais à implementação de cidades inteligentes. Uma política de vigilância e investimento em câmeras de monitoramento não permitem que se conclua que uma cidade é inteligente. Necessária a existência de estudos prévios que viabilizem a identificação de um projeto estruturado à implementação, manutenção e aperfeiçoamento da cidade a seus cidadãos, em diversos aspectos: saúde, economia, educação, acessibilidade, segurança.

Por isso, o primeiro fundamento conduz à compreensão de que algumas definições enfatizam aspectos tecnológicos, enquanto outras priorizam o desenvolvimento do capital humano ou da infraestrutura física. O conhecimento das múltiplas definições de cidades inteligentes não pretende restringir as possibilidades. Ao invés disso, serve como instrumento a cidadãos e ao Poder Público, pois a adoção de determinada opção, em detrimento de outra, deve ser adequada às

[17] CRAWFORD, Kate; WHITTAKER, Meredith; ELISH, Madeleine; BAROCAS, Solon; PLASEK, Aaron; FERRYMAN, Kadija. **The AI Now Report**: the Social and Economic Implications of Artificial Intelligence. Tabled with the White House Office of Science and Technology Policy for their Future of Artificial Intelligence Series, 2016. Disponível em: <https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3.pdf>. Acesso em 21 out de 2020.

finalidades pretendidas, permitindo que sejam identificados os melhores meios técnicos, jurídicos e sociais à eleição de uma ou mais definições.

O segundo fundamento apresenta ao leitor bases técnicas e jurídicas no âmbito nacional que representam, também, instrumentos à transformação digital, permitindo que se identifique a gestão de dados e de informação como tônica às estratégias de governança digital. Assim, partiu-se ao terceiro fundamento, referente à proteção de dados no Poder Público, como forma de garantir a sustentabilidade da cidade inteligente, em relação aos dados. Prestação de contas, transparência, fiscalização e instrumentos de minimização e anonimização são necessários, mas não contemplam, de forma suficiente, todas as peculiaridades, como, por exemplo, a possibilidade de alcançar-se determinada ilicitude na operação de dados, que os envolvam sob uma perspectiva coletiva, referente ao comportamento de uma comunidade, por exemplo.

Assim, o compartilhamento de dados entre entidades privadas e Poder Público, uma vez que a implementação da tecnologia, caso venha a ser realizada por meio de parcerias com organismos privados, dependerá, como visto, de acesso e tratamento aos dados coletados pelo Poder Público, representa um ponto sensível e merecedor de análise prévia, fiscalização constante e guias às melhores práticas que garantam, ao Poder Público, autonomia e independência. Essas mesmas tecnologias da informação, em resumo, servirão à promoção de mecanismos de tutela à autodeterminação informativa, bem como aos demais direitos fundamentais, em exercício, na sociedade da informação.

Em outras oportunidades de escrita, já referenciado, mas sempre necessário, é o trecho do Prólogo de Hannah Arendt à obra Responsabilidade e Julgamento, em 1975, sobre o risco de um governo que não seja

> nem da lei, nem dos homens, mas de escritórios ou computadores anônimos, cuja dominação inteiramente despersonalizada pode vir a se tornar uma ameaça maior à liberdade e àquele mínimo de civilidade sem o qual nenhuma vida comunitária é concebível, do que jamais foi a mais abusiva arbitrariedade dos tiranos do passado.[18]

[18] ARENDT, Hannah. **Responsabilidade e Julgamento**. Tradução Rosaura Eichenberg. São Paulo: Companhia das Letras, 2004.
Contraponto interessante à ideia de computadores anônimos é a proposta de Bruno Bioni à utilização do *Blockchain* como infraestrutura técnica de promoção de transparência e proteção da privacidade: "*Blockchain* seria uma das bases de toda essa infraestrutura técnica por meio da qual uma rede de computadores descentralizada automatizaria as permissões dos cidadãos sobre o uso de seus dados, bem como registraria todo o seu acesso e utilização por terceiros. Em vez de centenas de políticas de privacidade, cujo leque de opções é binário (aceitar ou recusar) e depende da

O que se pretende consolidar, para que não ocorra o vaticinado por Arendt, é o papel emancipador da transformação digital à sociedade, e não de dominação ou vigilância. Para isso, é preciso viabilizar a participação democrática, a proteção de dados, por meio da observância aos princípios, e o constante acompanhamento às melhores práticas de governança, garantindo-se a liberdade negativa, contra intervenções arbitrárias.

## REFERÊNCIAS


ARENDT, Hannah. **Responsabilidade e Julgamento**. Tradução Rosaura Eichenberg. São Paulo: Companhia das Letras, 2004.

BIONI, Bruno. "Ecologia: uma narrativa inteligente para a Proteção de Dados Pessoais nas Cidades Inteligentes". *In*: TIC GOVERNO ELETRÔNICO. **Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro**. São Paulo: Comitê Gestor da Internet no Brasil, 2018, p. 53-60.

CRAWFORD, Kate; WHITTAKER, Meredith; ELISH, Madeleine; BAROCAS, Solon; PLASEK, Aaron; FERRYMAN, Kadija**.** ***The AI Now Report*****:** *the Social and Economic Implications of Artificial Intelligence. Tabled with the White House Office of Science and Technology Policy for their Future of Artificial Intelligence Series*, 2016. Disponível em: <https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3.pdf >. Acesso em 21 out de 2020.

DONEDA, Danilo*.* **Da privacidade à proteção de dados pessoais***.* Rio de Janeiro: Renovar, 2006.

FALEIROS JÚNIOR, José Luiz de Moura. **Administração Pública Digital***:* proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. Indaiatuba: Editora Foco, 2020.

FLORIDI, Luciano. ***The 4th revolution****: How the infosphere is reshaping human reality.* Oxford: Oxford University Press, 2014.

GOVERNO FEDERAL. Ministério do Desenvolvimento Regional. **Carta Brasileira para Cidades Inteligentes.** 23 ago. 2019. Disponível em: <https://bityli.com/aAaHA>. Acesso em: 21 out. de 2020.

GOVERNO FEDERAL. **Estratégia brasileira para a transformação digital***.* 2018. Disponível em: <https://bit.ly/3d1SXjG>. Acesso em: 21 out. de 2020.

INTERNATIONAL TELECOMMUNICATION UNION. ***Smart Sustainable Cities***: *An Analysis of Definitions. ITU-T Focus Group on Smart Sustainable Cities, Telecommunication Standardization Sector of the International Telecommunication Union*, 2014.


---

intervenção manual dos cidadãos, e que, na prática, garante pouca transparência sobre o seu processamento, haveria uma "arquitetura distribuída de gerenciamento dos dados" controlada de forma granular pelos cidadãos e sob escrutínio público constante". In: BIONI, Bruno. *op. cit.,* 2018, p. 58.

MISURACA, Gianluca; VAN NOORDT, Colin. ***Overview of the use and impact of AI in public services in the EU****.* Luxembourg: Publications Office of the European Union, 2020.

TRIBUNAL DE CONTAS DA UNIÃO**. Política pública de inclusão digital***.* Brasília: Seinfra Aero Telecom, 2015.

VARGAS, Isadora Formenton; BASSANI, Matheus Linck Bassani. *Standards* mínimos à contratação de *cloud service* pelo poder público: estudos preliminares*. In*: I Congresso Internacional de Direito e Inteligência Artificial, 2020, Virtual. **Governança sustentável.** Belo Horizonte - MG: Skema Business School, 2020. v. II. p. 119-126.

VARGAS, Isadora Formenton; JOELSON, Marcela; PAGANELLA, Victoria Dickow. Proteção de dados pessoais e COVID-19: promoção da segurança jurídica a partir da eficácia dos princípios*. In*: SQUEFF, Tatiana Cardoso; D'AQUINO, Lúcia Souza; MUCELIN, Guilherme. **O Direito em tempos de crise:** impactos da COVID-19 nas relações sociojurídicas. Curitiba: Editora CRV, 2020, p. 363-380.

# GOVERNANÇA DE DADOS E O PODER PÚBLICO: PERSPECTIVAS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

José Luiz de Moura Faleiros Júnior[1]

## 1 INTRODUÇÃO

Mesmo antes da vigência da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 14 de agosto de 2018 –, notou-se grande preocupação do Poder Público com a edição de políticas de governança direcionadas ao recrudescimento de seu papel como agente de tratamento de dados, assim definido em razão de expressa previsão contida nos artigos 1º e 23 a 32 da referida lei.

Tratar de governança, porém, significa falar no estabelecimento de parâmetros específicos para as atividades relacionadas a dados, no âmbito de atuação de cada ente político. Representa, enfim, uma discussão para além da assunção de deveres, quanto à edição de normas; é, essencialmente, um desdobramento da necessidade de que o Estado, efetivamente, se reformule e passe a atuar preventivamente quanto à segurança de dados.

Forte nessa premissa, hoje se fala em uma "Administração Pública digital", conceito amplo e que reflete as nuances precaucionais que envolvem o desempenho das atividades estatais na sociedade da informação. E, sendo o próprio Estado o grande coletor e processador de dados pessoais (inclusive sensíveis) dos cidadãos, seria natural que iniciativas específicas surgissem, durante o período de *vacatio legis* da LGPD.

A União prontamente se mobilizou, com parametrizações que remontam ao ano de 2017 (momento prévio à promulgação da LGPD), quando foi editado o Decreto nº 9.203; iniciativas posteriores demonstraram uma preocupação específica

[1] Mestre em Direito pela Universidade Federal de Uberlândia - UFU. Especialista em Direito Processual Civil, Direito Civil e Empresarial, Direito Digital e *Compliance*. Participou de curso de extensão em direito digital da University of Chicago. Bacharel em Direito pela Universidade Federal de Uberlândia - UFU. Associado Fundador do Instituto Avançado de Proteção de Dados – IAPD. Membro do Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC. Advogado.

do governo federal com sua governança de dados (Decretos nº 10.046 e 10.047, ambos de outubro de 2019).

Nos planos estadual e municipal, também já se nota o surgimento de iniciativas similares. Para análise, elege-se, em razão da opção metodológica desta investigação, o Decreto Estadual nº 49.265/2020, do Estado de Pernambuco, e o Decreto nº 59.767/2020, do Município de São Paulo, como exemplos de iniciativas estatais relacionadas à governança de dados para além do âmbito federal.

Problematiza-se como pode, o Estado, adaptar-se à realidade inaugurada, no Brasil, com a vigência da LGPD e, para responder a essa inquietação hodierna, trabalha-se com a governança de dados (e, em linhas mais específicas, com o *compliance* digital), como hipótese de pesquisa centrada na potencialidade dos mecanismos de governança para a superação de modelos desestruturados, burocratizados e atrasados de atuação pública. Nesse intuito, a pesquisa se dedicará, pelo método indutivo, à análise dos mencionados marcos normativos relacionados à governança de dados nos planos federal, estadual e municipal.

Ao final, buscar-se-á uma conclusão assertiva e capaz de contrastar as normas sob análise à lei de regência da matéria.

## 2 A POLÍTICA DE GOVERNANÇA DA ADMINISTRAÇÃO PÚBLICA FEDERAL DIRETA, AUTÁRQUICA E FUNDACIONAL (DECRETO Nº 9.203/2017)

O Decreto nº 9.203, de 22 de novembro de 2017, foi uma sinalização importante quanto à preocupação da União em relação à delimitação de conceitos fundamentais, objetivos e parametrizados, para a governança pública. Assim como no corporativismo privado, no âmbito da Administração Pública, o domínio do conhecimento sobre os programas de *compliance* passa pela reestruturação de algumas bases essenciais da estrutura estatal.

Embora o tema remonte a período já longínquo – desde eventos históricos, como o Caso Watergate, até legislações anticorrupção como o *Foreign Corrupt Practices Act* e o *Sarbanes-Oxley Act*, nos Estados Unidos da América –, nota-se que “inúmeras normas passaram a ser promulgadas com a intenção de incutir deveres de conduta, ordenando a criação de políticas de *compliance* para a

Administração Pública e para os gestores públicos"[2], algo que já era notado, no Brasil, desde a Lei de Improbidade Administrativa[3] (Lei nº 8.429, de 2 de junho 2 1992), mas que veio a se consolidar com a promulgação da Lei Anticorrupção (Lei nº 12.846, de 1º de agosto de 2013) e, com detalhamentos mais específicos, a partir da Lei nº 13.303/2016, que estabeleceu o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, abrangendo todas as empresas pertencentes à União, aos estados, ao Distrito Federal e aos municípios e que explorem atividade econômica de produção ou comercialização de bens ou de prestação de serviços[4].

O decreto, enfim, cuidou de resumir conceitos e delimitar parâmetros. Em termos conceituais, a governança pública (artigo 2º, inc. I), destacada em seu texto, é definida como o conjunto de mecanismos de liderança, estratégia e controle, postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução das políticas públicas e à prestação de serviços de interesse da sociedade[5].

Por sua vez, denomina-se valor público (artigo 2º, inc. II) todo produto ou resultado gerado, preservado ou entregue pelas atividades de uma organização e que representem respostas efetivas e úteis às necessidades ou às demandas de interesse público, modificando aspectos do conjunto da sociedade, ou de grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos. Há clara inspiração nas diretrizes da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE)[6] e, em linhas gerais, trabalha-se com uma

---

[2] FALEIROS JÚNIOR, José Luiz de Moura; MIGLIAVACCA, Viviane Furtado. A parametrização das políticas de compliance na Administração Pública: uma análise dos mecanismos de governança definidos pelo Decreto 9.203/2017. **Revista do Tribunal Regional Federal da 1ª Região**, Brasília, ano 32, n. 1, p. 56-70, jan./jun. 2020, p. 67.

[3] A Lei 12.846/2013, denominada Lei Anticorrupção, dispôs sobre a responsabilização objetiva administrativa e civil de pessoas jurídicas, pela prática de atos contra a Administração Pública, nacional ou estrangeira. Para outros detalhes, confira-se, por todos: FERREIRA FILHO, Manoel Gonçalves. Corrupção e democracia. **Revista de Direito Administrativo**, Rio de Janeiro, v. 226, n. 4, p. 213-218, out./dez. 2001, p. 214.

[4] COELHO, Cláudio Carneiro Bezerra Pinto. *Compliance* na Administração Pública: uma necessidade para o Brasil. **Revista de Direito da Faculdade Guanambi**. Guanambi, v. 3, n. 1, p. 75-95, jul./dez. 2016, p. 76; CASTRO, Rodrigo Pironti Aguirre de; GONÇALVES, Francine Silva Pacheco. ***Compliance* e gestão de riscos nas empresas estatais**. 2. ed. Belo Horizonte: Fórum, 2019, p. 123.

[5] FALEIROS JÚNIOR, José Luiz de Moura; MIGLIAVACCA, Viviane Furtado. A parametrização das políticas de compliance na Administração Pública, *op. cit.*, 2020, p. 60-61.

[6] A cartilha de princípios da OCDE, agregada aos demais axiomas citados, despertou os valores que dão sustentação ao modelo de Governança Corporativa, que se desenhou desde então. Para Andrade e Rossetti, os seguintes pilares deram origem à nova teoria: (i) *fairness*, compreendido como o senso de justiça e a equidade no tratamento dos acionistas; (ii) *disclosure* ou a transparência nas

mudança de paradigma que é, assim sintetizada, por Amaru Maximiano e Irene Patrícia Nohara:

> [...] as atividades de nível estratégico relacionam-se com a viabilização continuada de operações da organização. Nesse nível, a gestão de pessoas olha para o futuro e para o ambiente, estudando as tendências sociais, competitivas, tecnológicas etc., procurando determinar quais as competências serão necessárias para fazer face às ameaças e oportunidades, de quantas pessoas a organização precisará e que programas deverão ser colocados em prática para atraí-las, desenvolvê-las e mantê-las. O mais importante das atividades de nível estratégico é participar do processo de definir a estratégia corporativa e definir políticas de gestão de pessoas para toda a organização, realizar programas de desenvolvimento organizacional, desenhar carreiras e planos de competências e implementar programas e projetos inovadores.[7]

O decreto ainda conceitua a "gestão de riscos", em seu artigo 2º, inc. IV, como o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, sendo destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Sem dúvidas, o desempenho administrativo já é objeto de estudos reiterados, que propugnam nova articulação[8], ainda que não isente de influências internacionais decorrentes do próprio fenômeno globalizatório[9], embora não se trate, efetivamente, de uma tendência a uma "governança sem governo".[10] Os ecos da predileção pelo *compliance,* nas rotinas gerenciais do Estado[11], trazem à tona um

---

informações; (iii) *accountability*, a prestação de contas; (iv) *compliance*, o atuar em conformidade, cujo consagrado conceito foi sendo aprimorado pela doutrina especializada, tornando-se o paradigma almejado. Para mais: ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. ***Towards a sound integrity framework***: *instruments, processes, structures and conditions for implementation OECD* - Public Governance Committee, 2009. Disponível em: <http://www.oecd.org>. Acesso em: 18 set. de 2020, p. 9.

[7] MAXIMIANO, Antonio Cesar Amaru; NOHARA, Irene Patrícia. **Gestão pública**: abordagem integrada da administração e do direito administrativo. São Paulo: Atlas, 2017, p. 330.

[8] BENTO, Leonardo Valles. **Governança e governabilidade na reforma do estado:** entre a eficiência e a democratização. Barueri: Manole, 2003, p. 85.

[9] MESSA, Ana Flávia. Transparência, compliance e práticas anticorrupção na Administração Pública. São Paulo: Almedina, 2019, p. 191.

[10] PETERS, B. Guy; PIERRE, Jon. Governance without government? Rethinking public administration. **Journal of Public Administration Research Theory**, Oxford, v. 8, n. 2, p. 223-243, abr. 1998, p. 230.

[11] MARRARA, Thiago. Quem precisa de programas de integridade (compliance)? *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coords.). ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 291. O autor comenta: "O primeiro desses elementos se expressa no *comprometimento da alta administração*. Dele se extrai, como condição de sucesso de instrumentos de controle, a necessidade de se superar o modelo de legalidade dúplice, diferenciada ou assimétrica, que perdura na Administração Pública brasileira, pela qual o ordenamento externo e a ordem interna da entidade valem em sua inteireza, somente para os agentes de menor escalão, enquanto os agentes de maior hierarquia são submetidos a um sistema normativo privilegiado, diferenciado, marcado pela menor efetividade e maior brandura. Sem que a

debate mais profundo, relacionado, em essência, à reinserção da ética nas atividades públicas.

O que se percebe, a partir do rol de conceitos que o decreto apresenta, é, sim, uma tendência à parametrização – o que se revela salutar do ponto de vista da finalidade de qualquer propósito relacionado ao prestígio da governança pública –, na medida em que, segundo Ricardo Villas Bôas Cueva, "[u]m programa de fachada, que não preencha os requisitos mínimos ou que os preencha apenas formalmente, pode de fato resultar em penalidades maiores do que aquelas que seriam aplicáveis em sua ausência"[12].

Em seu artigo 3º, o Decreto nº 9.203/2017 elenca alguns princípios de regência das políticas de integridade, sendo eles: capacidade de resposta; integridade; confiabilidade; melhoria regulatória; prestação de contas e responsabilidade; e transparência.

O principal destaque é sem nenhuma dúvida, o paradigma de motivação e responsividade (*responsiveness*)[13], que se espera de um arcabouço hígido de políticas de *compliance*, principalmente para que não se propicie a criação de programas que, ao invés de consubstanciarem uma 'autorregulação regulada', representem mera estrutura '*pro forma*'.

Não há dúvidas de que a motivação é um importante elemento para que se saiba qual é o 'modelo' de governança pública que se deseja ter[14], especialmente quando se pretenda implementar uma adequada gestão de riscos, uma vez que é a motivação o elemento essencial para a garantia do contínuo desenvolvimento de competências, para a melhoria do desempenho geral das atividades de Estado e para formatar o comprometimento dos servidores públicos com a instituição e com os objetivos delineados.

---

alta administração se envolva e, também, proponha-se a observar as normas internas com, no mínimo, o mesmo comprometimento dos servidores de menor escalão, certamente o programa não decolará, nem sequer obterá apoio necessário, inclusive financeiro. Ademais, a falta de compromisso das lideranças ocasionará a perda de sua legitimidade entre os demais agentes públicos".

[12] CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de compliance. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coords.). ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 61.

[13] STIVERS, Camilla. The listening bureaucrat: responsiveness in public administration. **Public Administration Review,** Nova Jersey, v. 54, n. 4, p. 364-369, jul./ago. 1994, p. 364. Anota: "The most common strategy for dealing with the idea of responsiveness is to treat it as an aspect of responsibility. [...]."

[14] CAILLOSSE, Jacques. ***Quel droit la gouvernance publique fabrique-t-elle?*** *Droit et Société*, Paris, v. 71, p. 461-470, 2009, p. 467-468.

O foco, nesse sentido, está atrelado ao papel das lideranças, exercido pelos ocupantes de cargos da alta administração – e, em certa medida, também dos chamados *compliance officers,* notadamente por se esperar o "bom exemplo", requisito "intitulado normalmente como *tone from the top"*[15], afastando a complacência e a leniência quanto a comportamentos antiéticos que, se admitidos, em detrimento das regulações existentes, colocarão em descrédito todo o programa de governança: trata-se da integridade (*integrity*).[16]

Fernando Martins acentua que "um Estado sem controle navega contra a ideia de democracia, porquanto não há transparência para a aferição de sua atuação, vigorando a completa submissão de seus governados"[17]. Nesse campo, em sintonia com os dizeres de Ricardo Simonsen, "[é] necessário que os funcionários e executivos percebam que o programa é uma prioridade da alta direção"[18].

Noutro norte, a responsabilidade (aqui compreendida como *accountability*)[19] também surge como uma importante prática, inerente ao papel de liderança, não devendo ser entendida como mera divisão de tarefas ou competências, mas como uma característica intrínseca ao servidor eficiente, ético e transparente, que ocupa determinado cargo de liderança, pois a norma é hialina ao se referir a padrões de comportamento e práticas humanas (artigo 5º, inc. I), e não a institutos jurídicos.

---

[15] FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de compliance. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coords.). ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 98.

[16] AULICH, Chris; WETTENHALL, Roger; EVANS, Mark. *Understanding integrity in public administration: guest editors' introduction. **Policy Studies***, Oxfordshire, v. 33, n. 1, p. 1-5, jan. 2012, p. 2.

[17] MARTINS, Fernando Rodrigues. **Controle do patrimônio público**. 5. ed. São Paulo: Revista dos Tribunais, 2013, p. 292.

[18] SIMONSEN, Ricardo. Os requisitos de um bom programa de compliance. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coords.). ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 118.

[19] O termo 'responsabilidade' não é um termo de significado único. Seu escopo é ainda mais amplo em idiomas como o francês ou o espanhol, nos quais a 'responsabilidade' é usada em relação a um campo muito amplo de relações jurídicas, políticas e econômicas e, dentro delas, às suas respectivas dimensões diferentes. Em inglês, a existência de termos diferentes para se referir às várias dimensões da responsabilidade – *responsibility*, *accountability*, *liability* – permite uma aplicação mais precisa do conceito. No entanto, isso não impede totalmente a confusão e o debate sobre a aplicação de um ou outro termo às diferentes relações de responsabilidade continua, ocorrendo no campo do direito público. Para mais elucidações, conferir: CAIDEN, Gerald E. *The problem of ensuring the public accountability of public official*. *In:* JABBRA, Joseph G.; DWIVEDI, Onkar Prasad (Eds.). ***Public service accountability**: a comparative perspective*. West Hartford: Kumarian, 1989, p. 17-38; OSBORNE, David; GAEBLER, Ted. ***Reinventing government***: *how the entrepreneurial spirit is transforming the public sector*. Reading: Addison-Wesley, 1992, p. 27.

Ainda, é importante destacar o conceito de interdependência estrutural, que implica uma reinvenção da própria política, impondo a aceitação da autoridade e do poder de decisão, além de uma nova delimitação de funções e responsabilidades de governantes de forma que o Estado tenha outro papel e não seja amplamente dominante[20].

Outrossim, merece destaque o princípio da responsividade, insculpido no artigo 3º, inciso I, do Decreto nº 9.203/2017, que corresponde à capacidade de resposta da Administração Pública, o que reforça a eficiência do servidor público incumbido do exercício de determinada atividade, com vistas ao atendimento dos anseios da sociedade, o que se relaciona, estritamente, com a efetiva prestação de contas aos destinatários das políticas públicas. Trata-se de um efeito do que se denomina *accountability*.

O Decreto nº 9.203/2017 previu, ainda, a criação do Comitê Interministerial de Governança - CIG, conforme dicção de seu artigo 7º, "com a finalidade de assessorar o Presidente da República na condução da política de governança da administração pública federal". Desde que foi implantado, o Comitê realizou algumas Reuniões Ordinárias, sendo a primeira delas no dia 19 de fevereiro de 2018, ocasião em que se iniciaram os trabalhos junto ao Ministério da Transparência e Controladoria-Geral da União (CGU). Durante a terceira reunião ordinária do Comitê, foram lançadas as diretrizes gerais e o guia orientativo para a elaboração de Análise de Impacto Regulatório (AIR)[21]. Nota-se o objetivo de traçar parâmetros claros para que se decidam situações em que o papel regulatório é salutar ou, até mesmo, casos em que a omissão regulatória se mostra mais adequada à finalidade almejada.

Segundo já tivemos a oportunidade de registrar:

> Já se cogitou de uma série de adjetivos para conceituar a Administração Pública pós-social: espacial, funcional, política, decisória, regulatória, gerencial, dialógica, interorgânica, intergeracional, consensual... Mas, se os efeitos que a caracterizam são, agora, os da Quarta Revolução Industrial, cuja marca mais proeminente é o surgimento da Internet, como evitar a classificação de uma 'Administração Pública digital'? [...]. Destacou-se o papel do *compliance* para a ressignificação do papel do Estado no século XXI, agora 'digitalizado' e de fronteiras translúcidas, a demandar parâmetros

[20] ARNAUD, André-Jean. ***La gouvernance**: un outil de participation*. Paris: LGDJ, 2014, p. 181-185.
[21] O tema ganhou força, com a promulgação da Lei da Liberdade Econômica (Lei nº 13.874/2019). Outros detalhes podem ser obtidos em: BINENBOJM, Gustavo. Art. 5º: Análise de Impacto Regulatório. *In:* MARQUES NETO, Floriano de Azevedo; RODRIGUES JÚNIOR, Otavio Luiz; LEONARDO, Rodrigo Xavier (Coords.). **Comentários à Lei da Liberdade Econômica (Lei 13.874/2019)**. São Paulo: Thomson Reuters Brasil, 2019, p. 223-224.

> extranormativos (como os da governança) para a alavancagem e ressignificação do usual modelo de legalidade estrita do *civil law*[22].

A implementação de um Comitê técnico, voltado a asserções desse jaez, revela uma necessidade de corroboração fiscalizatória *ex ante* para muito além do papel já exercido pelos controles internos (o que denota a suposta ineficiência destes). A presença de um Comitê se traduz em confiabilidade, o que reforça a legitimação do processo decisional e, por conseguinte, reflete a almejada boa administração, de viés inclusivo[23] e interativo[24], que se espera dos atores estatais. Nesse sentido, em que pese a, ainda embrionária, atuação do CIG, observa-se razões essenciais de sua existência que, a depender da forma pela qual sua atuação se conduzir, contribuirão para o incremento das políticas de governança pública.

Sobre isso, Thiago Marrara aponta que:

> Em apertada síntese, retomando alguns aspectos que desenvolvi em outro estudo sobre o tema, os fatores que dificultam a eficiência do controle podem ser resumidos a:
> i) *Falta de especialização técnica*: Controlar pressupõe conhecer uma situação ou objeto e entendê-lo. Sem isso, não se controla ou, na melhor das hipóteses, controla-se muito mal. [...]
> ii) *Proximidade entre controlador e controlado*: A Administração Pública, seja em suas tarefas executórias, seja nas funções de controle que lhe cabem, sofre forte influência, ora lícita, ora ilícita, de uma série de fatores, incluindo os de ordem política e econômica, assim como as influências pessoais derivadas de sentimentos, relações de amizade, coleguismo, inimizade ou parentesco. [...] Essas pressões derivam de eventuais articulações políticas manejadas contra o controlador, de seu medo frente a retaliações presentes ou futuras, de ameaças expressas e, não é de se descartar a hipótese, de reais danos físicos, morais ou profissionais. [...]
> iii) *Corporativismo e clientelismo*: o corporativismo pode ser simplificadamente definido como um movimento de autoproteção dos interesses de classes profissionais que também sucede dentro da Administração Pública e, em estágio mais avançado, busca a imunização recíproca de grupos de agentes públicos contra fatores desestabilizadores externos e a manutenção de privilégios e benefícios; [...]. No clientelismo, os controladores, sobretudo os que dependem de eleição pelos pares, trocam seu apoio a situações irregulares ou ilícitas por votos e apoio político. [...]

---

[22] FALEIROS JÚNIOR, José Luiz de Moura. **Administração Pública digital**: proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. Indaiatuba: Foco, 2020, p. 338.

[23] RODRÍGUEZ-ARANA MUÑOZ, Jaime. El derecho fundamental a la buena administración en la constitución española y en la Unión Europea. **Revista Euro latinoamericana de Derecho Administrativo,** Santa Fe, v. I, n. 2, jul./dez. 2014, p. 77. Comenta: "En efecto, el ciudadano es ahora, no sujeto pasivo, receptor mecánico de servicios y bienes públicos, sino sujeto activo, protagonista, persona en su más cabal expresión, y, por ello, debe poner tener una participación destacada en la configuración de los intereses generales porque éstos se definen, en el Estado social y democrático de Derecho, a partir de una adecuada e integrada concertación entre nos poderes públicos y la sociedad articulada."

[24] LONGHI, João Victor Rozatti. **Processo legislativo interativo**: interatividade e participação por meio das Tecnologias da Informação e Comunicação. Curitiba: Juruá, 2017, p. 314-315.

> iv) *Impunidade ou insuficiência punitiva*: A impunidade reinante na Administração Pública brasileira e as insuficiências punitivas por deformações institucionais e procedimentais ou falhas de gestão configuram outro inimigo do controle interno. [...] Não se trata de um problema derivado da insuficiência de mecanismos jurídicos de controle, mas sim da falta de vontade e de condições políticas para se aplicá-los com efetividade. [...]
> v) *Custos elevados*: o direito não é movido sem custos! As normas não saltam do texto legal e transformam-se em realidade sem intervenções naturais. [...]. Por esses outros fatores, a efetividade do controle pressupõe a superação das dificuldades financeiras e orçamentárias de cada entidade estatal, além de luta contra as restrições culturais a investimentos fundamentais em atividades do gênero.[25]

Nesse sentido, o cumprimento de algumas das competências do CIG, conforme arroladas no artigo 15 do decreto[26], porquanto têm caráter executivo, parecem contribuir para a preservação do princípio da juridicidade[27] e para a garantia de um nível de uniformização das políticas de governança; e, ademais, para assegurar a segregação de tarefas criativas e executivas sob viés consultivo. Nesse aspecto, o implemento de novas tecnologias abre importantíssimas portas para esta 'nova' Administração Pública[28] e, nesse cenário, a governança de dados merece ser especificamente analisada.

## 3 INICIATIVAS BRASILEIRAS PARA A GOVERNANÇA DE DADOS

A informação é elemento diferenciador do contexto no qual se insere a governança pública, no século XXI. Não há dúvidas de que o processo de evolução, que culminou na integração das tecnologias informacionais, com destaque para a ascensão da Internet e sua proeminência como mecanismo de afetação democrática, alterou, sobremaneira, a forma como o vetusto conceito de 'governo

---

[25] MARRARA, Thiago. Quem precisa de programas de integridade (*compliance*)?, *Op.cit.,* 2018, p. 287-288.
[26] FALEIROS JÚNIOR, José Luiz de Moura; MIGLIAVACCA, Viviane Furtado. **A parametrização das políticas de compliance na Administração Pública**, *op. cit.*, 2020, p. 61. Explicam: "No que se refere às sanções, o art. 15, incisos I e II do decreto preveem a aplicação de multa e publicação extraordinária da decisão sancionadora. Quando as condutas lesivas à Lei 12.846/2013 configurarem, também, infração à Lei 8.666/1993, e tendo ocorrido à apuração conjunta, a pessoa jurídica ficará sujeita, além das sanções do art. 15, incisos I e II, à sanção de restrição de participação em licitações e celebração de contratos administrativos, nos termos do art. 16".
[27] MOREIRA NETO, Diogo de Figueiredo. **Curso de direito administrativo**. 16. ed. Rio de Janeiro: Forense, 2014, p. 85.
[28] BREGA, José Fernando Ferreira. **Governo eletrônico e direito administrativo**. Brasília: Gazeta Jurídica, 2015, p. 268. Diz: "O efetivo aproveitamento das oportunidades proporcionadas pela tecnologia exige uma visão mais aprofundada e crítica a esse respeito".

eletrônico', apresentado com larga aceitação e grande potencial disruptivo[29], vem sendo ressignificado à luz de novos preceitos e formatações que ampliam seu escopo para além do prisma concorrencial[30], seja sob o aspecto orgânico, seja sob o aspecto funcional, relacionado à integração que propicia[31].

Entra em cena a governança de dados:

> Extraída do contexto maior da governança corporativa e tangenciando pontos da Governança de TI, a de dados foca em princípios de organização e controle sobre esses insumos essenciais para a produção de informação e conhecimento das empresas. O controle mais estrito e formal de dados não é um desafio surgido nos dias de hoje. Os dados, dentre os insumos corporativos, são aqueles que mais apresentam características de fluidez, perpassam diversos processos e sofrem mais transmutações, pois são trabalhados em diversos pontos do seu ciclo de vida, dando origem a outros, além de nem sempre possuírem uma fonte e um destino claramente formalizados[32].

Iniciativas específicas estão surgindo, em nível empresarial, por certo, mas o Estado não tem se quedado inerte, quanto ao atendimento do comando normativo da LGPD para o período de *vacatio legis*. Há iniciativas em todos os níveis, e algumas merecem menção.

## 3.1 A GOVERNANÇA DE DADOS NO ÂMBITO FEDERAL (DECRETOS Nº 10.046/2019 E Nº 10.047/2019)

A tendência à governança ganhou novos contornos com o advento da Lei nº 13.709, de 14 de agosto de 2018 (a Lei Geral de Proteção de Dados Pessoais, ou LGPD), que, em seu artigo 23[33], impõe a identificação da finalidade pública para o tratamento de dados. Na esteira do Regulamento Geral sobre a Proteção de Dados europeu (RGPD, ou GDPR, na sigla em inglês)[34], uma das peculiaridades mais notáveis da LGPD brasileira diz respeito ao seu artigo 46[35], que prevê o dever geral

---

[29] GRÖNLUND, Åke; HORAN, Thomas A. Introducing e-Gov: history, definitions, and issues. **Communications of the Association for Information Systems**. Nova York, v. 15, n. 39, p. 713-729, jan. 2004, p. 721-723.

[30] STUCKE, Maurice E.; GRUNES, Allen P. ***Big Data and competition policy***. Oxford: Oxford University Press, 2016, p. 271.

[31] MESSA, *op. cit.*, 2020, p. 234.

[32] BARBIERI, Carlos. **Governança de dados**. Rio de Janeiro: Alta Books, 2019, p. 35.

[33] "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: [...]."

[34] VOIGT, Paul; VON DEM BUSSCHE, Axel. ***The EU General Data Protection Regulation (GDPR)***: *a practical guide*. Basileia: Springer, 2017, 38-40.

[35] "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

de segurança da informação e pavimenta o caminho para o detalhamento ulteriormente trazido pelo artigo 50 e para a imposição do *compliance* no tratamento de dados, com impactos para o Poder Público[36].

Paulatinamente, várias mudanças sociais passaram a afetar o ritmo de inovação e propiciaram o surgimento de novas tecnologias, acirrando riscos já existentes e produzindo outros. Nessa linha, a mera existência da norma não será suficiente para garantir proteção e contingenciamento a todas as particularidades envolvidas na efetiva proteção à privacidade.

Segundo Stuart Madden, "ao mesmo tempo, e pelos mesmos meios que a responsabilidade civil desencoraja a elevação extracontratual do risco, regras de responsabilização encorajam comportamentos mais seguros"[37] e, com toda razão, este deve ser o espírito da referida norma: o estímulo constante à prevenção de riscos, à mitigação de danos e à propagação de uma cultura de boas práticas.

Nesse compasso, ressalta-se a aplicabilidade da lei ao Poder Público, com o Capítulo IV, especialmente dedicado a isso e composto pelos artigos 23 a 32, que contemplam diversas nuances relacionadas às atividades de coleta e tratamento de dados, no âmbito público, a demandar compreensão específica de uma série de institutos correlatos, especialmente no que concerne à proteção da privacidade.

Outro não poderia ser o desfecho desta tendência, senão a edição, pela União, de uma normativa especificamente voltada à regência de sua política de governança de dados, que passa a se apresentar em sintonia exata com os propósitos da LGPD. Trata-se do Decreto nº 10.046, de 07 de outubro de 2019, que assim prevê, em seu artigo 1º:

---

[36] Sobre o tema, conferir: FALEIROS JÚNIOR, José Luiz de Moura. **Administração Pública digital**, *op. cit.*, 2020, p. 118-124; CRAVO, Daniela Copetti Cravo. Portabilidade de dados no poder público? **Jota.info**, 15 ago. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/portabilidade-de-dados-no-poder-publico-15082020>. Acesso em: 19 set. de 2020; HANOFF, Roberta Volpato; NIELSEN, Thiago Henrique. A Lei Geral de Proteção de Dados Pessoais na administração pública brasileira: é possível implementar governança de dados antes de se implementar a governança em gestão? *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020, p. 391-406.

[37] MADDEN, M. Stuart. *Tort law through time and culture: themes of economic efficiency*. *In:* MADDEN, M. Stuart (Ed.). ***Exploring tort law***. Cambridge: Cambridge University Press, 2005, p. 48, tradução livre. No original: *"(…) at the same time, and by the same means as tort law discourages extracontractual elevation of risk, tort rules encourage safer behavior*."

> Art. 1º. Este Decreto estabelece as normas e as diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, com a finalidade de:
> I - simplificar a oferta de serviços públicos;
> II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;
> III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;
> IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e
> V - aumentar a qualidade e a eficiência das operações internas da administração pública federal.

O compartilhamento de dados entre órgãos e entidades da Administração Pública federal já estava previsto, em caráter programático, no artigo 27 da LGPD, que traz três exceções em seus incisos.[38] O objetivo precípuo, sem dúvida alguma, é a delimitação de políticas institucionais adequadas aos propósitos elencados pelo legislador no que concerne à proteção de dados pessoais.

O artigo 2º, inciso XV, do decreto conceitua como 'governança de dados' o "exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos". No cotejo do compartilhamento, por sua vez, o artigo 4º define três níveis essenciais: (i) amplo; (ii) restrito; (iii) específico[39].

---

[38] "Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto: I - nas hipóteses de dispensa de consentimento previstas nesta Lei; II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou III - nas exceções constantes do § 1º do art. 26 desta Lei."

[39] Art. 4º 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. § 1º A categorização do nível de compartilhamento será feita pelo gestor de dados, com base na legislação. § 2º A categorização do nível de compartilhamento será detalhada de forma a tornar clara a situação de cada item de informação. § 3º A categorização do nível de compartilhamento como restrito ou específico será publicada pelo respectivo gestor de dados no prazo de noventa dias, contado da data de publicação das regras de compartilhamento de que trata o art. 31. § 4º A categorização do nível de compartilhamento como restrito e específico especificará o conjunto de bases de dados por ele administrado com restrições de acesso e as respectivas motivações. § 5º A categorização do nível de compartilhamento, na hipótese de ainda não ter sido feita, será realizada pelo gestor de dados quando responder a solicitação de permissão de acesso ao dado. § 6º A categorização do nível de compartilhamento será revista a cada cinco anos,

Sendo certo que o *Big Data* público já é uma realidade, o controle de dados, exercido pelo Poder Público, passa a ostentar nova dimensão com a possibilidade de compartilhamento interorgânico. Nesse aspecto, a criação do 'Cadastro Base do Cidadão' (artigo 16 e seguintes), por exemplo, revela a possibilidade de cognição ampla sobre aspectos relacionados a todas as esferas da vida do cidadão. A integração, a partir do fornecimento de informações pelos Cartórios de Registro Civil, bem como o cruzamento de dados extraídos de bases, como a da Receita Federal do Brasil e a do Instituto Nacional do Seguro Social, propiciam a consolidação de verdadeira 'vigilância de dados' estatal.

O projeto de regulamentação de uma política de governança de dados, específica para o Poder Público, a ser fiscalizada por um Comitê também definido pelo decreto (artigos 21 e seguintes) se alinha à premência de que sejam iniciadas as atividades da Agência Nacional de Proteção de Dados – ANPD[40], o órgão[41] criado pela LGPD (artigos 55-A e seguintes) e estruturado pelo Decreto nº 10.474, de 27 de agosto de 2020, para atuar na fiscalização e gestão do atendimento às disposições específicas contidas na lei, que, embora formalmente criada, ainda não está em operação.

Também é de imperioso registro o papel do Decreto nº 10.047, que dispõe sobre a governança do Cadastro Nacional de Informações Sociais – CNIS[42] e institui

---

contados da data de publicação deste Decreto ou sempre que identificadas alterações nas diretrizes que ensejaram a sua categorização. § 7º Os órgãos e entidades de que trata o art. 1º priorizarão a categoria de compartilhamento de dados de maior abertura, em compatibilidade com as diretrizes de acesso à informação, previstas na legislação.

[40] LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**: de acordo com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 e as alterações da Lei nº 13.853/2019), o Marco Civil da Internet (Lei nº 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020, p. 313. A autora ainda conclui: "Disto se conclui que a confluência do direito e da tecnologia é fundamental para assegurar a proteção dos dados pessoais, um dos direitos de personalidade, pelo menos quanto aos princípios da transparência (conhecimento de que há coleta de dados pelo indivíduo) e do consentimento (prévia anuência do titular dos dados). Tais ferramentas serão eficazes se tiver a coordenação da trilogia: i) sistemas de informação; ii) boas práticas de mercado; e iii) *design* físico e infraestrutura da rede."

[41] Comentando especificamente a natureza de 'órgão' atribuída à ANPD, ver: NOHARA, Irene Patrícia. Autoridade Nacional de Proteção de Dados: reflexões funcionais sobre a natureza jurídica de órgão. *In:* RAIS, Diogo; PRADO FILHO, Francisco Octavio de Almeida (Coords.). **Direito público digital:** o Estado e as novas tecnologias; desafios e soluções. São Paulo: Thomson Reuters Brasil, 2020, p. 22-24.

[42] O CNIS passa a ser composto e operacionalizado por 51 sistemas e bases de dados distintos, listados no Anexo único do decreto, a saber: 1. Cadastro Nacional da Pessoa Jurídica - CNPJ; 2. Cadastro Nacional de Imóveis Rurais - Cnir; 3. Cadastro Nacional de Obras - CNO; 4. Cadastro de Atividade Econômica da Pessoa Física - CAEPF; 5. Cadastro de Imóveis Rurais - Cafir; 6. Cadastro de Pessoas Físicas - CPF; 7. Sistema Nacional de Cadastro Rural - SNCR; 8. Sistema Integrado de Administração de Recursos Humanos - Siape; 9. Fundo de Garantia do Tempo de Serviço - FGTS;

o programa ‘Observatório de Previdência e Informações’. Com maior foco em dados relacionados à Previdência, o relevante papel deste segundo decreto se alinha aos propósitos da governança estabelecida, em linhas mais amplas, no primeiro.

O CNIS é a principal base de dados (somada às bases CAGED e RAIS) da infraestrutura que permite, dentre outras ações, a gestão do pagamento de benefícios como o ‘auxílio emergencial’, instituído pela Lei nº 13.982, de 2 de abril de 2020, e revisitado pela Medida Provisória nº 1.000, de 2 de setembro de 2020. Em tempos pandêmicos, teria sido de curial valor que tal sistema apresentasse funcionamento efetivo. Porém, o que se notou, no curso da responsividade estatal brasileira aos problemas decorrentes do cruzamento de dados no referido sistema, foi uma reiteração de falhas que beneficiou quem não estava qualificado para o recebimento do benefício assistencial[43].

Trata-se de um único exemplo, mas seus impactos são emblemáticos quanto às repercussões que acarreta para a (in) eficiência estatal em manter bancos de dados hígidos e suficientemente coesos para prevenir tratamento indevido. A vigência da LGPD, ao menos por impor a responsabilidade como um princípio, em

---

10. Sistema Integrado de Administração Financeira do Governo Federal - Siafi; 11. Registro Nacional de Veículos Automotores - Renavam; 12. Registro Nacional de Carteira de Habilitação - Renach; 13. Programa Nacional de Acesso ao Ensino Técnico e Emprego - Pronatec; 14. Programa Universidade para Todos - ProUni; 15. Sistema de Seleção Unificada - Sisu; 16. Monitoramento da frequência escolar do Programa Bolsa Família - Presença; 17. Financiamento Estudantil - Fies; 18. Programa Nacional de Fortalecimento da Agricultura Familiar - Pronaf; 19. Base de dados do sistema GTA; 20. Sistema de Informações de Projetos de Reforma Agrária - Sipra; 21. Cadastro Nacional de Estabelecimentos de Saúde - Cnes; 22. Prontuário Eletrônico do Paciente - PEP; 23. Programa de Volta para Casa - PVC; 24. Sistema de Acompanhamento da Gestante - SisPreNatal; 25. Sistema de Informações do Programa Nacional de Imunizações - SIPNI; 26. Sistema de Informações sobre Mortalidade - SIM; 27. Sistema de Cadastro de usuários do SUS - Cadsus; 28. Sistema de Informação sobre Nascidos Vivos - Sinasc; 29. Folha de Pagamento do Programa Bolsa Família; 30. Cadastro Único - CadÚnico; 31. Sistema de Registro Nacional Migratório - Sismigra; 32. Sistema de Informação do câncer do colo do útero - Siscolo; 33. Sistema de Informação do câncer de mama - Sismama; 34. Sistema Nacional de Passaportes - Sinpa; 35. Sistema Nacional de Informações de Segurança Pública - Sinesp; 36. Registro Administrativo de Nascimento e Óbito de Indígenas - Rani; 37. Sistema ProVB - Programa de Vendas em Balcão; 38. Sistema de Cadastro Nacional de Produtores Rurais, Público do PAA, Cooperativas, Associações e demais Agências - Sican; 39. Observatório da Despesa Pública; 40. Sistema de Gerenciamento de Embarcações da Marinha do Brasil - Sisgemb; 41. Sistema da Declaração de Aptidão ao Pronaf - Sistemas DAP; 42. Cadastro da Agricultura Familiar - CAF; 43. Cadastro Ambiental Rural - CAR; 44. Sistema de Cadastramento Unificado de Fornecedores - Sicaf; 45. Cadastro Nacional de Empresas - CNE; 46. Folha de Pagamento do Seguro-Desemprego; 47. Folha de Pagamento do Programa Garantia Safra; 48. Base de Beneficiários do Plano Safra; 49. Folha de Pagamento do Bolsa Estiagem; 50. Auxílio econômico a produtores independentes de cana-de-açúcar; 51. Sistema Aguia.

[43] MARCHESINI, Lucas. **Governo falha e repassa auxílio emergencial a pessoas com mais de 10 CNPJs**. Metrópoles, 11 jun. 2020. Disponível em: <https://www.metropoles.com/brasil/governo-falha-e-repassa-auxilio-emergencial-a-pessoas-com-mais-de-10-cnpjs>. Acesso em: 19 set. de 2020.

seu caráter preventivo (art. 6º, inc. X), contribuiria para a mitigação de eventos como este.

## 3.2 O EXEMPLO DO ESTADO DE PERNAMBUCO (DECRETO ESTADUAL Nº 49.265/2020)

Atuando em sentido similar ao do governo federal, alguns Estados passaram a editar regulamentos próprios e Pernambuco foi um dos mais assertivos, ao editar o Decreto nº 49.265, de 6 de agosto de 2020.

O decreto estadual estabelece o Plano Quadrienal Estratégico de Proteção dos Dados Pessoais ("PPDP"), que será o instrumento utilizado pelo governo do estado para traçar as prioridades relativas à governança de dados e implementar as medidas de proteção no Estado. Ademais, o decreto também traz disposições referentes à "Governança da Política Estadual", ao exercício dos titulares dos dados e ao compartilhamento, entre entes públicos, e avança quanto às diretrizes há muito estabelecidas pela Lei Estadual nº 12.985, de 2 de janeiro de 2006 (Política de Tecnologia da Informação e Comunicação do Estado de Pernambuco).

Referida lei estadual criou, em 2006, o Comitê Executivo de Governança Digital –CEGD, o Comitê Técnico de Governança Digital – CTGD e a Agência de Tecnologia da Informação – ATI, que, com 14 anos de existência, agora assumem deveres (arts. 7º, 8º e 10) especificamente voltados à alavancagem das diretrizes de governança de dados no âmbito do referido Ente Político.

Noutro norte, o artigo 2º do decreto estadual apresenta, dentre suas várias diretrizes, duas que são particularmente interessantes, no que concerne à propensão de uma Administração Pública efetivamente "digital", quais sejam, "o atendimento simplificado e eletrônico das demandas do cidadão" (inc. II) e "o alinhamento e o equilíbrio com a promoção da transparência pública" (inc. IV). São iniciativas de reforço ao fundamento constitucional da cidadania (art. 1º, inc. II, da Constituição da República), que, agora, transcende ao mundo virtual – uma "cibercidadania", como sempre sugeriu Pérez Luño[44].

O artigo 2º, inciso I, do decreto ainda aponta para a necessidade de que sejam estabelecidos parâmetros de governança:

---

[44] A assim chamada "cibercidadania", nos dizeres de Pérez Luño, implica a consideração dos impactos que a tecnologia traz para o elemento central da participação do povo no processo deliberativo democrático, especialmente pela presença de participantes privados na intermediação dessas comunicações. Confira-se: PÉREZ LUÑO, Antonio Enrique. ***¿Ciberciudadaní@ o cidadaní@.com?*** Barcelona: Gedisa, 2004.

> Art. 2º. [...]
> I - as regras de boas práticas e governança estabelecidas pelo controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

Nota-se refinamentos adicionais às indicações contidas no artigo 50 da LGPD, que, embora tenha delimitado a governança de dados como uma faculdade do agente de tratamento (devido ao emprego do verbo 'poder', em lugar de 'dever'[45]), fê-lo de modo a espelhar o *compliance* digital como desdobramento profícuo do princípio da responsabilidade, contido no art. 6º, inciso X, da LGPD. Já o decreto pernambucano, adotando medidas de planejamento, sinaliza o alinhamento para a adequação local e regional da governança de dados, ao prever que as Políticas de Proteção de Dados Pessoais Locais - PPDPL deverão considerar as prioridades previstas no Plano Quadrienal Estratégico de Proteção de Dados Pessoais – PPDP (art. 6º, §1º).

O Estado de Pernambuco também cuidou especificar, no artigo 13 do decreto, as atribuições do encarregado de dados[46] (*data protection officer*, ou DPO, como é usualmente chamado), algo que a própria LGPD não fez, uma vez que se limitou a descrever suas atividades (art. 41, §2º). A razão para isso está no fato de o tratamento de dados, para ser realizado pelo Poder Público, pressupor a indicação do encarregado, como explica Fabrício da Mota Alves:

---

[45] MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança, boas práticas, governança e compliance. *In:* LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020, p. 364-365.

[46] "Art. 13. Compete ao encarregado e sua equipe de apoio: I - gerenciar a Política de Proteção de Dados Local para: a) inventariar os tratamentos do controlador, inclusive os eletrônicos; b) analisar a maturidade dos tratamentos em face dos objetivos e metas estabelecidos e do consequente risco de incidentes de privacidade; c) avaliar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito; d) adotar as providências cabíveis para implementar as medidas de segurança avaliadas; e e) cumprir os objetivos e metas previstas na Política de Proteção de Dados Pessoais Locais. II - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, em articulação com a Ouvidoria de cada órgão e entidade; III - receber comunicações da Agência Nacional de Proteção de Dados Pessoais - ANPD e adotar providências; IV -orientar os funcionários e os contratados no cumprimento das práticas necessárias à privacidade de dados pessoais; V - quando provocado, entregar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade; VI - atender às normas complementares da Agência Nacional de Proteção de Dados Pessoais; e VII - informar à Agência Nacional de Proteção de Dados Pessoais e aos titulares dos dados pessoais eventuais incidentes de privacidade de dados pessoais, dentro da execução de um plano de respostas a incidentes".

> [...] diferentemente do que ocorre quando o agente de tratamento é pessoa jurídica de direito privado ou, ainda, pessoa natural, a LGPD estabelece um conjunto de condições – em particular, a indicação do encarregado – para o tratamento de dados pessoais pela União, Estados, Distrito Federal e Municípios, inclusive as entidades que compõem a administração pública indireta, de todos os Poderes republicanos.[47]

Trabalhou-se enfaticamente, outrossim, com o compartilhamento de dados (artigos 19 a 23), excetuando pontualmente os dados pessoais sensíveis relativos à saúde do escopo de compartilhamento[48].

Há diversas outras nuances e, por certo, a efetividade dos agentes estaduais quanto à delimitação da política instituída pelo decreto dependerá, em grande parte, do empenho federal (particularmente da ANPD, quanto ao exercício de seu poder regulamentar) e da adesão dos municípios pernambucanos à proposta.

## 3.3 O EXEMPLO DO MUNICÍPIO DE SÃO PAULO (DECRETO Nº 59.767/2020)

Já se anotou que o chamado *compliance* é fruto de "análise jurídica e técnica que transcende o Direito, impondo um diálogo transversal e interdisciplinar"[49], mas igualmente amplo e multissetorial. Os municípios, naturalmente, assumem deveres específicos, quanto a esse escopo, colhido da alusão feita, no próprio artigo 1º da LGPD, às pessoas jurídicas de direito público, consideradas em sentido amplo.

Com base nisso, foi publicado o Decreto nº 59.767, de 15 de setembro de 2020, do Município de São Paulo, que regulamenta a aplicação da LGPD em seu âmbito, reitera conceitos essenciais e adota providências interessantes.

Um dos pontos curiosos do decreto municipal da capital paulista é a delimitação de atribuições ao encarregado público de dados (o DPO municipal), assim como, no exemplo anterior, do Estado de Pernambuco. Em linhas específicas, o artigo 5º[50] do decreto do Município de São Paulo elegeu o Controlador Geral do Município para tal função e lhe atribuiu largo rol de deveres[51], prevendo, ainda, que

---

[47] ALVES, Fabrício da Mota. Estruturação do cargo de DPO em entes públicos. *In:* BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (Coords.). ***Data Protection Officer (encarregado)*:** teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Brasil, 2020, p. 528.

[48] "Art. 20. O compartilhamento entre controladores públicos não poderá ser realizado quando envolver dados pessoais sensíveis referentes à saúde."

[49] FALEIROS JÚNIOR, José Luiz de Moura. Notas introdutórias ao *compliance* digital. *In:* CAMARGO, Coriolano Almeida; CRESPO, Marcelo; CUNHA, Liana; SANTOS; Cleórbete (Coords.). **Direito digital**: novas teses jurídicas. 2. ed. Rio de Janeiro: Lumen Juris, 2019, p. 123.

[50] "Art. 5º Fica designado o Controlador Geral do Município como o encarregado da proteção de dados pessoais, para os fins do art. 41 da Lei Federal nº 13.709, de 2018."

[51] "Art. 6º São atribuições do encarregado da proteção de dados pessoais: I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II – receber comunicações da autoridade nacional e adotar providências; III – orientar os funcionários e os

"[...] terá os recursos operacionais e financeiros necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como acesso motivado a todas as operações de tratamento" (art. 6º, §1º).

Em sentido similar ao exemplo do Estado de Pernambuco, percebe-se a preocupação do Município de São Paulo, com o atendimento de diretrizes estabelecidas pela ANPD (art. 15, inc. II) e quanto ao compartilhamento de dados[52] (art. 14), realçando-se a preocupação com o atendimento de dever legal, recomendação da agência ou mediante coleta prévia do consentimento do titular, observadas as hipóteses ressalvadas pela lei federal.

O debate volta ser, essencialmente, sobre integridade governamental[53] , o que reforça a preocupação com a verdadeira – e esperada – *accountability* pública. Far-se-á necessário verdadeiro entrelaçamento, nas diversas esferas de atuação do Poder Público, para que se possa levar a efeito a verdadeira proteção de dados pessoais.

---

contratados da Administração Pública Direta a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; IV – editar diretrizes para a elaboração dos planos de adequação, conforme art. 4º, inciso III deste decreto; V – determinar a órgãos da Prefeitura a realização de estudos técnicos para elaboração das diretrizes previstas no inciso IV deste artigo; VI - submeter à Comissão Municipal de Acesso à Informação (CMAI), sempre que julgar necessário, matérias atinentes a este decreto; VII – decidir sobre as sugestões formuladas pela autoridade nacional a respeito da adoção de padrões e de boas práticas para o tratamento de dados pessoais, nos termos do art. 32 da Lei Federal nº 13.709, de 2018; VIII – providenciar a publicação dos relatórios de impacto à proteção de dados pessoais previstos pelo art. 32 da Lei Federal nº 13.709, de 2018; IX - recomendar a elaboração de planos de adequação relativos à proteção de dados pessoais ao encarregado das entidades integrantes da Administração indireta, informando eventual ausência à Secretaria responsável pelo controle da entidade, para as providências pertinentes; X - providenciar, em caso de recebimento de informe da autoridade nacional com medidas cabíveis para fazer cessar uma afirmada violação à Lei Federal nº 13.709, de 2018, nos termos do art. 31 daquela lei, o encaminhamento ao órgão municipal responsável pelo tratamento de dados pessoais, fixando prazo para atendimento à solicitação ou apresentação das justificativas pertinentes; XI - avaliar as justificativas apresentadas nos termos do inciso X deste artigo, para o fim de: a) caso avalie ter havido a violação, determinar a adoção das medidas solicitadas pela autoridade nacional; b) caso avalie não ter havido a violação, apresentar as justificativas pertinentes à autoridade nacional, segundo o procedimento cabível; XII - requisitar das Secretarias e Subprefeituras responsáveis as informações pertinentes, para sua compilação em um único relatório, caso solicitada pela autoridade nacional a publicação de relatórios de impacto à proteção de dados pessoais, nos termos do artigo 32 da Lei Federal nº 13.709, de 2018; XII – executar as demais atribuições estabelecidas em normas complementares."

[52] KUJAWSKI, Fábio Ferreira; CASTELLANO, Ana Carolina Heringer. Compartilhamento de dados pessoais no âmbito da administração Pública sob a égide da Lei Geral de Proteção de Dados. *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020, p. 321 *et set*.

[53] CAVALIERI, Davi Valdetaro Gomes. Governança de dados e programa de compliance digital na administração pública: contribuições da LGPD para a integridade governamental. *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020, p. 379.

# 4 CONSIDERAÇÕES FINAIS

Em linhas conclusivas, pode-se anotar que o propósito da edição de uma legislação especificamente voltada para a proteção de dados pessoais, no que concerne ao papel do Poder Público para a estipulação de medidas de governança de dados, é fruto de uma materialização transversal que visa mitigar riscos regulatórios.

A LGPD brasileira é o epítome de uma tendência há muito vislumbrada e que vem mobilizando o Estado, em todos os seus âmbitos, à edição de regramentos próprios e voltados às particularidades de suas esferas de atuação. Não por outra razão, a União editou o Decreto nº 9.203/2017 – analisado neste breve ensaio – bem antes da promulgação da própria LGPD e, avançando no tema, delineou sua política de governança de dados (Decretos nº 10.046 e 10.047 de 2019), ainda durante o período de *vacatio legis* da festejada norma.

Iniciativas dos estados e dos municípios já existem, como foi possível observar pelos exemplos do Estado de Pernambuco e do Município de São Paulo, tomados como objetos para análise mais detalhada das nuances próprias que essas normas apresentam em comparação à lei federal e, de plano, foram observados alguns pontos que merecem nota: (i) a cautela que estados e municípios deverão ter com a indicação de um encarregado (*data protection officer*) para que possam realizar o tratamento de dados pessoais e a possibilidades de que autoridades das esferas de controle interno assumam tal função; (ii) a estipulação de políticas claras para o compartilhamento de dados, inclusive em seus âmbitos internos; (iii) a imperiosidade de observância e respeito aos direitos do titular para que se proceda ao tratamento, com imprescindível obtenção do consentimento nas hipóteses elencadas na legislação federal (e reiteradas nas normas estaduais e municipais).

Pela proposta de averiguação indutiva, embora se tenha anunciado, desde o início, que o debate sobre a governança de dados dá a tônica de uma preocupação muito maior, foi possível constatar, pelo presente estudo, que há muitos outros desafios a se desvelar pela busca natural e incessante de parâmetros que vão além do direito, nessa estruturação de atividades em torno do *compliance*, e que visam à reinserção da ética nos afazeres de Estado. Espera-se que a LGPD – e os atos normativos nela inspirados – sejam sinais dessa inexorável mudança de paradigma.

# REFERÊNCIAS


ALVES, Fabrício da Mota. Estruturação do cargo de DPO em entes públicos. *In:* BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (Coords.). ***Data Protection Officer* (encarregado)**: teoria e prática de acordo com a LGPD e o GDPR. São Paulo: Thomson Reuters Brasil, 2020.

ARNAUD, André-Jean. ***La gouvernance***: *un outil de participation*. Paris: LGDJ, 2014.

AULICH, Chris; WETTENHALL, Roger; EVANS, Mark. *Understanding integrity in public administration: guest editors' introduction.* ***Policy Studies***. Oxfordshire, v. 33, n. 1, p. 1-5, jan. 2012.

BARBIERI, Carlos. **Governança de dados**. Rio de Janeiro: Alta Books, 2019, p. 35.

BENTO, Leonardo Valles. **Governança e governabilidade na reforma do estado**: entre a eficiência e a democratização. Barueri: Manole, 2003.

BINENBOJM, Gustavo. Art. 5º: Análise de Impacto Regulatório. *In:* MARQUES NETO, Floriano de Azevedo; RODRIGUES JÚNIOR, Otavio Luiz; LEONARDO, Rodrigo Xavier (Coords.). **Comentários à Lei da Liberdade Econômica (Lei 13.874/2019).** São Paulo: Thomson Reuters Brasil, 2019.

BRASIL. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm>. Acesso em: 15 set. de 2020.

_____.**Decreto nº 10.046, de 9 de outubro de 2019**. 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. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm>. Acesso em: 15 set. de 2020.

_____. **Decreto nº 10.047, de 9 de outubro de 2019**. Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10047.htm>. Acesso em: 15 set. de 2020.

_____. **Lei nº 13.709, de 14 de agosto de 2019**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 set. de 2020.

BREGA, José Fernando Ferreira. **Governo eletrônico e direito administrativo**. Brasília: Gazeta Jurídica, 2015.

CAIDEN, Gerald E. *The problem of ensuring the public accountability of public official. In:* JABBRA, Joseph G.; DWIVEDI, Onkar Prasad (Eds.). ***Public service accountability***: *a comparative perspective*. West Hartford: Kumarian, 1989.

CAILLOSSE, Jacques. ***Quel droit la gouvernance publique fabrique-t-elle?*** *Droit et Société*, Paris, v. 71, p. 461-470, 2009.

CASTRO, Rodrigo Pironti Aguirre de; GONÇALVES, Francine Silva Pacheco. ***Compliance* e gestão de riscos nas empresas estatais**. 2. ed. Belo Horizonte: Fórum, 2019.

CAVALIERI, Davi Valdetaro Gomes. Governança de dados e programa de compliance digital na administração pública: contribuições da LGPD para a integridade governamental. *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

COELHO, Cláudio Carneiro Bezerra Pinto. *Compliance* na Administração Pública: uma necessidade para o Brasil. **Revista de Direito da Faculdade Guanambi**, Guanambi, v. 3, n. 1, p. 75-95, jul./dez. 2016.

CRAVO, Daniela Copetti Cravo. Portabilidade de dados no poder público? **Jota.info**, 15 ago. 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/portabilidade-de-dados-no-poder-publico-15082020>. Acesso em: 19 set. de 2020.

CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de compliance. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coords.). ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

FALEIROS JÚNIOR, José Luiz de Moura. **Administração Pública digital**: proposições para o aperfeiçoamento do regime jurídico administrativo na sociedade da informação. Indaiatuba: Foco, 2020.

_____. Notas introdutórias ao *compliance* digital. *In:* CAMARGO, Coriolano Almeida; CRESPO, Marcelo; CUNHA, Liana; SANTOS; Cleórbete (Coords.). **Direito digital:** novas teses jurídicas. 2. ed. Rio de Janeiro: Lumen Juris, 2019.

FALEIROS JÚNIOR, José Luiz de Moura; MIGLIAVACCA, Viviane Furtado. A parametrização das políticas de compliance na Administração Pública: uma análise dos mecanismos de governança definidos pelo Decreto 9.203/2017. **Revista do Tribunal Regional Federal da 1ª Região**, Brasília, ano 32, n. 1, p. 56-70, jan./jun. 2020.

FERREIRA FILHO, Manoel Gonçalves. Corrupção e democracia. **Revista de Direito Administrativo**, Rio de Janeiro, v. 226, n. 4, p. 213-218, out./dez. 2001.

FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de compliance. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coords.). ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

GRÖNLUND, Åke; HORAN, Thomas A. *Introducing e-Gov*: *history, definitions, and issues. **Communications of the Association for Information Systems***, Nova York, v. 15, n. 39, p. 713-729, jan. 2004.

HANOFF, Roberta Volpato; NIELSEN, Thiago Henrique. A Lei Geral de Proteção de Dados Pessoais na administração pública brasileira: é possível implementar governança de dados antes de se implementar a governança em gestão? *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

KUJAWSKI, Fábio Ferreira; CASTELLANO, Ana Carolina Heringer. Compartilhamento de dados pessoais no âmbito da administração Pública sob a égide da Lei Geral de Proteção de Dados. *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a efetividade da Lei Geral de Proteção de Dados**: de acordo com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 e as alterações da Lei nº 13.853/2019), o Marco Civil da Internet (Lei nº 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). São Paulo: Almedina, 2020.

LONGHI, João Victor Rozatti. **Processo legislativo interativo**: interatividade e participação por meio das Tecnologias da Informação e Comunicação. Curitiba: Juruá, 2017.

MADDEN, M. Stuart. *Tort law through time and culture: themes of economic efficiency*. *In:* MADDEN, M. Stuart (Ed.). ***Exploring tort law***. Cambridge: Cambridge University Press, 2005.

MARCHESINI, Lucas. Governo falha e repassa auxílio emergencial a pessoas com mais de 10 CNPJs. **Metrópoles**, 11 jun. 2020. Disponível em: <https://www.metropoles.com/brasil/governo-falha-e-repassa-auxilio-emergencial-a-pessoas-com-mais-de-10-cnpjs>. Acesso em: 19 set. de 2020.

MARRARA, Thiago. Quem precisa de programas de integridade (compliance)? *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coords.). ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

MARTINS, Fernando Rodrigues. **Controle do patrimônio público**. 5. ed. São Paulo: Revista dos Tribunais, 2013.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança, boas práticas, governança e compliance. *In:* LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020.

MAXIMIANO, Antonio Cesar Amaru; NOHARA, Irene Patrícia. **Gestão pública**: abordagem integrada da administração e do direito administrativo. São Paulo: Atlas, 2017.

MESSA, Ana Flávia. **Transparência, compliance e práticas anticorrupção na Administração Pública**. São Paulo: Almedina, 2019.

MOREIRA NETO, Diogo de Figueiredo. **Curso de direito administrativo**. 16. ed. Rio de Janeiro: Forense, 2014.

MUNICÍPIO DE SÃO PAULO. **Decreto nº 59.767, de 15 de setembro de 2020**. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta. Disponível em: <http://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020>. Acesso em: 16 set. 2020.

NOHARA, Irene Patrícia. Autoridade Nacional de Proteção de Dados: reflexões funcionais sobre a natureza jurídica de órgão. *In:* RAIS, Diogo; PRADO FILHO, Francisco Octavio de Almeida (Coords.). **Direito público digital**: o Estado e as novas tecnologias; desafios e soluções. São Paulo: Thomson Reuters Brasil, 2020.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. ***Towards a sound integrity framework***: *instruments, processes, structures and conditions for implementation* OECD - Public Governance Committee, 2009. Disponível em: <http://www.oecd.org>. Acesso em: 18 set. de 2020.

OSBORNE, David; GAEBLER, Ted. ***Reinventing government***: *how the entrepreneurial spirit is transforming the public sector. Reading: Addison-Wesley*, 1992.

PÉREZ LUÑO, Antonio Enrique***. ¿Ciberciudadaní@ o cidadaní@.com****?* Barcelona: Gedisa, 2004.

PERNAMBUCO. **Decreto nº 49.265, de 6 de agosto de 2020**. Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). Disponível em: <https://legis.alepe.pe.gov.br/texto.aspx?id=51399>. Acesso em: 16 set. de 2020.

PETERS, B. Guy; PIERRE, Jon. *Governance without government? Rethinking public administration*. ***Journal of Public Administration Research Theory***, Oxford, v. 8, n. 2, p. 223-243, abr. 1998.

RODRÍGUEZ-ARANA MUÑOZ, Jaime. *El derecho fundamental a la buena administración en la constitución española y en la Unión Europea*. ***Revista Eurolatinoamericana de Derecho Administrativo.*** Santa Fe, v. I, n. 2, jul./dez. 2014.

SIMONSEN, Ricardo. Os requisitos de um bom programa de compliance. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Coords.). ***Compliance*****:** perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

STIVERS, Camilla. *The listening bureaucrat: responsiveness in public administration*. ***Public Administration Review***, Nova Jersey, v. 54, n. 4, p. 364-369, jul./ago. 1994.

STUCKE, Maurice E.; GRUNES, Allen P**.** ***Big Data and competition policy***. Oxford: Oxford University Press, 2016.

VOIGT, Paul; VON DEM BUSSCHE, Axel. ***The EU General Data Protection*** **Regulation (GDPR)**: a practical guide. Basileia: Springer, 2017.

# O RECONHECIMENTO FACIAL NO SETOR PÚBLICO E A PROTEÇÃO DE DADOS PESSOAIS

Fabiano Menke[1]
Sílvia Levenfus[2]

## 1 INTRODUÇÃO

Reconhecidas distopias[3] já retrataram o totalitarismo estatal, a vigilância massiva dos cidadãos e a ausência de liberdade. O exemplo da cidade de Londres, nos dias de hoje, reflete as possibilidades que se colocam para os governos: cerca de 500.000 câmeras, posicionadas nas ruas e nas estações de metrô, realizam o monitoramento contínuo dos transeuntes. Quem se locomove, naquela cidade, tem a sua imagem captada, em média, 300 vezes ao dia.[4]

O processamento de dados pessoais dessa magnitude suscita a questão da possível imposição de limites aos meios empregados para as finalidades perseguidas, não só pela municipalidade de Londres, que é apenas um exemplo de incontáveis casos espalhados pelo mundo.

Nos Estados Unidos da América, por exemplo, algumas municipalidades proibiram ou impuseram severas restrições à utilização do reconhecimento facial. São os casos de Boston, São Francisco, Oakland e Portland.[5]

Há que se recordar, nesse contexto, todo o debate e os desdobramentos da Lei do Censo alemã (*Volkszählungsgesetz*), de 1982, que foi contestada pela população por meio de reclamações constitucionais aviadas por associações[6], e

---

[1] Professor da Graduação e da Pós-Graduação da Faculdade de Direito da UFRGS. Mestre pelo Programa de Pós-Graduação em Direito da UFRGS. Doutor em Direito pela Universidade de Kassel, Alemanha. Advogado. TCE/RS - Webconferência: Lei Geral de Proteção de Dados e o Poder Público - Mesa 1. Disponível em <https://www.youtube.com/watch?v=z3xCD-rK0tE>. Acesso em: 19 set. de 2020.

[2] Mestranda em Direito Privado no Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul - UFRGS.

[3] Exemplifica-se com 1984, de George Orwell, e Admirável Mundo Novo, de Aldoux Huxley.

[4] COESTER, Ulla. FUHLERT, Bernd. *Gesichtserkennung - eine Frage der Ethik?* ***Datenschutz und Datensicherheit (DuD),*** Vol. 1, 2020, p. 50.

[5] Ver em: <https://cities-today.com/portland-bans-private-companies-from-using-facial-recognition-technology/> Acesso em: 20 set. de 2020.

[6] SIMITIS, Spiros. *Die informationelle Selbstbestimmung: Grundbedingung einer verfassungskonformen Informationsordnung.* ***Neue Juristische Wochenschrift,*** 1984, v. 8, p. 394-405.

acabou por gerar, no ano seguinte, a emblemática decisão que criou o direito à autodeterminação informativa.[7] Ainda que inaugurado esse reconhecimento pela via jurisprudencial, com base em dispositivos constitucionais no âmbito do direito alemão[8] , o seu desenvolvimento influenciou diversos países na área da proteção de dados, valendo mencionar a Lei Geral de Proteção de Dados do Brasil (LGPD - Lei nº 13.709/2018), que ergueu a autodeterminação informativa como fundamento da disciplina da proteção de dados pessoais (art. 2º, II), bem como o julgamento da ADI 6.387, pelo Supremo Tribunal Federal, no qual houve o reconhecimento da natureza de direito fundamental da proteção de dados.

Como bem refere a sentença[9] , o processamento eletrônico de dados[10] pode acarretar a ausência de controle do indivíduo acerca da exatidão e do uso das informações relacionadas à sua pessoa, o que justifica um reforço da tutela no âmbito do tratamento de dados pessoais, observada a ideia de autodeterminação individual, em consonância com o livre desenvolvimento da personalidade.[11] Portanto, a autodeterminação está embasada em uma liberdade de o indivíduo

---

[7] Ver sobre em: MARTINS. Leonardo. **Tribunal Constitucional Federal Alemão**: decisões anotadas sobre direitos fundamentais**.** Vol. 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS. 2016; SCHWABE, J. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. MARTINS, Leonardo; HENNIG, Beatriz *et al* (trad). Uruguai: Konrad-Adenauer Stiftung – KAS 2005.
O conceito de autodeterminação informativa tem relação intrínseca com a privacidade, muito embora, nos dias de hoje, a autodeterminação informativa e a proteção de dados tenham adquirido um *status* autônomo. É importante relembrar que a preocupação com o advento de novas tecnologias e a proteção da privacidade não é recente. Ver sobre em: WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, Vol. 4, N. 5, p.193-220, 1890; SIMITIS, Spiros*. Reviewing Privacy in information Society**. University of Pennsylvania Law Review***. v.135. n. 3, p. 707-746, 1987; RODOTÁ, Stefano. **A vida na sociedade da vigilância***:* a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[8] O direito à autodeterminação informativa foi fundamentado pela corte alemã no art. 1º, alínea 1 (dignidade da pessoa humana), em combinação com o art. 2º, alínea 1 (livre desdobramento da personalidade), ambos da Lei Fundamental.

[9] Destaca-se que, antes desta decisão, em 1981, foi publicada a Convenção nº 108, do Conselho da Europa, primeiro instrumento europeu de proteção de dados focado na tutela dos titulares de dados em relação ao processamento automático de dados pessoais.

[10] O que inclui diversos dados, inclusive específicos, sobre uma pessoa determinada ou determinável, armazenados e passíveis de serem acessados rapidamente, a todo o momento e independentemente da distância e de serem combinados com bancos de dados e transformar aquelas informações em um “quadro” da personalidade.

[11] MARTINS. Leonardo**. Tribunal Constitucional Federal Alemão**: decisões anotadas sobre direitos fundamentais**.** Vol. 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS. 2016, p. 57-58.

desdobrar a sua personalidade[12], projetando-a em suas ações e, para que esse objetivo seja atingido, há que estar protegido contra um irrestrito levantamento, armazenamento, uso e transmissão dos dados relacionados a sua pessoa.[13]

Nesse contexto, se questiona até que ponto o processamento de dados determina uma sociedade democrática[14], posto que haja riscos, como a rotulagem de indivíduos, erros, manipulação nos dados, e o consequente aumento do controle social.[15] Assim, o debate atual não se pauta somente na liberdade de fornecimento ou não de dados pessoais, como no caso do referido censo alemão, mas, também, até que ponto as informações acerca do próprio corpo podem ser disponibilizadas. Como aduz Rodotá, o corpo está se tornando "objeto de um continuo *data mining*, efetivamente uma mina a céu aberto da qual é possível extrair dados ininterruptamente. Repetimos: o corpo, em si, está se tornando uma *password".*[16]

Tendo em vista o aprimoramento das tecnologias e as suas consequentes novas aplicações, como a utilização da biometria e do reconhecimento facial, é certa a necessidade de um olhar atento sobre o tema. Isso porque é indubitável que o advento desses progressos da técnica pode conflitar, diretamente, com a autodeterminação informativa, posto que seja possível a coleta de informações de forma não transparente[17] e, consequentemente, sem o conhecimento do titular, muito menos consentimento.

Portanto, resta identificar em que medida esta tecnologia permite (ou não) o exercício da autodeterminação informativa dos indivíduos. Para tanto, o presente estudo foca a sua análise na utilização do reconhecimento facial pelo poder público

---

[12] Sobre a autodeterminação informativa e o aspecto do desdobramento da personalidade, ver MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*. In*. MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, Inovação e Tecnologia**. V. 1. São Paulo: Saraiva, 2015, p. 205-230.

[13] MARTINS. Leonardo. **Tribunal Constitucional Federal Alemão**: decisões anotadas sobre direitos fundamentais**.** Vol. 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS. 2016, p. 58.

[14] SIMITIS, Spiros. *Reviewing Privacy in an information Society***. *University of Pennsylvania Law Review.*** v.135. n. 3, p. 707-746, 1987, p. 746.

[15] Ver mais sobre Big Data em: MAYER- SCHONBERGER, Viktor; CUKIER, Kenneth. ***Big Data****:* como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana*.* Trad: Paulo Polzonoff Junior. 1. ed. Rio de Janeiro: Elsevier, 2013.

[16] RODOTÁ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 265

[17] LI, Stan Z; JAIN, Anil K (Eds). **Handbook of Face Recognition**. 2. ed. New York: Springer Verlag London Limited, 2011, p. 1.

brasileiro. Tem-se como ponto de partida uma breve análise sobre o reconhecimento facial e o seu enquadramento na Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), e, após, um exame sobre a implantação da tecnologia pelo poder público no Brasil, apresentando-se alguns casos e os desafios envolvidos.

## 2 O RECONHECIMENTO FACIAL E O SEU ENQUADRAMENTO NA LGPD

Para que seja realizada uma melhor análise sobre o reconhecimento facial, no setor público brasileiro, parte-se de sucintas considerações históricas da disciplina da proteção de dados no Brasil.

Primeiramente, destaca-se que inexistia, até a edição da LGPD, regramento sobre proteção de dados pessoais previsto em uma normativa específica acerca da temática, de corte transversal sobre todas as áreas. Em relação ao quadro constitucional, observa-se a garantia à inviolabilidade da intimidade, da vida privada, da honra e da imagem. Ademais, em relação à informação, a Carta Magna garante o direito à informação e, também, à liberdade de expressão, tendo em vista que pode vir a confrontar com a proteção da personalidade, especificamente a privacidade. O *habeas data*, inclusive, é ação criada que visa a assegurar o conhecimento de informações e também retificação de dados pessoais.[18]

Observa-se que já havia normas setoriais que tratavam sobre proteção de dados, tais como o Código de Defesa do Consumidor (CDC – Lei nº 8.078/1990), a Lei do Cadastro Positivo (LCP – Lei nº 12.414/2011), a Lei de Acesso à Informação (LAI - Lei nº 12.527/2011) e o Marco Civil da Internet ( MCI – Lei nº12.965/2014). Entretanto, inexistia, até então, uma norma passível de aplicação a todos os setores privados e públicos, caso da LGPD, que por ter essa característica é denominada de "lei geral".[19]

Ainda que a LGPD não seja o ato normativo que inaugure o tratamento da disciplina da proteção de dados pessoais no país, o advento da lei permite uma consolidação dos valores e princípios já existentes, sobretudo possibilitando uma tutela lícita, efetiva e clara, em relação às atividades de tratamento de dados

[18] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico**. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011, p. 103-104.
[19] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, Brasília, v. 120/2018, nov./dez. 2018, p. 26.

pessoais[20]. Ademais, permite garantias no que diz respeito ao uso dos dados relacionados aos cidadãos. Trata-se de um considerável incremento nos mecanismos que são colocados à disposição dos titulares de dados para a tutela de sua personalidade e exercício de seus direitos, de modo que passem a, efetivamente, decidir acerca dos dados que lhes digam respeito, em consonância com a autodeterminação informativa, cunhada conceitualmente pela Corte Constitucional alemã.[21]

Não é a toa que, consoante salientado, a LGPD estabelece, como um de seus fundamentos - especificamente no art. 2º, II[22]; a autodeterminação informativa. É importante para o presente estudo destacar, também, que a legislação tem como fundamentos: (I) o respeito à privacidade; (III) a liberdade de expressão, de informação, de comunicação e de opinião; (IV) a inviolabilidade da intimidade, da honra e da imagem; (V) o desenvolvimento econômico e tecnológico e a inovação; (VI) a livre-iniciativa, a livre concorrência e a defesa do consumidor e; (VII) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Conforme se depreende de seus fundamentos, a LGPD busca encontrar um ponto de equilíbrio entre o fluxo dos dados pessoais e a proteção da personalidade do indivíduo. Nessa ordem de ideias, deve ser analisado esse marco legal para a finalidade de perquirir acerca do enquadramento do reconhecimento facial no conjunto de suas regras. Antes disso, examine-se no que consiste o reconhecimento facial.

## 2.1 DELINEAMENTOS CONCEITUAIS ACERCA DO RECONHECIMENTO FACIAL

Como antecedente da biometria, da forma como hoje é conhecida, a ciência do direito e a técnica se debruçaram sobre o uso da imagem em conjunto com a tecnologia.

---

[20] DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. *In*: **Lei Geral de Proteção de Dados (Lei nº 13.709/2018):** a caminho da efetividade: contribuições para a implementação da LGPD. CUEVA, Ricardo Villas Bôas; DONEDA, Danilo, MENDES, Laura Schertel (coord.). 1. ed. São Paulo : Thomson Reuters Brasil, 2020. *Ebook.*

[21] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, Brasília, v. 120/2018, p. 555-587, nov./dez. 2018, p. 25-26.

[22] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] II - a autodeterminação informativa [...]".

Desde 1890, Warren e Brandeis[23] já referiam que as novas invenções da época necessitavam um olhar voltado à proteção da pessoa e à sua individualidade - o que o Juiz Colley referiu como o direito de estar só; posto que estes adventos tecnológicos, como a fotografia e os jornais, estavam invadindo os recintos da vida privada e doméstica.[24] Essas novas formas de comunicação do século XIX, igualmente, estavam provocando um fenômeno denominado "*ubiquitous incorporeal replicas*"[25], que seria a criação de um homólogo humano dissociado do corpo.[26]

Portanto, o surgimento das técnicas biométricas - tais como a impressão digital, a leitura da íris e o reconhecimento de voz, assim como o reconhecimento facial, objetivava sanar a preocupação das "sociedades desencarnadas" e, justamente, permitir uma conexão da identidade ao corpo.[27] Assim, as espécies de tecnologias biométricas teriam sido justamente arquitetadas para sanar os problemas relativos à identificação que foram surgindo e, permitir assim, uma conexão imediata do corpo com a identidade.[28]

Contudo, por óbvio que a identificação biométrica não pode ser entendida apenas como imposição de identificação, mas também visa a atender outras demandas e necessidades da sociedade.[29] Cita-se o exemplo do denominado conforto, ou comodidade, para usuários de aplicativos, no âmbito público ou privado, que têm os seus esforços diminuídos, quando utilizam o reconhecimento facial como mecanismo de identificação, ao invés de terem que lembrar e digitar uma senha.[30]

Consoante recente definição brasileira, a biometria é considerada como a "verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de meios automatizados".[31]

Na área de segurança da informação, faz parte do jargão corrente a utilização das figuras dos três fatores de autenticação: "ter", "saber" e "ser", no que diz respeito

---

[23] WARREN, Samuel D; BRANDEIS, Louis D. *The Right to Privacy. Harvard Law Review,* Vol. 4, N. 5, p.193-220, 1890, p. 197. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 22 jul.de 2020.
[24] *Idem,* p. 195.
[25] Tradução livre: "réplicas incorpóreas onipresentes".
[26] GATES, Kelly A. ***Our Biometric Future****: Facial Recognition Technology and the Culture of Surveillance.* New York: New York University Press, 2011, p. 12.
[27] *Idem Ibidem*.
[28] *Idem*, p. 14.
[29] *Idem Ibidem.*
[30] COESTER, Ulla. FUHLERT, Bernd. *Gesichtserkennung - eine Frage der Ethik?* ***Datenschutz und Datensicherheit (DuD)***, Vol. 1, 2020, p. 48.
[31] BRASIL. **Portaria nº 93 de 26 de setembro de 2019***.* Aprova o Glossário de Segurança da Informação. Disponível em: <http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 21 Ago.de 2020.

aos mecanismos de identificação que possam ser empregados. O "ter", no sentido de possuir, pode ser implementado a partir de um dispositivo, como um cartão inteligente, que seja atribuído, exclusivamente, ao sujeito que se pretenda identificar. Os métodos baseados no "saber", como as senhas, estribam-se numa informação de conhecimento reservado do usuário. E, por fim, o "ser", corresponde a uma característica ou atributo associado ao próprio corpo ou comportamento da pessoa. É nessa última modalidade que se encontra a biometria e o reconhecimento facial.

Em relação ao reconhecimento facial, questionam-se quais seriam os seus diferenciais, quando comparado com outras tecnologias biométricas.[32] Diferentemente de outras modalidades, essa não é intrusiva[33], visto que a sua captação é à distância e, também, pode ser realizada de forma encoberta.[34]

É possível dividir o reconhecimento facial em duas categorias, tendo a clareza de que a sua utilização pode incluir ambas, a depender do caso. Estas seriam: (i) verificação facial (ou autenticação) e (ii) identificação facial (ou reconhecimento). A primeira engloba a compatibilidade de um para um ("*one-to-one match*"[35]), em que uma imagem facial é comparada com outra que está sendo reivindicada. Exemplos típicos: a verificação para a imigração usando o *E-passport*[36] e o desbloqueio do celular por meio da verificação do usuário.[37] Enquanto que, na segunda categoria, há a correspondência não de um para um, mas de um para vários ("*one-to-many matching*"[38]), em que se compara uma face de consulta com múltiplos rostos de bancos de dados.[39] Elucida-se com a utilização policial para a identificação de suspeitos e pessoas desaparecidas.[40]

Em um estudo realizado por Huang, Xiong e Zhang, com algoritmos de reconhecimento facial de 10 sistemas comerciais, foram elencadas, em rol exemplificativo, categorias de aplicações dessa tecnologia: identificação facial,

---

[32] GATES, *op. cit.*, 2011, p. 44.
[33] Nesse mesmo sentido: "*As one of the most nonintrusive biometrics* [...]".HUANG, Thomas; XIONG, Ziyou; ZHANG, Zhenqiu. Face Recognition Applications. *In*: LI, Stan; JAIN, Anil K (Eds.). ***Handbook os Face Recognition.*** 2. ed. London: Springer, 2011. p. 618.
[34] LI, Stan Z; JAIN, Anil K (Eds). ***Handbook of Face Recognition***. 2. ed. New York: Springer Verlag London Limited, 2011, p. 1.
[35] *Idem*, p. 2.
[36] *Idem*, p. 2-3.
[37] BOUCHER, Philip Nicholas. ***Artificial intelligence:*** *How does it work, why does it matter, and what can we do about it?* Brussels: European Parliment, 2020, p. 24.
[38] LI *et al., op. cit.*, 2011, p. 3.
[39] *Idem Ibidem.*
[40] BOUCHER, *op. cit.*, 2020, p. 24.

controle de acesso, segurança, cartões inteligentes, aplicações legais, bancos de dados de faces, gestão multimídia, interação humano-computador e outros.[41]

No âmbito público, o reconhecimento facial permite, aos governos, não só observar ações em espaços públicos, como também gravar essas imagens e utilizá-las conforme a necessidade escolhida. Essa vigilância massiva, que não requer suspeita de algum indivíduo específico para ocorrer, ainda é gratuita e produz muito conhecimento em forma de *terabytes*.[42]

Observa-se, a seguir, em que medida tal tecnologia é passível de ser enquadrada no ordenamento jurídico nacional, especificamente no que diz respeito ao setor público.

## 2.2 ENQUADRAMENTO NA LGPD

Delineadas essas breves considerações, sobre a tecnologia do reconhecimento facial, cabe analisar o seu enquadramento na legislação brasileira, relacionada à matéria, mais precisamente na LGPD.

Antes, contudo, é preciso observar o que o Regulamento Geral de Proteção de Dados europeu (GDPR- 2016/679), que se encontra na tradição europeia acerca da matéria, tradição essa que em certa medida influenciou a LGPD, contempla disciplina sobre o assunto. No Art. 4º do GDPR, são elencadas definições de termos utilizados pela normativa. Observa-se, no referido artigo, o conceito de dado biométrico[43], que prevê o tratamento dos dados, por meio de imagens faciais ou dados datiloscópicos, e que permita ou confirme a identidade de uma pessoa.

Diferentemente, salienta-se que o Art. 5º, II[44], da LGPD, conceitua dado pessoal sensível, contemplando a biometria.[45] O Art. 11 determina, em rol exaustivo,

---

[41] HUANG, Thomas; XIONG, Ziyou; ZHANG, Zhenqiu. *Face Recognition Applications*. In: LI, Stan; JAIN, Anil K (Eds.). ***Handbook os Face Recognition***. 2. ed. London: Springer, 2011, p. 618.

[42] DONOHUE, Laura K.. *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age.* ***Georgetown Law Faculty Publications and Other Works****, p.* 409. Disponível em: <https://scholarship.law.georgetown.edu/facpub/1036>. Acesso em: 23 jul, de 2020.

[43] "Dados biométricos: dados pessoais resultantes de um tratamento técnico específico, relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;".

[44] "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".

[45] O legislador europeu optou por não definir expressamente o significado de dado pessoal sensível, referindo-os como categoria especial de dado pessoal: "(10) [...] O presente regulamento também dá

as possibilidades para o tratamento desses dados. Em regra, somente poderão ser tratados quando o titular ou o seu responsável consentir, de forma específica e destacada, para finalidades específicas.[46] Caso contrário, o inciso II, do referido artigo, enumera as exceções - igualmente taxativas, para a desnecessidade de consentimento[47], tais como quando o dado seja necessário para estudos por órgãos de pesquisa e para o exercício regular de direitos.

É o termo 'dado biométrico' que será fundamental para desenvolver as reflexões que se propõe. Isso porque, apesar de a LGPD não estabelecer a definição de dado biométrico, ao contrário do GDPR, é possível uma compreensão integrativa de ambas as legislações e, também, do entendimento (já mencionado) acerca da definição deste.

Tendo em vista que a biometria é dado sensível, pela definição da LGPD, o reconhecimento facial se enquadra nesta categoria de dados pessoais. Fixada essa premissa, conforme a LGPD, há hipóteses determinadas em que é permitido o tratamento de dados pessoais sensíveis, sem que se faça necessária a obtenção do consentimento. Tais hipóteses se dão de forma justificada, com o intuito de assegurar que a proteção do titular seja efetiva e garanta ao máximo a tutela destes dados, cujo conteúdo é mais sensível.

Nesse sentido, cumpre a análise da possibilidade de o poder público tratar dados sensíveis, o que se torna possível a partir de autorizações dispersas na LGPD, demandando uma análise conjunta de dispositivos.

---

aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»)".

[46] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas".

[47] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; ou f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

# 3 IMPLEMENTAÇÃO DO RECONHECIMENTO FACIAL NO PODER PÚBLICO BRASILEIRO

Como decorrência lógica do estudo que ora se propõe, necessário se faz adentrar no tema do poder público, frente ao reconhecimento facial. Dessa forma, observa-se, a seguir, como se dá o seu papel diante das regras da LGPD.

Primeiramente, cumpre ressaltar que a LGPD não se aplica ao tratamento de dados pessoais, quando este for realizado exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.[48] Ademais, a Lei prevê que, para o tratamento com estes propósitos será elaborada legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público.[49] Outrossim, como regra geral, a exceção da segurança pública não é aplicável às pessoas jurídicas de direito privado[50] que prestam serviços de segurança privada.[51]

Ressalte-se que a LGPD dedica um capítulo exclusivo para abordar o tratamento de dados pessoais pelo poder público. Assim, determina que o tratamento pelas pessoas jurídicas de direito público tem de atender à finalidade pública e ao interesse público[52], com transparência da finalidade, dos procedimentos e práticas empreendidas para o tratamento.[53] A segunda

[48] "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: 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."

[49] "Art. 4º, III, §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."

[50] "Art. 4º, III, §2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo".

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

[52] "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 [...]".

[53] "Art. 23, 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".

condicionante da LGPD para o tratamento de dados pessoais pelo poder público é a da indicação de um encarregado.[54]

Além disso, na Seção II do Capítulo II da LGPD, que disciplina o tratamento de dados pessoais sensíveis (caso dos dados biométricos, como visto), estão previstas, no inciso II do art. 11, as hipóteses em que o tratamento desses dados poderá ocorrer sem o fornecimento de consentimento pelo titular.[55] Dentre as possibilidades, figura a que permite o tratamento dos dados pessoais sensíveis, desde que seja indispensável para o "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos" (alínea b).

Outra possibilidade de dispensa do consentimento, e de grande relevância para os sistemas de reconhecimento facial, é a da alínea "g", do inciso II do art. 11 da LGPD, sempre que o tratamento do dado sensível for indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro, em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD[57] e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular, que exijam a proteção dos dados pessoais.

Todavia, ainda que seja dispensável o consentimento para o tratamento dos dados sensíveis, nesta hipótese, é necessário que seja dada publicidade à dispensa de consentimento.[58] Mas, como determina o §6º[59], do art. 7º, ainda que haja a dispensa de consentimento em determinados casos, tal não desincumbe o agente

---

[54] "Art. 23, III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;".

[55] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;".

[56] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

[57] "Art. 11 § 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do *caput* deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do *caput* do art. 23 desta Lei".

[58] "Art. 7, § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular".

de tratamento de cumprir com suas as obrigações, observar princípios e preservar os direitos do titular.

Portanto, depreende-se que o poder público está autorizado, de certa forma, a utilizar a biometria e, por consequência, o reconhecimento facial, por meio da leitura conjunta de dispositivos esparsos na lei. Em síntese, estes, então, seriam; (i) a autorização geral de tratamento de dados pelo poder público, desde que respeitadas as condicionantes do art. 23 da LGPD; (ii) a dispensa de consentimento para o tratamento compartilhado de dados sensíveis pela administração pública quando essencial para a execução de políticas públicas[59]; (iii) a dispensa de consentimento nos casos em que seja indispensável para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Expostas as regras que dispõem acerca das permissões para o tratamento de dados pessoais e sensíveis pelo poder público, calha a análise de exemplos e desafios, da aplicação do reconhecimento facial por parte deste setor.

## 3.1 UTILIZAÇÃO NA SEGURANÇA PÚBLICA E NO CONTROLE DOS ADMINISTRADOS

A utilização do reconhecimento facial, no Brasil, não é algo que se cogite como uma realização para o futuro: pelo contrário, já se trata de realidade em alguns contextos. É possível observar aplicações desta tecnologia, no setor público brasileiro, valendo-se aqui dos exemplos de utilização para o combate de fraudes e para controle dos administrados, assim como para fins de segurança pública. A seguir, destacam-se alguns exemplos.

No que tange à utilização da tecnologia para evitar fraudes no transporte público, desde 2017, Porto Alegre conta com câmeras com reconhecimento facial nas frotas de ônibus.[60] Curitiba passou a contar com uma nova frota de ônibus, com

[59] Art. 11, II, b), da LGPD.

[60] PORTO ALEGRE. **Decreto nº 19. 836, de 22 de setembro de 2017**. Estabelece prazos e critérios gerais no Sistema de Transporte Coletivo por Ônibus para a implantação do reconhecimento facial no Sistema de Bilhetagem Eletrônica (SBE), de equipamentos e serviços de posicionamento global (GPS) e de câmeras de segurança (CFTV) do Sistema de Supervisão e Controle Operacional (SSCO) e do Serviço de Informação ao Usuário (SIU), e dispõe sobre os equipamentos de ar condicionado nos ônibus. Porto Alegre: Prefeitura Municipal de Porto Alegre, 2017. Disponível em: <http://dopaonlineupload.procempa.com.br/dopaonlineupload/2230_ce_20170922_executivo.pdf>. Acesso em: 03 ago. de 2020.

funcionalidades e inovações tecnológicas, dentre elas a biometria facial, cujo intuito é a prevenção de fraudes no uso de cartões de estudantes, isentos, idosos e portadores de necessidades especiais.[61]

Ainda, no que diz respeito ao controle do administrado, cabe mencionar o emprego do reconhecimento facial, desde 2016, pela Receita Federal, para o controle de viajantes brasileiros que retornam ao país. De acordo com as informações do órgão, ao lançar o sistema, a funcionalidade visa a trazer maior agilidade no atendimento ao viajante, uma vez que o controle recai preferencialmente sobre passageiros que apresentem risco potencial de apresentar irregularidades aduaneiras ou o cometimento de outras infrações, inclusive penais.[62]

Ademais, destaca-se a recente aplicação da tecnologia pelo Tribunal de Justiça do Distrito Federal e dos Territórios, aos visitantes que adentram no local. Ao entrar nas dependências do tribunal, o sujeito se apresenta à recepção, é tirada uma foto sua e comparada no sistema, verificando se já há cadastro registrado. Assim, é possível identificar possíveis fraudes de identidade. De acordo com o tribunal, o sistema, denominado AMON, permite mais segurança aos membros do local, assim como um maior controle sobre quem entra.[63]

Quanto à segurança pública, destaca-se que, na Bahia, no final de 2018, foi lançado um sistema de reconhecimento facial, com o objetivo de identificar pessoas foragidas e desaparecidas. A tecnologia compara imagens de pessoas que circularam na área de monitoramento das câmeras, com reconhecimento facial, com o banco de dados da Secretaria da Segurança Pública (SSP). Na primeira vez da utilização do sistema, no carnaval baiano, no ano seguinte, foi flagrado, por um dos portais de abordagens da Secretaria da Segurança Pública (SSP), um criminoso que

---

[61] PREFEITURA MUNICIPAL DE CURITIBA. **Prefeitura supera meta e alcança a marca recorde de 514 novos ônibus**. Disponível em: <https://www.curitiba.pr.gov.br/noticias/prefeitura-supera-meta-e-alcanca-a-marca-recorde-de-514-novos-onibus/55719>. Acesso em: 04 ago.de 2020.

[62] Ver em <https://receita.economia.gov.br/noticias/ascom/2016/agosto/receita-federal-apresentou-hoje-1-8-em-coletiva-de-imprensa-detalhes-sobre-o-novo-sistema-de-reconhecimento-facial-1>. Acesso em: 07 out. de 2020. Notem-se os cinco passos do controle da Receita Federal, consoante as informações da notícia: 1. Ao fazer o check-in no exterior os dados do passageiro são coletados; 2. Após a decolagem, ocorre a transmissão de dados para a Receita Federal; 3. O sistema de gerenciamento de risco da Receita Federal analisa perfis e padrões dos viajantes; 4. Na chegada, determinados passageiros previamente selecionados são identificados com o uso do reconhecimento facial; 5. Após a identificação, os passageiros selecionados são encaminhados para a verificação aduaneira pela Receita Federal.

[63] TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. **TJDFT aprimora segurança com implantação de sistema de reconhecimento facial para controle de acesso de visitantes**. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/junho/tjdft-aprimora-seguranca-com-implantacao-de-sistema-de-reconhecimento-facial-para-controle-de-acesso-de-visitantes>. Acesso em: 09 nov. de 2020.

estava com mandado de prisão expedido.[64] Em março de 2020, o Estado já havia localizado e prendido 189 foragidos em virtude da utilização dessa tecnologia.[65]

Igualmente, a Secretaria da Segurança Pública e Defesa Social do Estado do Ceará (SSPDS/CE) está utilizando a tecnologia do reconhecimento facial para a segurança pública, ao fazer o cruzamento da foto de suspeitos com um banco de imagens[66] , assim como o Rio de Janeiro. Esse estado da federação, recentemente, lançou o uso de uma nova tecnologia de patrulhamento, em que os agentes policiais fazem uso de câmeras individuais instaladas no uniforme, com o intuito de monitorar ações policiais, placas de automóveis e fazer uso do reconhecimento facial. O intuito é que as imagens sejam captadas simultaneamente, auxiliando na identificação de veículos roubados e criminosos foragidos, e serão cedidas, por meio de um convênio, ao Ministério da Justiça.[66]

Salienta-se que, nos casos de prevenção às fraudes, as modalidades de reconhecimento facial empreendidas compreendem a biometria do tipo "*one-to-one matching*". Já nas hipóteses de segurança pública e de controle do administrado, cuida-se da modalidade "*one-to-many matching*". Outrossim, percebe-se que, nas hipóteses de controle do administrado, aplica-se a LGPD, enquanto que, nos outros exemplos mencionados, incide a exceção de aplicação do art. 4º, III, a), da LGPD, posto que se trate de segurança pública, defesa nacional e segurança do Estado ou atividades de investigação e repressão de infrações penais. No caso do reconhecimento facial da Receita Federal, ocorre a incidência da LGPD no que diz respeito ao controle das infrações aduaneiras e a sua não incidência quando a tecnologia é utilizada para fins de segurança pública.

---

[64] GOVERNO DO ESTADO DA BAHIA**. Reconhecimento Facial impede entrada de homicida em circuito.** Secretaria da Segurança Pública. SSP/BA. Disponível em: <http://www. ssp.ba.gov.br/2019/03/5310/Reconhecimento-facial-impede-entrada-de-homicida-emcircuito-.html>. Acesso em: 06 jul. de 2020.

[65] GOVERNO DO ESTADO DA BAHIA. **Procurado por roubo é o 189° preso via Reconhecimento Facial.** Secretaria da Segurança Pública. SSP/BA. Disponível em: <http://www.ssp.ba.gov.br/2020/03/7423/Procurado-por-roubo-e-o-189o-preso-via-Reconhecimento-Facial.html>. Acesso em: 06 jul. de 2020.

[66] GOVERNO DO ESTADO DO CEARÁ. **Suspeito de roubar farmácia é preso pela Polícia Civil com auxílio do reconhecimento facial**. Secretaria da Segurança Pública e Defesa Social (SSPDS/CE). Disponível em: <https://www.sspds.ce.gov.br/2020/04/29/suspeito-de-roubar-farmacia-e-preso-pela-policia-civil-com-auxilio-do-reconhecimento-facial/>. Acesso em: 04 ago. de 2020.

[67] PREFEITURA DA CIDADE DO RIO DE JANEIRO. **Município estende Rio+Seguro à Zona Oeste com câmeras de reconhecimento facial.** Disponível em: <https://prefeitura.rio/cidade/municipio-estende-rioseguro-a-zona-oeste-com-cameras-de-reconhecimento-facial/>. Acesso em: 04 ago. de 2020.

## 3.2 DESAFIOS E RISCOS

Não há alternativa senão a de discutir, também, os riscos e os desafios advindos do uso do reconhecimento facial. É imprescindível ter a clareza de que, apesar de os dados biométricos possibilitarem novos mecanismos na implementação de medidas de segurança, facilitarem atividades rotineiras, permitirem identificar e verificar com mais acerto a identidade - inclusive em investigações, há que se pensar acerca da precisão desta técnica, posto que possam haver percentuais altos de erros. Tal ocorre principalmente em virtude da experimentação ou pelo contexto em que é utilizada a tecnologia.[68]

Apesar do sucesso de utilização nos casos de segurança pública mencionados, nem sempre ocorrerá o tão almejado objetivo pretendido. Em estudo realizado por pesquisadores do MIT (*Massachusetts Institute of Technology*) e da *Microsoft*, para descobrir a precisão dos classificadores de gêneros da IBM, da *Microsoft* e do *Face*++, constatou-se que a acurácia, na identificação, é mais alta em indivíduos de cor clara e, também, do sexo masculino, e a precisão é menor em mulheres afrodescendentes.[69]

Ainda, o NIST (*National Institute os Standards and Technology*) realizou pesquisas sobre as consequências do reconhecimento facial.[70] Em um trabalho sobre se as diferenças demográficas teriam influência no reconhecimento do rosto[71], descobriu-se que os diferenciais de falsos positivos[72] eram bem maiores do que os de falsos negativos.[73] A pesquisa exemplifica com o uso de uma verificação para aplicativo: o falso negativo pode impedir o desbloqueio do celular do usuário, a sua entrada em uma instalação, ou para atravessar uma fronteira. Tal pode ser resolvido

---

[68] RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

[69] BOULAMWINI, Joy; GEBRU, Timnit. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification***.** *Proceedings of Machine Learning Research 81.* ***Conference on Fairness, Accountability, and Transparency***, 2018, p. 1-15. Disponível em: <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em: 14 ago. de 2020. Ver mais em: <http://gendershades.org/>. Acesso em: 14 ago. de 2020.

[70] Ver mais em: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt>. Acesso em: 14 ago. de 2020.

[71] A base de dados utilizada era de fotografias coletadas pelo governo americano, tais como fotos de viajantes que cruzam a fronteira e de candidatos ao benefício de imigração e visto - ***NIST. Face Recognition Vendor Test (FRVT)****, Part 3: Demographic Effects*. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 14 ago. de 2020.

[72] Identificação errônea do indivíduo

[73] Impossibilidade de definição da identidade. E, também***, NIST. Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects***. p. 2-3. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 16 ago. de 2020.

em uma segunda tentativa. Já o falso positivo, acarreta outros problemas, como de segurança, posto que possa permitir a entrada de outros, que não aquele que está se requerendo a identificação.[74] Ou seja, é mais provável ocorrer uma identificação equivocada, do que uma identificação propriamente dita.

Nesse contexto, há que se atentar aos chamados "ataques-*morphing*"[75], em que, por meio do emprego de técnicas avançadas, as imagens dos rostos de duas ou mais pessoas são combinadas para formar uma nova imagem, que, armazenada com êxito em banco de dados de reconhecimento facial, pode fazer com que a imagem do rosto de cada uma das pessoas seja aceita pelo sistema. Assim, duas ou mais pessoas podem se passar por uma, burlando, por exemplo, um controle de passaportes, baseado em reconhecimento facial.

Mencione-se, ainda, que os bancos de dados contendo os dados biométricos de reconhecimento facial deverão observar rígidas regras de segurança por outra razão: como se sabe, o dado biométrico vazado resta por, praticamente, comprometer a sua utilização futura, por conta de sua unicidade e vinculação inequívoca ao titular. Já as senhas, ou chaves privadas, em caso de vazamento, podem ser descartadas e novas poderão ser geradas.

Ademais, recente estudo igualmente realizado pelo NIST[76], buscou identificar a acurácia do reconhecimento facial em indivíduos utilizando máscaras.[77] Dentre as conclusões encontradas, exemplifica-se que, quando comparadas à utilização de máscaras azul claro e preto, o erro maior de acurácia se dá nas pretas. Até o momento da pesquisa, não se tinha descoberto o motivo para tal, mas se entendeu que, até mesmo a cor da máscara é capaz de afetar a produção de um modelo a partir de uma imagem.[78] Assim, verifica-se que a precisão do reconhecimento facial

---

[74] *NIST. Face Recognition Vendor Test (FRVT),* Part 3: Demographic Effects. p. 7. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 16 ago. de 2020.
[75] MERKLE, Johannes; RATHGEB, Christian; SCHERHAG, Ulrich; BUSCH, Christoph. *Morphing-Angriffe: Ein Sicherheitsrisiko für Gesichtserkennungssysteme*. ***Datenschutz und Datensicherheit (DuD),*** Vol. 1, 2020, p. 38.
[76] *NIST. Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms****. U.S. Department of Commerce***. 2020, p. 5. Disponível em: <https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report.pdf>. Acesso em: 16 ago. de 2020.
[77] O estudo foi realizado com uma base de algoritmos fornecidos antes de março de 2020, se aplicando a algoritmos fornecidos antes da pandemia COVID-19 e os desenvolvedores não tinham conhecimento de que o *NIST* utilizaria estes para pesquisas de reconhecimento facial envolvendo máscaras. Portanto, após será divulgado outro estudo, mais preciso, com algoritmos mais recentes. - *NIST. Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms****. U.S. Department of Commerce***. 2020, p. 11.
[78] *Idem,* p. 6.

pode encontrar variações, dependendo do contexto, da iluminação, do traje do sujeito - se está com óculos, algo que cubra a boca, entre outros elementos.

Ao trazermos estes estudos para o contexto brasileiro, observa-se que, no transporte público, pode ser possível a prevenção de fraudes mesmo com os sujeitos utilizando máscaras.[79] Contudo, tal é decorrência do tipo de sistema aplicado e das circunstâncias sob análise. Pode haver uma variação para outra cidade ou estado, assim como para outra frota de veículos, a depender, principalmente, do desenvolvedor da tecnologia e da escolha dos algoritmos.

Para tanto, em que pese a possibilidade do uso da tecnologia, na segurança pública, exemplificado anteriormente, não se pode olvidar que o art. 4º,§1º[80], da LGPD, menciona que o tratamento para estes propósitos excepcionais deverá ser regido por legislação específica, na qual serão previstas medidas proporcionais e estritamente necessárias.

Tratando-se de dados pessoais sensíveis e tendo reflexo direto em questões relativas à autodeterminação informativa, é necessário um olhar atento à matéria. A própria LGPD refere que a norma a ser editada deverá prever, ainda, a necessidade de observância aos princípios da lei e aos direitos do titular. Dentre os princípios, podem-se destacar os da finalidade, adequação, necessidade e transparência, segurança, prevenção e não discriminação.[81]

A esses princípios deve ser dada fundamental atenção, quando da escolha e configuração do sistema de reconhecimento facial. Deve-se esclarecer, com muita transparência, o funcionamento, a necessidade e a finalidade do sistema que se está a implementar, justificando, criteriosamente, o interesse público envolvido e cada medida ou decisão tomada pelo mecanismo e com base nele.

A não discriminação é princípio ao qual deve ser dada especial ênfase e que está no foco de preocupação de muitas municipalidades norte-americanas que baniram o reconhecimento facial, justamente para evitar tratamentos que

---

[79] Ver exemplo em: <https://mobilidadeportoalegre.com.br/empresas-de-onibus-adaptam-tecnologia-da-biometria-facial-para-reconhecer-passageiros-com-mascara/>. Acesso em: 14 ago. de 2020.

[80] "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: 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;§ 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."

[81] Art. 6º da LGPD.

discriminem as pessoas em virtude da cor da pele, da origem étnica ou de outras características.[82]

A elaboração de relatório de impacto à proteção de dados pessoais[83], no caso da implementação de sistemas de reconhecimento facial, é medida necessária, haja vista que, consoante dispõe o art. 32 da LGPD, "a autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público".[84]

Nesse contexto, há que se recordar que a boa-fé é princípio basilar da Lei Geral de Proteção de Dados, em posição preferencial entre os princípios, uma vez que situado no *caput* do art. 6º. E se há uma lição que se extrai do preenchimento dessa cláusula geral, é a de que ela engloba a lealdade, a transparência e o respeito das expectativas nas relações jurídicas.

Assim, é fundamental que o emprego de qualquer dado, pelo poder público, mas notadamente a coleta do dado pessoal sensível biométrico, obtido por meio de reconhecimento facial, respeite os ditames da boa-fé, para fins de agregar ao tratamento todas as cautelas necessárias e, especialmente, o elemento da não-surpresa ao titular dos dados pessoais.

## 4 CONCLUSÃO

Ainda que o caminho seja nebuloso, repleto de desafios, não resta alternativa senão a de utilizar com parcimônia esta tecnologia que já permeia o novo mundo tecnológico.

Por óbvio que as novas tecnologias e a suas aplicações não devem deixar de observar os direitos fundamentais dos titulares de dados pessoais. E, portanto, não é permitido analisar o reconhecimento facial sem antes ter a clareza de que se trata

---

[82] Ver em: <https://cities-today.com/portland-bans-private-companies-from-using-facial-recognition-technology/>. Acesso em: 20 set. de 2020.

[83] De acordo com o conceito do art. 5º, XVII da LGPD, consiste o relatório de impacto à proteção de dados pessoais em "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

[84] Acerca das metodologias de elaboração do relatório de impacto de proteção de dados, ver o interessante artigo de MARTIN, Nicholas; SCHLERING, *In*; FRIEDWALD, Michael. *Methoden der Datenschutz-Folgenabschätzung: Welche Unterschiede weisen die verschiedenen methodischen Ansätze auf?* ***Datenschutz und Datensicherheit (DuD),*** Vol. 3, 2020, p. 154-160.

de ferramenta capaz de invadir a privacidade de forma abrupta e com possível violação às expectativas do titular dos dados pessoais.

Apesar dos inegáveis benefícios do reconhecimento facial, é preciso um olhar atento para as aplicações nele baseadas, principalmente quando se trata de utilização, por parte do setor público, cujo dever inafastável é o de tutela dos indivíduos, de modo a garantir a observância de seus direitos fundamentais.

Nesse sentido, a utilização do reconhecimento facial, pelo poder público, deve levar em consideração a natureza de dado sensível das informações processadas, bem como a necessidade da justificativa por sua implementação no interesse público e, preferencialmente, mediante a elaboração de relatório de impacto à proteção de dados pessoais.

Da mesma forma, os sistemas de reconhecimento facial devem estar conforme os princípios da LGPD e, dentre estes, merecem destaque os princípios da boa-fé, da finalidade, adequação, necessidade e transparência, segurança, prevenção e não discriminação.

Há iniciativas que mitigam os possíveis riscos que envolvem a atividade do reconhecimento facial no setor público e representam um marco inicial na cultura de proteção de dados envolvendo este setor. Exemplifica-se com a criação da Comissão de Dados Pessoais, em 2018, pelo Ministério Público do Distrito Federal e Territórios (MPDFT)[85], sendo o cerne desta primeira iniciativa nacional, a busca tanto pela privacidade, quanto pela tutela dos dados pessoais dos brasileiros.[86]

Ademais, a Recomendação nº 73, de 20 de agosto de 2020, do CNJ (Conselho Nacional de Justiça), recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados (LGPD).

---

[85] BRASIL. Ministério Público do Distrito Federal e Territórios. **Portaria Normativa PGJ nº539, de 12 de abril de 2018**. Disponível em: <https://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Portaria_PGJ_n2018_0539.pdf>. Acesso em 27, jul. de 2020.

[86] Desde a sua instituição, a Comissão já instaurou dois Inquéritos Civis Públicos (Portaria nº01/2018), assim como mediou a realização de audiência pública para tratar sobre a utilização de ferramentas de reconhecimento facial por entes públicos e também privados. Em relação à audiência, o foco era justamente o debate sobre uma utilização ética de dados pessoais e de que forma as tecnologias de captação biométrica e facial podem ser aplicadas. Ver: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10779-mpdft-audiencia-publica-debate-uso-ferramentas-de-reconhecimento-facial>. Acesso em 21 jul. de 2020.

Sabe-se que a matéria é embrionária, mas é papel do Direito, como ciência em constante evolução, acompanhar esse fenômeno, de modo que o necessário equilíbrio entre a proteção da personalidade e o fluxo informacional, buscado pelas leis de proteção de dados e privacidade, seja atingido.

## REFERÊNCIAS


BOUCHER, Philip Nicholas. ***Artificial intelligence***: *How does it work, why does it matter, and what can we do about it?* Brussels: European Parliment, 2020. Disponível em: <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf>. Acesso em: 30 jul. de 2020.

BOULAMWINI, Joy; GEBRU, Timnit. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research 81.* ***Conference on Fairness, Accountability, and Transparency***, 2018, p. 1-15. Disponível em: <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em: 13 set. 2020.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria nº 93, de 26 de setembro de 2019.** Glossário de Segurança da Informação. Disponível em: <http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Acesso em: 21 jul. de 2020.

_____> Ministério Público do Distrito Federal e Territórios. **Portaria Normativa PGJ nº 539, de 12 de abril de 2018.** Disponível em: <https://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Portaria_PGJ_n2018_0539.pdf>. Acesso em 21 jul. de 2020.

COESTER, Ulla; FUHLERT, Bernd. *Gesichtserkennung - eine Frage der Ethik?* ***Datenschutz und Datensicherheit (DuD)*****,** Vol. 1, 2020, p. 48-51.

DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. *In:* CUEVA, Ricardo Villas Bôas; DONEDA, Danilo, MENDES, Laura Schertel (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018):** a caminho da efetividade: contribuições para a implementação da LGPD**.** 1. ed. São Paulo: Thomson Reuters Brasil, 2020. *Ebook.*

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico.** Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 91-108.

DONOHUE, Laura K., *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*. ***Georgetown Law Faculty Publications and Other Works***, p. 407-559. Disponível em: <https://scholarship.law.georgetown.edu/facpub/1036>. Acesso em: 23 jul. de 2020.

GATES, Kelly A. ***Our Biometric Future****: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press, 2011.

GOVERNO DO ESTADO DA BAHIA. **Procurado por roubo é o 189° preso via Reconhecimento Facial.** Secretaria da Segurança Pública. SSP/BA. Disponível em:

<http://www.ssp.ba.gov.br/2020/03/7423/Procurado-por-roubo-e-o-189o-preso-via-Reconhecimento-Facial.html>. Acesso em: 06 jul. de 2020.

GOVERNO DO ESTADO DA BAHIA**. Reconhecimento Facial impede entrada de homicida em circuito.** Secretaria da Segurança Pública. SSP/BA. Disponível em: <http://www.ssp.ba.gov.br/2019/03/5310/Reconhecimento-facial-impede-entrada-de-homicida-emcircuito-.html>. Acesso em: 06 jul. de 2020.

GOVERNO DO ESTADO DO CEARÁ**. Suspeito de roubar farmácia é preso pela Polícia Civil com auxílio do reconhecimento facial.** Secretaria da Segurança Pública e Defesa Social (SSPDS/CE). Disponível em: <https://www.sspds.ce.gov.br/2020/04/29/suspeito-de-roubar-farmacia-e-preso-pela-policia-civil-com-auxilio-do-reconhecimento-facial/>. Acesso em: 04 ago. de 2020.

HUANG, Thomas; XIONG, Ziyou; ZHANG, Zhenqiu. *Face Recognition Applications. In: LI, Stan; JAIN, Anil K (Eds.)*. ***Handbook of Face Recognition***. 2. ed. London: Springer, 2011, p. 617-638.

LI, Stan Z; JAIN, Anil K. Introduction. *In*: LI, Stan; JAIN, Anil K (Eds.). ***Handbook of Face Recognition***. 2. ed. London: Springer, 2011, p. 1-15.

MARTIN, Nicholas; SCHLERING, Ina; FRIEDWALD, Michael. *Methoden der Datenschutz-Folgenabschätzung: Welche Unterschiede weisen die verschiedenen methodischen Ansätze auf?* ***Datenschutz und Datensicherheit (DuD*)**, Vol. 3, 2020, p. 154-160.

MARTINS. Leonardo**. Tribunal Constitucional Federal Alemão:** decisões anotadas sobre direitos fundamentais. Vol. 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016.

MENDES, Laura Schertel. Autodeterminação informativa: origem e desenvolvimento conceitual na jurisprudência da Corte Constitucional alemã. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo, MENDES, Laura Schertel (coord.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018):** a caminho da efetividade: contribuições para a implementação da LGPD. 1. ed. São Paulo : Thomson Reuters Brasil, 2020. Ebook.

_____. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**. vol. 79. 2011, p. 45-81.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v.120, nov./dez. 2018, p. 469-483.

_____. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, Brasília, v. 120/2018, nov./dez. 2018, p. 555-587.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In. MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, Inovação e Tecnologia**. V. 1. São Paulo: Saraiva, 2015, p. 205-230.

MERKLE, Johannes; RATHGEB, Christian; SCHERHAG, Ulrich; BUSCH, Christoph. *Morphing-Angriffe: Ein Sicherheitsrisiko für Gesichtserkennungssysteme*. ***Datenschutz und Datensicherheit (DuD),*** Vol. 1, 2020, p. 38-42.

NIST. ***Face Recognition Vendor Test (FRVT), Part 3****: Demographic Effects*. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 13. set, de 2020.

NIST. ***Ongoing Face Recognition Vendor Test (FRVT) Part 6A***: *Face recognition accuracy with masks using pre-COVID-19 algorithms. U.S. Department of Commerce*. 2020. Disponível em: <https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report.pdf>. Acesso em: 13 set. de 2020.

PREFEITURA DA CIDADE DO RIO DE JANEIRO. **Município estende Rio+Seguro à Zona Oeste com câmeras de reconhecimento facial.** Disponível em: <https://prefeitura.rio/cidade/municipio-estende-rioseguro-a-zona-oeste-com-cameras-de-reconhecimento-facial/>. Acesso em: 04 ago. de 2020.

PORTO ALEGRE**. Decreto nº 19. 836, de 22 de setembro de 2017***.* Estabelece prazos e critérios gerais no Sistema de Transporte Coletivo por Ônibus para a implantação do reconhecimento facial no Sistema de Bilhetagem Eletrônica (SBE), de equipamentos e serviços de posicionamento global (GPS) e de câmeras de segurança (CFTV) do Sistema de Supervisão e Controle Operacional (SSCO) e do Serviço de Informação ao Usuário (SIU), e dispõe sobre os equipamentos de ar condicionado nos ônibus. Porto Alegre: Prefeitura Municipal de Porto Alegre, 2017. Disponível em: <http://dopaonlineupload.procempa.com.br/dopaonlineupload/2230_ce_20170922_executivo.pdf>. Acesso em: 03 ago. de 2020.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SIMITIS, Spiros. *Die informationelle Selbstbestimmung: Grundbedingung einer verfassungskonformen Informationsordnung*. ***Neue Juristische Wochenschrift****,* 1984, v. 8, p. 394-405.

SIMITIS, Spiros. *Reviewing Privacy in an information Society****. University of Pennsylvania Law Review****.* v.135. n. 3, p. 707-746, 1987.

SNIJDER, Max**. *Biometrics, surveillance and privacy***. Bruxelas: União Europeia, 2016, p. 2. Disponível em: <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC104392/biometrics_surveillance_and_privacy_final.pdf>. Acesso em: 01 ago. de 2020.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. **TJDFT aprimora segurança com implantação de sistema de reconhecimento facial para controle de acesso de visitantes.** Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/junho/tjdft-aprimora-seguranca-com-implantacao-de-sistema-de-reconhecimento-facial-para-controle-de-acesso-de-visitantes>. Acesso em: 09 nov. de 2020.

WARREN, Samuel D; BRANDEIS, Louis D. ***The Right to Privacy****. Harvard Law Review*, Vol. 4, N. 5, p.193-220, 1890. Disponível em:

<https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 22 jul. de 2020.

# A LGPD E O COMBATE AO CORONAVÍRUS

Guilherme Bier Barcelos[1]

## 1 INTRODUÇÃO

Depois de diversas prorrogações, a Lei Geral de Proteção de Dados – LGPD entrou em vigor, em plena pandemia do novo Coronavírus. Num momento em que dados são tão relevantes para se determinar políticas públicas, o objeto desta investigação é examinar as implicações do novo diploma, no que diz respeito às políticas utilizadas pelo Poder Público para conter a epidemia. Noutras palavras, como não ultrapassar as barreiras de privacidade, na tentativa de evitar o caos sanitário?

As dúvidas acima são determinantes para o desenrolar das ações governamentais de combate à pandemia e somente uma análise pormenorizada poderá chegar a conclusões sobre o tema. O regime legal é novo e foi pouco explorado, mas isso não é razão para desrespeitá-lo. Após dois anos de *vacatio*, é chegado o momento de gestores públicos e empresas acelerarem o processo de adaptação e conformidade à LGPD.

Em relação aos princípios basilares da LGPD, pode-se mencionar o princípio da finalidade, da adequação e da transparência, não devendo o agente responsável pelo tratamento se exceder nas atividades realizadas, coletando, sempre, o mínimo de informações possíveis e mantendo-se transparente quanto ao tratamento por ele realizado.

Além dos princípios, a doutrina reconhece a existência de uma base normativa que autorize o tratamento de dados como um dos eixos predominantes da

[1] Guilherme Bier Barcellos é graduado em Ciências Jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul – UFRGS, Mestre em Direito pela mesma instituição de ensino e Doutorando em Direito Comercial na Universidade de São Paulo (USP). Foi pesquisador visitante junto ao Max Planck Institute for Comparative and International Private Law, em Hamburgo (Alemanha) no ano de 2018. Membro da Comissão de Sociedades de Advogados da OAB/RS, e associado junto ao Turnaround Management Association do Brasil, ao Comitê Brasileiro de Arbitragem (CBAR) e ao Instituto de Estudos Culturalistas (IEC). Foi reconhecido pela REVISTA ANÁLISE 500, em 2019, como um dos advogados mais admirados do Brasil.

LGPD.[2] Nesse ponto, apesar de haver polêmica quanto à relevância do consentimento, como hipótese autorizativa, fato é que não existe uma hierarquia entre as hipóteses autorizativas[3], podendo os controladores e operadores fazer uso de qualquer uma delas, a fim de possibilitar a realização do tratamento de dados.

Assim, é preciso que também se dedique atenção a outras hipóteses de tratamento de dados que a LGPD oferece. Como decorrência da existência de um conjunto de hipóteses autorizativas que resultam em um sistema coeso[4], deve-se atentar para a existência de base normativa, sempre que for realizado o tratamento para que, caso não haja nenhuma outra, entenda-se a necessidade de buscar o consentimento do titular de dados. Caso contrário, estar-se-á desrespeitando as disposições da LGPD e, por isso, sujeito às sanções civis e administrativas chanceladas pela Lei.

Por conta disso, esse artigo pretende abordar as implicações da LGPD nas ações de combate à pandemia da Covid-19 e, em especial, da empresa Inloco, que vem fornecendo dados de localização para a realização de estatísticas pelo poder público. Na primeira parte do artigo, serão analisadas as hipóteses de dispensa de consentimento no tratamento de dados pessoais. Na segunda, analisar-se-á o caso específico da plataforma Inloco, promovendo-se uma avaliação preliminar sobre a conformidade deste modelo às disposições da LGPD.

Esclarece-se, de início, que a plataforma vem coletando informações, através de aplicativos parceiros, com a finalidade de fornecer dados sobre a Pandemia da Covid-19 para os governos estaduais e municipais - a tecnologia do site, segundo informação que nele consta, entende o comportamento de localização de 60 milhões de brasileiros.[5] A plataforma destaca que os dados são disponibilizados de forma não individualizada e que servem apenas para aferir os índices de isolamento social em cada local. Contudo, há que se questionar a finalidade e a base normativa que justificaria esse tratamento de dados pela Inloco.

---

[2] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, vol. 120/2018, p. 469-483.
[3] CARNEIRO, Isabelle da Nobrega Rito; TABACH, Danielle; SILVA, Luiza Caldeira Leite. Tratamento de Dados Pessoais. *In*: FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords). **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2019, p. 60-61.
[4] MENDES, *op. cit.*, 2018. p. 469-483.
[5] Informação disponível em: <https://www.inloco.com.br/covid-19>. Acesso em: 20 nov. de 2020.

## 2 TRATAMENTO DE DADOS PESSOAIS E HIPÓTESES AUTORIZATIVAS

No art. 7º da LGPD, estão as hipóteses que autorizam a realização do tratamento de dados, definido, de acordo com o conceito que consta do Art. 5º, X, como toda operação realizada com dados pessoais, como é o caso da "[...] coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

A primeira hipótese de autorização do tratamento reside, justamente, no fornecimento de consentimento pelo titular. Sobre esse consentimento, o art. 8º da Lei ainda impõe mais limites. O dispositivo exige que o consentimento seja fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular, informando-se finalidade específica, pois são nulas as autorizações genéricas. Se for por escrito, deve haver cláusula destacada das demais.

Especificamente, em relação à finalidade do consentimento, é importante que haja esse esclarecimento, pois assegura que os titulares realmente tenham ciência sobre o uso de seus dados e tenham o direito de conhecer a finalidade concreta da coleta e do acesso aos dados.[6] Uma autorização meramente genérica seria, nas palavras de Bioni, emitir um "cheque em branco", o que impediria qualquer controle efetivo por parte do titular quanto à utilização dos seus dados.[7]

É importante notar, no entanto, que o procedimento por meio do qual esse consentimento é dado nem sempre permite que se respeitem todas as características exigidas pela lei. Muitas vezes, a aceitação de políticas de privacidade ou termos de uso garante uma espécie de consentimento, que, no entanto, não é qualificado como exigido pela LGPD. Por conta disso, é preciso aprimorar o processo de coleta do consentimento, a fim de que sua coleta se dê de acordo com os parâmetros exigidos pela LGPD.[8] Ademais, defende-se que a interpretação do consentimento seja restritiva, não podendo ser estendida para

[6] PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2018, p. 65.
[7] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019 (*E-Book*), p. 196.
[8] Tal análise é feita por BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019 (*E-Book*).

outros meios, para momento posterior, para fim diverso ou para pessoa distinta da que recebeu autorização.[9]

Contudo, apesar de haver um afã por coletar o consentimento para realização de qualquer tratamento de dados, existem diversas outras hipóteses autorizativas que constam do art. 7º, as quais podem ser utilizadas pelos controladores para justificar o tratamento de dados pessoais por eles realizado, desde que respeitados os demais princípios constantes da LGPD, como adequação, finalidade, necessidade e transparência. Aliás, há críticas, na doutrina, de que essas hipóteses poderiam tornar a LGPD insuficiente, por serem de difícil fiscalização e demasiado amplas.[10] Em sentido contrário, parte da doutrina entende que as hipóteses servem para formar um sistema coeso de bases autorizativas.[11]

De qualquer forma, fato é que a Lei listou diversas hipóteses que permitem o tratamento de dados sem consentimento. São elas: para o cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, inciso II); para o tratamento e uso compartilhado pela administração pública de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (art. 7º, inciso III); para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (art. 7º, inciso IV); quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (art. 7º, inciso V); para o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, inciso VI); para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, inciso VII); para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 7º, inciso VIII); quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do

[9] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de Teffé. Capítulo 10: Consentimento e proteção de dados pessoais na LGPD. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, RB-10.2 (*E-book*).

[10] XAVIER, Luciana Pedroso; XAVIER, Marília Pedroso; SPALER, Mayara Guibor. Capítulo 3: Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contrato. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, RB-18.5 (*Livro Eletrônico*).

[11] MENDES, *op. cit.*, 2018, p. 469-483.

titular que exijam a proteção dos dados pessoais (art. 7º, inciso IX); para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (art. 7º, inciso X).

Para fins do combate à pandemia do novo Coronavírus, o gestor poderia, por exemplo, se utilizar dos incisos II, III, IV e VIII do Art. 7º para vários aspectos do desenvolvimento das políticas públicas de combate à doença, manutenção do isolamento, pesquisa de tratamentos e vacinas. Contudo, é de se questionar se outras entidades – privadas - também poderiam se utilizar dessas hipóteses autorizativas para o tratamento de dados com finalidade de combater a pandemia da Covid-19.

Seria só o Poder Público o autorizado a realizar o tratamento de dados nestas hipóteses? Parece que não. Claro, quando se fala de execução de políticas públicas, acredita-se que não há essa margem de interpretação, mas, pelo contrário, quando se fala em pesquisa e em tutela de saúde, o cenário pode ser diferente. Afinal, a LGPD não impõe restrições para que essas hipóteses sejam utilizadas apenas pelo Poder Público e não por entidades privadas. Contudo, a LGPD impõe limitações aos conceitos de órgão de pesquisa, sendo que essa entidade não poderá ter finalidade lucrativa, seguindo-se o disposto no art. 5º, inc. XVIII.

Nesse sentido, pode-se dizer que entidades privadas também poderiam lançar mão dessas bases autorizativas para justificar o tratamento de dados em prol da pesquisa e em prol da tutela da saúde. O importante a se analisar é, no entanto, quais situações estariam abarcadas por essas hipóteses e em que circunstância a entidade privada poderia as utilizar. Estariam, dentre elas, obviamente, os dados de uma pesquisa para realização de vacina, os dados dos testes dessa mesma vacina, os dados coletados de pacientes tratados por Coronavírus. No entanto, quando começamos a falar de dados sobre o respeito ao isolamento, por meio da utilização de dados de GPS, não é tão claro que isso poderia ser feito por entes privados. Principalmente se, nesse caso, os dados forem usados também com finalidade lucrativa.

Pelo Poder Público, não há dúvidas que se houvesse política pública de controle de isolamento prevista em lei ou regulamentos seria possível tratar tais dados com a finalidade de executar as referidas políticas. Contudo, em se tratando de uma entidade privada, parece que não há essa possibilidade.

Poderia, com a justificativa de auxiliar políticas públicas de combate à pandemia, uma empresa realizar o tratamento de dados pessoais sem

consentimento específico? Essa é a questão que será abordada no próximo ponto, pois a Inloco é uma empresa que vem fornecendo dados de localização, ao Poder Público, a fim de realizar estatísticas e auxiliar na definição de políticas públicas de combate à pandemia.

## 3 O CASO INLOCO

A Inloco é uma empresa que vende, dentre outras soluções de tecnologia, dados de localização para que empresas possam tomar decisões do seu negócio com base na localização e no comportamento das pessoas.[12] No próprio site, a empresa diz ter acesso a mais de 60 milhões de dispositivos, pelo Brasil, utilizando-se de uma tecnologia 30 vezes mais precisa que o GPS para desvendar os comportamentos de localização das pessoas.[13]

Com o intuito de combater a pandemia da Covid-19, a Inloco se propôs a fornecer estatísticas sobre o desenvolvimento da pandemia gratuitamente em seu Website.[14] Na política de privacidade específica do site, há a referência de que os índices de mobilidade populacionais seriam anônimos, para fins de planejamento urbano e para ajudar instituições no combate à COVID-19.[15] A política refere que pode, também, servir para verificar a ocupação de lojas físicas comparada à capacidade usual de visitantes.[16] Quanto aos projetos desenvolvidos, a empresa refere a produção do índice de desenvolvimento social, a comunicação com a população via notificações *push* por aplicativos do Poder Público, análise de visitas a hospitais, análise de visita a estabelecimentos não essenciais, análise de visitas a lojas físicas, por segmento comercial, análise de ocupação de lojas físicas.[17]

Mais interessante para LGPD do que os projetos da Inloco é a explicação sobre como a empresa faz o tratamento de todos os dados, para chegar a esses resultados. Na política de privacidade, está descrito que a coleta dos dados se dá através de um Módulo de Desenvolvimento de *Software* (SDK), que é instalado nos aplicativos dos clientes, que devem informar, então, aos usuários para quais

[12] Informação disponível em: <https://www.inloco.com.br>. Acesso em: 20 nov. de 2020.
[13] *Idem Ibidem.*
[14] Informação disponível em: <https://www.inloco.com.br/covid-19> Acesso em: 20 nov. de 2020.
[15] *Idem Ibidem.*
[16] *Idem Ibidem.*
[17] Informação disponível em: <https://www.inloco.com.br/politicas/covid-19>. Acesso em: 20 nov. de 2020.

finalidades a tecnologia Inloco será utilizada.[18] A política destaca que a base normativa para o uso dos dados seria, portanto, o consentimento de acordo com a definição da LGPD:[19]

> O tratamento de dados pessoais feito pela Inloco para as finalidades descritas nesta Política é baseado no consentimento, isto é, a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII, Lei Nº 13.709/2018).

Os dados que são coletados são dados de GPS, sinal de Wi-Fi, sinal de Bluetooth-LE, sinal de telefone, atividade (correndo, andando ou dirigindo), cliques, cliques não intencionais, visualizações, dados do dispositivo utilizado, e dados de aplicativos como tempo de utilização.[20] Pode-se perceber que são coletados, portanto, uma infinidade de dados pessoais.

Para defender a privacidade no tratamento que é feito, a Inloco esclarece que, para suas iniciativas de combate à pandemia, esses dados são consolidados em "clusters" – grupos de usuários não identificados.[21] Ou seja, pretende-se que esses dados sejam considerados anônimos, visto que incapazes de revelar a identidade de uma pessoa.[22] Segundo a política de privacidade, a tecnologia não coleta ou utiliza dados pessoais identificados, tendo sido desenvolvida de forma a impedir o acesso a dados pessoais identificáveis.[23]

Mesmo diante de todos esses *disclaimers* que constam da política de privacidade, é preciso refletir criticamente sobre a coleta de dados que tal plataforma vem realizando. Afinal, apesar de se mencionar que os dados não são identificáveis, esse pode não ser bem o caso. Pode-se estar, por exemplo, diante do fenômeno da pseudoanonimização, que ocorre quando o próprio agente de tratamento de dados tem informações adicionais, ainda que mantidas separadas, que permitem a

---

[18] Informação disponível em: <https://www.inloco.com.br/politicas/covid-19>. Acesso em: 20 nov. de 2020.
[19] *Idem Ibidem.*
[20] *Idem Ibidem.*
[21] *Idem Ibidem.*
[22] BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel. **Lei geral de proteção de dados (Lei nº 13.709/2018)** São Paulo: Thomson Reuters Brasil, 2020, RB 3.1 (*E-book*).
[23] Informação disponível em: <https://www.inloco.com.br/politicas/covid-19>. Acesso em: 20 nov. de 2020.

reversão do processo de anonimização, transmudando um dado aparentemente anonimizado em um dado pessoal.[24]

Outro ponto a se considerar são as bases autorizativas usadas pela Inloco. A empresa refere que o tratamento de dados é feito por meio da hipótese do consentimento. No entanto, considerando que o consentimento muitas vezes se dá através de termos de uso de outros aplicativos parceiros da Inloco, é questionável se tal consentimento se adequa às exigências da LGPD. Afinal, os usuários dos aplicativos em questão podem não ter conhecimento que seus dados de localização serão tratados para esse fim.

Ausente o consentimento, haveria alternativa a fim de justificar o tratamento de dados realizado pela Inloco? Preliminarmente, parece que não. Como a entidade é privada, não se poderia estender a hipótese que se refere à realização de políticas públicas. Afinal, até onde se tem notícia, não há uma parceria formal entre um ente federado e a empresa que justifique a execução de políticas públicas.

Não poderia, portanto, a Inloco agir como se poder público fosse e tratar dados pessoais, a fim de recolher estatísticas sobre o Coronavírus, sob a justificativa de realização de políticas públicas. Também não se está diante de uma entidade de pesquisa[25], ou da tutela de saúde realizada por profissional da saúde ou por autoridade sanitária. Assim, parece que, realmente, o consentimento é a melhor alternativa para que a Inloco continue com o tratamento que vem sendo realizado no combate ao Coronavírus e na sua atividade empresarial.

No entanto, a questão do consentimento envolve, também, o modo pelo qual ele será coletado. Devido à curta vigência da LGPD, ainda não há um parâmetro interpretativo muito claro sobre os limites do consentimento. Nesse contexto, acredita-se que a estratégia mais segura para o caso Inloco seria coletar os dados através de aplicativo próprio, que só os que consentirem iriam baixar. Desse modo, seriam evitadas discussões sobre desvio de finalidade ou sobre consentimento não informado. E, mesmo que isso ocorresse, seria necessário esclarecer quais dados

[24] BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel. **Lei geral de proteção de dados (Lei nº 13.709/2018).** São Paulo: Thomson Reuters Brasil, 2020, RB 3.2 (*E-book*).

[25] De acordo com a definição do art. 5º, XVIII, poderá ser considerado órgão de pesquisa as entidades da administração pública direta ou indireta e as de direito privado sem fins lucrativos, como associações e fundações sediadas no Brasil, que incluam em seu objeto social a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. São Paulo: Thomson Reuters Brasil, 2019, RL 1.3 (*E-book*).

pessoais estariam sendo tratados e para qual finalidade o consentimento teria sido outorgado. Fato é que os usuários não têm como averiguar se e como alguns dados são anonimizados, sendo que o ônus desta prova recai à plataforma.

Nesse sentido, o dever de transparência da plataforma adquire especial relevância. Isso porque é preciso informar aos usuários, de forma clara, os procedimentos utilizados para garantir a criptografia e eventual anonimização. O tema é sensível, porque, ao mesmo, tempo, tal abertura pode revelar segredos relativos à propriedade intelectual, que podem consistir em diferenciais competitivos das empresas.

A solução, como se percebe, não é fácil. Até o advento da LGPD, tutelavam-se, basicamente, os interesses empresariais. Com a edição do novo diploma, os interesses dos usuários também passaram a ser tutelados, o que dará ensejo a um reequilíbrio dessas forças. Por ora, é muito cedo para extrair conclusões definitivas. Contudo, é possível afirmar que modelos de negócios que realizam tratamento de dados sem a observância da LGPD tendem a enfrentar severas dificuldades com o passar dos anos, porque o tema não se restringe ao nosso país. Em realidade, o Brasil nada mais fez do que seguir os parâmetros europeus atinentes ao assunto.

## 4 CONSIDERAÇÕES FINAIS

A base autorizativa, para o tratamento de dados, é de extrema importância para que as empresas evitem quaisquer ilegalidades potenciais quando do tratamento de dados. Nem sempre o consentimento é necessário, mas, quando o for, deve-se atentar, cautelosamente, aos requisitos impostos a esse consentimento, que deverá ser sempre livre e informado.

Consentir, no sentido da LGPD, também é respeitar as finalidades dadas ao tratamento de dados. Por conta disso, um exame do caso apresentado, neste artigo, é tão importante, pois demonstra a complexidade do debate. Preliminarmente, avaliamos que o consentimento, através de políticas de privacidade de outros aplicativos, não parece se enquadrar em todas as exigências da LGPD. Logo, poder-se-ia questionar a existência de autorização, no âmbito da LGPD, para que se realize o tratamento de dados na forma como tem sido feita no projeto de combate à pandemia.

Como se observou, avaliar se um determinado agente de tratamento de dados está em conformidade com a LGPD, ou não, é algo bastante complexo. Isso porque, mesmo possuindo base autorizativa, é possível que esse agente esteja agindo em desconformidade, ainda que parcial. Sem dúvida, é fundamental desenvolver mecanismos que auxiliem no combate à pandemia, mas tal combate precisa ocorrer dentro dos limites autorizados pela LGPD.

## REFERÊNCIAS


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

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In:* CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel. **Lei geral de proteção de dados (Lei nº 13.709/2018)**. São Paulo: Thomson Reuters Brasil, 2020, RB 3.1 (*E-book*).

CARNEIRO, Isabelle da Nobrega Rito; TABACH, Danielle; SILVA, Luiza Caldeira Leite. Tratamento de Dados Pessoais. In: FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords). **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2019, p. 60-61.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. São Paulo: Thomson Reuters Brasil, 2019, RL 1.3 (*E-book*).

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, vol. 120/2018, p. 469-483.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2018.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de Teffé. Capítulo 10: Consentimento e proteção de dados pessoais na LGPD. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, RB-10.2 (*E-book*).

XAVIER, Luciana Pedroso; XAVIER, Marília Pedroso; SPALER, Mayara Guibor. Capítulo 3*:* Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contrato. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, RB-18.5 (*E-book*).

# O DESAFIO DA LGPD PARA AS DEFENSORIAS PÚBLICAS NO BRASIL*

Rafael A. F. Zanatta[1]
Marina S. Kitayama[2]

## 1 INTRODUÇÃO

O presente ensaio tem, como objetivo, discutir o impacto da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) para as Defensorias Públicas, levando em consideração três aspectos centrais: (i) a aplicação da LGPD para as atividades de tratamento de dados realizadas pelas Defensorias, (ii) os cuidados com os dados pessoais de seus usuários e (iii) as oportunidades do uso de dados pessoais para atividades-fim e atividades-meio das Defensorias Públicas.

O enfoque nas Defensorias Públicas é importante por três motivos. O primeiro ponto a ser considerado é a própria missão e atribuição legal do órgão, encarregado pela defesa de direitos daqueles que se encontram em situação de vulnerabilidades.[3] As Defensorias são guardiãs de uma quantidade vultosa de dados pessoais, muitos dos quais, sensíveis. O perfil do público atendido corresponde, também, ao perfil daqueles que mais sofrem das lesões causadas pelo uso abusivo de dados pessoais, seja em virtude de processos de tomada de decisões automatizadas discriminatórias, seja em virtude do assédio de empresas que colocam a privacidade de seus consumidores em detrimento do acesso "gratuito" de serviços. A população assistida, tipicamente marcada por

* O presente ensaio foi produzido a partir do projeto "Defensorias Públicas e LGPD", coordenado por Bruno R. Bioni e Rafael A. F. Zanatta pela Associação Data Privacy Brasil de Pesquisa. O projeto é financiado pela Fundação Ford por um período de dois anos (2020-2022). Para elaboração deste ensaio, nos beneficiamos das discussões com Adriana Britto, Bruno Bioni, Estela Guerrini, Florisvaldo Fiorentino Junior, Luiz Fernando Baby, Juliana Belloque, Rafael Pitanga, Rodrigo Pacheco, Maria Tereza Sadek, Thomaz Fiterman Tedesco e os participantes do evento "Proteção de dados pessoais e o papel das Defensorias", realizado em 02 de setembro de 2020 pelas Defensorias do Estado de São Paulo e Rio de Janeiro, em parceria com a Associação Data Privacy Brasil de Pesquisa. Somos gratos aos debates e discussões que iluminaram este ensaio. A responsabilidade pelos erros e ausências de clareza é exclusivamente nossa.
[1] Doutorando pelo Instituto de Energia e Ambiente da USP. Mestre em Direito pela USP. Mestre em Direito e Economia Política pela Universidade de Turim. Diretor da Associação Data Privacy Brasil de Pesquisa.
[2] Graduanda em Direito pela USP. Pesquisadora da Associação Data Privacy Brasil de Pesquisa.
[3] RIBEIRO, Marcia Carla Pereira; DE PAULA MACHADO, José Alberto Oliveira. Acesso à Justiça e a Defensoria Pública na América Latina: democratização de direitos como desenvolvimento**. Direito e Desenvolvimento**, v. 8, n. 1, p. 89-106, 2017.

desigualdades e exclusão[4], tende a ser afetada de forma mais severa pela digitalização da sociedade. Como argumentado por Virginia Eubanks, populações socialmente vulneráveis são alvo de mais vigilância e controle, alimentando um "*feedback looping*" de automação e injustiças.[5] Esse quadro exige uma reflexão renovada para as Defensorias sobre as condições de igualdade e uma ordem jurídica justa.[6]

Um segundo motivo advém da sua constituição, enquanto órgão do poder público e integrante do sistema de justiça, o que, por lei, traz uma série de implicações sobre sua forma de atuação. Notoriamente, tais particularidades trazem impactos diretos sobre o modo como as Defensorias terão que lidar com o tratamento dos dados pessoais que lhes são confiados. Contudo, até o presente momento, pouco material foi produzido no que diz respeito à proteção de dados e as especificidades do poder público, com exceção dos trabalhos de Miriam Wimmer, que reconhece que "no setor público, o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social".[7]

O terceiro motivo que justifica o enfoque é o recente protagonismo das Defensorias Públicas nas discussões de proteção de dados pessoais. Isso é notável em razão da quantidade de eventos sobre LGPD organizados por Defensorias Públicas, o anúncio de estruturação de "encarregados pela proteção de dados pessoais" dentro das Defensorias e a participação ativa de Defensorias em ações civis públicas que questionam uso abusivo de dados pessoais, na prestação de serviços públicos. Esse engajamento demandará um compromisso *interno* com a LGPD, considerando que sua vigência teve início em setembro de 2020 em caráter definitivo.

Organizamos o ensaio em três partes. Na primeira, explicamos o escopo de aplicação da LGPD. Na segunda, analisamos a importância da proteção de dados pessoais para atividade meio. Na terceira, analisamos como a LGPD afeta as

---

[4] SILVA, Michelle Valéria Macedo *et al*. Direitos humanos. Acesso à justiça. Defensoria pública. Pobreza. Exclusão social. **Revista da Defensoria Pública da União**, n. 06, 2013.
[5] EUBANKS, Virginia. *Automating inequality: How high-tech tools profile, police, and punish the poor.* **St. Martin's Press**, 2018.
[6] SADEK, Maria Tereza. A Defensoria Pública no sistema de justiça brasileiro. São Paulo: **APADEP em Notícias**, p. 2-2, 2008. SADEK, Maria Tereza. Acesso à justiça: um direito e seus obstáculos. **Revista USP**, n. 101, p. 55-66, 2014.
[7] WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades. **Revista dos Advogados da AASP**, n. 144, nov., 2019, p. 127.

atividades-fim das Defensorias. Argumentamos que é preciso enfrentar a complexidade da tarefa de conformidade com a LGPD dentro das Defensorias Públicas e a importância dessa agenda para uma visão renovada do acesso à justiça e fortalecimento da cidadania no Brasil[8].

## 2 O ESCOPO DE APLICAÇÃO DA LGPD PARA AS DEFENSORIAS PÚBLICAS

A primeira razão que torna essencial a discussão da Lei Geral de Proteção de Dados no âmbito das Defensorias Públicas brasileiras é o próprio escopo de aplicação da normativa. Como remete seu nome, a Lei 13.709/2018 se propõe a abraçar de forma ampla as atividades de tratamento de dados pessoais, transformando o paradigma legal anterior, em que a matéria encontrava-se regulamentada de forma esparsa através de microssistemas setoriais.[9]

Conforme disposto pela própria LGPD, esta se aplica sobre todo o tipo de tratamento de dados pessoais realizado por pessoa física ou jurídica, de direito público ou privado[10], independentemente do meio, dentro de território nacional ou com o objetivo de gerar oferta de bens e serviços neste. O texto traz poucas exceções de aplicação da Lei, previstas de forma taxativa em seu art. 4º, a LGPD se coloca como não aplicável às atividade de tratamento para fins exclusivamente particulares e não econômicos (art. 4º, I), fins jornalísticos e artísticos (art. 4º, II), ou exclusivos de segurança pública e do Estado, defesa nacional e atividades de investigação criminal (art. 4º, III).[11]

Observada a amplitude de aplicação da normativa, percebe-se que, assim como a enorme maioria das instituições públicas e privadas, as Defensorias estão, inevitavelmente, submetidas aos ditames da LGPD, ficando sujeitas à fiscalização

---

[8] Nos referimos, evidentemente, aos trabalhos de Maria Tereza Sadek e acadêmicos do campo do acesso à justiça no Brasil. Ver nota acima.

[9] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2.ed. Rio de Janeiro: Forense, 2020, p. 103.

[10] Ao analisar a redação da LGPD, Wimmer argumenta que "a lei incorre em graves imprecisões técnicas, utilizando de maneira aparentemente intercambiável termos como Administração Pública, Poder Público e pessoas jurídicas de Direito Público". Para Wimmer, "o conceito de Poder Público é mais amplo que o de Administração Pública, visto que engloba também os Poderes Legislativo e Judiciário". WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades, **Revista dos Advogados da AASP**, n. 144, nov., 2019, p. 130.

[11] Conforme disposto no art. 4º, §1º, a hipótese será regulamentada por legislação específica, devendo observar os princípios gerais de proteção de dados e os direitos dos titulares previstos na Lei 13.709/18.

por parte da ANPD e à imposição do poder jurisdicional de outros entes competentes à julgar a matéria.

A constatação traz implicações profundas às Defensorias Públicas considerando sua complexidade de organização funcional e administrativa, assim como pela quantidade de dados pessoais por ela tratados. Enquanto órgão integrante do sistema de justiça, as Defensorias tem atuação sob a égide da legalidade e estão vinculadas a princípios diversos, o que, por si, já resulta na necessidade de um tratamento de dados específico. Sujeita à prestação de contas, por exemplo, além das finalidades principais da coleta, o órgão tem que levar em consideração seus usos secundários, como produção de relatórios, ou seja, nem sempre será possível eliminar informações logo que encerrada a finalidade primeira do tratamento.

Fora isso, em um país marcado por profundas desigualdades, a atribuição das Defensorias, sendo a de defesa de direitos daqueles em situação de vulnerabilidade, torna inevitável que o órgão detenha uma quantidade massiva de dados pessoais, como já observado por Defensores Públicos que escreveram sobre a LGPD.[12] Considerando que, diante a escassez de recursos, as Defensorias têm que criar critérios que determinem quem receberá atendimento, a grande maioria daqueles que buscam seus serviços tem de passar pelo procedimento de triagem socioeconômica, o que implica na coleta de enormes quantidades de dados de renda do indivíduo e de integrantes de seu núcleo familiar.

Este importante papel institucional desempenhado pelas Defensorias traz, para além dos trabalhos de se adequar à LGPD, o desafio de se consolidar enquanto ente apto a defender as disposições legais nele previstas, uma jornada dupla e de alta complexidade.

## 3 DO ATENDIMENTO AOS DADOS SENSÍVEIS: PREOCUPAÇÕES COM ATIVIDADE-MEIO DAS DEFENSORIAS PÚBLICAS

[12] SILVA, Franklyn R. Alves. A LGPD e o tratamento de dados dos assistidos pela Defensoria Pública. **Consultor Jurídico**, março de 2020. Disponível em: <https://www.conjur.com.br/2020-mar-31/tribuna-defensoria-lgpd-tratamento-dados-assistidos-defensoria>. FEICHAS, Roger. Principais Regras da LGPD para a Defensoria Pública. JusBrasil, maio de 2020. Disponível em: <https://professorrogerfeichas.jusbrasil.com.br/artigos/847086836/principais-regras-da-lgpd-para-a-defensoria-publica>. Acesso em> 13 set. de 2020

Tomando como o ponto de partida a própria adequação das Defensorias Públicas às previsões da LGPD, a complexidade da tarefa se evidencia pela robustez e importância do ente. O Brasil possui um sistema legal com muitos elementos que o tornam único. Para além de uma longa tradição no que diz respeito a direitos coletivos, criados durante os movimentos sociais da década de 80[13], o judiciário brasileiro é um dos poucos do mundo equipado com um ente público, cuja função é a defesa de direitos da população em situação de vulnerabilidade social ou econômica. A maioria dos estados desenvolveu as estruturas de suas Defensorias Públicas, a partir dos anos 50, sendo a primeira delas a do estado do Rio de Janeiro. Hoje, há dezenas de unidades espalhadas pelo país, as quais, juntas, representam uma camada extremamente importante da justiça social do sistema jurídico brasileiro.

De acordo com cientistas políticos[14], existem três razões principais que tornam as Defensorias Públicas brasileiras um órgão de relevância especial. A primeira delas é o fato de o Brasil ser um dos poucos países da América-Latina a possuir a instituição constitucional de um serviço público que promova assistência jurídica à população vulnerável. Em segundo lugar, dado os altos índices de desigualdade social, quase 90% da população brasileira está enquadrada dentro dos critérios da justiça gratuita, sendo o principal deles o de renda familiar de até três salários mínimos (IBGE, 2010).[15] A terceira razão é a existência recente da instituição, de modo que, apesar de ser um órgão relativamente jovem (segunda metade do século XX), já se apresenta como um relevante ator político, especialmente no sistema de justiça.

Considerando o cenário brasileiro de desigualdades sociais e regionais gritantes a expectativa de que sejam altos os números de atendimentos realizados pelas Defensorias se confirma. Completando apenas dez anos em 2016, a Defensoria Pública Estadual de São Paulo já havia realizado mais de 10 milhões de atendimentos, com média atual de 1,5 milhões de atendimentos por ano.[16]

---

[13] ZANATTA, Rafael. Tutela coletiva e coletivização da proteção de dados pessoais, *In*: PALHARES, Felipe (org.), **Temas Atuais de Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2020, p. 345-374.

[14] MADEIRA, Lígia Mori. *Institutionalisation, Reform and Independence of the Public Defender's Office in Brazi*l. ***Brazilian Political Science Review***, v. 8, n. 2, p. 48-69, 2014.

[15] Disponível em: <https://migalhas.uol.com.br/quentes/318863/parana-e-o-estado-com-menos-defensores-publicos-por-habitante-no-brasil>. Acesso em: 15 set. de 2020.

[16] Disponível em: <https://www.conjur.com.br/2016-jan-09/15-milhao-atendimentos-ano-defensoria-sp-faz-10-anos>. Acesso em: 20 set. de 2020.

Defensorias Públicas de estados com índices demográficos menores também apresentam números que denotam a magnitude da quantidade de informações tratadas diariamente por esses órgãos, a DPE-RS, apenas entre os dias 18 de março e 30 de junho de 2020, período pandêmico, realizou mais 200 mil atendimentos, sua grande maioria, de forma remota.[17]

Afora a quantidade massiva de atendimentos e, consequentemente, de dados pessoais tratados, ainda deve-se somar o processo de digitalização da sociedade. Acelerado pela crise do COVID 19, esse processo acentua uma série de desigualdades e torna extremamente desafiador o trabalho das Defensorias Públicas, no Brasil, sendo uma das consequências imediatas do isolamento social a necessidade de digitalização de seu atendimento. A instituição, sem ferramentais tecnológicos próprios para tanto, se viu obrigada a encontrar soluções alternativas disponíveis no mercado, as quais eram, muitas vezes, financeiramente bancadas pelos próprios defensores. Tornaram-se ferramentas padrão para o trabalho das Defensorias o armazenamento em nuvem, uso de drives compartilhados e de meios de comunicação por aplicativos. Apesar de ser a solução disponível em tempo, é notório que esta não se configura como a ideal na perspectiva de longo prazo, considerando a quantidade e a qualidade de dados pessoais tratados pelo ente.

Em síntese, as preocupações com a atividade-meio giram em torno de alguns problemas comuns: (i) os processos de atendimento automatizados e novas intermediações na relação entre Defensores e usuários, (ii) a utilização de sistemas integrados para fluxo de dados e compartilhamento de dados entre Defensorias[18], (iii) a necessidade de categorização de dados sensíveis e criação de regras de segurança de informação, garantindo princípios de “need to know” e necessidade do tratamento de dados pessoais para viabilizar acessos a determinados sistemas por servidores, estagiários, voluntários, e outros profissionais, (iv) a obtenção de base legal adequada para armazenamento dos dados pessoais e utilização para fins de pesquisa, bem como utilização em litígios estratégicos e situações onde os Defensores precisam “argumentar com base em dados”.

---

[17] Disponível em: <http://www.defensoria.rs.def.br/mais-de-200-mil-atendimentos-e-aumento-nos-pedidos-de-pensao-como-foram-esses-100-dias-de-pandemia-na-defensoria-publica>. Acesso em: 20 set. de 2020.

[18] Como observa um Defensor, “é muito comum que a Defensoria Pública de um Estado atue em favor de parte que resida em outra unidade federativa ou que haja declínio de atribuição, exigindo-se que as instituições sejam capazes de migrar seus dados entre si para a manutenção do serviço de assistência jurídica”. SILVA, Franklyn R. Alves. A LGPD e o tratamento de dados dos assistidos pela Defensoria Pública. **Consultor Jurídico**, março de 2020.

Essa situação ilustra a centralidade das Defensorias Públicas no sistema de justiça e o conjunto enorme de preocupações com a LGPD com relação às atividades-meio das Defensorias.

## 4 LITÍGIOS ESTRATÉGICOS E ATUAÇÃO DADOCÊNTRICA: ATIVIDADES-FIM DAS DEFENSORIAS PÚBLICAS

A jornada continua sob a perspectiva da atividade fim das Defensorias, órgão cujo papel primordial é a defesa de direitos, incluindo direitos fundamentais relativos e relacionados à proteção de dados. Conforme redação da Constituição Federal, após a Emenda Constitucional 80/2004, a Defensoria Pública é instituição permanente, essencial à função jurisdicional do Estado, cabendo-lhe, como expressão e instrumento do regime democrático, "a orientação jurídica, a promoção dos direitos humanos e a defesa, em todos os graus, judicial e extrajudicial, dos direitos individuais e coletivos, de forma integral e gratuita, aos necessitados" (art. 134, CF88).

A LGPD invoca questões ainda mais relevantes àqueles em situação de vulnerabilidade social ou econômica, perfil do público atendido pelas Defensorias. O direito à proteção de dados se consolida enquanto fundamental[19] pelos bens que tutela, dentre eles a dignidade humana, a liberdade e a privacidade[20], os quais são reiteradamente violados e ignorados, tratando-se de segmentos populacionais estigmatizados. Diante do papel central que os dados desempenham na sociedade atual, a matéria da proteção de dados se propõe como o meio que irá legitimar o tratamento de dados, estipulando critérios para conter seus potenciais danos, tais quais a acentuação de práticas discriminatórias.

Esse processo de acentuação de estigmas e discriminações é amplamente discutido no que toca ao uso de ferramentas de tomadas decisões automatizadas. Tais tecnologias se fundamentam a partir da modelagem de perfis comportamentais e análises estatísticas que se operam replicando padrões sociais identificados pelas informações com que as máquinas são alimentadas. Um exemplo disso são os

[19] SUPREMO TRIBUNAL FEDERAL. Voto da Relatora, MIN. ROSA WEBER. **Ações Diretas de Inconstitucionalidade número 6387, 6388, 6389, 6390 e 6393**. Julgamento de liminar com pedido de suspensão dos efeitos da Medida Provisória n. 954/2020. DJe. 07.05.2020.
[20] RODOTÀ, Stefano. Org. BODIN, Maria Celina. Trad. DONEDA, Danilo e DONEDA, Luciana. **A vida na sociedade de vigilância, a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p.17-19.

sistemas de modelagem de crédito, que a partir dos dados pessoais de uma gama de indivíduos cria uma série de perfis de "risco".[21] Nesse exemplo, aquele que será avaliado para tomar crédito não o é, exclusivamente, pelos seus dados enquanto um bom ou um mau pagador, mas também pela sua identificação dentro de um perfil comportamental predeterminado. Tais perfis podem ser compostos por informações das mais diversas, não se restringindo a dados de pagamento do consumidor. Eles podem incluir hábitos de compra, dados demográficos, faixa etária, entre muitos outros de difícil apreensão, já que os algoritmos de alta complexidade são capazes de criar seus próprios códigos, tornando-se verdadeiras caixas pretas.[22] Assim, da forma como operam, as técnicas de *credit scoring* sem uma devida observância dos ditames da proteção de dados, poderiam induzir e acentuar processos discriminatórios de uma maneira que é ainda pouco transparente.[23]

As pressões de mercado por um acesso amplo e facilitado de dados de crédito são um forte sinalizador de que a pauta merece atenção. Recentemente, a Lei do Cadastro Positivo passou por alterações de impacto profundo, na forma como as gestoras de bancos de dados obtém informações de pagamento.[24] A reforma alterou um ponto chave e que era há tempos uma demanda do mercado, ao invés do consumidor ter que, por padrão, dar o aceite sobre o compartilhamento de dados de compra, o compartilhamento tornou-se a regra e a recusa passou a ficar sujeita à manifestação do consumidor.[25] Cabe, ainda ressaltar uma particularidade da Lei Geral brasileira que possui, diferentemente de sua "equivalente" europeia, a GPDR, uma base legal própria que legitima o tratamento de dados com fins de proteção ao crédito, art. 7º, X da LGPD, o que é um indicativo da força que este mercado possui no contexto nacional.

Os potenciais riscos discriminatórios são, ainda, agravados pela forma como operam muitos dos modelos de negócios de empresas digitais, as quais oferecem

---

[21] ZANATTA, Rafael. **Pontuação de crédito e direitos dos consumidores***:* o desafio brasileiro. São Paulo: Idec, 2017.
[22] PASQUALE, Frank. *The Black Box Society. The secret algorithms that control money and information.* Cambridge: **Harvard University Press**, 2015.
[23] ZANATTA, Rafael; DONEDA, Danilo. O que há de novo no debate sobre "*credit score*" no Brasil? **Jota.info**, 2017. Disponivel em: <https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-que-ha-de-novo-no-debate-credit-score-no-brasil-09022017>. Acesso em: 20 nov.de 2020.
[24] O'NEIL, Cathy. ***Weapons of math destruction****: how big data increases inequality and threatens democracy.* Nova York: Crown, 2016, C. 8.
[25] BESSA, Leonardo Roscoe. **Nova Lei do Cadastro positivo**. São Paulo: Revista dos Tribunais, 2019.

serviços em troca da atenção ou dos dados pessoais de seus consumidores.[26] Não se pode ignorar a interpretação de que esta forma de permuta é positiva, ao permitir o acesso a serviços àqueles que não poderiam arcar financeiramente com seus custos. Os dilemas são, entretanto, mais profundos. Importa saber como e para que esses dados estejam sendo utilizados, verificando se há riscos de tais informações servirem para prejudicar o titular. Eventuais abusos no uso dos dados podem representar maiores perdas futuras do que benefícios imediatos.

Fora isso, há ainda situações que obrigam a população que não pode pagar por determinados serviços a abdicar de sua autodeterminação informativa. Em 2017[27], o governo municipal de São Paulo pretendia tornar obrigatório o cadastramento dos usuários das redes de *Wi-fi* público da cidade, isso porque a própria estrutura de fornecimento da rede pública seria financiada por entes privados, que utilizariam das informações para fins de *marketing* direcionado. O caso leva a questionamentos sobre a legalidade de vincular o serviço público ao compartilhamento de dados, considerando que este deveria ser garantido de forma gratuita pelo Estado.

Indagações semelhantes foram levantados no caso da Linha 4 do Metrô de São Paulo.[28] A concessionária do trecho instalou câmeras de identificação de expressões e emoções dos usuários do metrô, o que permitia a mensuração de impacto das publicidades transmitidas aos indivíduos. O Instituto Brasileiro de Defesa do Consumidor moveu um processo contra a prática da concessionária, contando com a assistência litisconsorcial da DPE-SP. A tese defendida pelos entes é justamente a da abusividade de sujeitar aqueles que não têm escolha de usar ou não o transporte público a estarem sujeitos a tal situação. Os serviços públicos consistem em atividades de cunho essencial, de modo que não há como garantir a autodeterminação informativa do titular quando a oferta de um serviço desta ordem é posta em detrimento ao compartilhamento de dados.

Diante do contexto de abusos e riscos a direitos fundamentais, uma Defensoria apta para atuar em defesa dos direitos à proteção de dados da

[26] WU, Tim. ***The attention merchants****: the epic scramble to get inside our heads*. Nova York: Knopf, 2016.
[27] BIONI, Bruno. *Expansão do Wi-Fi público à custa de dados pessoais.* Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/544067877/expansao-do-wi-fi-publico-as-custas-de-dados-pessoais>. Acesso em: 20 nov.de 2020.
[28] Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2018/08/31/concessionaria-do-metro-de-sp-e-processada-por-painel-que-faz-reconhecimento-facil-de-passageiros.ghtml>. Acesso em: 20 nov. de 2020.

população em situação de vulnerabilidade é, da perspectiva de seu papel institucional, de extrema relevância. Há, porém, ainda outro ponto relacionado à capacitação das Defensorias que tocam o exercício de suas atividades-fim. Espera-se que o processo de adequação à Lei Geral de Proteção de Dados traga como consequência um uso mais consciente e organizado das informações controladas pelos órgãos, o que abre uma janela de oportunidades para uma atuação mais estratégica das Defensorias.

O processo de adequação à LGPD força as instituições a se organizarem, a verificarem dados coletados, armazenados, as razões do tratamento e seu fluxo informacional. A consequência direta disto é que se torna mais fácil verificar possibilidades de tornar úteis aquelas informações. Como exemplo prático de uso estratégico de dados, pode-se citar a atuação da DPE-RJ, que, constatando que o número de demandas relativas a vagas em creches mais que dobrou de um ano para outro, entrou com uma ação civil pública contra a prefeitura do Rio de Janeiro requerendo a criação de novas vagas.[29] Parafraseando Evgeny Morozov, que fala da existência de um "capitalismo dadocêntrico"[30], é crucial pensarmos nas possibilidades de uma litigância dadocêntrica, que se apoia em análises agregadas de dados pessoais como estratégia argumentativa e de convencimento de agentes decisórios em casos complexos.

Produzir estatísticas e entender padrões com base em dados abre margem para uma série de atuações estratégicas, como a percepção de perfis mais afetados por uma determinada demanda, casos repetidos que dariam margem à propositura de ações civis coletivas e ações civis públicas, além de servirem, também, enquanto argumentos a serem levados perante o judiciário, em formação de acordos ou para ações de incidência em políticas públicas.

A concepção de uma atuação nesse sentido caminha em consonância com a perspectiva ampla da missão das Defensorias, que deu mais espaço para a atuação do ente e transformou a antiga visão de que o papel do órgão seria fornecer um "advogado" para quem não pode arcar com um por meios próprios.[31] A instituição,

---

[29] Disponível em: <https://g1.globo.com/rio-de-janeiro/noticia/mais-de-30-mil-criancas-aguardam-vagas-em-creches-do-rio.ghtml>. Acesso em: 20 nov. de 2020.

[30] MOROZOV, Evgeny; BRIA, Francesca. ***Rethinking the smart city****. Democratizing Urban Technology*. New York, NY: Rosa Luxemburg Foundation, 2018.

[31] CONGRESSO NACIONAL. **Lei Complementar nº 80, de 12 de janeiro de 1994**. Organiza a Defensoria Pública da União, do Distrito Federal e dos Territórios e prescreve normas gerais para sua organização nos Estados, e dá outras providências.

para além de  garantir a defesa de qualidade de seus usuários perante o judiciário, tem a missão de defender seus direitos em sentido lato, incluindo até mesmo questões relativas à educação em direitos. Em um país de desigualdades latentes e problemas sociais graves como o Brasil, cumprir esse papel é uma tarefa hercúlea e que demanda, diante recursos escassos, estratégias de atuação que permitam o maior alcance dentro das possibilidades financeiras disponíveis.

O domínio de informações sobre sua própria atuação é essencial, nesse sentido, razão pela qual um dos pontos centrais a ser ressaltado, no processo de adequação das Defensorias à LGPD, é o de enxergar o desafio como uma janela de oportunidades que permitirá ao ente dimensionar seu próprio trabalho, traçar planos de atuação e dominar informações que podem ser utilizadas diretamente na melhora de seu serviço.

Em síntese, os programas de governança de proteção de dados pessoais construídos pelas Defensorias Públicas nos próximos anos deverão levar em consideração: (i) de que modo a base legal de “exercício regular de direitos em processo judicial” poderá ser utilizada para legitimar tratamentos de dados pessoais dos usuários em litígios, (ii) quais informações devem ser prestadas sobre o uso agregado de informações para fins de pesquisa e de litigância estratégica, (iii) quais as possibilidades de armazenamento e retenção de dados pessoais para fins que não sejam específicos ao atendimento regular dos usuários, e (iv) quais técnicas de anonimização e pseudonimização podem ser mobilizadas para avançar em uma litigância dadocêntrica que não cause riscos significativos às liberdades civis e direitos fundamentais dos usuários, ao mesmo tempo que permitem uma atuação mais qualificada, estratégica e baseada em argumentos empíricos por parte dos Defensores Públicos.

Nesse sentido, programas de governança de dados não podem ser construídos a partir de modelos, templates, tabelas prontas e documentos ao estilo “copia e cola” produzidos pelo setor privado. Há uma necessidade de customização e de construção de programas de adequação à Lei Geral de Proteção de Dados Pessoais que levem em consideração as especificidades das Defensorias e a importância dos dados pessoais para atividades-meio e atividades-fim.

# 5 CONSIDERAÇÕES FINAIS

Os impactos da LGPD sobre entes do poder público merecem uma atenção própria. Não se podem ignorar as razões pelas quais há uma seção específica que disciplina a matéria para estes agentes. Observar tais prerrogativas não deve ser uma tarefa encarada enquanto um fim em si mesmo, pois as determinações da normativa objetivam a tutela de um bem jurídico e social. Nesse sentido, o Estado, que tem a função de garante de uma série serviços consagrados enquanto essenciais, deve servir de exemplo no tocante à proteção de dados pessoais dos cidadãos, considerando que todos estão, em certa medida, obrigados a confiar parte de sua personalidade ao poder público.[32]

No tocante às Defensorias, a questão é ainda mais sensível. Um sistema de justiça que se pretenda justo deve garantir que todos os cidadãos tenham condições mínimas para defender seus direitos. Assim, a atribuição legal da Defensoria é de natureza essencialíssima. Em segundo lugar, a população atendida pelas Defensorias é, por atribuição constitucional, uma população em situação de vulnerabilidade, isso implica que estes indivíduos não têm à sua disposição uma miríade de opções à que possam recorrer e tampouco podem exercer plenamente a ideia de “controle sobre os próprios dados” e formas de negociação e declarações de vontade com base em “consentimento livre e informado”. É preciso pensar em assimetrias informacionais, desigualdades e barreiras cognitivas que podem ressignificar a leitura do que é efetivamente consentimento, superando a ideia limitada de que esta é a única base legal para tratamento de dados pessoais de acordo com a LGPD.

Pensar no tratamento de dados nesse contexto deve ser uma razão a mais para que exista a máxima diligência e um programa de governança de excelência, não reduzindo aqueles que dependem da atuação do Estado a cidadãos de segunda categoria que devem abdicar de sua autodeterminação informativa para ter acesso a serviços básicos.

O dever de diligência sobressaltado do poder público torna significativo o desafio de sua conformação à LGPD, porém, ainda maior deve ser o olhar de que este processo se trata de uma oportunidade para que, organizando e sistematizando

---

[432] RODOTÀ, *op.cit*., 2008.

seu tratamento de dados, as funções desempenhadas pelas instituições estatais se deem de modo ainda mais eficiente e com ainda mais qualidade. Longe de oferecer respostas definitivas sobre *como construir programas de adequação dentro das Defensorias*, o que problematizamos, neste ensaio, é a *complexidade de tal tarefa* e a necessidade de uma olhar atento às atividades-meio e atividades-fim, colocando em marcha um esforço coletivo de construção de programas robustos de adequação por parte de Defensores, servidores e profissionais de diversas áreas que fazem parte dessa instituição que é, ao mesmo tempo, agente de transformação e de justiça social no Brasil.

## REFERÊNCIAS


BESSA, Leonardo Roscoe. **Nova Lei do Cadastro positivo***.* São Paulo: Revista dos Tribunais, 2019.

BIONI, Bruno Ricardo. **Expansão do Wi-Fi público às custas de dados pessoais***.* Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/544067877/expansao-do-wi-fi-publico-as-custas-de-dados-pessoais>. Acesso em: 15 set. de 2020.

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

EUBANKS, Virginia. *Automating inequality: How high-tech tools profile, police, and punish the poor. **St. Martin's Press***, 2018.

FEICHAS, Roger. Principais Regras da LGPD para a Defensoria Pública. **JusBrasil**, maio de 2020

MADEIRA, Lígia Mori. *Institutionalisation, Reform and Independence of the Public Defender's Office in Brazil*. ***Brazilian Political Science Review***, v. 8, n. 2, p. 48-69, 2014.

MOROZOV, Evgeny; BRIA, Francesca. ***Rethinking the smart city****. Democratizing Urban Technology.* New York, NY: Rosa Luxemburg Foundation, 2018.

O'NEIL, Cathy. ***Weapons of math destruction****: how big data increases inequality and threatens democracy.* Nova York: Crown, 2016.

PASQUALE, Frank. ***The Black Box Society***. *The secret algorithms that control money and information*. Cambridge: Harvard University Press, 2015.

RIBEIRO, Marcia Carla Pereira; DE PAULA MACHADO, José Alberto Oliveira. **Acesso à Justiça e a Defensoria Pública na América Latina**: democratização de direitos como desenvolvimento. Direito e Desenvolvimento, v. 8, n. 1, p. 89-106, 2017.

RODOTÀ, Stefano. Org. BODIN, Maria Celina. Trad. DONEDA, Danilo e DONEDA, Luciana. **A vida na sociedade de vigilância, a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SADEK, Maria Tereza. Acesso à justiça: um direito e seus obstáculos. **Revista USP**, n. 101, p. 55-66, 2014.

SADEK, Maria Tereza. A Defensoria Pública no sistema de justiça brasileiro. São Paulo: **APADEP em Notícias**, p. 2-2, 2008.

SILVA, Franklyn R. Alves. A LGPD e o tratamento de dados dos assistidos pela Defensoria Pública. **Consultor Jurídico**, março de 2020.

SILVA, Michelle Valéria Macedo *et al*. *Direitos humanos. Acesso à justiça. Defensoria pública. Pobreza. Exclusão social.* **Revista da Defensoria Pública da União**, n. 06, 2013.

ZANATTA, Rafael; DONEDA, Danilo. O que há de novo no debate sobre "*credit score*" no Brasil? **Jota.info**, 2017.

ZANATTA, Rafael. **Pontuação de crédito e direitos dos consumidores**: o desafio brasileiro. São Paulo: Idec, 2017.

WIMMER, Miriam. Proteção de dados pessoais no poder público: incidência, bases legais e especificidades, **Revista dos Advogados da AASP**, n. 144, nov., 2019, p. 127.

WU, Tim. ***The attention merchants****: the epic scramble to get inside our heads. Nova York: Knopf,* 2016.

# A ATUAÇÃO DA ADMINISTRAÇÃO PÚBLICA NO PROCESSAMENTO DE DADOS PESSOAIS NOS TRANSPORTES PÚBLICOS

Gabriel Araújo Souto[1]
Luísa Campos Faria[2]
Samanta Barbosa Tiveron[3]

## 1 INTRODUÇÃO

O transporte público está cada vez mais "inteligente", e isso é causado pelo aproveitamento máximo dos dados pessoais de seus usuários. Esse tipo de transporte é líder[4] em oportunidades para *open data*[5], devido ao alto grau de fluxo de pessoas que passam por seu serviço, bem como a variedade econômica, social, de gênero e personalidade que se confluem para uma mesma modalidade de transporte. Além de monitorar as pessoas que utilizam o transporte público, a Administração Pública, ou as concessionárias do serviço podem implementar tecnologias para usar dados pessoais a fim de personalizar o que oferecem a cada indivíduo, por meio de opções de viagem, reservas online, *download* de aplicativos e sugestões de destinos.

Nesse sentido, no bojo regulatório do processamento de dados pessoais, deve ser observada a evolução gradativa do direito à proteção de dados pessoais,

---

[1] Acadêmico de Direito do Instituto Brasiliense de Direito Público (IDP). Foi estudante visitante do LL.M. de Global Antitrust Law & Economics da Antonin Scalia Law School of George Mason University (2018) e cursou Digital Trade na Public Citizen em parceria com a American University (2018), em Washington D.C. Foi 2º Lugar nos Prêmios IBRAC-TIM de 2018 e 2019. Foi palestrante no Connected Life 2019 na The London School of Economics (LSE). É Law Student Ambassador da American Bar Association Section of Antitrust Law e membro do conselho editorial da Cartel & Joint Conduct Review. É Diretor Acadêmico do Laboratório de Políticas Públicas e Internet (LAPIN).

[2] Graduada em Direito pela Universidade de Brasília (2019). Foi 2º Lugar no Prêmio IBRAC-TIM de 2019. Analista de Políticas e Indústria II na Confederação Nacional da Indústria (CNI).

[3] Acadêmica de Direito do Instituto Brasiliense de Direito Público (IDP). Realizou o Curso de Inverno: O Profissional do Direito no Século XXI: Desafios e Perspectivas em São Paulo (2019) e foi estudante visitante do programa Direitos Fundamentais: Temas Emergentes da Universidade NOVA de Lisboa (NOVA) (2020). É integrante da Pacta, Empresa Júnior do IDP.

[4] OPEN DATA INSTITUTE. *Personal data in transport*: *exploring a framework for the future.* ***Open Data Institute Publications*****,** 2018, p. 11.

[5] Dados abertos são dados que podem ser usados livremente, compartilhados e integrados por qualquer pessoa, em qualquer lugar, para qualquer finalidade. O conceito também é relacionado ao *Open Innovation*, termo cunhado pelo professor Henry Chesbrough, definido como o uso de entradas e saídas de conhecimento em um ambiente para acelerar a inovação interna e expandir os mercados para uso externo da inovação. Cf. CHESBROUGH, Henry, *et al. Open innovation: Researching a new paradigm.* ***Oxford University Press on Demand***, 2006, p. 1.

que demonstra uma evolução no conceito de privacidade. Como o tratamento de dados pessoais é uma atividade que possibilita amplo acesso à esfera privada dos indivíduos, o direito fundamental à privacidade, tal qual delineado por Warren e Brandeis no século XX, deixou de ter um caráter fortemente individualista e ligado ao "direito de ser deixado só".[6]

Atualmente tem-se interpretado o direito à privacidade também como a proteção à inviolabilidade da personalidade dos indivíduos, rompendo com a noção de proteção da vida privada, associada diretamente à propriedade.[7] Assim, o século XX presenciou uma "inexorável reinvenção da privacidade" pois de um direito com dimensão estritamente negativa, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático.[8]

## 2 OS PRINCÍPIOS DA LGPD APLICADOS À ADMINISTRAÇÃO PÚBLICA

A chegada do 5G e da denominada a internet das coisas (*Internet of Things – IoT*) promete trazer o conceito relativo às cidades inteligentes, ou seja, com tecnologias urbanas interconectadas que, a partir do uso do Big Data[9], deve proporcionar a tomadores de decisões mais informações para que, assim, possamos otimizar o fornecimento de diversos serviços - incluindo aqueles de responsabilidade estatal, os serviços e políticas públicas. Dos setores mais afetados, encontra-se o de transporte, tendo em vista que a Internet das Coisas prevê a existência de veículos autônomos, que conseguirão repassar informações entre si de modo a melhor atender à sociedade, inclusive evitando acidentes.

Muito embora a realidade da Internet das Coisas pareça promissora, fato é que antes dela já contávamos com a digitalização de determinados serviços no transporte, de modo que hoje vivemos num contexto em que o Big Data se faz

---

[6] WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy.* ***Harvard Law Review***, 1890, p. 195.

[7] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 206.

[8] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor***:* linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 29.

[9] "Big Data caracteriza-se, portanto, pela grande quantidade de diferentes tipos de dados, gerados em alta velocidade a partir de múltiplas fontes, cuja manipulação e análise requerem processadores e algoritmos novos e mais poderosos". FARIA, Luísa Campos; SANTOS, Luiza Mendonça da Silva Belo. **O Big Data e a privacidade de dados pessoais no controle de estruturas**. Mulheres no antitruste Vol. II, 2019, p. 56.

presente para na gestão de serviços estatais e requerem que o tratamento de proteção de dados seja corretamente realizado por parte dos Governos. Um bom exemplo são os passes estudantis ou vales transporte, que são vinculados a um CPF titular e costumam ter dados capazes de informar a geolocalização das pessoas (quais as linhas principais de ônibus, por exemplo, que fazem uso, em qual local residem e trabalham, dentre outros). Antes de tratarmos sobre o uso de dados pessoais, coletados por meios de transportes, quando da utilização do transporte público dentro das cidades, cabe esclarecer alguns pontos acerca da aplicação da Lei Geral de Proteção de Dados Pessoais por parte da Administração Pública.

Importante frisar que a Lei Geral de Dados Pessoais faz diferenciações com relação aos tipos de dados que podem ser coletados, classificando alguns deles como sensíveis. Tais dados requerem um tratamento diferenciado, vez que dizem respeito a questões de foro íntimo passíveis de gerar algum tipo de tratamento diferente ou discriminado, e por tutelarem direito de personalidade.[10] São considerados dados pessoais sensíveis aqueles que versam acerca de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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, nos termos da Lei.

A Lei Geral de Proteção de Dados (LGPD), no entanto, inclusive por ser dotada de caráter principiológico, traz alguns princípios que devem ser sempre observados quando de sua aplicação, todos elencados no seu art. 6º. São eles os princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção e da não discriminação. Tais princípios têm por função precípua assegurar que o usuário, como titular de dados pessoais tenha livre acesso a seus próprios dados, que deverão ser tratados de maneira adequada e limitada, ou seja, quando tais dados forem considerados imprescindíveis para a realização das finalidades a que se propõe o controlador, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

---

[10] RIBEIRO, Paulo Dias de Moura. Lei Geral de Proteção de Dados: regulação. *In*: FONSECA, Reynaldo Soares da; COSTA, Daniel Castro Gomes da (coord.) **Direito regulatório***:* desafios e perspectivas para a Administração Pública**.** Belo Horizonte: Fórum, 2020, p. 133-137.

Os referidos princípios garantem também que as informações a respeito do tratamento conferido sejam claras, precisas e acessíveis, garantindo, aos titulares, exatidão, clareza, relevância e atualização dos dados de acordo com as finalidades para as quais são utilizados, de maneira a melhor garantir a segurança da informação tratada. Assim sendo, trataremos de cada um deles no contexto da atuação da Administração Pública.

O primeiro princípio é o da finalidade, que consiste na realização do tratamento dos dados pessoais para propósitos legítimos, explícitos, específicos. Tal princípio estabelece que ao titular seja garantido esclarecimento relativo ao propósito, à forma, à duração do tratamento realizado com seus dados pessoais, bem como, para o caso de eventual compartilhamento, o conhecimento acerca dessa ação. Após e de modo complementar, tem-se o princípio da adequação, que garante que o tratamento fornecido aos dados pessoais seja compatível com a finalidade informada, de modo que seja realizado um tratamento dentro dos limites da razoabilidade e da proporcionalidade.

O princípio da necessidade, por sua vez, estabelece que só deva ser objeto de tratamento aqueles dados estritamente necessários para o cumprimento da finalidade almejada pelo controlador, de modo que a abrangência dos dados pertinentes seja restrita e os dados tratados o sejam, sempre, de maneira proporcional e não excessiva. Já o princípio do livre acesso consiste na garantia legal, dada aos titulares, de que possam realizar consultas a seus próprios dados e ao tratamento a que estes estão submetidos de maneira fácil, integral e gratuita. Igualmente, o princípio da transparência visa que as informações tangentes ao tratamento realizado sejam sempre claras, precisas e facilmente acessíveis, de modo que o titular entenda o que está sendo feito por parte do controlador; e o princípio da qualidade assegura exatidão, clareza, relevância e atualização com relação ao tratamento fornecido para os titulares.

O legislador, em seguida, elencou princípios a fim de garantir a proteção dos dados pessoais de titulares, com os princípios da segurança da prevenção. Em suma, o princípio da segurança trata da utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de perda, alteração, destruição, comunicação ou difusão, conquanto o princípio da prevenção pugna pela adoção de medidas preventivas à ocorrência de danos decorrentes do manejo dos dados pessoais. Por

fim, trouxe a lei o princípio da responsabilização e prestação de contas, de modo a garantir a necessidade de demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Importante frisar, desta feita, que, muito embora existam regimes de exceção à atuação da Administração pública, por exemplo, se tomarmos os contratos fechados com esta, que contam com as denominadas cláusulas exorbitantes, em que é considerada a supremacia da Administração sobre o particular prevendo que essa, inclusive, faça modificações quanto àquilo que foi contratado unilateralmente[11], em se tratando de Proteção de Dados Pessoais, não pode a Administração de qualquer forma se sobrepor aos interesses particulares dos titulares, sob pena de incorrer na violação de direitos fundamentais dos cidadãos.[12] Antes de passar à análise do tratamento de dados pessoais colhidos com fins de propiciar o uso do transporte público dos cidadãos, deseja-se deixar bastante clara a vedação à Administração Pública de que possa se furtar em seguir quaisquer dos princípios elencados pela LGPD, assegurando proteção e respeitando direito fundamental dos administrados.

Além desses esclarecimentos, vale ressaltar que nem sempre pode a Administração realizar tratamentos de dados, ainda que estes estejam à sua disposição, mas tão somente à assunção de finalidades reconhecidas, nos termos dos princípios legais postos. Assim, passemos à análise das hipóteses nas quais a Administração Pública possa exercer esse tratamento.

## 3 HIPÓTESES DE PROCESSAMENTO DE DADOS PELA ADMINISTRAÇÃO PÚBLICA

A Administração Pública, como regra geral, se submete à LGPD quando lidar com dados pessoais para a execução de políticas públicas, previamente estipuladas por lei ou regulamentos ou, ainda, com respaldo em contratos, convênios ou instrumentos congêneres pela Administração Pública. Entre as muitas regras estabelecidas, encontra-se o princípio de responsabilidade, elemento central nas

[11] PELLEGRINO, Carlos Roberto**.** Os contratos da administração pública**. Revista de Direito Administrativo**, v. 179, 1990, p. 68-91.
[12] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico ***Journal of Law*** [EJJL], v. 12, n. 2, 2011, p. 91-108.

relações envolvendo a gestão de dados por empresas e entes da administração pública. De acordo com este princípio, os controladores passam a ser civilmente responsáveis pelo armazenamento e pela proteção dos dados pessoais que coletam e armazenam.

Excepcionalmente, quando os dados são utilizados, exclusivamente, com a finalidade de segurança pela Administração Pública, as exigências legais não serão obrigatórias, conforme o seu art. 4º, III, alínea "a". Outra possibilidade capaz de gerar efeitos à Administração Pública é a possibilidade de aproveitamento dos dados para a realização de estudos por órgãos de pesquisa (art. 7º, IV), preferencialmente com a anonimização dos dados pessoais dos participantes. Ainda, podem ser tratados os dados pessoais quando for necessário para a execução de contratos nos quais o titular seja parte e este deve ser feito a pedido do próprio titular, ou para a execução de políticas públicas, conforme o art. 7º, III da Lei.

A utilização de dados para proteção da vida ou de alguma incolumidade física do titular ou de terceiro (art. 7º, VII) se enquadra, também, como uma possibilidade, além da tutela da saúde em procedimento realizado por profissional de saúde, serviços de saúde ou autoridade sanitária (art. 7º, VIII). Ainda, quando necessário para atender interesses legítimos do controlador ou de terceiro (art. 7º, IX), exceto quando entrarem em conflito com direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.[13]

E, finalmente, a última base sustenta o tratamento de dados pessoais para proteção do crédito, em observância às regras específicas para este tema. Nesta senda, a Lei Geral de Proteção de Dados Pessoais brasileira classifica os dados biométricos como dados sensíveis (art. 5º, II). Dessa forma, conforme o art. 11 desta Lei, o tratamento poderá ocorrer sem o consentimento do titular desde que estejam de acordo com as hipóteses do artigo citado acima e já debatidas anteriormente.[14]

---

[13] Nesse sentido, para Daniel Sarmento, a pessoa "[...] tem um valor intrínseco, e não pode ser instrumentalizada. [...] O ser humano é concebido como um sujeito com capacidade para tomar decisões e o direito de fazê-lo – daí a garantia das liberdades individuais e da democracia (autonomias privada e pública)". Cf. SARMENTO, Daniel. **Dignidade da pessoa humana***:* conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 76-77.

[14] Importante frisar a lição de Daniela Cravo, que leciona que "a simples caracterização de um dado como sensível não é suficiente para impedir que haja o tratamento desses dados, já que isso obstaculizaria certas atividades lícitas em que o uso de tais dados é legítimo e necessário, como aquelas em que a própria razão de ser estaria comprometida caso não se pudesse obter informações deste gênero, a exemplo de organizações políticas ou religiosas. Destarte, é possível e até mesmo desejável, em certas circunstâncias, o tratamento dos dados sensíveis, desde que isso não

Portanto, o emprego de pressupostos para o tratamento de dados em transportes públicos precisa ser utilizado pela Administração Pública de forma consonante ao art. 7º da LGPD. Assim, a Administração Pública, ao modelar e prever os impactos da sua atuação no processamento de dados de usuários do transporte público, deve observar as finalidades do tratamento de dados pessoais dispostos nos incisos do art. 7º.

## 4 A UTILIZAÇÃO PRÁTICA DE DADOS SENSÍVEIS EM TRANSPORTES PÚBLICOS

Como apresentado, anteriormente, existem dez bases legais que sustentam a LGPD, neste momento, duas delas serão tratadas com maior destaque nesta seção: o consentimento do titular dos dados e o legítimo interesse do controlador. Conforme o art. 7º da LGPD, o tratamento de dados pessoais é condicionado ao fornecimento de consentimento do titular (inciso I), excluindo as exceções já mencionadas. O consentimento, descrito pelo art. 5º, inciso XII da mesma lei, é a manifestação livre, informada e inequívoca por meio da qual o titular concorda com o tratamento de seus dados para uma finalidade determinada, consonante à segunda geração de proteção de dados.[15]

Entretanto, o consentimento absoluto do titular em relação à utilização de seus dados é inviável. Esta base, *per se,* não é capaz de garantir a devida proteção ao indivíduo, assim como, não se pode considerar que este é capaz de desempenhar uma tomada de decisão segura e legítima sobre a utilização dos seus dados pessoais, haja vista a assimetria de informações entre o titular e o controlador e a complexidade do fluxo de informações, impossibilitando que ele tenha um conhecimento completo do tratamento. Neste momento, vale ressaltar a teoria da decisão da utilidade subjetiva[16] , que afirma que a tendência do ser humano é focar

---

proporcione uma utilização discriminatória". Cf. CRAVO, Daniela Copetti. **Direito à portabilidade de dados**. Rio de Janeiro: Lumen Juris, 2018, p. 37.

[15] Nesse sentido, destaca-se o entendimento de Bruno Bioni sobre a segunda geração de leis de proteção de dados que "transfere para o próprio titular dos dados a responsabilidade de protegê-los. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais". BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 171.

[16] KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacqelyn; BLACK, Katie. *Soft surveillance, hard consent. In*: KERR, Ian (Ed.). *Lessons from the identity trail*: *anonymity, privacy and identity in a networked society*. New York: ***Oxford University Press***, 2009. p. 17.

em resultados em curto prazo, o que limitaria o processo de desenvolvimento e, também, a teoria prospectiva[17] que defende que a tomada de decisões é baseada nas perdas e nos ganhos e, neste cenário, as primeiras são preponderantes às segundas.

Nesta senda, pode-se observar que a proteção de dados pessoais é valorizada pelos indivíduos, mas, paradoxalmente, suas atitudes não estão em consonância com esta valorização já que, por exemplo, permitem acesso aos seus dados a empresas sem ao menos ler os termos de uso e privacidade. Sob essa perspectiva, como seria possível confiar a proteção de dados pessoais ao consentimento individual? Vale ressaltar, também, que o excesso de utilização dessa base pode levar a fadiga do consentimento, de mesma forma que pode inviabilizar o processo de tratamento de dados pelo excesso de burocracias.

Outra base importante é a do legítimo interesse do controlador, o qual só poderá fundamentar o tratamento dos dados pessoais para fins legítimos exemplificados pelo rol do art. 10 da Lei Geral de Proteção de Dados.[18] Apesar de não se limitar às finalidades do art. 10, é importante perceber que este não pode se tornar uma maneira de relativizar direitos dos titulares. Ainda assim, a base legal em questão deve ser vista sob a perspectiva da necessidade, do balanceamento, da transparência e da minimização dos riscos ao titular.

Tendo esse contexto como base, e fazendo uma análise quanto à utilização de dados pessoais em transportes públicos, destacar-se-á alguns pontos. Em um primeiro estudo, em uma situação na qual o tratamento de dados for realizado para fins exclusivamente jornalísticos, artísticos, acadêmicos – em observância aos arts. 7º e 11º desta lei – e exclusivos de segurança pública, defesa nacional, segurança do Estado ou para atividades de investigação e repressão de infrações penais, não há a incidência da LGPD.

A dúvida paira quando se fala de finalidades não exclusivas àquelas elencadas pelo art. 4º e abordadas no parágrafo anterior. Há de se levar em

[17] KERR Ian *et al*. *op. cit.*, 2009, p. 18.
[18] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

consideração o princípio da supremacia da Constituição de 1988.[19] E, para tanto, relembrar os direitos fundamentais expostos no art. 5º da Constituição Federal. A segurança, como uma garantia constitucional e cláusula pétrea da Constituição de 1988, ao ser sopesada a outros direitos e princípios, deve ser considerada preponderante a outros não fundamentais.

Nesse sentido, a proteção de dados não é considerada como um direito de propriedade, mas sim de personalidade[20], o qual está previsto no Código Civil (art. 11 ao art. 21), norma infraconstitucional. Outro ponto a ser levantado é a tratamento de dados sensíveis, regulado pelo art. 11 da LGPD, o qual enfrenta menores obstáculos, principalmente nos casos que não necessitam do consentimento do titular, dispostos no inciso II quanto ao tratamento compartilhado de dados pela administração pública necessários à execução de políticas públicas.

## 5 CONSIDERAÇÕES FINAIS

Tendo em vista as situações expostas acima, conclui-se que a utilização de dados sensíveis seria flexibilizada para atender a garantia ao cumprimento de obrigações legais e regulatórias impostas ao controlador, para auxiliar principalmente no desenvolvimento de políticas públicas por parte da Administração Pública. Desta maneira, possibilita-se o respaldo do tratamento dos dados coletados em transportes públicos em bases legítimas. O ponto principal é definir de maneira clara a finalidade da utilização dos dados sensíveis, e de uma maneira mais geral, dos dados pessoais.

Vale ressaltar, também, os princípios basilares elencados pela própria LGPD em seu art. 6º, como os princípios da finalidade, da necessidade, da segurança e da prevenção, já discutidos anteriormente. Isto posto, quando a Administração Pública se utiliza de dados pessoais dos usuários de transportes públicos para os fins

[19] Para Paulo Gonet, "a supremacia fixa o *status* hierárquico máximo da Constituição no conjunto das normas do ordenamento jurídico. [...] positiva uma hierarquia entre as normas jurídicas, em que a Constituição aparece como o conjunto de normas matrizes do ordenamento jurídico, em posição de prevalência sobre todos os atos normativos que hão de nele encontrar fundamento jurídico último". Cf. MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional***,* 12 ed. rev. e atual. São Paulo: Saraiva, 2017, p. 62.

[20] Para Bruno Bioni, Personalidade significa as "características ou o conjunto de características que distingue uma pessoa da outra. [...] um dado, atrelado à esfera de uma pessoa, pode se inserir dentre os direitos da personalidade. Para tanto, ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular". Cf. BIONI, *op. cit.*, 2019. p. 99.

debatidos acima, não se vislumbra conflitos normativos, porém a análise deverá ser feita caso a caso.

Por exemplo, tem-se como exemplo a Ação Civil Pública nº 1090663-42.2018.8.26.0100, na qual o IDEC (Instituto Brasileiro de Defesa do Consumidor) litiga contra a Concessionária da Linha 4 do Metrô de São Paulo S.A (VIAQUATRO) contra o tratamento de dados sensíveis por meio de um sistema de portas de plataforma interativas no metrô de São Paulo. Nessa ocasião, decidiu-se deferir a tutela provisória de urgência para o fim de obrigar a VIAQUATRO a cessar a captação de imagens, sons e quaisquer outros dados através de câmeras ou outros dispositivos envolvendo portas digitais, sob pena de multa diária de R$ 50.000,00.[21] Assim, se tratando de finalidades diversas e, principalmente, quanto ao tratamento de dados sensíveis, a análise sobre a cadeia de captação, tratamento e armazenamento de dados é indispensável para a Administração Pública.

## REFERÊNCIAS


BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 171.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil).** DOU, 11 de janeiro de 2002, Seção 1, p. 1. Disponível em: <www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm>. Acesso em: 22 set. de 2020.

_____. **Constituição da República Federativa do Brasil de 1988**. DOU, 5 de outubro de 1988, Seção 1, p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 09 out. de 2020.

_____. **Lei nº 13.709, de 14 de agosto de 2018** *(Lei Geral de Proteção de Dados Pessoais).* DOU, 15 de agosto de 2018, Seção 1, p. 59. Disponível em: <www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 set. 2020.

CHESBROUGH, Henry, et al. *Open innovation: Researching a new paradigm.* ***Oxford University Press on Demand***, 2006, p. 1.

CRAVO, Daniela Copetti. **Direito à portabilidade de dados.** Rio de Janeiro: Lumen Juris, 2018, p. 37.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 206.


[21] TRIBUNAL DE JUSTIÇA DE SÃO PAULO**. ACP nº 1090663-42.2018.8.26.0100**. Relatora: Fabiana Marini, julgado em 14 de setembro de 2018, publicado em 18 de setembro de 2018.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico *Journal of Law***, v. 12, n. 2, 2011, p. 91-108.

FARIA, Luísa Campos; SANTOS, Luiza Mendonça da Silva Belo. **O Big Data e a privacidade de dados pessoais no controle de estruturas.** Mulheres no antitruste Vol. II, 2019, p. 56.

KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacqelyn; BLACK, Katie. Soft surveillance, hard consent. In: KERR, Ian (Ed.). *Lessons from the identity trail*: *anonymity, privacy and identity in a networked society*. New York: ***Oxford University Press***, 2009. p. 17.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014, p. 29.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional***,* 12 ed. rev. e atual. São Paulo: Saraiva, 2017, p. 62.

OPEN DATA INSTITUTE. *Personal data in transport: exploring a framework for the future*. ***Open Data Institute Publications***, 2018, p. 11.

PELLEGRINO, Carlos Roberto**.** Os contratos da administração pública. **Revista de Direito Administrativo**, v. 179, 1990, p. 68-91.

RIBEIRO, Paulo Dias de Moura. Lei Geral de Proteção de Dados: regulação*. In*: FONSECA, Reynaldo Soares da; COSTA, Daniel Castro Gomes da (coord.) **Direito regulatório***:* desafios e perspectivas para a Administração Pública. Belo Horizonte: Fórum, 2020, p. 133-137.

SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdo, trajetórias e metodologia. Belo Horizonte: Fórum, 2016, p. 76-77.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO**. ACP nº 1090663-42.2018.8.26.0100**. Relatora: Fabiana Marini, julgado em 14 de setembro de 2018, publicado em 18 de setembro de 2018.

WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy.* ***Harvard Law Review***, 1890, p. 195.

# A PROTEÇÃO E A TRANSPARÊNCIA DE DADOS SOB A PERSPECTIVA DOS CONTROLES EXTERNO E SOCIAL E A GOVERNANÇA DIGITAL

Daniela Zago Gonçalves da Cunda[1]
Letícia Ayres Ramos[2]
Roberto Debacco Loureiro[3]
Denizar Simioni[4]

## 1 CONSIDERAÇÕES INICIAIS

O imenso volume de dados pessoais utilizados pelo poder público, para o cumprimento de competências legais e para a execução de serviços e políticas públicas indica a importância da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) no setor público, sendo que o desafio de adequação às novas normas tem se mostrado proporcional ao tamanho desse universo de informações.

Além da natural complexidade do trabalho de avaliação e revisão de rotinas administrativas, com a necessária implantação de mudanças, a missão de alinhamento à LGPD, emanada pela Administração de cada órgão e instituição, precisa inicialmente superar as dificuldades geradas por divergências interpretativas em relação a matérias tratadas na Lei. Ainda que a falta de consenso seja natural na

[1] Conselheira-substituta do Tribunal de Contas do Rio Grande do Sul. Doutora e Mestre em Direito pela PUC/RS. Professora convidada em cursos de pós-graduação (PUC/RS e outros). Pesquisadora no Meeting of Researchers in Law and Sustainability e membro do grupo de pesquisa Estado Digital e Sustentável (PUC/RS). Autora de publicações nacionais e internacionais sobre gestão pública sustentável e transparente, direito/deveres fundamentais e controle externo. Presidente da Comissão de Sustentabilidade do TCE/RS. TCE/RS - Webconferência: Lei Geral de Proteção de Dados e o Poder Público - Mesa 1. Disponível em <https://www.youtube.com/watch?v=z3xCD-rK0tE>.

[2] Conselheira-substituta do Tribunal de Contas do Estado do Rio Grande do Sul. Mestre em Direito pela Universidade Federal do Rio Grande do Sul. Especialista em Direito Ambiental Nacional e Internacional pela UFRGS. Bacharel em Direito pela UFRGS. Membro do Comitê de Governança e da Comissão de Sustentabilidade do TCE/RS. TCE/RS - Webconferência: Lei Geral de Proteção de Dados e o Poder Público - Mesa 2. Disponível em <https://www.youtube.com/watch?v=Bn_0f4DgyMs>.

[3] Conselheiro-substituto do Tribunal de Contas do Estado do RS. Especialista em Direito Público pela Universidade Anhanguera-Uniderp. Bacharel em Direito pela Universidade Regional Integrada do Alto Uruguai e das Missões-URI Santo Ângelo. Presidente da Comissão de Estudos sobre a LGPD no TCE/RS. TCE/RS - Webconferência: Lei Geral de Proteção de Dados e o Poder Público - Mesa 2

[4] Oficial de Controle Externo do Tribunal de Contas do Estado do RS. Especialista em Direito Público pela Faculdade Projeção. Bacharel em Direito pela Universidade Ritter dos Reis. Relator da Comissão de Estudos sobre a LGPD no TCE/RS.

ciência jurídica, e com maior razão em relação a normas novas, a busca por uma relativa uniformidade nesta fase inicial de adaptação é dificultada pela incipiência da atuação da Autoridade Nacional de Proteção de Dados (ANPD)[5], órgão criado pela nova Lei com as atribuições, dentre outras, de elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, editar regulamentos, bem como deliberar, na esfera administrativa, sobre a interpretação da LGPD, além de promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança.

Nesse ambiente de incertezas, os gestores atuam premidos pela urgência, pois a LGPD está em vigor desde o dia 18 de setembro de 2020 (exceto os artigos 52 a 54, que tratam das sanções administrativas, com vigência prevista para 1º de agosto de 2021) e, desde aquela data, incidem regras rígidas para o tratamento de dados pessoais. Importante observar que a adequação deve se dar não somente em relação à LGPD, mas a todo o microssistema em que ela se insere, como a Lei nº 12.527/2011 (Lei de Acesso à Informação), a Lei nº 12.965/2014 (Marco Civil da Internet), a Lei nº 13.460/2017 (Lei do Usuário dos Serviços Públicos) e, mais recentemente, a Lei nº 14.129/2021 (que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública), além das necessárias diretrizes de governança.

O Poder Público, por expressa determinação legal[6], terá de se debruçar sobre a temática, pois obtém e trabalha com diversos dados relativos às pessoas. O Tribunal de Contas não está fora do âmbito da lei[7], pois dispõe de um acervo de informações daqueles que gerem os recursos públicos. Exemplificativamente, a dimensão do capital informacional disponível no banco de dados abertos do TCE/RS

---

[5] Apesar de os dispositivos da LGPD referentes à ANPD estarem em vigor desde 28/12/2018 (art. 65, inciso I, conforme alteração da Lei 13.853/2019), a indicação dos membros de sua primeira Diretoria foi referendada pelo Senado Federal somente em 20/10/2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/10/20/senado-confirma-primeira-diretoria-da-autoridade-nacional-de-protecao-de-dados>.

[6] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios (Incluído pela Lei nº 13.853, de 2019).

[7] No sentido de que os Tribunais de Contas encontram-se abrangidos pela Lei. MACIEL, Moisés. Os Tribunais de Contas no exercício do controle externo face à nova Lei Geral de proteção de Dados Pessoais. Disponível em <https://www.researchgate.net/publication/341377759_Os_tribunais_de_contas_no_exercicio_do_controle_externo_de_acordo_com_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais>. Acesso em: 20 mar. de 2020.

foi reconhecida recentemente como um dos dez maiores acervos no mundo.[8] No tocante a dados pessoais, alguns exemplos podem elucidar o seu significado: dados de denunciantes, dados de visitantes às dependências do Tribunal, dados dos gestores que necessitam realizar cadastro para fins da prestação de contas, dados pormenorizados acerca das despesas dos entes públicos, dados dos servidores e membros do Tribunal de Contas como também dos demais jurisdicionados, entre outros. Soma-se a isso o fato de que, num contexto de diversos atores no desempenho do controle externo, ganha importância o compartilhamento de informações na busca de uma maior eficiência no combate ao mau uso dos recursos públicos. Situação que contribui para a ampliação do capital de informações que o Tribunal de Contas tem à disposição[9] .

Além de armazenar o universo de dados que está sob sua guarda, o Tribunal de Contas terá de garantir segurança no trato das informações, pois não só empresas privadas são alvos de invasões com a consequente disseminação da informação, como também os órgãos públicos.[10]

---

[8] Conforme notícia disponível em: <http://www1.tce.rs.gov.br/portal/page/portal/tcers/administracao/gerenciador_de_conteudo/noticias/Plataforma%20de%20dados%20abertos%20do%20TCE-RS%20%E9%20uma%20das%20dez%20maiores%20do%20mundo>. Acesso em 13 out. de 2020.

[9] Conforme já afirmado em estudos anteriores: CUNDA, Daniela Zago G.; RAMOS, Letícia A. Os 20 anos da Lei de Responsabilidade Fiscal: transparência e proteção de dados a tutelar os direitos fundamentais à *cibercidadania* e à boa *ciber@dministração* pública. *In* FIRMO FILHO, Alípio Reis *et all* (coord.) **Responsabilidade na Gestão Fiscal***:* Estudos em homenagem aos 20 anos da Lei Complementar n. 101/2000, Belo Horizonte: Fórum, 2020. Ciber@dministração Público e Controle 4.0, seus desafios em tempo de pandemia do coronavírus, e a transparência ampliada (para além de translúcida). CUNDA, Daniela Zago G.; RAMOS, Letícia A. Ciber@dministração Pública e Controle 4.0, seus desafios em tempo de pandemia do coronavírus, e a transparência ampliada (para além de translúcida). *In* LIMA, Luiz Henrique *et all* (coord.) **Os Desafios do Controle Externo diante da pandemia da COVID 19:** Estudos dos Ministros e Conselheiros Substitutos dos Tribunais de Contas, Belo Horizonte: Fórum, 2020.
LOUREIRO, Roberto Debacco. Participação: princípio expresso na Constituição do Estado do Rio Grande do Sul. *In:* **Revista Eletrônica do TCE/RS***.* Edição Especial dos 30 anos da Constituição Estadual. Disponível em: <https://www.atricon.org.br/wp-content/uploads/2019/07/REVISTA-ELETRONICA-3-TCERS-1.pdf>. Acesso em: 13 out. de 2020.

[10] O CNJ sofre ataque hacker com vazamento de dados: Disponível em: <https://valor.globo.com/politica/noticia/2019/04/01/cnj-sofre-ataque-hacker-com-vazamento-de-dados.ghtml>. Acesso em: 09 jan. de 2021. Outro caso envolveu o Detran do Rio grande do Norte, onde dados de 70 milhões de brasileiros foram vazados por tempo indeterminado. Conforme informação disponivel em: <https://www.correiodopovo.com.br/not%C3%ADcias/pol%C3%ADtica/vazamento-do-detran-reacende-debate-sobre-prote%C3%A7%C3%A3o-de-dados-pessoais-1.372948>. Acesso em 10 jan. de 2021. Mais recentemente, veio à tona a invasão dos servidores do Tribunal de Justiça do Estado do Rio Grande do Sul, com a notícia do acesso indevido a dados processuais, dados de contas bancárias e das declarações de imposto de renda dos servidores daquela instituição, disponível em <https://gauchazh.clicrbs.com.br/geral/noticia/2021/04/sistema-do-tj-rs-segue-sob-ataque-de-invasores-que-emitem-mensagem-pedindo-pagamento-de-bitcoins-cko4704ma0006018mjsyixl18.html>. Acesso em: 11 mai. de 2021.

Ao lado dos riscos advindos do armazenamento de dados, há de se ter em mente que, para o desempenho de suas atividades em prol do controle externo, os Tribunais recebem e tratam dados para fins de dar cabo à sua missão constitucional. Para tanto, deverão observar o regime jurídico previsto no artigo 7º, inciso III e § 3º, combinado com o artigo 23 da LGPD. Tais disposições aplicam-se no desempenho de suas atividades administrativas e finalísticas, visto que toda atuação realizada por parte das Cortes de Contas é obrigatoriamente pautada no princípio da legalidade e na persecução do interesse público.

No entanto, para que a atividade fiscalizatória ocorra de maneira eficaz, com qualidade e eficiência, é necessário assegurar que os Tribunais de Contas executem suas competências constitucionais e legais de acordo com os princípios da publicidade, da eficiência, da supremacia do interesse público, da transparência das informações e do acesso geral às prestações de contas de maneira a viabilizar o mais amplo controle social (mediante uma leitura conjunta dos arts. 5º, 37 e 71 da CF88).

Diante disso, tem-se que a aplicação da Lei Geral de Proteção de Dados (LGPD) trará reflexos para os Tribunais de Contas tanto na execução de seus processos internos (administrativos) quanto no desempenho de suas atividades finalísticas. Não obstante, sua interpretação e aplicação deverão ser feitas em consonância com o aparato jurídico e constitucional já existente, sem retroceder em termos de publicidade, transparência e acesso à informação, conquistas constitucionais robustecidas na Lei de Responsabilidade Fiscal com os acréscimos trazidos pela Lei Complementar nº 131/2009, assim como também pela Lei de Acesso à Informação (Lei nº 12.527/2011), dentre outros normativos com objetos de tutela mais específicos como a “LAI Ambiental” (Lei nº 10.650/03).

Nesse aspecto, não devem ser olvidados os avanços dos últimos anos, em termos de transparência, controle social e participação popular, os quais só foram possíveis graças ao amplo acesso e à vasta disseminação de informações também robustecidas pela recente Lei nº 14.129, de 29 de março de 2021.

O presente estudo, nesse contexto, tem como objetivo contribuir na necessária tarefa de adaptação, buscando identificar as principais normas aplicadas especificamente ao setor público, assim como apresentar, de forma prática e simplificada, os passos iniciais dessa instigante caminhada, subsidiando os gestores com as informações essenciais para proceder ao alinhamento às novas normas de

proteção de dados pessoais, sem descurar-se da necessária transparência de dados a promover o controle social e a boa governança.

As reflexões a seguir foram confeccionadas da união de estudos científicos sobre o tema, sob a perspectiva da necessária cautela com a transparência pública e atuação dos Tribunais de Contas como provedores do controle social[11], assim como tendo por base os estudos e as pesquisas desenvolvidos durante os trabalhos da Comissão de Estudos sobre a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) do Tribunal de Contas do Estado do Rio Grande do Sul (TCE/RS)[12], que teve por objetivo apresentar orientações e sugestões, visando à correta adequação às novas normas, tanto para o referido órgão de controle, quanto para seus entes e órgãos jurisdicionados. Nesse âmbito, os esforços foram voltados para esclarecer quais os principais impactos da nova lei especificamente na atuação do setor público, bem como trilhar um caminho inicial para a implantação da LGPD, tecendo considerações, com viés prático, acerca da sequência de providências entendidas como necessárias com sintonia entre diretrizes emanadas pela alta administração e a implementação e execução pelo corpo técnico.

O enfrentamento do tema será sob a perspectiva do controle externo e controle social, também sob ótica do direito fundamental à informação, direito fundamental à proteção de dados[13], conjuntamente com uma abordagem sobre o direito/dever fundamental de boa administração pública (ou boa governança) e a necessária utilização das novas tecnologias delineando a *ciber@administração*, com destaque a aspectos relevantes sobre os temas centrais, tendo em mente a legislação vigente, centralizando o debate sobre três principais eixos: proteção de dados, transparência e governança tecnológica[14].

Trata-se, portanto, de uma pesquisa além de descritiva, também experimental, sobre a implementação da LGPD interligada às legislações referidas,

---

[11] CUNDA, *op. cit.*, 2020.

[12] Período de atuação: de 28/10/2020 a 15/02/2021. Integrantes: Roberto Debacco Loureiro (Presidente), Denizar Simioni (Relator), Alexandre Porto Debeluck, Andrea Mallmann Couto, Carlos Eduardo Manzoni Moreira, Cláudio Ferreira Baques, Daniela Russomano Hentschel, Fernanda Nunes, Isadora Formenton Vargas, Ricardo Fritsch e Vinicio Rossetto.

[13] Sobre a proteção de dados como um direito fundamental autônomo vide a Proposta de Emenda à Constituição (PEC) n.º 17 em 2019, que tem por objetivo a inserção de tal direito no inciso XII do artigo 5º da CF, ao lado dos direitos à inviolabilidade da comunicação de dados, correspondência e das comunicações telefônicas. Também sobre o tema: Medida Cautelar da ADI 6387 pelo Supremo Tribunal Federal (STF) em 2020.

[14] Os três eixos, além de suas previsões específicas, constam previstos e receberam reforço na recente Lei nº 14.129/2021.

assim como de uma pesquisa bibliográfica, documental e jurisprudencial. Busca-se, como resultado, propiciar reflexões aos órgãos públicos, com ênfase aos órgãos de controle, e conscientização da missão constitucional a ser assumida por todos como provedores do *direito fundamental à proteção de dados* e ao *direito de informação* (a incluir a transparência quanto ao tratamento dos dados)[15].

## 2 CONTEXTUALIZAÇÃO DO "MICROSSISTEMA DE PROTEÇÃO E DE TRANSPARÊNCIA DE DADOS" E O GOVERNO DIGITAL

No tocante às diretrizes da LGPD, pode-se dizer que irá concretizar o trato das informações no uso da internet, uma vez que o Marco Civil referenciou que a proteção dos dados pessoais ocorreria na forma da lei. Entretanto, não significa que o jurista terá de se debruçar apenas nesta lei. Na realidade, a lei em estudo se insere em um sistema com diversos diplomas que deverão dialogar entre si sem o esquecimento da Lei de Responsabilidade Fiscal[16].

Também é de destacar que a proteção dos dados não se encontrava desamparada antes da edição da Lei n 13.709/2019[17]. Situação que demonstra a

[15] Inclusive nos termos estabelecidos pela recente Lei 14.129/2021, conforme o art. 25. As Plataformas de Governo Digital devem dispor de ferramentas de transparência e de *controle do tratamento de dados pessoais* que sejam claras e facilmente acessíveis e que permitam ao cidadão o exercício dos direitos previstos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

[16] Conexão que foi reforçada pela Lei 14.129, de 29 de março de 2021, que no art. 29 trata do Governo como Plataforma e da abertura dos dados, estabelecendo no § 1.º a promoção da transparência ativa de dados, tendo a observância da publicidade dos dados como preceito geral e o sigilo como exceção. No § 2º ratifica a necessidade de publicação dos seguintes dados na internet: I - o orçamento anual de despesas e receitas públicas do Poder ou órgão independente; II - a execução das despesas e receitas públicas, nos termos dos arts. 48 e 48-A da Lei Complementar nº 101, de 4 de maio de 2000; III - os repasses de recursos federais aos Estados, aos Municípios e ao Distrito Federal; IV - os convênios e as operações de descentralização de recursos orçamentários em favor de pessoas naturais e de organizações não governamentais de qualquer natureza; V - as licitações e as contratações realizadas pelo Poder ou órgão independente; VI - as notas fiscais eletrônicas relativas às compras públicas; VII - as informações sobre os servidores e os empregados públicos federais, bem como sobre os militares da União, incluídos nome e detalhamento dos vínculos profissionais e de remuneração; VIII - as viagens a serviço custeadas pelo Poder ou órgão independente; IX - as sanções administrativas aplicadas a pessoas, a empresas, a organizações não governamentais e a servidores públicos; X - os currículos dos ocupantes de cargos de chefia e direção; XI - o inventário de bases de dados produzidos ou geridos no âmbito do órgão ou instituição, bem como catálogo de dados abertos disponíveis; XII - as concessões de recursos financeiros ou as renúncias de receitas para pessoas físicas ou jurídicas, com vistas ao desenvolvimento político, econômico, social e cultural, incluída a divulgação dos valores recebidos, da contrapartida e dos objetivos a serem alcançados por meio da utilização desses recursos e, no caso das renúncias individualizadas, dos dados dos beneficiários.

[17] OLIVEIRA, Marco Aurélio Belizze, LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei nº 13.709/2018. *In:* FRAZÃO, Ana,

maior complexidade, para compreensão de um sistema protetivo no tocante ao tratamento dos dados pessoais[18] .

Alguns exemplos podem elucidar o fato de que a Lei consolidou diretrizes já mencionadas em outros diplomas legais, como a necessidade de informação acerca de abertura de cadastro, prevista na Lei do Cadastro Positivo (inciso V do artigo 5º da Lei nº 12.414/2011). Da mesma forma, o livre acesso às informações, previsto no inciso IV desse mesmo artigo, também é amplamente tratado na Lei de Acesso à Informação em seu artigo 5º.

Importante ressaltar que a LGPD, já no seu artigo 2º, enumera seus fundamentos, destacando a proteção à privacidade e à autodeterminação do indivíduo no tocante aos dados pessoais[19]. Ao mesmo tempo em que procura prever uma maior proteção dos dados, o diploma não se fecha ao progresso científico, uma vez que assegura a não aplicação da lei, quando envolver fins acadêmicos, assim como, também, deverá ser interpretada em consonância com a Lei nº 14.129/2021[20], em um contexto de *ciber@dministração* pública e de controle externo 4.0[21].

Com o objetivo de instalar um verdadeiro "microssistema de proteção e transparência de dados" a lei traz em seu artigo 6° um rol de princípios que deverão

---

TEPEDINO, Gustavo; OLIVA, Milena Donato(Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1 ed. São Paulo: Thomson Reuters Brasil, 2019, p.62.

[18] OLIVEIRA, *op. cit.,* 2019, p.72.

[19] "Espaço de liberdade no qual a escolha do indivíduo sobre a publicização e o tratamento de seus dados pessoais deve prevalecer", conforme: MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação, *op. cit.,* p. 203.

[20] Sobre o tema, recomendável a interpretação conjunta com os artigos 17 e 44 da Lei sobre Governo Digital. O art. 44 refere que "os entes públicos poderão instituir laboratórios de inovação, abertos à participação e à colaboração da sociedade para o desenvolvimento e a experimentação de conceitos, de ferramentas e de métodos inovadores para a gestão pública, a prestação de serviços públicos, o tratamento de dados produzidos pelo poder público e a participação do cidadão no controle da administração pública. E também sobre as "redes de conhecimento". No art. 17 da mesma lei, há previsão das "Redes de Conhecimento": "o Poder Executivo federal poderá criar redes de conhecimento, com o objetivo de: I - gerar, compartilhar e disseminar conhecimento e experiências; II - formular propostas de padrões, políticas, guias e manuais; III - discutir sobre os desafios enfrentados e as possibilidades de ação quanto ao Governo Digital e à eficiência pública; IV - prospectar novas tecnologias para facilitar a prestação de serviços públicos disponibilizados em meio digital, o fornecimento de informações e a participação social por meios digitais." No parágrafo 2.º estabelece-se que "serão assegurados às instituições científicas, tecnológicas e de inovação o acesso às redes de conhecimento e o estabelecimento de canal de comunicação permanente com o órgão federal a quem couber a coordenação das atividades previstas neste artigo."

[21] Nos termos melhores detalhados nos seguintes estudos: CUNDA, Daniela Zago G.; RAMOS, Letícia A. Os 20 anos da Lei de Responsabilidade Fiscal: transparência e proteção de dados a tutelar os direitos fundamentais à cibercidadania e à boa *ciber@dministração* pública. *In* FIRMO FILHO, Alípio Reis *et all* (coord.) **Responsabilidade na Gestão Fiscal***:* Estudos em homenagem aos 20 anos da Lei Complementar n. 101/2000, Belo Horizonte: Fórum, 2020.

orientar a gestão da informação nos órgãos públicos e privados e sob o viés do *direito/dever de boa ciber@dministração*[22] deverão ser lidos em conjunto os princípios e diretrizes (art. 3º) atinentes à Prestação Digital dos Serviços Públicos na Administração Pública (Lei nº 14.129/2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública)[23].

Outro princípio que se encontra elencado é o de que seja respeitada a finalidade[24] com a consequente relação entre o tratamento de dados e a finalidade informada[25] . No tocante a este princípio, é de ressaltar que, em termos de direito público, o usuário da informação deverá respeitar os princípios da adequação e da necessidade, corporificados na proporcionalidade, que se encontra prevista

---

[22] Conforme já afirmado deste o seguinte estudo: CUNDA, Daniela Zago Gonçalves da. **O Dever Fundamental à Saúde e o Dever Fundamental à Educação na Lupa dos Tribunais (para além) de Contas**. *Ebook*, Porto Alegre: Editora Simplíssimo Livros, 2013.

[23] Art. 3º São princípios e diretrizes do Governo Digital e da eficiência pública: (...) IV - a transparência na execução dos serviços públicos e o monitoramento da qualidade desses serviços; V - o incentivo à participação social no controle e na fiscalização da administração pública; VI - o dever do gestor público de prestar contas diretamente à população sobre a gestão dos recursos públicos; VII - o uso de linguagem clara e compreensível a qualquer cidadão; VIII - o uso da tecnologia para otimizar processos de trabalho da administração pública; IX - a atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle dos serviços públicos, com o compartilhamento de dados pessoais em *ambiente seguro quando for indispensável para a prestação do serviço*, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e, quando couber, com a transferência de sigilo, nos termos do art. 198 da Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), e da Lei Complementar nº 105, de 10 de janeiro de 2001; XIV - a interoperabilidade de sistemas e a promoção de dados abertos; XVII - *a proteção de dados pessoais*, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais); XX - o estímulo a ações educativas para qualificação dos servidores públicos para o uso das tecnologias digitais e para a inclusão digital da população; XXI - o apoio técnico aos entes federados para implantação e adoção de estratégias que visem à transformação digital da administração pública; XXIII - a implantação do governo como plataforma e a *promoção do uso de dados, preferencialmente anonimizados,* por pessoas físicas e jurídicas de diferentes setores da sociedade, resguardado o disposto nos arts. 7º e 11 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), com vistas, especialmente, à formulação de políticas públicas, de pesquisas científicas, de geração de negócios e de controle social; XXV - a adoção preferencial, no uso da internet e de suas aplicações, de tecnologias, de padrões e de formatos abertos e livres, conforme disposto no inciso V do *caput* do art. 24 e no art. 25 da Lei nº 12.965, de 23 de abril de 2014(Marco Civil da Internet); e XXVI - a promoção do desenvolvimento tecnológico e da inovação no setor público. Foram selecionadas as principais diretrizes em conexão com o presente estudo.

[24] O princípio da finalidade também foi confirmado mais uma vez na Lei 14.129/2021 em seu art. 25, § 1.º, que as ferramentas previstas nas plataformas de Governo Digital deverão "disponibilizar, entre outras, as fontes dos dados pessoais, a finalidade específica do seu tratamento pelo respectivo órgão ou ente e a indicação de outros órgãos ou entes com os quais é realizado o uso compartilhado de dados pessoais, incluído o histórico de acesso ou uso compartilhado, ressalvados os casos previstos no inciso III do **caput** do art. 4º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)".

[25] Por fim, decisão da Justiça de SP determinou a paralisação da coleta de dados biométricos dos passageiros, em função de que não estava clara a finalidade da captação das imagens e a forma como seriam tratados os dados. Conforme: <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&UserActiveTemplate=mobile&UserActiveTemplate=site&infoid=48974&sid=18>. Acesso em: 10 jan. de 2020.

expressamente na LGPD, como, também, nas recentes alterações da LINDB, proferidas pela Lei nº 13.655/2018[26]. Ou seja, por exemplo, os termos de uso da informação deverão ser revisados para que estejam em consonância com os princípios trazidos pela nova lei, considerando ainda que devem estar norteados pela transparência, proporcionalidade e necessidade[27], assim como em sintonia com as previsões legais atinentes a Prestação Digital dos Serviços Públicos na Administração Pública[28].

É importante registrar que a doutrina tem apontado que um dos princípios mais marcantes da LGPD é o da transparência, não apenas às informações, mas, principalmente, de todo o processo de tratamento de dados.[29] Os contornos deste princípio podem ser encontrados nos artigos 9º, 10, 18 e 20. Este fato demonstra a similitude de premissas dogmáticas também com as constantes na Lei de Responsabilidade Fiscal e nas diretrizes de governança, no que diz respeito à transparência. Muda-se o enfoque, mas a premência da transparência é que permeia o sistema, temática de averiguação pelo controle externo e um dos principais instrumentos do controle social[30].

Registre-se que a LGPD condicionou a possibilidade de tratamento de dados pessoais ao enquadramento em alguma das hipóteses elencadas no seu artigo 7º[31].

---

[26] Alguns estudos sobre o tema: CUNDA, Daniela Zago G. da. Comentários ao art. 21 da LINDB. In: DUQUE, Marcelo Schenk; RAMOS, Rafael (Coord.). **Segurança Jurídica na aplicação do Direito Público**. Salvador: Editora Juspodivm, 2019, pp. 57-78. CUNDA, Daniela Zago G. A LINDB, suas profecias para o enfrentamento da pandemia e as necessárias reformulações da Administração Pública e do Respectivo Controle. da. *In:* MAFFINI, Rafael; RAMOS, Rafael. **Nova LINDB:** Consequencialismo, deferência judicial, motivação e responsabilidade do gestor público. Rio de Janeiro: Lumen Juris, 2020, p. 279 e ss.

[27] SANTOS, Fabíola Meira de Almeida, TALIBA, Rita. Lei Geral de Proteção de Dados no Brasil e os possíveis impactos. **Revista dos Tribunais Online**, vol. 998/2018, p.225-239, p. 227.

[28] Vide a Lei 14.129/2021 (que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública).

[29] Sobre o tema: OLIVEIRA, *op. cit.,* 2019, p.76.

[30] Maiores detalhes sobre o tema constam no estudo anteriormente já referido: CUNDA, *op.cit., 2019.*

[31] Art. 7º - I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; 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; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do

Percebe-se que o tratamento de dados pessoais pelo poder público estará embasado, na maioria das vezes, nos incisos II e III. Importante ressaltar que tais hipóteses de tratamento de dados pessoais dispensam o consentimento do titular, previsto no inciso I.

Deve-se observar, além disso, que a regularidade do tratamento de dados pessoais pelas pessoas jurídicas de direito público está também condicionada às exigências do artigo 23 da LGPD: atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, e, ainda, desde que sejam informadas as hipóteses em que ocorre o tratamento de dados pessoais, e seja indicado um encarregado.

Ademais, o poder público deve observar outros princípios que norteiam as atividades de tratamento de dados pessoais dispostos no *caput* e incisos do artigo 6º da LGPD[32] e, também, constantes no transcorrer da Lei nº 14.129/2021.

Em complemento, vale referir que algumas hipóteses de tratamento de dados pessoais - as quais devem ser identificadas detalhadamente a partir de inventário e mapeamento - podem não estar amparadas nas finalidades específicas de cada órgão ou entidade, o que enseja um tratamento diferenciado, principalmente em se tratando de dados sensíveis (art. 11 da LGPD), cabendo a análise de cada situação em particular.

---

titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

[32] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Demonstrada a repercussão da Lei Geral de Proteção de Dados na atuação dos órgãos públicos, assim como elucidada a necessária interpretação sistemática, seguem considerações atinentes à implementação prática realizada pela Comissão de Estudos sobre a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) do Tribunal de Contas do Estado do Rio Grande do Sul (TCE/RS).

## 3 IMPLEMENTAÇÃO DA LGPD NO TCE/RS COMO UMA ESTRUTURA PERMANENTE

Após detida análise da legislação e estudos da experiência de diversos órgãos e instituições na implantação da Lei, conclui-se que o primeiro passo, para se promover a adequação à nova legislação, é a criação, em norma interna, da estrutura que fará a gestão permanente da proteção de dados pessoais, com a definição das figuras do controlador e do encarregado, bem como a instituição de um grupo permanente de gestão – subordinado ao controlador –, com atribuições para deliberar e executar a política de proteção de dados.

A esse grupo permanente (geralmente denominado de “comitê” ou de “comissão”), com a participação do encarregado, caberá a efetiva implantação da nova política de proteção de dados pessoais, seu acompanhamento, a elaboração do inventário de dados pessoais e do relatório de impacto à proteção de dados pessoais, o tratamento de incidentes, a gestão de demandas de informação, a adequação dos processos de governança corporativa, a revisão documental com a melhoria de procedimentos e fluxos internos e externos e, como resultado desse trabalho, promover a mudança de cultura no tratamento de dados pessoais.

### 3.1 DO CONTROLADOR, DO OPERADOR E DO ENCARREGADO

A respeito da indicação do controlador, do operador e do encarregado, figuras criadas pela norma para identificar os responsáveis por determinados atos relacionados ao tratamento de dados pessoais, cabem algumas observações.

O controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (inciso VI do artigo 5º). Não restam dúvidas, portanto, de que o controlador é o próprio órgão ou entidade pública. O controlador pode exercer, diretamente, o tratamento dos dados ou designar um operador.

O operador é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (inciso VII do artigo 5º). Entende-se que tal figura é equivalente à do “subcontratado”, prevista inicialmente no Projeto de Lei nº 4060/2012, e está sujeito a duas condições: ser uma entidade diversa do controlador e tratar dados pessoais em nome do controlador.

Trata-se, de fato, daquele que é subcontratado para a realização do tratamento de dados pessoais. Consoante o artigo 42 da LGPD, o operador responde solidariamente com o controlador por danos causados no exercício de atividade de tratamento de dados pessoais.

A fim de melhor esclarecer a questão, que, registre-se, vem gerando interpretações divergentes (há órgãos entendendo que os operadores são os servidores e outros agentes que manejam dados pessoais), Teixeira e Armelin [33] destacam:

> O controlador e o operador são espécies do gênero agente de tratamento e aparecem na lei da mesma forma que previsto no GDPR, que lá receberam a nomenclatura de *controller* (controlador) e *processor* (operador). A importância da distinção dessas duas figuras se dá principalmente quando se fala no tratamento de dados por empresas, já que muitas vezes uma empresa contrata 'dando ordens', enquanto a outra executa essas ordens. A lei se aplica a ambas as figuras, tanto ao controlador quanto ao operador, o que acarreta em responsabilidade para ambos. Podemos citar como exemplo de operador aquele que apenas armazena os dados a pedido do controlador, os chamados *Cloud Service Provider* (Fornecedor de Serviços em Nuvem), em que seus servidores poderão estar localizados em diferentes países.

Nessa linha, importante, também, destacar excerto da Nota Técnica 001/2020, da Consultoria Técnica do Tribunal de Contas do Estado do Rio Grande do Sul[34] :

> No caso do Operador, poder-se-ia referir à pessoa natural ou jurídica que realiza o tratamento de dados em nome do controlador. Exemplo: SERPRO ou DATAPREV na esfera federal, os quais atuam como operadores quando processam dados pessoais de outros órgãos ou entidades.

Diante disso, entendeu-se que, no âmbito do Tribunal de Contas do Estado do Rio Grande do Sul, o tratamento dos dados deve ser dirigido e realizado pelo próprio controlador, não sendo adequada a designação de operador (es).

---

[33] TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais** - Comentada Artigo por Artigo. 2. ed. Salvador: JusPodivm, p. 45. 2020.
[34] RIO GRANDE DO SUL. Tribunal de Contas do Estado. Consultoria Técnica. **Nota Técnica nº 1, de 6 de março de 2020**. Lei Geral de Proteção de Dados. Porto Alegre, p. 5. 2020.

Por sua vez, o encarregado é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)", nos termos do inciso VIII do artigo 5º da LGPD.

Em uma leitura sistemática da legislação, no entanto, infere-se que a atuação do encarregado abrange outras atividades e que precisam ser considerados requisitos de experiência, conhecimento e formação para o desempenho da função. Portanto, demonstra ser recomendável uma leitura conjunta dos artigos 23 e 41 da LGPD[35].

Pode-se acrescentar ao rol de atribuições do encarregado, por determinação do controlador (inciso IV antes referido), o que é sugerido no Guia de Elaboração de Programa de Governança em Privacidade do Governo Federal[36] :

> 4. Apoiar a definição de diretrizes de construção do inventário de dados pessoais relativos ao registro das operações de tratamento de dados pessoais determinado pelo artigo 37 da LGPD;
>
> 5. Conduzir ou aconselhar a elaboração do relatório de impacto à proteção de dados pessoais, de acordo com casos previstos pela LGPD em que tal documento é necessário;
>
> 6. Conduzir ou aconselhar a implementação de regras de boas práticas e de governança especificadas pelo artigo 50 da LGPD;

---

[35] 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; II - (VETADO); e III - *seja indicado um encarregado* quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e IV - (VETADO). [...] Art. 41. *O controlador deverá indicar encarregado* pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

[36] BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital**. Guias Operacionais para adequação à LGPD**. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd. Acesso em: 2 fev. de 2021.

Conforme o mesmo guia (p. 12), convém que a indicação do encarregado recaia sobre servidor com experiência na análise e elaboração de respostas de pedidos de acesso à informação demandados pelo Serviço de Informações ao Cidadão ou pela Ouvidoria; com conhecimentos multidisciplinares, incluindo as áreas de gestão, segurança da informação, gestão de riscos, tecnologia da informação, proteção da privacidade e governança de dados, e que tenha concluído cursos de capacitação em proteção de dados no setor público e governança de dados.

Recentemente a Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia editou a Instrução Normativa SGD/ME nº 117[37], tratando de orientações aos órgãos e entidades da administração pública federal para a indicação do Encarregado pelo Tratamento dos Dados Pessoais. Dentre os temas tratados, destaca-se que o encarregado "deverá possuir conhecimentos multidisciplinares essenciais à sua atribuição" e "não deverá se encontrar lotado nas unidades de Tecnologia da Informação ou ser gestor responsável de sistemas de informação do órgão ou da entidade". Ainda, deverá ser assegurado ao encarregado "acesso direto à alta administração".

Observa-se, portanto, que o encarregado ocupa posição de maior importância do que aquela que a definição do artigo 5º da LGPD pode aparentar.

No âmbito do TCE/RS, a Presidência, por meio de portaria nº 22/2020, de 18 de dezembro de 2020, designou o Diretor-Geral para exercer a função de encarregado, e explicitou que o Tribunal é o controlador.

## 3.2 DO GRUPO PERMANENTE DE GESTÃO

Além disso, conforme referido, recomenda-se a criação de um grupo permanente de gestão da proteção de dados, que, sob a supervisão do controlador e com a participação do encarregado, terá a incumbência de fazer a implementação da nova política de privacidade.

Esse grupo, a ser composto por agentes públicos conhecedores da matéria e com envolvimento no tratamento de dados, deverá possuir poderes e atribuições para deliberar sobre casos específicos e sobre demandas baseadas na LGPD e,

[37] BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020**. Brasília, 2020. Diário Oficial da União, Brasília, 20 nov. 2020, ed. 222, seção 1, p. 92. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596. Acesso em: 2 fev. 2021.

inicialmente, realizar o inventário de dados pessoais**,** a verificação da atual política de segurança da informação (art. 46 da LGPD) e adotar as providências para viabilizar o livre acesso pelo titular às informações sobre o tratamento de seus dados (art. 9º da LGPD).

O grupo permanente, ademais, deve consistir no foro de debates e estudos a respeito da matéria no âmbito dos órgãos e entes públicos[38].

## 3.3 DA REGULAMENTAÇÃO DE NOVA POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

Passo fundamental, também, será a regulamentação interna da LGPD. Sugere-se que o órgão ou entidade pública edite norma instituindo sua própria Política de Proteção de Dados Pessoais, explicitando, com base na Lei, os principais princípios, diretrizes e conceitos, e designando a estrutura permanente, com suas atribuições, entre outras regras gerais, sem se perder de vista que tal Política, certamente, deverá ser regulamentada com maiores detalhes posteriormente, no decorrer dos trabalhos efetivos de implantação, momento em que ficarão mais claras as necessidades de cada órgão ou entidade, e quando poderão mais adequadamente ser colmatadas as hipóteses omissas.

## 3.4 DA REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Uma das principais preocupações do legislador foi a de garantir que o tratamento das informações pessoais ocorra com segurança, a fim de se evitar acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, devendo os agentes de tratamento adotar medidas técnicas e administrativas aptas a proteger os dados pessoais (art. 46 da LGPD).

Assim, uma das primeiras providências deve ser a análise e a revisão dos sistemas de informática por meio dos quais são tratados os dados, a fim de reforçar os instrumentos de proteção e mitigar os riscos.

---

[38] No que se refere ao TCE/RS, a Comissão de Estudos sobre a LGPD recomendou à Presidência a criação do Comitê Permanente de Gestão da Proteção de Dados Pessoais, a ser integrado pelo encarregado e por representantes da Presidência, dos Gabinetes dos Conselheiros, da Auditoria, do Ministério Público de Contas, da Supervisão de Informática, da Assessoria de Sistemas de Controle Externo, do Centro de Gestão Estratégica de Informação para o Controle Externo, da Ouvidoria, da Direção-Geral, da Direção de Controle e Fiscalização, da Direção Administrativa, da Supervisão de Gestão de Pessoas, da Escola Superior de Gestão e Controle Francisco Juruena e da Assessoria de Comunicação Social.

Vale ressaltar que a Lei exige que o agente, além adotar medidas para cumprimento das normas, deve ter condições de comprovar sua eficácia (inciso X do artigo 6º da LGPD).

## 3.5 DO INVENTÁRIO DE DADOS PESSOAIS

Outro desafio primordial a ser enfrentado pelos integrantes da estrutura permanente (comitê/comissão, com a participação do encarregado) é o atendimento aos artigos 37 e 38 da LGPD[39].

Para o registro das operações de tratamento de dados pessoais, é pré-requisito a identificação de quais dados pessoais são tratados, onde estão e que operações são realizadas com eles, procedimento que recebe a denominação de inventário de dados pessoais.

Isso porque a LGPD vincula o tratamento de dados pessoais pelo poder público a alguns requisitos, entre eles a publicização sobre as hipóteses de tratamento, sendo, portanto, imprescindível a verificação dos tipos de dados pessoais tratados na rotina administrativa e finalística do órgão ou entidade e, eventualmente, se há operação e tratamento de dados sensíveis, com requisitos próprios de tratamento definidos em lei. Esse mapeamento de dados também serve ao tratamento de incidentes com dados pessoais, resultando em atualização das ferramentas de segurança.

Será necessário manter atualizado o inventário para o atendimento ao artigo 37 e, se assim determinado pela Autoridade Nacional em regulamentação futura, para a elaboração do relatório de impacto à proteção de dados pessoais de que trata o artigo 38, bem como para atender aos princípios de proteção da privacidade, especialmente àqueles expressos no artigo 6º.

O Governo Federal disponibiliza, na internet, um guia pormenorizado para a realização do inventário, bem como uma planilha modelo[40], para auxiliar nesse

---

[39] Art. 37. O controlador e o operador devem manter *registro das operações de tratamento de dados pessoais* que realizarem, especialmente quando baseado no legítimo interesse. Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos *tipos de dados coletados,* a *metodologia utilizada para a coleta e para a garantia da segurança das informações* e a análise do controlador com relação a *medidas, salvaguardas e mecanismos de mitigação de risco adotados.*

[40] BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guias Operacionais para adequação à LGPD**. Disponível em:

levantamento, baseados na experiência de autoridades de dados de países com cultura de proteção já consolidada. No referido guia, consta como informações necessárias no inventário (p. 6):

> De uma forma geral, esse registro mantido pelo IDP envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:
> - atores envolvidos (agentes de tratamento e o encarregado);
> - finalidade (o que a instituição faz com o dado pessoal);
> - hipótese (arts. 7º e 11 da LGPD);
> - previsão legal;
> - dados pessoais tratados pela instituição;
> - categoria dos titulares dos dados pessoais;
> - tempo de retenção dos dados pessoais;
> - instituições com as quais os dados pessoais são compartilhados;
> - transferência internacional de dados (art. 33 LGPD); e
> - medidas de segurança atualmente adotadas.

## 3.6 DA PUBLICAÇÃO DAS HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

A LGPD, conforme referido, dispensou o consentimento do titular, quando o tratamento dos dados pessoais é realizado pelo poder público, obedecidos os requisitos antes mencionados. Em contrapartida, exigiu que fossem informadas ao titular as hipóteses em que admitido o tratamento de seus dados pessoais, com informações precisas e claras sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades[41].

Assim, dentre as medidas urgentes a serem colocadas em prática também está a publicização das hipóteses de tratamento de dados pessoais, preferencialmente, em sítio eletrônico, de maneira a conceder a transparência no tratamento dos dados, um dos enfoques a ser tratado no tópico a seguir.

---

https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd. Acesso em: 2 fev. 2021.

[41] Assim preceitua a LGPD: Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] II - para o cumprimento de obrigação legal ou regulatória pelo controlador; 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; [...] § 1º Nos casos de aplicação do disposto nos *incisos II e III* do caput deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, *o titular será informado das hipóteses em que será admitido o tratamento de seus dados.*[...] 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.

# 4 A NECESSÁRIA COMUNICAÇÃO DA LGPD COM OS NORMATIVOS QUE TUTELAM A TRANSPARÊNCIA DE DADOS E O CONTROLE SOCIAL

Como já delineado, no transcorrer do presente estudo e em pesquisas anteriores, pode-se considerar como eficiente a administração que tutela, com razoabilidade e proporcionalidade, os direitos à privacidade e à proteção de dados de um lado e de outro o direito à informação, através da publicidade e transparência, com primazia (em tese) ao direito fundamental à informação, como tutela à própria cidadania e dignidade da pessoa humana[42].

De maneira a confirmar a necessária harmonia entre a proteção e transparência de dados pelos órgãos públicos, a recente Lei nº 14.129/2021, que traz diretrizes ao governo digital, reforça a proteção de dados (art. 3º, inc. IX, XVII, XXIII; art. 4º, parágrafo único; art. 21, inc. X; art. 25; §§ 1º e 2º; art. 27; art. 29; art. 38 e art. 39) concomitantemente com o necessário zelo quanto à transparência (art. 3º, inc. IV; art. 4º, inc. XI; art. 25; art. 29; art. 36; art. 45, inc. V) e à publicidade (art. 29, § 1º, inc. I e art. 40).

Há, portanto, necessidade de uma harmonização, também, diante das novas tecnologias, entre os princípios da privacidade e proteção de dados em sintonia com os princípios da publicidade e transparência. Questões como a importância da informação na sociedade tecnológica; novas tecnologias publicizando os atos da administração pública; releitura dos controles clássicos do Estado e a cidadania eletrônica; os princípios da transparência e da publicidade e a tutela do direito à informação; diretrizes de governança, dentre outras questões, deverão ser levados em consideração na atuação dos Tribunais de Contas, tanto em seu âmbito interno (como gestor público), como em suas missões institucionais (no exercício do controle externo, acrescido do papel de provedor do controle social).

As novas tecnologias[43], sem sombra de dúvidas, tornaram a informação mais acessível à sociedade, viabilizando-se uma maior democracia. Possibilita-se, assim,

---

[42] Nos termos constantes na seguinte obra: SARLET, Ingo W. **Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988**. 7 ed. Porto Alegre: Livraria do Advogado, 2009.

[43] Dispondo sobre a Prestação Digital dos Serviços Públicos na Administração Pública e sobre Governo Digital, vide a Lei 14.129/2021, que trouxe importantes diretrizes a consubstanciar a *ciber@dministração* pública.

um “controle do controlador”, ou seja, um novo espaço para cidadania, através da possibilidade de controle social. Portanto, afirma-se um “redimensionamento dos controles clássicos do Estado”[44], através de uma *cibercidadania*[45]. Nos novos tempos, as limitações geográficas foram superadas no *ciberespaço*, ocasionando uma nova leitura do próprio modelo de Estado e da separação dos poderes. Diante das novas tecnologias, propiciando-se uma fiscalização recíproca e simultânea, por mais este motivo, encontra-se superada a clássica divisão dos poderes, possibilitando-se um novo tipo de controle, o “controle social”, como uma efetivação de democracia direta, ou seja, de uma “democracia participativa”[46].

Pode-se afirmar que o princípio da publicidade é o gênero do qual o princípio da transparência seria uma espécie. Por outro lado, o princípio da transparência vai além da necessária publicidade (prevista no art. 37 da Constituição Federal), englobando também o “direito à informação” (art. 5º, inc. XXXIII, da CF) e o princípio democrático. Na legislação infraconstitucional, o princípio da transparência consta previsto nos artigos 48 e seguintes da Lei de Responsabilidade Fiscal (controle e fiscalização da gestão fiscal, com inspiração no *accountability* do direito anglo-saxão)[47] e nas diretrizes de governança (*v.g.* o Decreto nº 9.203/2017). Não restam dúvidas, portanto, na importância de atuação eficiente dos Tribunais de Contas na

---

[44] Nesse sentido, e para possibilitar um maior aprofundamento quanto ao tema: LIMBERGER, Têmis. Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser informado e o princípio democrático**. R. Interesse Público**. Porto Alegre, n. 39, set./out. 2006, p. 55-71. LIMBERGER, Têmis. Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser in-formado e o princípio democrático. **Revista do Ministério Público do Rio Grande do Sul**. Porto Alegre, n. 60, ago./2007 a abr./2008, p. 47-65. LIMBERGER, Têmis. Efetividade da gestão fiscal transparente: o valor da cultura. **R. Interesse Público**. Porto Alegre, n. 52, 2009, p. 75-88 (complementação e conclusão dos estudos da autora acima referidos).

[45] Expressão encontrada na obra de: PÉREZ LUÑO, Antonio Enrique. ***Ciberciudadaní@ o ciudadanìa.com?*** Barcelona: Gedisa, 2004, p. 99.

[46] FREITAS, Juarez. O princípio da democracia e o controle do orçamento público brasileiro. **Interesse Público**, Porto Alegre, v. 4, volume especial , p. 11-12, 2002. FREITAS, Juarez. O controle social do orçamento público. R. **Interesse Público**, Porto Alegre: n. 11, p. 13-26, 2001. FREITAS, Juarez. Direito Constitucional à Democracia. *In*: **Direito à Democracia: Ensaios transdisciplinares**. São Paulo: Conceito Editorial, 2011, pp. 11-39.

[47] Nesse sentido: LIMBERGER, Têmis. Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser informado e o princípio democrático**. R. Interesse Público**. Porto Alegre, n. 39, set./out. 2006, p. 66. A autora refere à experiência de direito comparado “no sentido de que os países com informação mais transparente são os que apresentam menores índices de corrupção. Deste modo, valendo-se dos mecanismos de divulgação eletrônica, os dados estarão disponíveis à população”.

fiscalização do cumprimento das normas constantes na Lei de Responsabilidade Fiscal e da efetividade do princípio da transparência fiscal[48].

Convém lembrar, mais uma vez, que, quanto maior for a informação e maior for a transparência, menor será a margem para corrupções, ampliar-se-á a integridade e a confiabilidade, viabilizando-se, de maneira mais concreta e efetiva, o correto destino das verbas públicas para a satisfação dos direitos fundamentais.[49]. Passos no rumo desejável, acima transcrito, o Tribunal de Contas do Estado do Rio Grande do Sul disponibilizou em seu portal acesso amplo e irrestrito aos orçamentos dos municípios gaúchos (os quais deverão obrigatoriamente atualizar seus dados, nos termos estabelecidos pelo art. 48-A da Lei Complementar n.º 101/2000). As novas ferramentas tecnológicas estão disponíveis, bastará conjuntamente à vontade cidadã para dispor e usufruir o referido direito fundamental à informação.

Por sua vez, todo o esforço do constituinte e legislador para que se ultrapassasse a "cultura do segredo"[50] vem acompanhada da revolução tecnológica, com a consequente formação da sociedade em rede[51]. Esse processo caminha a uma velocidade que nem sempre vem acompanhada da necessária regulação[52].

O século XX foi marcado pelo forte progresso tecnológico, que possibilitou a captação de diversos dados dos indivíduos com a consequente possibilidade de

---

[48] Que, recentemente, receberam reforço nas diretrizes trazidas pela Lei n.º 14.129/2021, como já afirmado, com destaque ao art. 3º - que elenca como princípios e diretrizes do Governo Digital e da eficiência pública a transparência na execução dos serviços públicos e o monitoramento da qualidade desses serviços (inc. IV) e o incentivo à participação social no controle e na fiscalização da administração pública (inc. V).

[49] Quanto a este tema, para complementar: CUNDA, Daniela Zago G. da . Direito fundamental à boa administração tributária e financeira. **Revista Jurídica Tributária**. Porto Alegre: Nota Dez, vol. 10, 2010. CUNDA, Daniela Zago Gonçalves. Controle de Políticas Públicas pelos Tribunais de Contas: Tutela da efetividade dos direitos e deveres fundamentais. **Revista Brasileira de Políticas Públicas**, Brasília: UniCEUB, vol. 01, 2010. CUNDA, Daniela Zago G. da ; ZAVASCKI, Liane T. Controles da Administração Pública e a efetividade dos direitos fundamentais: breves anotações sobre a atuação dos Tribunais de Contas e do Controle Judicial da Discricionariedade Administrativa. Belo Horizonte: **Revista Interesse Público***, n.º 63*, 2010.

[50] HEINEN, Juliano. **Comentários à lei de Acesso à Informação**: Lei nº 12.527/2011. 2 ed. rev. e atual. Belo Horizonte: Fórum, 2015, p. 44.

[51] A sociedade em rede é uma expressão utilizada para um modelo de sociedade da informação cuja infraestrutura é organizada por meios de comunicação e redes sociais que viabilizam uma hiperconexão de todos. MENEZES, Joyceane Bezerra de, COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica?. . *In* FRAZÃO, Ana, TEPEDINO, Gustavo; OLIVA, Milena Donato(Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1 ed. São Paulo: Thomson Reuters Brasil, 2019, p.158.

[52] Abordando o tema e sobre governos paralelos, vide: MENDES, Gilmar Ferreira. Arts. 48 a 59, Capítulo IX – Da transparência, controle e fiscalização*. In:* MARTINS, Ives Gandra, NASCIMENTO, Carlos Valder do. **Comentários à Lei de Responsabilidade Fiscal**. 7 ed. São Paulo: Saraiva, 2014, p. 397

violações à intimidade[53/54]. Estudo recente refere que a utilização de dados pessoais era, principalmente, realizada pelo Estado, entretanto, atualmente, verifica-se que o acesso e o tratamento das informações encontram-se pulverizados tanto nos órgãos públicos, quanto nos organismos particulares[55].

Pode-se dizer que, ao lado da criação de instrumentos de controle, pelos cidadãos, do uso que fazem dos dados, há a definição de deveres às empresas e entes governamentais, no trato das informações que figurem em seus bancos de dados[56].

A temática lança luzes ao cotejo entre o direito ao acesso à informação e transparência e o direito à privacidade[57] , uma vez que a Lei de Acesso à Informação e a Lei de Responsabilidade Fiscal tratam o sigilo como exceção, a LGPD tem, como diretriz, a proteção à privacidade. Mais recentemente, a Lei nº 14.129/2021 deixa bem claro, em seu art. 29, § 1º, que "na promoção da transparência ativa de dados, o poder público deverá observar como requisito a observância da publicidade das bases de dados não pessoais como preceito geral e o sigilo como exceção" (inc. I).

No rol do que poderá ser considerado como requisito para o cumprimento do direito/dever fundamental de boa *ciber@dministração* pública[58] , pode-se incluir que

---

[53] Ana Frazão salienta a importância econômica dos dados pessoais, inclusive com menção à manchete da revista *The Economist* de 06.05.2017, que faz destaque ao fato de que a informação se tornou um grande insumo na atualidade. A autora refere que os dados pessoais já são conhecidos como o novo petróleo, em função das repercussões em praticamente todas as atividades econômicas situação que fez surgir a expressão *data-driven economy*. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-.resource-is-no-longer-oil-but-data. Acesso em 09/01/2020>.

[54] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – noções introdutórias para a compreensão da importância da lei Geral de Proteção de Dados. *In* FRAZÃO, Ana, TEPEDINO, Gustavo; OLIVA, Milena Donato(Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** 1 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 24. *A expressão *data-driven economy* significa economia movida a dados.

[55] REIS, Fernando Simões dos, RUARO, Regina Linden. A anonimização dos dados como forma de relativização da proteção de informações sigilosas e a atuação fiscalizatória dos tribunais de contas. **Revista de estudos e Pesquisas Avançadas do Terceiro Setor***,* Brasília, v.5, nº 2, p. 157-187,Jul-Dez, 2018.

[56] Na mesma linha são as tutelas trazidas pela Lei 14.129/2021, que tem, como uma de suas finalidades, promover a atuação integrada e sistêmica entre os órgãos e as entidades envolvidos na prestação e no controle dos serviços públicos com o com o compartilhamento de dados sensíveis em "ambiente seguro".

[57] Como é característico do nosso sistema, não há direito absoluto e, nesse sentido, o STF estabeleceu o regime de repercussão geral para a matéria no RE nº 601.314/SP.

[58] Conforme estudos que desenvolveram o tema de maneira mais detalhada: CUNDA, Daniela Zago G.; RAMOS, Letícia A. Os 20 anos da Lei de Responsabilidade Fiscal: transparência e proteção de dados a tutelar os direitos fundamentais à cibercidadania e à boa *ciber@dministração* pública. *In* FIRMO FILHO, Alípio Reis *et all* (coord.) **Responsabilidade na Gestão Fiscal***:* Estudos em homenagem aos 20 anos da Lei Complementar n. 101/2000, Belo Horizonte: Fórum, 2020. CUNDA,

a Administração deverá tutelar a "proteção de dados", respeitar a intimidade e privacidade de seus servidores e empregados públicos, bem como de seus jurisdicionados e todos os demais titulares dos dados disponíveis e utilizados no exercício de atividades de gestão pública e/ou de controle administrativo, ou seja, respeitar o "direito fundamental à intimidade e privacidade e o direito fundamental à proteção de dados". Para que a *ciber@dministração* pública seja eficiente, também deverão estar presentes os princípios e as diretrizes de governança (*v.g.* capacidade de resposta, integridade, confiabilidade, prestação de contas e responsabilidade, assim como a transparência).

É inquestionável que o incremento tecnológico potencialmente poderá lesar os direitos fundamentais[59], com destaque a privacidade, a intimidade e a proteção de dados, os quais deverão ser tutelados com o máximo de zelo, pelo gestor público e órgãos de controle. Hodiernamente, a Administração Pública dispõe de "instrumentos que podem ser utilizados para armazenar uma infinidade de conhecimentos, bem como para transmiti-los de uma maneira célere"[60], todavia há que se ter muita cautela para que não sejam desvirtuados, como, por exemplo, os "dados pessoais constantes nos bancos de dados". Pertinente, portanto, a observação de que "garantir a efetividade dos direitos fundamentais, em geral, e da intimidade diante do fenômeno informático, em particular, é a grande questão enfrentada pelos juristas, considerando as invasões que se costumam ocorrer nos bancos de dados"[61].

Diante das questões expostas, na presente seção, percebe-se que se trata de um grande desafio, ao mesmo tempo, proteger os dados informatizados e, também, possibilitar o primordial acesso às informações, tutelando o direito fundamental à informação, questões detalhadas a seguir.

---

Daniela Zago G.; RAMOS, Letícia A. Ciber@dministração Pública e Controle 4.0, seus desafios em tempo de pandemia do coronavírus, e a transparência ampliada (para além de translúcida). *In* LIMA, Luiz Henrique et all (coord.) **Os Desafios do Controle Externo diante da pandemia da COVID 19**: Estudos dos Ministros e Conselheiros Substitutos dos Tribunais de Contas, Belo Horizonte: Fórum, 2020.

[59] Sobre o assunto, obras que serviram como vetor para as abordagens do tópico em estudo: LIMBERGER, Têmis**. O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado. LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. *In:* **Direitos Fundamentais, Informática e Comunicação: algumas aproximações.** Org: Ingo Wolfgang Sarlet. Porto Alegre: Livraria do Advogado Ed., 2007, pp. 195-225.

[60] *Idem,* p. 195.

[61] *Idem,* p. 196.

A Constituição Federal e vários dispositivos legais infraconstitucionais (com destaque aos artigos. 48 e ss. da Lei de Responsabilidade Fiscal e a Lei de Acesso à Informação), já de longa data, vedam a opacidade na Administração Pública; na mesma linha são os princípios e as diretrizes de governança. Em pesquisas antecessoras[62], procurou-se demonstrar que o "direito fundamental à boa *ciber@dministração* pública"[63] pressupõe uma administração que utiliza as novas tecnologias para viabilizar a otimização do trabalho desempenhado por seus servidores e que, também, utiliza as novas tecnologias para prestar serviços públicos *on-line,* atendendo prontamente demandas urgentes. Este processo deve se desenvolver num cenário de publicidade e transparência a promover o mais amplo controle social, sem se descuidar da proteção dos dados de todos os envolvidos[64].

Pode-se afirmar que, da união dos princípios da administração pública, constantes no artigo 37 da Constituição Federal (legalidade, impessoalidade, moralidade, publicidade e principalmente o princípio da eficiência), em conjunto com o artigo 5º da Constituição Federal, extrai-se e se corporifica o "direito fundamental à boa administração pública", correlacionado às diretrizes de governança, que "irradia forte carga axiológica, na busca dos melhores resultados possíveis"[65] (incluindo-se a utilização responsável das novas tecnologias e a promoção dos princípios da

---

[62] Com amparo e, em complementação a estudos anteriores: CUNDA; RAMOS, *In* FIRMO FILHO, *op. cit.*, 2020. Vide também, a primeira abordagem sobre o direito/dever fundamental à boa ciber@dministração em: CUNDA, *op. cit.*, 2013.

[63] Tendo, como referencial teórico, as seguintes obras: FALZONE, Guido. ***Il Dovere di Buona Amministrazione***. Milano: Dott. A. Giuffrè Editore, 1953. CANOTILHO, José Joaquim Gomes. ***Brancosos e Interconstitucionalidade****:* itinerários dos discursos sobre a historicidade constitucional. Coimbra: Almedina, 2006. Nesta obra, o autor trata do constitucionalismo e geologia da *good governance* (p. 325 e ss.). E, no Brasil: FREITAS, Juarez. **Direito Fundamental à boa Administração Pública**. 3.ed. edição. São Paulo: Malheiros, 2014. Sobre a temática "cibercidadania": PÉREZ LUÑO, Antonio Enrique. ***Ciberciudadaní@ o ciudadanìa.com?*** Barcelona: Gedisa, 2004. PÉREZ LUÑO, Antonio Enrique. ***Los Derechos Fundamentales***. Madrid: Editorial Tecnos. 9. ed., 2007. PÉREZ LUÑO, Antonio Enrique. ***Cibernética, Informática y Derecho (Un análisis metodológico)*.** Bolonia: Publicaciones Del Real Colégio de España, 1976.

[64] CUNDA, Daniela Zago G.; RAMOS, Letícia A. **Os 20 anos da Lei de Responsabilidade Fiscal**: transparência e proteção de dados a tutelar os direitos fundamentais à *cibercidadania* e à boa *ciber@dministração* pública; e CUNDA, Daniela Zago G.; RAMOS, Letícia A. *Ciber@dministração* Pública e Controle 4.0, seus desafios em tempo de pandemia do coronavírus, e a transparência ampliada (para além de translúcida).

[65] GRANDO, Felipe Esteves. O direito fundamental à boa administração pública e seu diálogo com o direito tributário. Belo Horizonte: **Revista Interesse Público**. v. 12, n. 59, nov./dez. 2009, p.218.

publicidade e transparência como instrumentos do controle social e *cibercidadania*)[66].

## 5 CONSIDERAÇÕES FINAIS

A Lei nº 13.709/2018, com o escopo de conferir maior proteção aos dados pessoais (um inquestionável "direito fundamental" de seus titulares), elencou uma série de princípios e regras que resultam na necessidade de adaptações por parte daqueles que utilizam informações pessoais.

Dada a significativa quantidade de exigências, mostra-se útil a sistematização do processo de adequação em etapas, a fim de facilitar a organização interna e a execução dos comandos legais, com a identificação e o destaque das normas que demandam os maiores esforços na fase inicial de alinhamento ao novo ordenamento.

Ressalve-se que as sugestões (constantes na seção 3) têm, por objetivo, compartilhar estudos e análises voltados aos aspectos primordiais de adaptação, sem, por óbvio, a pretensão de esgotar o tema, nem de afastar outras formas e caminhos de atendimento às normas, certamente também adequados e corretos; afinal, cada órgão ou entidade possui características próprias, que evidentemente devem ser levadas em consideração nas tomadas de decisão.

Cabe observar, também, que se buscou apresentar as referidas etapas em uma ordem lógica, a fim de facilitar a compreensão da matéria, mas não há uma rigidez cronológica de implantação, dependendo das peculiaridades dos órgãos e entidades e da conveniência de cada controlador.

Por fim, sublinhe-se que a gestão da privacidade e da proteção de dados pessoais é um processo permanente, que envolve conhecimentos de diversas áreas, e que demandará esforços contínuos da Administração Pública na tarefa de concretizar o "direito fundamental à proteção de dados pessoais", sempre, diga-se, em harmonia com os demais princípios e regras relacionados ao tema, com vistas ao atendimento do interesse público primário, mediante uma eficiente e cibernética

[66] Sobre o tema, vide: POSTER, Mark. ***CyberDemocracy****:Internet and the Public Sphere***.** Disponível em: <www.forumglobal.de/soc/bibliot/p/cyberdemocracy_poster.htm>. Acesso em: julho de 2020.

governança (com capacidade de resposta, integridade, confiabilidade, prestação de contas, responsabilidade e transparência).

Não se pode perder de vista a necessária harmonia entre a proteção e a transparência de dados pelos órgãos públicos. A recente Lei nº 14.129/2021 traz diretrizes tanto para a *ciber@dministração* pública, como para o "controle externo 4.0", que necessariamente deverão ser provedores do controle social e da *cibercidadania*. Nesse âmbito, a LGPD ensejará uma leitura conjunta com a Lei do Governo Eletrônico, de maneira a fomentar, para além de "redes de conhecimento" (art. 17), "redes de cidadania" (art. 45, inc. V, da Lei nº 14.129/2021) sempre tendo, como norte, a transparência responsável (uma das principais diretrizes de governança).

## REFERÊNCIAS


BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guias Operacionais para adequação à LGPD**. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd>. Acesso em: 2 fev. 2021.

_____. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital**. Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020**. Brasília, 2020. Diário Oficial da União, Brasília, 20 nov. 2020, ed. 222, seção 1, p. 92. Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-117-de-19-de-novembro-de-2020-289515596>. Acesso em: 2 fev. 2021.

CANOTILHO, José Joaquim Gomes. **Brancosos e Interconstitucionalidade**: itinerários dos discursos sobre a historicidade constitucional. Coimbra: Almedina, 2006. Na obra o autor trata do constitucionalismo e geologia da good governance.

CUNDA, Daniela Zago Gonçalves da. Controle de Políticas Públicas pelos Tribunais de Contas: Tutela da efetividade dos direitos e deveres fundamentais. **Revista Brasileira de Políticas Públicas***,* Brasília: UniCEUB, vol. 01, 2010.

_____. **Controle de sustentabilidade pelos Tribunais de Contas**. 2016. Tese (Doutorado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, 2016.

_____. Controle de sustentabilidade pelos Tribunais de Contas e a necessária ênfase à dimensão ambiental. *In*: MIRANDA, Jorge; GOMES, Carla Amado; PENTINAT, Susana Borràs (Coord.). **Diálogo Ambiental, Constitucional e Internacional**. Volume 10, *E-Book* Internacional (ISBN: 978-989-8722-42-3). Lisboa: Faculdade de Direito da Universidade de Lisboa (CJP e CIDP), abril de 2020, pp. 293-341.

_____. Comentários ao art. 21 da LINDB. *In*: DUQUE, Marcelo Schenk; RAMOS, Rafael (Coord.). **Segurança Jurídica na aplicação do Direito Público**. Salvador: Editora Juspodivm, 2019, pp. 57-78.

_____. A LINDB, suas profecias para o enfrentamento da pandemia e as necessárias reformulações da Administração Pública e do Respectivo Controle. *In:* MAFFINI, Rafael; RAMOS, Rafael. **Nova LINDB***:* Consequencialismo, deferência judicial, motivação e responsabilidade do gestor público. Rio de Janeiro: Lumen Juris, 2020, pp. 279 e ss.

CUNDA, Daniela Zago G.; RAMOS, Letícia A. *Ciber@dministração* Pública e Controle 4.0, seus desafios em tempo de pandemia do coronavírus, e a transparência ampliada (para além de translúcida). *In* LIMA, Luiz Henrique *et all* (coord.) **Os Desafios do Controle Externo diante da pandemia da COVID 19:** Estudos dos Ministros e Conselheiros Substitutos dos Tribunais de Contas, Belo Horizonte: Fórum, 2020.

_____. Os 20 anos da Lei de Responsabilidade Fiscal: transparência e proteção de dados a tutelar os direitos fundamentais à *cibercidadania* e à boa *ciber@dministração* pública. *In* FIRMO FILHO, Alípio Reis *et all* (coord.) **Responsabilidade na Gestão Fiscal***:* Estudos em homenagem aos 20 anos da Lei Complementar n. 101/2000, Belo Horizonte: Fórum, 2020.

CUNDA, Daniela Zago G. da ; ZAVASCKI, Liane T. Controles da Administração Pública e a efetividade dos direitos fundamentais: breves anotações sobre a atuação dos Tribunais de Contas e do Controle Judicial da Discricionariedade Administrativa. Belo Horizonte: **Revista Interesse Público***, n.º 63*, 2010.

FALZONE, Guido. ***Il Dovere di Buona Amministrazione****.* Milano: Dott. A. Giuffrè Editore, 1953.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais - noções introdutórias para a compreensão da importância da lei Geral de Proteção de Dados. *In* FRAZÃO, Ana, TEPEDINO, Gustavo; OLIVA, Milena Donato(Coord**.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1 ed. São Paulo: Thomson Reuters Brasil, 2019, p. 24.

FREITAS, Juarez. O princípio da democracia e o controle do orçamento público brasileiro. **Revista Interesse Público***,* Porto Alegre, v. 4 (volume especial), p. 11-12, 2002.

_____. O controle social do orçamento público. **Revista Interesse Público***,* Porto Alegre: n. 11, p. 13-26, 2001.

_____. Direito Constitucional à Democracia. *In*: **Direito à Democracia**: Ensaios transdisciplinares. São Paulo: Conceito Editorial, 2011, p. 11-39.

_____. **Direito Fundamental à boa Administração Pública**. 3. ed. São Paulo: Malheiros, 2014

GRANDO, Felipe Esteves. O direito fundamental à boa administração pública e seu diálogo com o direito tributário. Belo Horizonte: **Revista Interesse Público**. v. 12, n. 59, nov./dez. 2009, p.218.

HEINEN, Juliano. **Comentários à lei de Acesso à Informação: Lei nº 12.527/2011**. 2 ed. rev. e atual. Belo Horizonte: Fórum, 2015, p. 44.

INSTITUTO RUI BARBOSA. **Nota Técnica nº 01/2019**. LGPD. Considerações sobre a aplicação no âmbito dos Tribunais de Contas. Disponível em: <https://www.atricon.org.br/documentos/nota-tecnica-no-012019-instituto-rui-barbosa/>. Acesso em: 3 fev. de 2021.

LIMBERGER, Têmis. Efetividade da gestão fiscal transparente: o valor da cultura. **Revista Interesse Público**. Porto Alegre, n. 52, 2009, p. 75-88.

_____. **O direito à intimidade na era da informática**: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

_____. Direito e informática: o desafio de proteger os direitos do cidadão. *In:* **Direitos Fundamentais, Informática e Comunicação**: algumas aproximações**.** Org: Ingo Wolfgang Sarlet. Porto Alegre: Livraria do Advogado Ed., 2007, p. 195-225.

_____. Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser in-formado e o princípio democrático. **Revista do Ministério Público do Rio Grande do Sul**. Porto Alegre, n. 60, ago./2007 a abr./2008, p. 47-65.

_____. Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser informado e o princípio democrático. **Revista Interesse Público**. Porto Alegre, n. 39, set./out. 2006, p. 55-71.

LOUREIRO, Roberto Debacco. Participação: princípio expresso na Constituição do Estado do Rio Grande do Sul. *In:* **Revista Eletrônica do TCE/RS**. Edição Especial dos 30 anos da Constituição Estadual. Disponível no site: <https://www.atricon.org.br/wp-content/uploads/2019/07/REVISTA-ELETRONICA-3-TCERS-1.pdf>. Acesso em: 20 mar. de 2020.

MACIEL, Moisés. Os Tribunais de Contas no exercício do controle externo face à nova Lei Geral de proteção de Dados Pessoais. Disponível em: <https://www.researchgate.net/publication/341377759_Os_tribunais_de_contas_no_exercicio_do_controle_externo_de_acordo_com_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais>. Acesso em: 20 mar. de 2020.

MENDES, Gilmar Ferreira. Arts. 48 a 59, Capítulo IX – Da transparência, controle e fiscalização. *In*: MARTINS, Ives Gandra, NASCIMENTO, Carlos Valder do. **Comentários à Lei de Responsabilidade Fiscal**. 7. ed. São Paulo: Saraiva, 2014, p. 397

MENEZES, Joyceane Bezerra de, COLAÇO, Hian Silva. Quando a Lei Geral de Proteção de Dados não se aplica? *In:* FRAZÃO, Ana, TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord***). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*****.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019, p.158. (157-197)

OLIVEIRA, Marco Aurélio Belizze, LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei nº 13.709/2018. *In*: FRAZÃO, Ana, TEPEDINO, Gustavo; OLIVA, Milena Donato(Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. .1 ed. São Paulo: Thomson Reuters Brasil, 2019, p.62.

OLIVETTI, Marco. *Diritti Fondamentali e Nuove Tecnologie: uma mappa del dibattito italiano. In: **Journal of Institutional Studies**, v. 6, n. 2 p. 395-430, maio/ago. 2020.*.

PÉREZ LUÑO, Antonio Enrique. ***Los Derechos Fundamentales***. Madrid: Editorial Tecnos. 9. ed., 2007.

_____. ***Ciberciudadaní@ o ciudadanìa.com?*** Barcelona: Gedisa, 2004, p. 99.

_____. **Cibernética, Informática y Derecho** (Un análisis metodológico). Bolonia: Publicaciones Del Real Colégio de España, 1976.

POSTER, Mark***. CyberDemocracy:*** *Internet and the Public Sphere.* Disponível em: <www.forumglobal.de/soc/bibliot/p/cyberdemocracy_poster.htm>. Acesso em: julho de 2020.

REIS, Fernando Simões dos, RUARO, Regina Linden. A anonimização dos dados como forma de relativização da proteção de informações sigilosas e a atuação fiscalizatória dos tribunais de contas. **Revista de estudos e Pesquisas Avançadas do Terceiro Setor***,* Brasília, v.5, nº 2, p. 157-187, Jul-Dez, 2018.

SÁNCHEZ, Miguel J. Arjona. *La información em La era de internet. El caso de las fake news*. ***Journal of Institutional Studies***, v. 6, *n.* 2 p.376-394, maio/ago. 2020

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais** - Comentada Artigo por Artigo. 2. ed. Salvador: JusPodivm, 2020.

RIO GRANDE DO SUL. Tribunal de Contas do Estado. Consultoria Técnica. **Nota Técnica nº 1, de 6 de março de 2020***.* Lei Geral de Proteção de Dados. Porto Alegre, 2020.

SANTOS, Fabíola Meira de Almeida, TALIBA, Rita. Lei Geral de Proteção de Dados no Brasil e os possíveis impactos. **Revista dos Tribunais Online**, vol. 998/2018, p.225-239, p. 227. Disponível em: <https://www.livrariart.com.br/>. Acesso em: julho de 2020.

SARLET, Ingo W. **Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988.** 7 ed. Porto Alegre: Livraria do Advogado, 2009.

WILLEMAN, Mariana Montebello. ***Accountability*** **democrática e o desenho institucional dos Tribunais de Contas no Brasil**. Belo Horizonte: Fórum, 2017, p. 19-20.