

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PÚBLICO E FILOSOFIA DO DIREITO

Bárbara de Matos Peralta

AGENTES DE TRATAMENTO DA NOVA LEI GERAL DE PROTEÇÃO DE
DADOS PESSOAIS BRASILEIRA: FUNÇÕES E RESPONSABILIDADES

Porto Alegre

2019

BÁRBARA DE MATOS PERALTA

**AGENTES DE TRATAMENTO DA NOVA LEI GERAL DE PROTEÇÃO DE
DADOS PESSOAIS BRASILEIRA: FUNÇÕES E RESPONSABILIDADES**

Monografia apresentada como requisito parcial para obtenção do grau de Bacharela em Ciências Jurídicas e Sociais pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Rafael da Cás Maffini

Porto Alegre

2019

BÁRBARA DE MATOS PERALTA

**AGENTES DE TRATAMENTO DA NOVA LEI GERAL DE PROTEÇÃO DE
DADOS PESSOAIS BRASILEIRA: FUNÇÕES E RESPONSABILIDADES**

Aprovada em: ____ de _____ de 2019.

BANCA EXAMINADORA:

Professor Doutor Rafael da Cás Maffini

Mestranda Luciana Luso de Carvalho

Mestranda Graziela Harff

AGRADECIMENTOS

Agradeço, em primeiro lugar, aos meus pais, meus maiores exemplos e inspirações, pois nunca mediram esforços para investir na minha educação e me proporcionar uma vida confortável.

À minha irmã, Marília, por ser um exemplo a ser seguido.

Aos meus amigos Olavo, Bibiana, Camila e Júlia, pela disponibilidade e boa vontade que tiveram ao me ajudar a superar provas e demais obstáculos da graduação. À Amanda e à Melina, amigas que transformaram meus momentos na faculdade mais doces e agradáveis. A todos meus demais amigos, alegrias em minha vida, pelo incansável apoio.

Ao Leonardo, pelo carinho, motivação e parceria, que iniciaram no curso pré-vestibular e, desde então, tornam a minha caminhada mais leve e tranquila.

Por fim, ao meu orientador, um dos melhores professores dessa faculdade, detentor da minha admiração e, indubitavelmente, da grande maioria dos alunos, por lecionar excelentes e prazerosas aulas. Também, pela paciência tida, apesar dos seus inúmeros compromissos, diante das minhas dúvidas e solicitações no desenvolvimento do presente trabalho.

RESUMO

O presente trabalho versa sobre Lei Geral de Proteção de Dados (LGPD) e as novas figuras dos agentes de tratamento trazidas pela lei, buscando-se verificar quais são suas funções e responsabilidades. Para isso, inicia-se o trabalho por uma definição daquilo que se define como “dados pessoais”, fazendo-se uma análise comparativa entre a definição do termo pelo ordenamento jurídico europeu e, posteriormente, brasileiro. Também, faz-se uma definição daquilo que se qualifica como “dados sensíveis”, que mereceram definição especial no art. 5º da referida Lei. Após tal disposição, demonstrou-se o motivo pelo qual os dados pessoais careciam de proteção, constituindo-se a proteção de dados pessoais, inclusive, como um direito de personalidade autônomo. A fim de adentrar na evolução do ordenamento jurídico brasileiro a respeito do tema, fez-se uma breve disposição a respeito do ordenamento jurídico europeu, grande inspiração à LGPD. Assim, ao adentrar no direito brasileiro, demonstrou-se a carência do nosso ordenamento a respeito do tema e, ao analisar a nova legislação geral, fez-se uma análise a seu respeito dividindo-a em cinco eixos principais, quais sejam: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados e v) responsabilização dos agentes. Os dois últimos, portanto, ao se referirem aos agentes de tratamento de dados pessoais – *controlador* e *operador* – foram analisados no último capítulo do trabalho, a fim de responder os questionamentos propostos por essa pesquisa.

Palavras-chave: Dados pessoais. Lei Geral de Proteção de Dados (LGPD). Agentes de tratamento.

ABSTRACT

This paper deals with the General Law of Data Protection (LGPD) and the new figures of treatment agents created by the law, seeking to verify their functions and responsibilities. For this, the paper begins with the definition of what is defined as “personal data”, making a comparative analysis between the definition of the term by the European and later Brazilian legal system. Also, a definition is made of what is qualified as “sensitive data”, which merited special attention in the article 5th of the referred Law. Following this provision, the reason why personal data needs protection was demonstrated, and the protection of personal data was even constituted as an autonomous personality right. In order to enter into the evolution of the Brazilian legal system on the subject, a brief provision was made regarding the European legal system, a great inspiration to the LGPD. Thus, entering in the Brazilian law, the lack of our organization on the subject was demonstrated and, by analyzing the new general legislation, an analysis was made about it, dividing it into five main axes, namely: i) unity and generality of law enforcement; ii) legitimation for data processing (authoritative hypotheses); iii) principles and rights of the holder; iv) obligations of data processing agents and v) accountability of agents. The last two, therefore, referring to personal data processing agents – *controller* and *processor* – were analyzed in the last chapter of the paper, in order to answer the questions proposed by this research.

Keywords: Personal data. General Law of Data Protection (LGPD). Treatment agents.

SUMÁRIO

1 Introdução	8
2 Dados Pessoais	10
2.1 Conceito e Necessária Proteção	10
2.2 A Proteção de Dados Pessoais como um Direito de Personalidade Autônomo perante o Direito à Privacidade	14
2.3 Proteção Legal dos Dados Pessoais	16
2.3.1 A Proteção de Dados no Cenário Europeu	17
3 Lei Geral de Proteção de Dados	22
3.1 A Proteção de Dados como um Direito Fundamental no Brasil e a Proposta de Emenda à Constituição n. 17 de 2019	22
3.2 Evolução do Tratamento no Brasil	26
3.2.1 Legislação Esparsa	26
3.2.2 Marco Civil da Internet	31
3.3 Disposições Gerais	34
3.3.1 Eixos Principais	38
4 Agentes de Tratamento de Dados Pessoais.....	43
4.1 A Criação das Figuras do <i>Controlador</i> e do <i>Operador</i>	43
4.2 Do <i>Encarregado</i> pelo Tratamento de Dados Pessoais	47
4.3 Responsabilidade e Ressarcimento de Danos	50
4.4 Princípios da Segurança e da Prevenção.....	57
5 Conclusão	61
Referências Bibliográficas	65

1 Introdução

Vivemos hoje na chamada *sociedade da informação*, em que a conjugação das inovações tecnológicas deu origem a uma nova estrutura socioeconômica, através da facilidade de acesso à informação. Dentre tais inovações destaca-se, principalmente, a internet, responsável por criar um *ciberespaço*, onde informações de qualquer tipo, inclusive sobre a personalidade das pessoas, estão sendo coletadas, armazenadas e processadas como nunca fora possível. Desse modo, os indivíduos, com consciência ou não, estão fornecendo às empresas, através dos *sites* e, principalmente, das redes sociais, inúmeros dados a seu respeito, como informações e interesses pessoais, posicionamento político, lugares frequentados, pessoas com as quais se relacionam, dentre diversas outras informações que deveriam ser mantidas na esfera privada.

Tal facilidade de coleta de dados chamou atenção aos olhos da sociedade através de casos alarmantes, como, por exemplo, o relativo à venda de dados pelo Facebook à Cambridge Analytica, empresa privada considerada responsável por manipular os votos dos cidadãos americanos nas eleições que elegeram o presidente Donald Trump. Por meio de testes, os usuários forneciam informações pessoais à rede social, que as repassava, sem consentimento, à empresa privada, que tratava tais dados de maneira a entregar ao cidadão um conteúdo personalizado de propaganda, influenciando seu voto. Através de incidentes como esse que se percebeu, então, que, cada vez mais, a privacidade e a intimidade das pessoas estão sendo “atropeladas” pelos inúmeros mecanismos do mundo moderno, seja pelas redes sociais ou por quaisquer outros meios facilitadores da difusão de informações.

Desse modo, na era da informação, a proteção dos dados pessoais torna-se indispensável, uma vez que eles nos definem, nos classificam, nos dão acesso e nos privam de serviços e produtos, públicos e privados. Sob essa perspectiva, portanto, o direito à proteção de dados surge como um elemento fundamental para assegurar a igualdade, a cidadania e a liberdade. Foi assim que países do mundo todo passaram a se dedicar à criação de leis que regulamentassem o tratamento desses dados pessoais, estando entre eles o Brasil, que, apesar do relativo atraso em relação aos demais países, sancionou, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD).

Embora antes do surgimento da Lei os dados pessoais tivessem por fundamento normativo o direito à vida privada e à intimidade, consagrados no art. 5º, X, da

Constituição Federal e estivessem respaldados por demais legislações esparsas, como o Código Civil, o Marco Civil da Internet e a Lei do Cadastro Positivo, por exemplo, não havia uma uniformidade em relação ao tema. Portanto, é através da LGPD que os dados pessoais alcançam sua maior proteção e destaque no ordenamento jurídico brasileiro. Ainda, tendo como inspiração o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD traz importantes inovações, dentre elas a criação das figuras dos agentes de tratamento, sobre as quais a presente monografia debruçou-se, buscando responder aos seguintes questionamentos: Quem são os agentes de tratamento? Quais são seus papéis no tratamento de dados pessoais? De que modo podem ser responsabilizados por suas condutas? O que se pretende com a criação de tais figuras?

Assim, a fim de responder tais questionamentos, iniciou-se o trabalho através de uma conceituação de dados pessoais, para que se pudesse compreender quais dados são os protegidos pelo legislador e, portanto, quais serão objeto de tratamento pelos agentes da nova Lei. Também, para que se pudesse compreender a importância de uma proteção aos referidos dados, destacou-se a sua dimensão fundamental. Já no segundo capítulo, adentrando no regramento brasileiro, através de uma prévia disposição no capítulo anterior a respeito do regulamento europeu, fez-se uma evolução do ordenamento jurídico brasileiro para que se pudesse, finalmente, compreender a carência brasileira de uma legislação geral a respeito do tema. Por fim, chegou-se ao capítulo central desse trabalho, que, embora tenha regramento sucinto na LGPD, teve sua limitação inspirada no ensinamento fundamental de Umberto Eco de que “quanto mais se restringe o campo, melhor e com mais segurança se trabalha”¹.

¹ ECO, Umberto. *Como se faz uma tese*. Tradução: Gilson Cesar Cardoso de Souza. São Paulo: Perspectiva, 2012. 24ª ed., p. 10.

2 Dados Pessoais

2.1 Conceito e Necessária Proteção

Para que se possa compreender o assunto determinante da presente monografia, ou seja, a proteção de dados, faz-se necessária, primeiramente, uma conceituação do que se define como “dados pessoais”. Nas palavras de Laura Schertel Mendes “o regime jurídico da proteção de dados depende, naturalmente, do que se considera um dado pessoal e quais tipos de processamento de dados estão abrangidos pela regulação”. Portanto, a abordagem desses conceitos faz-se indispensável, determinando o alcance e os limites da tutela jurídica².

Sob essa perspectiva, para que se faça tal qualificação, deve-se compreender, primeiramente, o conceito jurídico de “dado” e “informação”³. Segundo Lacombe, dados poderiam ser definidos como “um conjunto de registros sobre fatos, passíveis de serem ordenados, analisados e estudados para se alcançar conclusões” e quando “organizados e ordenados de forma coerente e significativa para fins de compreensão e análise”, são chamados de informação⁴.

Ou seja, dado é o estado primitivo da informação⁵, pois não é algo *per se* que acresce conhecimento. Dados são simples *fatos brutos* que, quando processados⁶ e organizados⁷, se convertem em algo inteligível, podendo ser deles extraída uma informação⁸. Além disso, somando-se o termo “pessoais” a “dados”, surge então uma personalização do conceito, de maneira que “dados pessoais” se qualificam como “um conjunto de registros referentes a um indivíduo”⁹. Nessa senda, afirma Catarina Sarmento

² MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014, p. 55.

³ *Ibidem*.

⁴ LACOMBE, Francisco José Masset et al. *Administração: princípios e tendências*. São Paulo: Saraiva, 2003, p. 490.

⁵ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 152 apud BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 36.

⁶ ROB, Peter. *Sistemas de bancos de dados: projeto e implementação*. Trad. All Tasks. São Paulo: Cengage Learning, 2011. p. 4 apud *ibidem*, p. 36.

⁷ STAIR, Ralph; REYNOLDS, George W. *Princípios de sistema de informação: uma abordagem gerencial*. Tradução Flávio Soares Correa. São Paulo: Cengage Learning, 2009. p. 4 apud *ibidem* p. 36.

⁸ FINOCCHIARO, Giusella. *Privacy e protezione dei dati personali*. Torino: Zanichelli Editore, Torino, 2012. p. 33 apud *ibidem*, p.36.

⁹ TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. *Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil*. Tribunal de Justiça de São Paulo, 2016. Disponível em

e Castro que esses “compreendem qualquer informação alfabética, gráfica, fotográfica, acústica, independente do suporte (som e imagem), referente a pessoa identificada ou identificável”¹⁰.

A Diretiva n. 95/46/CE da União Europeia, que tutela o direito das pessoas singulares através do tratamento de “dados pessoais”, define tal expressão como “qualquer informação relativa a uma pessoa singular identificada ou identificável”, considerando-se identificável “todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos de sua identidade física, fisiológica, psíquica, econômica, cultural ou social” (artigo 2º, “a”)¹¹. Além disso, através da alínea *b* do mesmo dispositivo, conclui-se que o tratamento desses é “qualquer operação ou conjunto de operações (automatizadas ou não) que vise à coleta, ao registro, à conservação, à elaboração, à modificação, à comunicação ou à divulgação dessas informações pessoais”¹².

Também, em seu artigo 8º, I, a Diretiva europeia abarcou uma subespécie de dados pessoais, os chamados dados sensíveis, qualificando-os do seguinte modo:

Dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual¹³.

Contudo, o Regulamento Geral de Proteção de Dados Europeu - GDPR, que veio a substituir a Diretiva em 25 de maio de 2018¹⁴, trouxe um alargamento do conceito de

<<http://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ii%204.pdf?d=636680444556135606>>. Acesso em: 30 de outubro de 2019, p. 156.

¹⁰ CASTRO, Catarina Sarmento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005, p. 70-88.

¹¹ TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. *Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil*. Tribunal de Justiça de São Paulo, 2016. Disponível em <<http://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ii%204.pdf?d=636680444556135606>>. Acesso em: 30 de outubro de 2019, p. 157.

¹² ANDRADE, Frederico Pupo Carrijo de. *Análise comparativa do tratamento de dados pessoais à luz do direito de personalidade*. Estudos avançados de direito digital/coordenação Cíntia Rosa Pereira Lima, Lydia Neves Bastos Telles Nunes. 1ª ed. Rio de Janeiro: Elsevier, 2014, p. 232.

¹³ TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. *Op. cit.* Acesso em: 30 out. 2019, p. 157.

¹⁴ FERREIRA, Ricardo Barreto; BRANCHER, Paulo; TALIBERTI, Camila; CUNHA, Vitor Koketu da. *Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia*. Migalhas, 2018. Disponível em <<https://www.migalhas.com.br/dePeso/16,MI281042,81042-Entra+em+vigor+o+Regulamento+Geral+de+Protecao+de+Dados+da+Uniao>> Acesso em: 30 de outubro de 2019.

dados sensíveis, incluindo, para além dos mencionados no inciso I do artigo 8º da Diretiva, os dados genéticos e biométricos¹⁵.

No ordenamento jurídico brasileiro, apenas houve uma definição legal do termo “dados pessoais” em 2016, através do Decreto nº 8771, que regulamenta o Marco Civil da Internet, conforme se depreende do texto legal abaixo:

Art. 14. Para os fins do disposto neste Decreto, considera-se:

I - **dado pessoal** - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e

II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, *arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*¹⁶. (grifo próprio)

Ainda, a nova Lei Geral de Proteção de Dados (Lei nº 13.709/18), no seu artigo 5º, inciso II, trouxe uma definição de dado pessoal sensível no mesmo sentido do Regulamento europeu, classificando-o como:

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 natural¹⁷.

De La Cueva destaca a importância de tais definições, uma vez que os dados pessoais se encontram essencialmente vinculados à personalidade e dignidade humanas, tornando-os “objeto de garantia substantiva a través de outros derechos fundamentales”¹⁸. “Por serem informações de inquestionável importância, não podem ser submetidas a atividades arbitrárias por parte dos agentes controladores, sendo elas direitos essenciais”, ressalta, ainda, Adriano de Cuspis¹⁹.

¹⁵ CRAVO, Daniela Copetti: *Direito à portabilidade de dados Interface entre defesa da concorrência, do consumidor e proteção de dados*. Rio de Janeiro: Lumen Juris, 2018, p. 194.

¹⁶ BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Planalto. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/ Ato2015-2018/2016/Decreto/D8771.htm> Acesso em: 31 de outubro de 2019.

¹⁷ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/ ato2015-2018/2018/lei/L13709.htm> Acesso em: 31 de outubro de 2019.

¹⁸ DE LA CUEVA, Pablo Lucas Murillo. *Informática y protección de datos personales*. Madrid: Centro de Estudios Constitucionales, 1993, p. 69-70.

¹⁹ SILVA, Joseane Suzart Lopes da. *A proteção de dados pessoais dos consumidores e a Lei 13.709/2018: Em busca da efetividade dos direitos à privacidade, intimidade e autodeterminação*. Revista de Direito do Consumidor 2019, RDC21, p. 379.

Em virtude das algumas peculiaridades derivadas de fatores, como, por exemplo, os oriundos da busca de exploração econômica, segundo De Cuspis, tornou-se indispensável o desenvolvimento de meios de tutela específicos para os dados pessoais, principalmente os sensíveis²⁰. Conforme o autor, existem certos direitos sem os quais “a personalidade restaria uma susceptibilidade completamente irrealizada, privada de todo o valor concreto”, de modo que, sem eles, todos os demais “perderiam todo o interesse para o indivíduo – o que equivale a dizer que, se eles não existissem, a pessoa não existiria como tal”. Sendo, portanto, “direitos essenciais, com os quais se identificam precisamente os direitos de personalidade”²¹.

No que tange à necessária proteção dos dados pessoais, tal disciplina surge em meio à sociedade da informação, através de uma necessidade de tutelar a personalidade do indivíduo contra os iminentes riscos a serem causados pela falta de tratamento de dados pessoais. Ressalta-se que a sua função não é a proteção dos dados *per se*, mas a proteção da pessoa titular dos dados²².

Tendo em vista que as informações pessoais são ligações entre a pessoa e a sociedade, segundo Danilo Doneda, “a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito”²³. Pode-se concluir, portanto, que os dados pessoais são parte da personalidade do indivíduo, merecendo tutela jurídica, a fim de assegurar a igualdade e a liberdade²⁴.

Segundo Laura Schertel Mendes, no contexto moderno de desenvolvimento da tecnologia da informação, “o direito à privacidade transforma-se para dar origem à disciplina da proteção de dados pessoais, de modo a se adaptar aos desafios impostos pelo avanço da técnica”²⁵. Ainda, acrescenta que:

Sob essa perspectiva, pode-se compreender que a proteção de dados adquire um âmbito mais abrangente. Primeiramente, ela passa a ser compreendida como um fenômeno coletivo, na medida em que os danos causados pelo processamento impróprio de dados pessoais são, por

²⁰ DE CUSPIS, Adriano. *I diritti della personalità*. Milano: Giuffrè, 1982, p. 13.

²¹ *Ibidem*.

²² MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014, p. 32.

²³ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*, cit. apud MENDES, Laura Schertel, *op. cit.*, p. 32.

²⁴ MENDES, Laura Schertel. *Op. cit.*, p. 32.

²⁵ *Ibidem*, p. 35.

natureza, difusos, exigindo igualmente uma tutela jurídica coletiva. Em segundo lugar, a privacidade, antes compreendida, prioritariamente, como o direito negativo de ser deixado em paz (*right to be let alone*), passa a significar também o controle dos dados pessoais pelo próprio indivíduo, que decide quando, como e onde os seus dados pessoais devem circular²⁶.

Nas palavras de Frederico de Andrade, o motivo da proteção da vida privada na nova era, ou seja, a era da informação, configura-se como:

Além da garantia da integridade ao conjunto valorativo da personalidade, a concessão de plenos poderes à autodeterminação do indivíduo. Não estão mais em jogo somente as noções de segredo, ou o direito de ser deixado só. Percebe-se que o grande paradoxo do período descrito é que a privacidade não é uma mera ruptura com a ligação social, mas sim uma forma de se reconstruir livremente essa mesma ligação. Essas novas dimensões da vida privada consagram, assim, um conceito funcional, tangendo à possibilidade do sujeito de conhecer, controlar e interromper o fluxo de informações que a ele se referem²⁷.

Portanto, depreende-se das disposições acima que a proteção de dados, diante da necessária tutela exigida pela nova era informacional, desprende-se da privacidade para constituir um novo direito fundamental indispensável a uma sociedade democrática moderna, com fundamentos na personalidade e na dignidade humana. Permitindo ao indivíduo, desse modo, a disposição dos seus dados pessoais, reconstruindo a sua velha conexão com a sociedade.

2.2 A Proteção de Dados Pessoais como um Direito de Personalidade Autônomo perante o Direito à Privacidade

Inicialmente, cabe ressaltar que a tutela da proteção de dados pessoais surgiu como um desdobramento do direito à privacidade. A partir do momento em que a informação ganhou importância, a matéria dos dados pessoais passou a se destacar frente aos olhos da temática da privacidade²⁸.

No entanto, ao longo do tempo, passou-se a enxergar o direito à proteção de dados como um direito de personalidade, figurando ao lado de direitos fundamentais de qualquer pessoa humana, como, por exemplo, o direito à vida, à integridade física, à honra e à imagem. Segundo Fabiano Menke, estes são “direitos sem os quais a pessoa é incompleta

²⁶ MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014, p. 36.

²⁷ ANDRADE, Frederico Pupo Carrijo de. *Análise comparativa do tratamento de dados pessoais à luz do direito de personalidade*. Estudos avançados de direito digital/coordenação Cíntia Rosa Pereira Lima, Lydia Neves Bastos Telles Nunes. 1ª ed. Rio de Janeiro: Elsevier, 2014, p. 235.

²⁸ CRAVO, Daniela Copetti. *Direito à portabilidade de dados Interface entre defesa da concorrência, do consumidor e proteção de dados*. Rio de Janeiro: Lumen Juris, 2018, p. 30.

nos atributos mínimos de sua personalidade, não podendo desfrutar de uma vida digna”. Semelhante é o caso da proteção de dados, de modo que se o indivíduo não tiver “um mínimo controle e conhecimento de quem tem suas informações e o que com elas faz, não poderá desenvolver sua personalidade de maneira satisfatória”²⁹.

Logo, a proteção de dados diz respeito aos direitos da personalidade, uma vez que está diretamente ligada aos aspectos morais do indivíduo. No entanto, o fundamento da privacidade e dos dados pessoais é ontologicamente o mesmo, tendo como base a dignidade da pessoa humana, já que os dados nada mais são do que “a interpretação da própria privacidade, em termos de gestão da informação pessoal” (DONEDA, Danilo, 2008, p.1)³⁰.

Assim sendo, a proteção dos dados pessoais é uma espécie herdeira da privacidade, que dá a ela atualização e contornos próprios³¹. Portanto, apesar da disciplina dos dados pessoais ser um desdobramento do direito da privacidade, tais direitos não são idênticos³².

A privacidade, de modo geral, protege o indivíduo de uma intromissão ao seu espaço privado, enquanto a proteção de dados regula o processamento de dados de um indivíduo, sendo esses dados privados ou não. Por conseguinte, a finalidade da proteção de dados é evitar que eventual associação desses viole o direito de personalidade do indivíduo³³.

A respeito dos direitos de personalidade na era da informação, dispõe Bruno Bioni da seguinte forma:

Os direitos da personalidade não representam somente uma inovação no ordenamento jurídico brasileiro, trata-se, também, de um componente central de uma nova hermenêutica que coloca o ser humano como o “coração do direito civil contemporâneo”. Daí porque os direitos de personalidade fazem parte de uma cláusula geral de proteção de tutela e promoção da pessoa humana ou de um sistema geral de tutela à pessoa humana, cuja consequência principal é a sua

²⁹ MENKE, Fabiano. *Fundamentos da proteção de dados*. Inédito, p.1.

³⁰ DONEDA, Danilo. *Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais*. *Âmbito Jurídico*, v. 52, 2008, p.1.

³¹ BRASIL. Escola Nacional de Defesa do Consumidor. *A proteção de dados pessoais nas relações de consumo: para além da informação creditícia*. Brasília: SDE/DPDC, 2010, p. 25 apud CRAVO, Daniela Copetti. *Direito à portabilidade de dados Interface entre defesa da concorrência, do consumidor e proteção de dados*. Rio de Janeiro: Lumen Juris, 2018, p. 32.

³² CRAVO, Daniela Copetti: *Direito à portabilidade de dados Interface entre defesa da concorrência, do consumidor e proteção de dados*. Rio de Janeiro: Lumen Juris, 2018, p. 32.

³³ *Ibidem*.

elasticidade. Os direitos de personalidade são uma “noção inacabada” que deve ser “cultivada”, especialmente frente ao manancial de dados produzidos pelas pessoas na sociedade da informação. Por meio dessa premissa, é possível identificar uma nova variante desta categoria jurídica para naquela enquadrar a proteção dos dados pessoais. Nesse sentido, os direitos de personalidade não se limitam às situações previstas no Código Civil Brasileiro, sendo o seu rol *numerus apertus* (rol aberto). Eles não se exaurem naquelas espécies enumeradas nos arts. 11 a 21 do CC, o que abre caminho para o reconhecimento da proteção de dados pessoais como um *novo direito da personalidade*³⁴.

Por fim, interessante ressaltar o entendimento de Rodotà de que, nos tempos modernos, “vivencia-se uma reinvenção conceitual da proteção de dados, não apenas pelo reconhecimento expreso como direito fundamental autônomo, mas pelo papel indispensável para o desenvolvimento da personalidade”³⁵. Assim, “a proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio”³⁶.

2.3 Proteção Legal dos Dados Pessoais

Através do desenvolvimento do comércio e das atividades econômicas, verificou-se o surgimento do banco de dados pessoais, cuja proteção interessava tanto para os Estados e entre privados, quanto para os cidadãos e clientes, que se preocupavam com o mau uso ou abuso das informações pelos seus detentores. Entretanto, a preocupação dos indivíduos tornou-se ainda maior a partir dos anos 60, quando os dados passaram a ser acumulados em computadores, tornando-se facilmente acessíveis³⁷.

A respeito, José Afonso da Silva diz que:

[...] o intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadramento das pessoas, que ficam com sua individualidade inteiramente devastada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento³⁸.

³⁴ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 59-60.

³⁵ FORTES, Vinicius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet*. Rio de Janeiro: Lumen Juris, 2016, p. 37.

³⁶ RODOTÀ, Stefano. *A vida privada na sociedade da vigilância – A privacidade hoje*. Rio de Janeiro: Renovar, 2008, p.17.

³⁷ ZANON, João Carlos. *Direito à proteção dos dados pessoais*. São Paulo: Revista dos Tribunais, 2013, p. 69-70.

A informação, independentemente de sua espécie, tornou-se um bem jurídico de valor extraordinário, de modo que “os Estados, as associações, as empresas são tão ou mais poderosas conforme disponham de grandes volumes de informação”³⁹ e que “o melhor acesso a mais informações é a marca da economia informacional”⁴⁰. Nas palavras de Marcel Leonardi, “o avanço da tecnologia, aliado ao aumento da velocidade das redes e à melhora dos mecanismos de busca, gera mais atividade econômica baseada na economia da informação”⁴¹.

Contudo, foi com o surgimento da internet que a questão tornou-se ainda mais preocupante, uma vez que tudo pode ser encontrado na imensa mina de dados pessoais. Na contemporânea sociedade da informação e das redes, na qual vivemos hoje, as possibilidades de coleta, de tratamento e de armazenamento de dados pessoais são praticamente infinitas. Também, através da utilização dos serviços *on-line*, deixamos rastros eletrônicos que são coletados e garimpados o tempo todo⁴².

Dessa forma, verifica-se uma grande exposição do indivíduo, que não possui mais controle sobre seus dados pessoais. Portanto, essa alarmante realidade chamou a atenção dos legisladores para a importância da proteção dos dados pessoais na sociedade contemporânea, fazendo com que surgissem, na década de 70, as primeiras leis que buscavam regular o uso de dados e os bancos de dados pessoais⁴³. Foi assim que, desde então, houve uma grande evolução legislativa e doutrinária sobre o assunto⁴⁴, a qual será vista no ponto a seguir.

2.3.1 A Proteção de Dados no Cenário Europeu

Diante da imensidão de leis e países que existem hoje no mundo, o presente trabalho atentar-se-á para uma evolução do regramento da proteção de dados apenas em âmbito europeu, uma vez que, como será demonstrado nos capítulos seguintes, a nova Lei

³⁸ SILVA, José Afonso da. *Curso de direito constitucional positivo*. São Paulo: Malheiros, 2012, p. 209-210.

³⁹ SUÁREZ, José María Álvarez-Cienfuegos, *La defensa de la intimidad de los cuidados y la tecnología informática*. Colección Divulgación Jurídica, Navarra: Aranzadi, 1999, p.13, apud LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012, p. 68.

⁴⁰ DOCTOROW, Cory. *Content: Selected Essays on Technology, Creativity, Copyright and the Future of the Future*. São Francisco: Tachyon Publications, 2008, p. 61, apud ibidem.

⁴¹ LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012, p. 68.

⁴² ZANON, João Carlos. *Direito à proteção dos dados pessoais*. São Paulo: Revista dos Tribunais, 2013, p.71.

⁴³ Ibidem, p. 74.

⁴⁴ ZANON, João Carlos. *Op. cit.*, p.74.

Geral de Proteção de Dados brasileira inspirou-se, claramente, na “General Data Protection Regulation” (GDPR), ou seja, a nova lei geral de proteção de dados da União Europeia.

Após o crescimento e desenvolvimento do cenário tecnológico computacional na década de 60, em 1970 surgiu o primeiro texto com força de lei de proteção de dados informatizados, no estado alemão de Hesse, a chamada “Hessisches Datenschutzgesetz”, o qual tinha o objetivo de zelar pelas informações pessoais de indivíduos armazenadas em meios eletrônicos. A lei, ainda que pioneira ao tratar da coleta e tratamento de dados de indivíduos, não o fez de maneira objetiva e segmentada⁴⁵.

A seguir, em 1973, foi editada a lei de proteção de dados sueca, a primeira nacional da história a respeito do tema, a Sw. Datalagen ou o Ato de Dados Sueco⁴⁶. Similar à lei de Hesse, a lei sueca abordava a proteção dos dados genericamente, não abarcando, por exemplo, as situações nas quais a coleta de dados poderia ou não ocorrer, dispondo apenas que para tal coleta era necessária a autorização da agência governamental competente. Além disso, a lei não trazia princípios gerais do tratamento de dados pessoais, algo recorrente nas leis modernas sobre o assunto. Todavia, inovou ao trazer o tema da proteção de dados para a agenda pública de governo⁴⁷.

Espelhando-se nesses países, em 1979 diversas outras nações europeias como, por exemplo, França, Alemanha e Dinamarca, já possuíam legislações a respeito da proteção de dados. Tais leis, ainda que muito importantes, eram genéricas, assim como o texto sueco e o texto alemão. Ressalta-se também que, ainda no final dos anos 70, Portugal, Espanha e Áustria passaram a considerar a privacidade como um direito fundamental em

⁴⁵ MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriana Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERINI, Pamela Michelena De Marchi. *Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos*. Disponível em: <<https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>>. Acesso em: 23 de outubro de 2019, p. 7.

⁴⁶ ÖMAN, Sören. *Implementing Data Protection in Law*. Disponível em: <<http://www.scandinavianlaw.se/pdf/47-18.pdf>>. Acesso em: 18 de agosto de 2018. Apud MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriana Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERINI, Pamela Michelena De Marchi, ibidem, p.7.

⁴⁷ MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriana Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERINI, Pamela Michelena De Marchi. *Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos*. Disponível em: <<https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>>. Acesso em: 23 de outubro de 2019, p. 7.

suas Constituições, ilustrando muito bem a importância dada à proteção de dados por essas nações⁴⁸.

O direito comunitário europeu, segundo Bruno Bioni, “exprime bem a travessia do consentimento no percurso geracional das leis de proteção dos dados pessoais, cuja linha evolutiva permanece em curso até hoje; a começar pela influência das *guidelines* da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)”. A Convenção 108 do Conselho da Europa, de 1981, de *Strasbourg*, por exemplo, é resultado do movimento promovido pela OCDE, a fim de facilitar a harmonização das legislações de proteção de dados pessoais⁴⁹.

Dessa forma, conforme se depreende de seu preâmbulo, a Convenção 108 foi aprovada por considerar:

[...] desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado⁵⁰.

A Convenção representa, para a história, o primeiro marco legal vinculativo transnacional sobre proteção de dados. Entretanto, nota-se ainda no Convênio uma forte vinculação ao princípio da “liberdade de informação”, posto que em nenhum momento se exige o consentimento do afetado para a recolha dos dados⁵¹. Assim, ainda que vinculante a respeito do tema, o objetivo da Convenção não foi alcançado, uma vez que “o excessivo apoio em princípios e não regras e a amplitude com que confere exceções permitiram regimes absolutamente distintos nos países que assumiram a Convenção”⁵².

⁴⁸ RUDGARD, Sian. *Origins and Historical Context of Data Protection Law*. Disponível em: <https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf>. Acesso em: 18 de agosto de 2018, apud MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriana Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERINI, Pamela Michelena De Marchi, *ibidem*, p.7.

⁴⁹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 122.

⁵⁰ PORTUGAL. Convenção 108 de 28 de janeiro de 1981. Disponível em: <<https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>>. Acesso em: 04 de novembro de 2019.

⁵¹ SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014, p. 112.

⁵² RAMIRO, Mónica Arenas. *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Agencia Española de Protección de Datos, 2006, p. 156 apud SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014, p. 112.

Passadas então duas décadas, através da crescente evolução do cenário tecnológico, as leis de proteção de dados tornaram-se mais importantes e desenvolvidas, adquirindo um formato mais semelhante às leis atuais, fenômeno que se consolidou quando a União Europeia, em 24 de outubro de 1995, promulgou a Diretiva 95/46/CE⁵³, a primeira e principal norma comunitária dirigida aos Estados-membros. A norma foi um marco no campo da proteção de dados, pois serviu de inspiração e impulso unificados para as legislações internas dos países-membros do bloco, visto que determinava, em seu artigo 32, a obrigatória adoção de seu conteúdo, em até 3 anos, pelas normas nacionais dos países⁵⁴, colocando, portanto, todos sob a mesma legislação.

A Diretiva passou a estabelecer como deveria ser feita a coleta e o tratamento dos dados e abarcou uma série de princípios que deveriam ser seguidos, referentes aos objetivos de comportamento dos envolvidos na relação da proteção de dados, dentre os quais destacam-se o da licitude do tratamento, da limitação dos propósitos, da adequação, da necessidade e da transparência, que objetivavam impedir possíveis abusos por parte dos responsáveis pelos dados, permitindo a manutenção da eficácia da ação do Estado⁵⁵. Além disso, a Diretiva trouxe não só direitos aos titulares dos dados pessoais, mas também deveres aos *data controllers* – aqueles que processam os dados pessoais – de aperfeiçoar a estratégia regulatória. O princípio da proporcionalidade contido nela, por exemplo, traz a ideia de minimização, ou seja, cria a obrigação de o *data controller* não coletar dados excessivos, além dos necessários, permitindo com que o titular dos dados pessoais “maximize a sua esfera de controle sobre as suas informações pessoais”⁵⁶.

No entanto, apesar de trazer mudanças significativas ao tema da proteção de dados, a Diretiva sofreu alguns impasses, como, por exemplo, no tocante aos distintos

⁵³ PARLAMENTO EUROPEU. Directiva 95/46/CE de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao o tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>>. Acesso em: 18 de agosto de 2018. Apud MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriana Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERINI, Pamela Michelena De Marchi, *ibidem*, p.7.

⁵⁴ SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014, p. 114.

⁵⁵ MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriana Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERINI, Pamela Michelena De Marchi. *Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos*. Disponível em: <<https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>>, p. 7-8.

⁵⁶ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 123.

tratamentos adotados no direito interno dos países membros. Foi assim que, diante dos avanços da revolução tecnológica, a Diretiva 95/46/CE – que vigorou até maio de 2018 – passou a ser substituída pelo “General Data Protection Regulation – GDPR”, de 27 abril de 2016, a nova lei geral de proteção de dados da União Europeia, que reforçou a privacidade na internet.

O Regulamento, todavia, diferentemente da antiga Diretiva, que previa uma data limite para sua adoção pelo direito nacional dos países, é diretamente aplicável a cada Estado membro da UE, sem necessidade de uma legislação de implementação, unificando, portanto, a legislação do bloco a respeito do tema⁵⁷. Ademais, ele possui um objetivo adicional para além da proteção da intimidade dos indivíduos, qual seja, a consolidação do Mercado Único Digital, para o qual são indispensáveis a uniformidade de regras e a remoção das barreiras técnicas e legais⁵⁸.

A GDPR, que constitui-se como uma evolução da Diretiva 95/46/EC, traz uma extensão à proteção, incluindo, em seu escopo de aplicação, para além dos dados de pessoas naturais localizados na União Europeia, todo o fluxo de dados existente nos países membros e nos países ao redor do mundo que possuam pontos de contato com o mercado europeu. Assim, os principais avanços da nova disposição legal são a ampliação de direitos dos usuários e a maior responsabilização dos agentes que realizam o processamento de dados⁵⁹.

No que tange à aplicação material do Regulamento, por se tratar de uma lei geral, depreende-se que basicamente toda a operação relativa a dados pessoais passa a sujeitar-se a ele, como, por exemplo, relações de consumo, interações por meio de internet, questões envolvendo relações de emprego e tratamento de dados de crianças e adolescentes⁶⁰. É nesse ponto também que o Regulamento se diferencia da Diretiva e dos

⁵⁷ BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção de dados do consumidor*. São Paulo: Almedina, 2018, p. 117.

⁵⁸ CRAVO, Daniela Copetti. *Direito à portabilidade de dados Interface entre defesa da concorrência, do consumidor e proteção de dados*. Rio de Janeiro: Lumen Juris, 2018, p. 37.

⁵⁹ MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriana Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERINI, Pamela Michelena De Marchi. *Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos*. Disponível em: <<https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>>

⁶⁰ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice, coordenadores. *Comentários ao GDPR: Regulamento Geral da Proteção da Dados da União Europeia*. São Paulo: Thomson Reuters Brasil, 2018, p. 27.

demais países com legislações setoriais, uma vez que possui aplicabilidade ampla, não se restringindo a legislações específicas a respeito da proteção de dados.

3 Lei Geral de Proteção de Dados

3.1 A Proteção de Dados como um Direito Fundamental no Brasil e a Proposta de Emenda à Constituição n. 17 de 2019

Os direitos humanos só passam a ser considerados fundamentais quando presentes na Constituição de um país, juntamente com os elementos de juridicidade que garantem tal fundamentalidade, quais sejam: a *eficácia direta* e *vinculação a todos os Poderes Públicos*, a regulação somente com *reserva de lei* e com respeito a um *conteúdo essencial* e a garantia de um *controle de constitucionalidade* a tais normas⁶¹. Nesse sentido, Robert Alexy distingue tais direitos com as seguintes palavras:

As perguntas a respeito de quais direitos você tem como pessoa e como cidadão de uma comunidade, a quais princípios a lei estadual está sujeita e o que é aquilo que exige a realização da dignidade humana, libertação e igualdade são importantes temas da filosofia prática e pontos controversos centrais das lutas políticas passadas e atuais. Se convertem em problemas jurídicos quando uma Constituição - como a Lei Fundamental da República Federal da Alemanha (LF) - estabelece que as normas de direito fundamentais, como efeito imediato, vinculam a legislação ao Poder Executivo e ao Poder Judiciário, e apenas isso está vinculado ao amplo controle por um Tribunal Constitucional⁶².

Dessa forma, pode-se depreender do parágrafo anterior que, ainda que seja um direito humano reconhecível e de elevada importância na era da informação, o direito à proteção de dados só pode ser considerado fundamental quando incorporado à Constituição de um determinado povo, o que não acontece no Brasil, uma vez que não há uma previsão direta à proteção de dados na Constituição Federal Brasileira de 1988. Todavia, há autores que discordam da seguinte conclusão, alegando que a falta da devida previsão não significa a ausência de proteção constitucional a respeito do tema.

Portanto, seguindo essa corrente, pode-se verificar, em consulta à Constituição, que existem três incisos no artigo 5º que tangenciam o tema, os quais fazem parte dos “direitos e deveres individuais e coletivos”. São eles: o inciso X⁶³, que define como

⁶¹ SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014, p.32.

⁶² ALEXY, Robert. *Teoria de los derechos fundamentales*. Madrid: Centro de Estudios Constitucionales, 2007, p.1.

⁶³ “X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

inviolável a vida privada e a intimidade; o inciso XII⁶⁴, que garante o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, e o inciso LXXII⁶⁵, que trata da ação de *habeas data*, permitindo o direito de acesso e retificação de dados pessoais⁶⁶.

Contudo, ao longo dos debates no julgamento do RE 418.416/SC⁶⁷, em maio de 2006, o Supremo Tribunal Federal afirmou por unanimidade que a proteção do inciso XII tem como âmbito normativo somente diferentes formas de *comunicação* de dados, não favorecendo a informação pessoal propriamente dita. Complementam afirmando que o uso do termo “dados”, no mencionado inciso, é fruto de certa impropriedade do constituinte, uma vez que, ao buscar atualizar o §9º do artigo 150 da CF de 1967⁶⁸, desejava preservar não o objeto que poderia ser transmitido a outrem, mas a *modalidade de comunicação* que se realizava por meio de computadores. Havendo uma garantia, por conseguinte, ao *momento* da fala, mas não ao seu *conteúdo*⁶⁹.

Já o min. Carlos Ayres de Britto, em seu voto, interligou a proteção de dados pessoais com a inviolabilidade do domicílio do inciso XI e com a vida privada e intimidade do inciso X. Havendo, logo, não um sigilo de qualquer informação, mas daquelas conectadas com o alcance desses outros direitos constitucionais. Por isso, o dado individualmente considerado só estaria constitucionalmente garantido *prima facie*, no que tange à sua revelação, se de conteúdo *íntimo* ou *privado*.

⁶⁴ “XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”.

⁶⁵ “LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se preferir fazê-lo por processo sigiloso, judicial ou administrativo”.

⁶⁶ SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014, p.55.

⁶⁷ Ementa: PROCESSO PENAL. HABEAS CORPUS. CRIME MILITAR. MENSAGENS CRIMINOSAS ENVIADAS PELA INTERNET. ACESSO AO CONTEÚDO DAS COMUNICAÇÕES DISPONIBILIZADO PELOS DESTINATÁRIOS. ACESSO AOS DADOS DE COMPUTADOR EM LAN HOUSE COM AUTORIZAÇÃO DO PROPRIETÁRIO JUDICIAL. INTERROGATÓRIO POR PRECATÓRIA. INVALIDADES NÃO RECONHECIDAS (RE. 418.416/SC - Pleno do STF - Rel. Min. Sepúlveda Pertence - por maioria - j. em 10.5.2006).

⁶⁸ “São invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas”.

⁶⁹ JUNIOR, Tércio Sampaio Ferraz. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. São Paulo: Quartier Latin, 2005, p. 23, apud SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2018, p. 56.

Isso significa, segundo Carlos Bruno, que “não se admite no Brasil a inclusão dos dados cadastrais na garantia de inviolabilidade da intimidade e da vida privada constante no inciso X do artigo 5º da Constituição Federal”, complementando com a posição majoritária de Tércio Sampaio Ferraz Júnior, que assim dispõe:

Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos – como nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc., condicionam o intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção de dados em si, pelo sigilo, não faz sentido⁷⁰.

À vista disso, conclui Carlos Bruno que “a própria utilização da palavra *sigilo* demonstra o predomínio da proteção estática e limitada dos dados no direito brasileiro, uma vez que está ligada a uma obrigação, daquele que tem acesso às informações, de mantê-las secretas”. Sendo assim, a proteção e o controle dos dados pelo particular, através do *habeas data*, fica relegada a segundo plano. Ressalta-se que não quer dizer que não seja um instrumento adequado à proteção de dados, mas que a jurisprudência majoritária no Brasil não admite nenhuma abrangência que ultrapasse os limites já reconhecidos da intimidade, estabelecendo obstáculos processuais que desestimulam o uso judicial do instrumento⁷¹.

Destarte, é diante das dificuldades exemplificadas que se faz necessária uma emenda à Constituição, a fim de assegurar a proteção de dados como um direito fundamental, não sendo necessário que se discuta, a cada caso, se o dado do caso concreto é parte daqueles para os quais se voltou a intenção do legislador no inciso XI do artigo 5º da CFB. Foi assim que, em 12 de março de 2019, foi veiculada a Proposta de Emenda à Constituição nº 17.

O texto, aprovado no Plenário do Senado e que segue agora para a votação na Câmara dos Deputados, propõe o acréscimo do inciso XII-A⁷², ao art. 5º, e o inciso

⁷⁰ JUNIOR, Tércio Sampaio Ferraz. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*. São Paulo: Quartier Latin, 2005, p. 28, apud SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2018, p. 57.

⁷¹ SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014, p. 58-62.

⁷² “XII-A - é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais”.

XXX⁷³, ao art. 22, da Constituição Federal, para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria⁷⁴. Buscando uma uniformização da legislação quanto à proteção e tratamento de dados, o texto possui em sua justificativa os seguintes parágrafos:

A proteção de dados pessoais é fruto da evolução histórica da própria sociedade internacional: diversos são os Países que adotaram leis e regras sobre privacidade e proteção de dados. Isso porque o assunto, cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão.

O avanço da tecnologia, por um lado, oportuniza racionalização de negócios e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por outro lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados⁷⁵.

Ainda, menciona o atraso do nosso ordenamento jurídico frente as demais legislações internacionais, uma vez que “já se vislumbra, dadas as suas peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado”, para além de uma lei ordinária sobre o assunto, como é o caso da LGPD⁷⁶. Ressalta-se, ainda, que além de instituir o direito fundamental à proteção de dados pessoais, a PEC busca também disciplinar a competência constitucional para legislar sobre o tema, assim dispendo:

Sabemos que existem diversas propostas de leis estaduais e municipais versando sobre o assunto, inclusive em flagrante réplica da LGPD. Não há racionalização nisso: a fragmentação e pulverização de assunto tão caro à sociedade deve ser evitada. O ideal, tanto quanto se dá com outros direitos fundamentais e temas gerais relevantes, é que a União detenha a competência central legislativa. Do contrário, pode-se correr o risco de, inclusive de forma inconstitucional, haver dezenas – talvez milhares – de conceitos legais sobre o que é "dado pessoal" ou sobre quem são os "agentes de tratamento" sujeitos à norma legal⁷⁷.

É através dos referidos argumentos que a Proposta de Emenda à Constituição n. 17 busca, então, o enquadramento da proteção de dados como um direito *jusfundamental*, adequando-se à realidade internacional da disciplina da matéria. Todavia, para além do

⁷³ “XXX - proteção e tratamento de dados pessoais”.

⁷⁴ BRASIL. Proposta de Emenda à Constituição n. 17, de 2019. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1571776978885&disposition=inline>>. Acesso em: 05 de novembro de 2019.

⁷⁵ Ibidem.

⁷⁶ Ibidem.

⁷⁷ Ibidem.

regramento constitucional a respeito do tema, houve, no Brasil, legislações esparsas ao longo dos anos a respeito do tema, a serem verificadas a seguir.

3.2 Evolução do Tratamento no Brasil

3.2.1 Legislação Esparsa

O ordenamento jurídico brasileiro dispõe de diversas leis esparsas que abordam diferentes aspectos das relações jurídicas que envolvem dados pessoais, a partir de relações ou circunstâncias específicas. No entanto, faz-se interessante ressaltar que as referidas leis pouco adentraram à temática da privacidade, o fazendo de forma pouco tímida e, até mesmo, incoerente⁷⁸, conforme verificar-se-á através da citação das principais leis incidentes no Brasil anteriormente à aprovação da LGPD, bem como suas principais disposições, que passo a fazer agora.

Inicialmente, convém ressaltar que, ainda que não seja um produto da legislação brasileira, a Declaração Universal dos Direitos Humanos, de dezembro de 1948, estabeleceu como universal o direito à vida privada, preservando-a de interferências externas, consoante disposição do artigo 12:

Artigo 12 – Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Observando seu contexto histórico, verifica-se que a Declaração foi uma das formas empreendidas pelas nações para colocar ordem aos períodos de guerra, na qual muitos seres humanos foram perseguidos e executados, por exemplo, por suas convicções políticas ou religiosas. Ou seja, em razão dos elementos abrigados pela intimidade e pela privacidade, razão pela qual a Assembleia das Nações Unidas passou a prever expressamente a proibição de interferências nessa esfera da personalidade, como diretriz a ser seguida por todos os países⁷⁹.

Além disso, verifica-se que, em consonância com a CF/88 e no mesmo sentido das discussões da UE à época, a Lei nº 8078 de setembro de 1990, chamada de Código

⁷⁸ OLIVEIRA, Ricardo Alexandre de. *Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico*. São Paulo: Revista dos Tribunais, dezembro 2018, vol. 998, ano 107, p. 244.

⁷⁹ *Ibidem*.

de Defesa do Consumidor (CDC), disciplinou a criação de bancos de dados de consumidores, nos termos do seu artigo 43:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor (Incluído pela Lei nº 13.146, de 2015)⁸⁰.

Observe-se que, apesar de não tratar expressamente do consentimento, os parágrafos do artigo acima condicionam a abertura de cadastro, ficha, registro e dados pessoais e de consumo à comunicação por escrito ao consumidor, de forma objetiva, clara, verdadeira e em linguagem de fácil compreensão⁸¹. Nessa esteira, a legislação consumerista optou por conferir ao consumidor o direito de controlar suas informações pessoais, uma vez que deve ter ciência do fluxo de seus dados, caracterizando a atividade como *transparente*⁸².

A referida transparência só tem razão de ser em razão dos direitos (acesso, retificação e cancelamento – mencionados no caput e §3º do artigo 43 do CDC, respectivamente) e princípios (transparência, qualidade [exatidão] e limitação temporal – indicados no §1º do artigo 43) contidos no artigo acima, que gravitam em torno do consumidor, para que ele, enquanto titular dos dados pessoais, exerça controle sobre suas

⁸⁰ BRASIL. Lei nº 8.078 de 11 de setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078.htm>. Acesso em: 06 de novembro de 2019.

⁸¹ BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia. *Proteção de dados pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018*. Belo Horizonte: Fórum, 2019, p. 26.

⁸² BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 127.

informações. Em suma, conforme Bruno Bioni, “o Código de Defesa do Consumidor buscou conferir a autodeterminação informacional, o que perpassa desde regras para garantir a exatidão dos dados até limitações temporais para o seu armazenamento”⁸³.

Importante ressaltar, outrossim, que a aplicação do artigo 43, no plano jurisprudencial, normalmente se cingia a uma discussão voltada à importância dos bancos de dados de consumo para a diminuição da inadimplência e redução dos juros de mercado, ou, ainda, a problemas relacionados a vinculações do direito à honra. Todavia, o rel. Min. Ruy Rosado de Aguiar, ao interpretar o referido dispositivo legal, no julgamento do REsp 22.337/RS, proferiu voto reconhecendo um novo conceito do direito à privacidade, aproximando-o do direito à proteção dos dados pessoais, conforme se pode concluir de parte do seu voto⁸⁴:

A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão e delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. Nos países mais adiantados, está posta no nível das garantias fundamentais, com o direito à autodeterminação informacional (o cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, à semelhança do *ombudsman*, com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para garantia dos limites permitidos na legislação⁸⁵.

O voto interliga, portanto, o uso de dados pessoais à intimidade e à vida privada dos indivíduos e evidencia a necessidade de transparência no tratamento dos dados e o

⁸³ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 127.

⁸⁴ ZANON, João Carlos. *Direito à proteção de dados pessoais*. São Paulo: Editora Revista dos Tribunais, 2013, p. 140.

⁸⁵ STJ, REsp 22.337/RS, 4ª Turma, julgado em 12 fev. 1995, v.u., rel. Min. Ruy Rosado de Aguiar, DJ 20 mar. 2005.

direito de acesso e de controle por parte do seu titular. Além disso, observa-se a referência ao direito à autodeterminação informacional como um direito fundamental.

Diferentemente do CDC, o Código Civil Brasileiro, Lei 10.406 de 2002, ainda que tenha estabelecido regras mais gerais, deu maior detalhamento aos direitos inerentes à personalidade, dentre os quais se encontram a privacidade e a intimidade:

Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.

[...]

Art. 16. Toda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome.

Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória⁸⁶.

Ademais, o Código Civil previu expressamente que o juiz deverá adotar as providências necessárias para cessar a violação da vida privada.

Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma⁸⁷.

Já a Lei nº 12.527, Lei de Acesso à Informação, de 18 de novembro de 2011, diferenciando informações comuns de informações pessoais, delimita o tratamento de dados pessoais no seu âmbito de aplicação:

Art. 4º Para os efeitos desta Lei, considera-se:

I - **informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

IV - **informação pessoal**: aquela relacionada à pessoa natural identificada ou identificável;

V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

⁸⁶ BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 06 de novembro de 2019.

⁸⁷ BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 06 de novembro de 2019.

VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

[...]

Art. 31. 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.**

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III - ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V - à proteção do interesse público e geral preponderante.

§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal⁸⁸. (grifos próprios)

No entanto, pode-se concluir que a mencionada lei, ainda que tenha caminhado no sentido de promover o direito fundamental à proteção de dados pessoais, trouxe em seu artigo 31 um retrocesso, uma vez que negligenciou o *princípio de proibição do tratamento de dados sensíveis*, permitindo a coleta e o tratamento de dados de intimidade e da vida privada das pessoas sem o consentimento do titular e sem especificar em que condições e situações poderiam ocorrer. Esse princípio, garantia fundamental a respeito

⁸⁸ BRASIL. Lei nº 12.737 de 18 de novembro de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/2011/lei/l12527.htm>. Acesso em: 06 de novembro de 2019.

do tema, garante que o Estado não colete e trate dados sensíveis sem a expressa anuência do seu titular, a não ser nos casos excepcionais e justificados previstos em lei⁸⁹.

Também, no âmbito das normas infralegais, observam-se três disposições que estabelecem direitos de proteção sobre dados pessoais e que contemplam os *princípios de finalidade* e da *confidencialidade*, quais sejam: o Decreto nº 6.523/2008, que regulamenta o serviço do SAC e, em seu artigo 11, prescreve que “os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para fins do atendimento”; o Decreto nº 6.425/2008, que dispõe sobre o censo anual de educação e, em seu artigo 6º, prevê a vedação da utilização dos dados pessoais para fins alheios aos previstos na legislação aplicável e assegura o sigilo e a proteção de dados pessoais colhidos e, por fim, o Decreto nº 6.135, que instituiu o cadastro único para fins de programas sociais do Governo Federal, estabelecendo, em seu artigo 8º, que os dados pessoais das famílias são sigilosos e que somente serão utilizados para finalidades especiais nele previstas⁹⁰.

3.2.2 Marco Civil da Internet

A Lei n. 12.965/2014, conhecida como Marco Civil da Internet (MCI), surge como uma norma específica a fim de regular os direitos e garantias do cidadão nas relações travadas na internet⁹¹. No entanto, note-se que, embora aborde consideravelmente o tratamento de dados pessoais, só o faz em relação àqueles que transitaram pela internet, sem contemplar os colhidos *off-line* ou por redes privadas⁹², conforme se conclui a partir da leitura do seu artigo 1º.

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria⁹³.

⁸⁹ ZANON, João Carlos. *Direito à proteção de dados pessoais*. São Paulo: Editora Revista dos Tribunais, 2013, p. 144.

⁹⁰ *Ibidem*.

⁹¹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019, p. 130.

⁹² COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. São Paulo: Thomson Reuters, 2019, p. 36.

⁹³ BRASIL. Lei nº 12.965 de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/lei/112965.htm. Acesso em: 07 de novembro de 2019.

Já os artigos 2º e 3º da Lei dispõem sobre os fundamentos e princípios para o uso da Internet no Brasil, respectivamente⁹⁴. Das suas leituras faz-se duas principais conclusões: a primeira diz respeito à defesa do consumidor, a qual, juntamente com a livre iniciativa e a livre concorrência, é trazida como um dos fundamentos da Lei, permitindo-nos concluir que a Lei nº 12.965/2014 deve ser aplicada em conformidade com o princípio da vulnerabilidade do consumidor e as normas do ordenamento que disponham sobre a proteção do consumidor, como o CDC, a Lei do Cadastro Positivo e a LGPD; a segunda, no entanto, diz respeito aos princípios de proteção da privacidade e proteção dos dados pessoais – mencionados no artigo 3º – uma vez que se pode afirmar que “houve um amadurecimento do ordenamento jurídico brasileiro no sentido de reconhecer que a proteção de dados pessoais não se circunscreve ao direito à privacidade, nem é somente uma concretização desse direito”⁹⁵.

Passando-se a uma breve análise dos artigos 7º e seguintes, esse, que inaugura do capítulo 2 do MCI, trata mais claramente dos direitos dos usuários, dentre os quais destacam-se, por exemplo: o não fornecimento a terceiros de seus dados pessoais (inciso

⁹⁴ Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 07 de novembro de 2019.

⁹⁵ DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). *Direito & Internet III – Tomo I: Marco Civil da Internet (Lei nº 12.965/2014)*. São Paulo: Quartier Latin, 2015, p. 338-339.

VII), inclusive registros de conexão e de acesso a aplicações de internet, a não ser que haja “consentimento livre expresso e informado ou nas hipóteses previstas em lei”⁹⁶; o direito do usuário de ter “informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet” (inciso VIII)⁹⁷, determinando o cumprimento do princípio da finalidade da coleta de dados por parte dos fornecedores, que só será justificada para as atividades declaradas⁹⁸; o direito ao consentimento expresso qualificado do usuário sobre a coleta, o uso, o armazenamento e o tratamento de dados pessoais (inciso IX) e, por fim, o direito ao esquecimento (inciso X), que trata do direito à exclusão definitiva dos dados pessoais, pelo seu responsável, a pedido do titular, ao término da relação entre as partes⁹⁹.

Além disso, ressalta-se que o artigo 11 da Lei dispõe sobre a coleta, o armazenamento, a guarda e o tratamento dos registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicação de internet em território nacional. Também, o artigo 12 determina sanções para as infrações às normas previstas nos artigos 10 e 11 da Lei, sem prejuízos às demais sanções cíveis, criminais ou administrativas¹⁰⁰.

Todavia, ainda que o MCI possua semelhanças com a LGPD, como em relação a alguns de seus princípios e fundamentos, é insuficiente para regular o tratamento de dados pessoais como um todo, visto que somente é aplicável às relações jurídicas dependentes do uso da internet, conforme mencionado acima. Dessa forma, conforme outras leis citadas no tópico anterior, o MCI apresenta apenas alguns aspectos pertinentes ao

⁹⁶ BRASIL. Lei nº 12.965 de 23 de abril de 2014. **Artigo 7º, inciso VII**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/lei/112965.htm. Acesso em: 10 de novembro de 2019.

⁹⁷ Ibidem. **Artigo 7º, inciso VIII**. Acesso em: 10 de novembro de 2019.

⁹⁸ DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). *Direito & Internet III – Tomo I: Marco Civil da Internet (Lei nº 12.965/2014)*. São Paulo: Quartier Latin, 2015, p. 344-345.

⁹⁹ BRASIL. Lei nº 12.965 de 23 de abril de 2014. **Artigo 7º, incisos IX e X**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/lei/112965.htm. Acesso em: 10 de novembro de 2019.

¹⁰⁰ DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). *Op. cit.*, p. 349-350.

tratamento de dados pessoais, quais sejam, aqueles realizados mediante participação ou utilização da internet.

Por fim, ressalta-se que não se está diante de uma antinomia de normas entre o MCI e a LGPD, uma vez que a proteção intencionada na LGPD não exclui a proteção prevista em outras leis, conforme estabeleceu o artigo 64:

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Portanto, segundo Alexandre de Oliveira, trata-se de uma “coabitação de duas leis complementares, ambas aplicáveis ao mesmo caso concreto, que geram dupla camada de proteção aos titulares que têm seus dados tratados por meio da Internet, que é o ponto de convergência entre as duas legislações”¹⁰¹.

Ressalta-se que as leis acima são apenas exemplos considerados mais significativos em relação à proteção de dados antes do advento da LGPD, o que nos permite concluir que, excepcionada a Constituição Federal e o Código Civil Brasileiro, tais leis são aplicáveis apenas em relação aos seus destinatários e às relações jurídicas que dispõem. Trazendo, assim, uma dificuldade tanto para o julgador, quanto para os particulares, que deverão se adaptar aos regulamentos distintos de tratamento de dados.

3.3 Disposições Gerais

A Lei 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), assinada pelo presidente Michel Temer em 14 de agosto de 2018, inaugurou no Brasil um regime geral de proteção de dados, fazendo com que o Brasil passasse a integrar o grupo de países que dispõe de uma lei geral sobre o tema. Originária do PLC 53/18, que foi resultante da união de outros dois projetos, a Lei estabeleceu um período de *vacatio legis* de 18 meses, contados a partir de sua publicação.

Refletindo-se a respeito das principais influências que permitiram o surgimento da nova Lei, verifica-se que ela se inspira, primeiramente, no modelo europeu de proteção

¹⁰¹ OLIVEIRA, Ricardo Alexandre de. *Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico*. Revista dos Tribunais, vol. 998, ano 107, p. 241-261. São Paulo: Ed. RT, dezembro de 2018, p. 249-252.

de dados, ou seja, naquele amparado na Convenção 108 de 1981, na Diretiva 46/95/CE e no Regulamento Geral de Proteção de Dados (GDPR), referidos no capítulo anterior. Tal conclusão pode ser verificada a partir da leitura de vários artigos da Lei, como, por exemplo, aqueles referentes à exigência de uma base legal para o tratamento de dados, aos princípios gerais, aos dados sensíveis, à responsabilidade do *operador* e do *controlador* – novas figuras criadas pela Lei chamadas de “agentes de tratamento” – e à portabilidade de dados, outra inovação trazida pela LGPD. Além disso, assemelha-se à legislação europeia também no que concerne à criação de uma autoridade nacional para a aplicação da Lei¹⁰².

Decorrente das novas necessidades de uma sociedade digital que exige maior transparência nas relações, a LGPD foi criada com a intenção de fortalecer a proteção da privacidade dos usuários e dos seus dados pessoais; dispondo, por conseguinte, sobre o tratamento destes por pessoa jurídica de direito público ou privado, inclusive nos meios digitais¹⁰³. Uma das grandes inovações trazidas pela Lei diz respeito ao acesso pelo cidadão a informações de como seus dados são coletados, processados e armazenados. Ou seja, seu objetivo é proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural¹⁰⁴.

De acordo com as definições trazidas pelo artigo 5º da Lei nº 13.709, “tratamento” compreende-se como “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”¹⁰⁵. Todas essas operações que envolvem dados, no entanto, estando em território nacional, independentemente de sua cidadania e origem, devem ser abarcadas pelas novas regras. Isso significa, portanto, que todas as empresas envolvidas com operações de tratamento de dados passam a se sujeitar à LGPD, não importando o meio

¹⁰² MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120, ano 27, p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018, p. 470.

¹⁰³ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. **Artigo 1º**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 11 de novembro de 2019.

¹⁰⁴ Ibidem.

¹⁰⁵ Ibidem. **Artigo 5º, inciso X**.

de tratamento e o país de sede ou de origem dos dados, bastando que estes estejam localizados no Brasil¹⁰⁶.

Ademais, a LGPD, para além da definição de tratamento, como mencionado no parágrafo anterior, preocupou-se com as *definições legais*, uma vez que tornam seus termos mais claros e objetivos, conforme se pode depreender da leitura do artigo 5º:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: 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);

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

¹⁰⁶ PINHEIRO, Patrícia Peck Garrido. *Nova Lei Brasileira de Proteção de Dados Pessoais (LGPD) e o impacto nas instituições públicas e privadas*. Revista dos Tribunais, vol. 1000, ano 108, p. 309-323. São Paulo: Ed. RT, fevereiro de 2019, p. 310.

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: 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;

XVII - relatório de impacto à proteção de dados pessoais: 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;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída 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; e

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional¹⁰⁷.

Importante ressaltar que a Lei, ao definir *dados pessoais*, adotou o critério expansionista, uma vez que, ao contrário do critério reducionista, que define como pessoais apenas os dados que identificam imediatamente uma pessoa natural, o mencionado artigo – em seu inciso I – abarcou também os dados que tornam a pessoa identificável de forma não imediata ou direta. Dessa forma, se uma empresa dispuser de dados de um usuário que, se mesclados ou conjugados, o identifiquem, estes serão considerados pessoais, ainda que isoladamente não identifiquem o indivíduo¹⁰⁸.

Por fim, observa-se que a nova lei geral tem como principal linha condutora a transparência, ou seja, mesmo nas hipóteses em que não se é exigido o consentimento prévio e expresso do titular dos dados, ele deve ser transparente. Assim sendo, a regulamentação traz novos direitos aos usuários e novas obrigações às empresas, dividindo-se em alguns eixos principais, os quais passam a ser analisados a seguir.

¹⁰⁷ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 13 de novembro de 2019.

¹⁰⁸ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada* – 2ª ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019, p. 71-72.

3.3.1 Eixos Principais

Segundo Laura Schertel e Danilo Doneda, é possível verificar cinco eixos principais em torno dos quais a nova Lei se articula, sendo eles: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados e v) responsabilização dos agentes¹⁰⁹. No entanto, no presente tópico far-se-á uma breve disposição a respeito dos três primeiros eixos, uma vez que os restantes serão abarcados no capítulo seguinte, referente às figuras dos “agentes de tratamento”.

O primeiro eixo, portanto, faz menção ao âmbito de aplicação material da Lei, que tem como base a generalidade e unidade. Conforme se depreende da leitura do artigo 3º, ela se concentra na proteção dos dados do cidadão, não importando quem realiza o seu tratamento, aplicando-se tanto ao setor público quanto ao privado¹¹⁰. Ademais, conforme mencionado acima, o âmbito de aplicação da Lei circunscreve-se a qualquer operação de tratamento que tenha ocorrido dentro do Brasil ou que possua como objetivo final o oferecimento de bens e serviços a pessoas que estejam em território nacional, independentemente se os dados foram coletados *off-line* ou *on-line*, ou seja, por meios físicos ou digitais, os quais diferenciam-se da seguinte forma:

Os dados pessoais coletados *on-line* são aqueles que se valem de métodos automatizados, normalmente preenchidos por uma pessoa em protocolados na internet, por meio de redes sociais, aplicativos, ou contratação de serviços. A coleta de dados *off-line* ocorre pela obtenção desses sem utilizar processos automatizados, seja do preenchimento de pesquisas de intenção, seja por meio de clientes de uma determinada empresa¹¹¹.

Além do mais, apenas os dados referentes a pessoas naturais são protegidos pela LGPD, excluindo-se da proteção da Lei aqueles referentes a pessoas jurídicas, conforme arts. 1º e 5º, I. Também, destaca-se que, ante a impossibilidade de se manter regras inflexíveis diante das diversas relações sociais, a Lei também traz exceções, não se aplicando quando o tratamento de dados é realizado por uma pessoa natural com fins exclusivamente particulares e não econômicos, quando possui fins exclusivamente

¹⁰⁹ MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120, ano 27, p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018, p. 472.

¹¹⁰ *Ibidem*.

¹¹¹ RODRIGUES, Yuri Gonçalves dos Santos; FERREIRA, Keila Pacheco. *A privacidade no ambiente virtual: avanços e insuficiências da Lei Geral de Proteção de Dados no Brasil (Lei 13.1709/18)*. Revista de Direito do Consumidor, vol. 122, ano 28, p. 181-202. São Paulo: Ed. RT, mar.-abr. 2019, p. 196-197.

jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado ou de atividades de investigação e repressão de infrações penais¹¹².

Contudo, conclui-se que as suas poucas exceções se fundamentam ou em direito fundamental (como, por exemplo, no que tange à liberdade de informação na atividade jornalística) ou em interesse público relevante (exemplificando-se pelas exceções relativas à segurança pública e defesa nacional), moldadas de forma a não comprometer a sua integridade, uma vez que no próprio artigo faz-se referência à legislação especial¹¹³, 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 na Lei¹¹⁴.

No que tange ao seu segundo eixo, verifica-se na Lei que o tratamento de dados não poderá ser realizado sem que haja uma base normativa que o autorize, ou seja, só poderá acontecer se ele estiver embasado em uma das hipóteses autorizativas previstas no art. 7º, no art. 11 – no que tange aos dados sensíveis – ou no art. 23º da LGPD.

Conforme disposição do art. 7º, inciso I, verifica-se que o consentimento constitui uma das hipóteses autorizativas, merecendo certo destaque. Uma vez que possui nítida natureza contratual, pois, de um lado, há a manifestação da vontade de uma parte em tratar os dados pessoais para determinada finalidade e, de outro, alguém que anui com tal tratamento¹¹⁵, para que possua validade, deve preencher os requisitos de validade do art. 104 do Código Civil¹¹⁶. Ainda no que tange aos seus requisitos, para além daqueles previstos no art. 104 do CC, estes podem ser verificados já nas definições legais do art. 5º, que refere a necessidade de um consentimento livre, informado, inequívoco e com

¹¹² BRASIL. Lei nº 13.709 de 14 de agosto de 2018. **Artigo 4º**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 de novembro de 2019.

¹¹³ RODRIGUES, Yuri Gonçalves dos Santos; FERREIRA, Keila Pacheco. *Op. cit.*, p. 472.

¹¹⁴ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. **Artigo 4º, §1º**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 de novembro de 2019.

¹¹⁵ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada* – 2ª ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019, p. 88.

¹¹⁶ Art. 104. A validade do negócio jurídico requer:

I - agente capaz;

II - objeto lícito, possível, determinado ou determinável;

III - forma prescrita ou não defesa em lei.

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 12 de novembro de 2019.

finalidade determinada. Além disso, em caso de tratamento de dados sensíveis, nos termos do art. 11, inciso I, deve ser fornecido de forma específica e destacada¹¹⁷. Caso tais requisitos não sejam respeitados e sejam prestados de forma genérica ou a partir de informações enganosas prestadas ao titular, nos termos da Lei, o consentimento será nulo, conforme §4º do art. 8º da Lei e inciso IV do art. 166, do Código Civil¹¹⁸.

Além disso, o §6º do art. 8º da LGPD vem a completar o §4º, uma vez que se houver alteração do consentimento original quanto à finalidade específica do tratamento, forma, duração ou compartilhamento, a informação deve ser fornecida ao titular que, caso não concorde, poderá revogá-lo. Observa-se que com a revogação do consentimento não se perde o direito de tratar os dados, podendo o controlador enquadrar o tratamento nas demais bases legais do art. 7º. Todavia, caso não seja possível, ele será interrompido imediatamente. Ademais, entende-se que a revogação do tratamento deve se dar de modo facilitado, ou seja, no mínimo pelo mesmo meio pelo qual o consentimento foi coletado¹¹⁹.

Todavia, ainda que o consentimento seja o instrumento no qual a expressão de vontade do titular dos dados classicamente encontre sua expressão, há diversas outras hipóteses autorizativas presentes na Lei que são capazes de legitimar o tratamento dos dados, como, por exemplo, o cumprimento de obrigação legal ou regulatória, a execução de contrato do titular – a seu pedido – ou pela administração pública, a realização de interesses legítimos do controlador ou do operador, dentre outras. Todavia, em relação à última, prevista no inciso IX do art. 7º, destaca-se que constitui uma espécie de cláusula geral, em que se opera um teste de proporcionalidade entre os interesses na utilização dos

¹¹⁷ MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120, ano 27, p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018, p. 472-473.

¹¹⁸ **Art. 8º** O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

[...]

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

[...]

Art. 166. É nulo o negócio jurídico quando:

[...]

IV - não revestir a forma prescrita em lei;

[...]

Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 12 de novembro de 2019.

¹¹⁹ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada – 2ª ed. rev., atual. e ampl.* – São Paulo: Thomson Reuters Brasil, 2019, p. 92

dados pessoais (que são do controlador ou de terceiro) e os direitos do titular. Assim, verifica-se se a finalidade do tratamento dos dados, à qual corresponde o interesse legítimo, possui efeito para os direitos e liberdades fundamentais do titular, uma vez que, caso estes restem afetados, o legítimo interesse não deve ser considerado como uma hipótese autorizativa para o tratamento¹²⁰.

O terceiro eixo da LGPD, contudo, compõe-se pelos princípios e direitos do titular, propiciando meios para que o cidadão controle o uso de seus dados por terceiros e conferindo unidade sistêmica à disciplina da proteção dos dados pessoais¹²¹. Primeiramente, faz-se uma breve disposição a respeito da importância dos princípios no ordenamento jurídico brasileiro, uma vez que representam valores positivados, perpassando todo o nosso arcabouço normativo¹²². Nesse sentido, relevante a definição de Celso Antônio Bandeira de Mello:

Princípio é, por definição, mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas compondo-lhes o espírito e servindo de critério para sua exata compreensão e inteligência exatamente por definir a lógica e a racionalidade do sistema normativo, no que lhe confere a tônica e lhe dá sentido harmônico. É o reconhecimento dos princípios que preside a intelecção das diferentes partes componentes do todo unitário que há por nome sistema jurídico positivo¹²³.

Pois bem, feita breve disposição a respeito da importância dos princípios, frisa-se que a LGPD os dedicou ao tratamento dos dados pessoais, elencando-os em seu art. 6º, a fim de orientar tal atividade. Ressalta-se, também, que esses princípios basilares foram inspirados em consensos internacionais, como, por exemplo, nas diretrizes da OCDE, que visam resistir às constantes transformações tecnológicas.

Sendo assim, no tratamento de dados pessoais, deve-se observar a boa-fé – conforme caput do artigo mencionado acima – e os seguintes princípios: (i) finalidade; (ii) adequação; (iii) necessidade; (iv) livre acesso; (v) qualidade dos dados; (vi) transparência; (vii) segurança; (viii) prevenção; (ix) não discriminação e (x)

¹²⁰ MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120, ano 27, p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018, p. 473.

¹²¹ Ibidem, p. 474.

¹²² BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia (coord.). *Proteção de Dados Pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018*. Belo Horizonte: Fórum, 2019, p. 68.

¹²³ MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*, 27ª ed. São Paulo: Malheiros, 2010, p. 958-959.

responsabilização e prestação de contas¹²⁴, ou seja, é necessário que o agente demonstre a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção dos dados, e, também, a eficácia de tais medidas¹²⁵.

Embora sejam complementares entre si, alguns desses princípios merecem destaque. Primeiramente, destaca-se o *princípio da finalidade*, uma vez que vincula o tratamento dos dados pessoais a um fim específico e determinado que tenha justificado sua coleta, sendo vedada a sua modificação sem um novo consentimento do titular. Destaca-se a sua importância através das palavras de Paulo Brancher e Ana Cláudia Beppu:

A especificação da **finalidade** é o primeiro passo para se aplicar as regulações de proteção de dados e estabelecer os direitos do titular. Ela é pré-requisito essencial não só para a aplicação dos demais princípios [...] como também para a própria definição do tipo de dado que será coletado, o período de retenção dessa informação e todos os demais aspectos que determinarão de que forma os dados serão processados para aquele propósito específico¹²⁶. (grifo próprio)

Ademais, decorrentes da finalidade, destacam-se também os princípios da *adequação*, que permite-nos concluir que os dados coletados não poderão ser utilizados com finalidade incompatível com aquela originalmente informada pelo titular ou com tratamento dissociado daquilo que o titular razoavelmente pretendeu ao fornecê-los, e da *necessidade*, que indica que em qualquer atividade de tratamento de dados se deve utilizar somente os necessários para a realização daquela operação.

Os princípios elencados acima permitem-nos concluir, por conseguinte, que se está diante de uma nova era de *minimização* de dados, onde não há mais uma coleta irrestrita, mas sim uma imposição de coleta mínima, apenas para a finalidade do produto ou serviço a ser prestado.

Em relação aos direitos dos titulares dos dados pessoais, o artigo 17 da LGPD estabelece que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade, e de privacidade, nos

¹²⁴ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. **Artigo 6º**. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 13 de novembro de 2019.

¹²⁵ SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. *Lei Geral de Proteção de Dados no Brasil e os possíveis impactos*. Revista dos Tribunais, vol. 998, ano 107, p 225-239. São Paulo: Ed. RT., dezembro de 2018, p. 227.

¹²⁶ BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia (coord.). *Proteção de Dados Pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018*. Belo Horizonte: Fórum, 2019, p. 70.

termos desta Lei”¹²⁷. Desse modo, a Lei assegura às pessoas naturais a titularidade dos seus dados pessoais frente aos agentes de tratamento, que podem apenas submeter tais dados a uma atividade de tratamento quando autorizados por uma das bases legais autorizativas, conforme disposto acima.

Portanto, a nova Lei, em seu artigo 18, estipula diversos direitos do titular que podem ser exercidos frente aos agentes de tratamento, os quais, conforme Joseane Suzart, reúnem-se em cinco grupos:

[...] versando o primeiro sobre a confirmação da existência da atividade; o segundo concerne ao acesso ao conteúdo registrado; o terceiro diz respeito à obtenção de informações vinculadas ao assunto; o quarto abarca a modificação ou exclusão das informações constantes nos arquivos; e o derradeiro refere-se à questão da portabilidade¹²⁸.

Ademais, quanto ao exercício desses direitos, destaca-se o §3º do referido artigo, que dispõe que eles “serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento”¹²⁹.

Esses são, portanto, três dos cinco principais eixos da LGPD, sendo os dois últimos relativos às obrigações e responsabilidades dos agentes de tratamento, as quais dizem respeito ao tema deste trabalho, passando a ser analisadas no capítulo que segue.

4 Agentes de Tratamento de Dados Pessoais

4.1 A Criação das Figuras do *Controlador* e do *Operador*

Os agentes de tratamento de dados pessoais, inovações trazidas pela nova Lei Geral de Proteção de Dados, conforme disposição do seu artigo 5º, inciso IX, constituem-se pelas figuras do *controlador* e o *operador*. Inicialmente, para que se possa compreender melhor a importância dessa inovação legal, Ricardo Alexandre de Oliveira faz uma interessante analogia, ao compará-las com as definições de *consumidor* e

¹²⁷ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. **Artigo 17º**. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 15 de novembro de 2019.

¹²⁸ SILVA, Joseane Suzart Lopes da. *A proteção de dados pessoais dos consumidores e a Lei 13.709/2018: em busca da efetividade dos direitos a privacidade, intimidade e autodeterminação*. Revista de Direito do Consumidor, vol. 121, ano 28, p. 367-418. São Paulo: Ed. RT, jan.-fev. 2019, p. 392.

¹²⁹ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 15 de novembro de 2019.

fornecedor trazidas pelo Código de Defesa do Consumidor quando do seu surgimento em 1990.

Ressalta, primeiramente, que mesmo que existam divergências a respeito das suas definições, decorrente da condição de certas pessoas em alguns casos concretos – como o comércio entre pessoas jurídicas, por exemplo – se o referido código não trouxesse tais definições, a dificuldade seria redobrada. Dessa forma, assim como o CDC, a LGPD criou as figuras do *operador* e do *controlador* a fim de delimitar direitos e deveres, deixando mais clara a posição de cada personagem participante do tratamento de dados. Assim, o autor define que o *controlador* “é quem decide sobre o tratamento” e o *operador* “é quem trata dos dados por ordem do primeiro”¹³⁰.

Além disso, ressalta o autor que:

A definição será bastante útil para a responsabilização dos agentes, o que fará com que as empresas em geral delimitem muito bem o papel que desejam assumir no tratamento de dados. Por exemplo: se uma empresa deseja decidir sobre os dados recebidos, assumirá o papel de *Controlador* e responderá diretamente pelos danos causados ao titular, de forma solidária com outros *Controladores* presentes na mesma relação. Contudo, se a empresa deseja simplesmente prestar serviços delimitados em contratos comerciais, sem se envolver em processos decisórios quanto ao tratamento, essa empresa se enquadrará na figura do *Operador*, respondendo apenas pelos danos que der causa por descumprimento da lei ou do contrato¹³¹.

Destaca-se que tal definição tem o potencial de inibir o compartilhamento indiscriminado dos dados pessoais, uma vez que o *controlador* não permitirá mais que seus *operadores* se apropriem das bases de dados recebidas pelo seu contratante, como era comum. Dessa forma, tais definições permitem que não haja mais um compartilhamento dos dados do titular numa escala nunca pretendida por ele¹³².

Ainda se tratando da definição dos agentes de tratamento trazidos pela nova Lei, ressalta-se que ela inspirou-se claramente no Regulamento Geral de Proteção de Dados da União Europeia, o GDPR. De acordo com o seu artigo 5º, a LGPD define como *controlador* a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”¹³³, equivalendo-se à

¹³⁰ OLIVEIRA, Ricardo Alexandre de. *Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico*. Revista dos Tribunais, vol. 998, ano 107, p. 241-261. São Paulo: Ed. RT, dezembro 2018, p. 255.

¹³¹ *Ibidem*.

¹³² *Ibidem*.

definição de *data controller* do artigo 4º, item 7, da GDPR¹³⁴. Já em relação à figura do *operador*, a LGPD o define como a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”¹³⁵, também equivalendo-se a uma das definições da GDPR, isto é, ao item 8 do artigo 4º, o *data processor*¹³⁶.

Diante das disposições acima, conclui-se que o *controlador* constitui-se como figura central quando se trata de proteger os direitos dos titulares, ou seja, é o principal tomador de decisão em relação aos dados pessoais. Como resultado, a maioria das responsabilidades pela conformidade com a LGPD recai sobre ele, possuindo como função, portanto, controlar a finalidade e os meios gerais de como os dados devem ser usados. Isto é, o *controlador* decide o porquê da coleta dos dados do titular; como fará seu tratamento, através das hipóteses autorizativas do art. 7º; sobre quais indivíduos irá coletar os dados; quais dados pessoais irá coletar (em relação ao conteúdo dos dados); a finalidade ou os propósitos para os quais os dados serão usados; se divulga, compartilha ou transfere os dados e por quanto tempo retê-los-á¹³⁷.

Para além de suas funções, conforme disposição legal, o *controlador* possui também como responsabilidades: (i) obter consentimento, quando necessário (art. 7º, §5º e art. 8º, §6º); (ii) informar e prestar contas (art. 9º, art. 18 e art. 20); (iii) garantir a transparência no tratamento de dados baseado em legítimo interesse (art. 10, §2º); (iv) manter registro das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse (art. 37); (v) elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, com observância dos segredos comercial e industrial (art. 10, §3º e art. 38); (vi)

¹³³ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. **Artigo 5º, VI**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 24 de novembro de 2019.

¹³⁴ “[...] pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais [...]”. Disponível em: <<https://gdpr-info.eu/art-4-gdpr/>>. Acesso em 24 de novembro de 2019.

¹³⁵ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. **Artigo 5º, VII**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 24 de novembro de 2019.

¹³⁶ “[...] pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes [...]”. Disponível em: <<https://gdpr-info.eu/art-4-gdpr/>>. Acesso em 24 de novembro de 2019.

¹³⁷ HOSKEN, Maria. *Agentes de tratamento de dados na LGPD*. Disponível em: <http://www.anspnet.org.br/wp-content/uploads/2018/11/maria_hosken.pdf>. Acesso em: 01 de dezembro de 2019.

indicar o encarregado pelo tratamento de dados (art. 41); (vii) reparar danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais (art. 42); (viii) comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48); (ix) salvaguardar os direitos dos titulares mediante a adoção de providências, e.g., divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente (art. 48, §2º) e (x) observar as boas práticas e padrões de governança (art. 50).

Em relação ao *operador* de dados, faz-se difícil delimitar suas funções, uma vez que está limitado ao processamento dos dados de acordo com as instruções e o propósito dado pelo *controlador*, não podendo controlar os dados e alterar a finalidade do seu tratamento. No entanto, tem como responsabilidade fornecer garantias para implementar “medidas técnicas e organizacionais” adequadas, de modo que o processamento cumpra os requisitos legais e de segurança. Ou seja, o *operador* tem a liberdade de usar o conhecimento técnico para decidir como executar certas atividades em nome do *controlador*, mas não toma decisões sobre o que é feito com os dados¹³⁸.

No que tange à diferenciação entre as figuras dos dois agentes, na prática, nas ocasiões em que o tratamento de dados pessoais envolver mais de uma empresa, deve-se fazer o seguinte questionamento a fim de identificá-los: teria a empresa contratada realizado determinada atividade de tratamento de dados pessoais, da forma como ocorreu, se não fosse a solicitação da contratante? Se a resposta for positiva, está-se diante de uma situação em que as duas empresas são as responsáveis pelo tratamento dos dados pessoais. No entanto, caso seja negativa, a empresa contratante será a responsável pelo tratamento, ou seja, qualificando-se como agente *controlador*, e a contratada, por outro lado, qualificar-se-á como agente *operador*, ou seja, realizando o tratamento de dados pessoais conforme as instruções da primeira¹³⁹.

¹³⁸ HOSKEN, Maria. *Agentes de tratamento de dados na LGPD*. Disponível em: <http://www.anpnet.org.br/wp-content/uploads/2018/11/maria_hosken.pdf>. Acesso em: 01 de dezembro de 2019.

¹³⁹ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia*. São Paulo: Thomson Reuters Brasil, 2018, p. 114.

Tomemos como exemplo um *site* de comércio eletrônico, em que uma empresa “x”, fabricante de artigos esportivos, a fim de criar um site de *e-commerce*, contrata uma plataforma virtual com diversas empresas, delegando a cada uma delas atividades diferentes para a consolidação do seu projeto. Dessa forma, todas as empresas terão acesso aos dados pessoais dos usuários do *site*, mas apenas a empresa “x” encaixar-se-á na figura do agente *controlador*, de modo que as demais apenas seguirão suas orientações para concretizar o pedido e entregar o produto, por exemplo, não decidindo por si só o que será feito com os dados recebidos, sendo todas, portanto, empresas *operadoras*¹⁴⁰.

Nessa senda, dispõe a LGPD da seguinte forma:

Art. 39 O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Dessa forma, o artigo deixa claro o conceito de que o *operador* somente tratará os dados pessoais de acordo com as instruções fornecidas pelo *controlador*, sem fazer qualquer discricionariedade. Todavia, ressalta-se que isso não exime o *operador* de adotar medidas para conformidade com a legislação de proteção de dados, bem como medidas técnicas e organizacionais de segurança¹⁴¹, referidas no art. 46 da LGPD¹⁴².

4.2 Do Encarregado pelo Tratamento de Dados Pessoais

Primeiramente, ressalta-se que embora a Lei defina, em seu artigo 5º, inciso IX, que os agentes de tratamento são apenas as figuras mencionadas acima – o *controlador* e o *operador* – faz-se importante, para melhor compreensão do capítulo, também uma disposição a respeito do *encarregado*, figura não menos importante, uma vez que também faz parte do Capítulo VI da LGPD, qual seja, o relativo aos “Agentes de Tratamento de Dados Pessoais”. Assim, a lei brasileira, inspirando-se novamente no Regulamento europeu (GDPR), trouxe a presença de um *encarregado* no tratamento de dados pessoais,

¹⁴⁰ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada* – 2ª ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019, p. 165.

¹⁴¹ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *LGPD: Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2019, p. 310.

¹⁴² 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. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 24 de novembro de 2019.

cargo equivalente, portanto, ao do *data protection officer* da legislação europeia, conforme verifica-se abaixo:

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. [...] ¹⁴³. (grifo próprio)

Segundo a definição legal do inciso VII do artigo 5º da nova Lei, o *encarregado* qualifica-se como “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)”¹⁴⁴. No entanto, diferentemente da GDPR, a Lei brasileira não estabeleceu critérios objetivos que obrigam a nomeação da figura do *encarregado* no tratamento dos dados pessoais, ficando tal tarefa a cargo da ANPD, que irá dispor, em suas orientações e resoluções, quem legalmente está obrigado a tal nomeação¹⁴⁵, conforme previsão do §3º, do artigo 41¹⁴⁶.

Assim sendo, concluindo a empresa pela nomeação do *encarregado*, seja voluntariamente ou por obrigatoriedade, passa-se à análise de quais serão as suas funções, seu perfil profissional e sua posição dentro da estrutura organizacional da empresa. Em primeiro lugar, no que diz respeito às suas funções, faz-se necessário observar o §2º do referido artigo 41:

§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.

¹⁴³ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 25 de novembro de 2019.

¹⁴⁴ Ibidem.

¹⁴⁵ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 314.

¹⁴⁶ [...] § 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. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 25 de novembro de 2019.

No entanto, conforme depreende-se do inciso IV, não se trata de uma lista exaustiva. Ademais, considerando-se as funções exemplificadas acima, conclui-se que ele precisa estar acessível aos titulares da ANPD, motivo pelo qual o §1º do referido artigo estabelece a obrigatoriedade de se divulgar, de forma clara e objetiva, os dados de contato do *encarregado*. Assim, embora não seja um requisito expresso da Lei, recomenda-se a sua localização em território brasileiro, a fim de facilitar a realização de suas funções¹⁴⁷.

Além disso, também a fim de facilitar a realização das funções designadas ao *encarregado* pelo tratamento de dados pessoais, requer-se algumas observações. Primeiramente, tal nomeação deve ocorrer baseada nas qualidades profissionais do indicado, como, por exemplo, seu conhecimento a respeito da legislação da proteção de dados e das práticas de tratamento dos dados pessoais. Também, deve-se verificar se não há conflito de interesses com outras funções que o colaborador possa eventualmente exercer para a organização, uma vez que uma das suas funções é monitorar a conformidade das atividades de tratamento de dados pessoais com a regulamentação e as normas vigentes. Por conseguinte, uma vez sendo o próprio responsável por uma atividade de tratamento de dados pessoais, dificilmente poderá monitorar a conformidade de sua própria atividade. Por fim, é recomendável que ele esteja desvinculado das áreas tradicionais da empresa, inclusive com reporte direto à Diretoria e à Presidência, com todos os recursos necessários para executar suas funções¹⁴⁸.

No que concerne à responsabilidade civil do *encarregado*, em face de uma eventual não conformidade da empresa com os requisitos de proteção de dados, como regra geral, ela inexistente, dedicando-se a Lei apenas aos agentes de tratamento. Portanto, o *encarregado* não é pessoalmente responsável, uma vez que o *controlador* e o *operador* é que são responsáveis por demonstrar a adequação de suas atividades conforme a disposição legal. Todavia, caso aja com dolo, poderá responder perante o empregador e, até mesmo, perante terceiros¹⁴⁹.

Não obstante, o *encarregado* não está isento de responder por seus atos na esfera penal, em decorrência da execução de suas atribuições. Observando-se suas funções, conclui-se que há a possibilidade de cometimento de irregularidades, como, por exemplo,

¹⁴⁷ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 315-316.

¹⁴⁸ *Ibidem*.

¹⁴⁹ *Ibidem*.

comunicação de informação ilícita ou abusiva e orientação equivocada ou de má-fé, ações que não podem ser totalmente controladas pelo agente *controlador*, que não poderia mitigar tal risco sem distorcer ou invalidar a figura do *encarregado*. Desse modo, para que se afastem tais responsabilizações, excluindo-se, logicamente, a má-fé e o dolo, deve o encarregado precaver-se através de meio que validem sua atuação, ou, ainda, que preservem as instruções recebidas pelo *controlador*.

4.3 Responsabilidade e Ressarcimento de Danos

Diante da vivência de uma nova era, qual seja, a era da informação, conforme disposto ao longo do trabalho, a responsabilidade civil faz-se essencial em matéria de proteção de dados, uma vez que uma rápida busca na internet tem o condão de iniciar ou alimentar um infundável perfil sobre as preferências e interesses do usuário da rede, com massivo tratamento dos dados pessoais envolvidos. Dessa forma, em razão da facilitação trazida pela internet e por outros meios facilitadores da comunicação à difusão dos dados pessoais dos indivíduos, fez-se necessário não só o surgimento de um regramento mais rígido, mas também o estabelecimento de uma responsabilidade civil aos agentes responsáveis quando a atividade importar em danos aos titulares dos dados¹⁵⁰.

Nessa senda, o artigo 42 da LGPD trata da responsabilidade civil dos agentes de tratamento de dados pessoais, evidenciando a possibilidade de reparação dos danos patrimoniais, morais, individuais ou coletivos, sempre que decorrerem de uma violação à LGPD:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação,

¹⁵⁰ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 318.

houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso¹⁵¹.

Conforme se depreende da leitura do caput do artigo, conclui-se que cada um dos agentes de tratamento, seja o *controlador* ou o *operador*, é responsável pelos atos praticados e danos causados, não havendo, via de regra, responsabilidade solidária ou subsidiária entre eles, sujeitando-se às regras gerais de responsabilidade civil previstas no Código Civil, quais sejam¹⁵²:

Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem¹⁵³.

Contudo, a LGPD trouxe três hipóteses de responsabilidade solidária. Duas delas dizem respeito à responsabilidade solidária entre o *controlador* e o *operador*, quando este descumpra a Lei, ou age em desacordo com as ordens do primeiro, ressaltando a necessidade de o *operador* ser conhecedor das normas relacionadas à proteção de dados pessoais, mesmo que sua função esteja limitada às ordens e instruções do *controlador*. Observe-se que as duas hipóteses previstas no §1º, I, do artigo 42 não são cumulativas, apesar de na maioria das vezes o ato de não seguir as instruções esteja diretamente ligado aos princípios da LGDP, violando-a indiretamente¹⁵⁴.

¹⁵¹ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 25 de novembro de 2019.

¹⁵² COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada* – 2ª ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019, p. 174-175.

¹⁵³ BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 26 de novembro de 2019.

¹⁵⁴ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 319.

Para além disso, a LGPD prevê também a responsabilidade solidária entre *controladores* no inciso II do §1º do referido artigo, o que é interessante, visto que o tratamento de dados pessoais, frequentemente, envolve mais de um agente, impossibilitando que o titular dos dados tivesse o ônus de descobrir, dentro de uma cadeia econômica, quem deu causa ao dano sofrido¹⁵⁵. No entanto, entre eles poderá haver ação de regresso, nos termos do artigo 934 do CC e do §4º do artigo 42, acima mencionado, da LGPD¹⁵⁶.

Contudo, a LGPD não é clara quanto à aplicabilidade da responsabilidade subjetiva (aquela em que há dolo ou culpa – por negligência, imprudência ou imperícia – por parte do agente) ou objetiva (aquela que independe de culpa, bastando um nexo causal entre a ação ou omissão do agente e o dano). Nesse sentido, quando há incidentes que geram danos a *consumidores*, a possibilidade de um enquadramento de responsabilidade objetiva, ou seja, independente de dolo ou culpa, torna-se mais evidente¹⁵⁷, uma vez que se aplica ao caso o Código de Defesa do Consumidor, que dispõe em seus artigos 12, 13 e 14 a possibilidade da responsabilidade mencionada¹⁵⁸.

Dessa forma, nas relações de consumo há possibilidade de uma ampla responsabilização, englobando também a teoria do risco ou da atividade, em que o risco fica a cargo do empreendedor, a quem cabe calcular os riscos envolvidos na atividade *versus* os benefícios que dela pode obter. Portanto, nos casos envolvendo incidentes que

¹⁵⁵ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 319.

¹⁵⁶ Art. 934. Aquele que ressarcir o dano causado por outrem pode reaver o que houver pago daquele por quem pagou, salvo se o causador do dano for descendente seu, absoluta ou relativamente incapaz. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 26 de novembro de 2019.

¹⁵⁷ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Op. cit.*, p. 319-320.

¹⁵⁸ Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.

Art. 13. O comerciante é igualmente responsável, nos termos do artigo anterior, quando:

I - o fabricante, o construtor, o produtor ou o importador não puderem ser identificados;

II - o produto for fornecido sem identificação clara do seu fabricante, produtor, construtor ou importador;

III - não conservar adequadamente os produtos perecíveis.

Parágrafo único. Aquele que efetivar o pagamento ao prejudicado poderá exercer o direito de regresso contra os demais responsáveis, segundo sua participação na causação do evento danoso.

Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078.htm>. Acesso em: 26 de novembro de 2019.

causam danos a consumidores, é provável a aplicação da responsabilidade objetiva da legislação consumerista, facilitando a responsabilização da empresa e a indenização ao consumidor, razão pela qual os registros e controles das operações envolvendo os dados pessoais devem ser rigorosos e estritos, a fim de viabilizar uma possível defesa por parte da empresa¹⁵⁹.

Todavia, em que pese em algumas atividades específicas de tratamento de dados pessoais seja possível que a existência de um risco inerente à atividade, em razão de sua natureza ou de elementos presentes, pode-se dizer que a responsabilidade objetiva não é regra geral na nova legislação de dados pessoais. Em versões anteriores do Projeto de Lei que deu origem ao novo regramento, chegaram-se a incluir disposições que conceituavam a atividade de tratamento de dados pessoais como uma atividade de risco, mas acabaram sendo retiradas da proposição ao longo do seu processo legislativo¹⁶⁰.

Por isso, é possível que se sustente que a regra geral da LGPD é a da responsabilidade civil subjetiva, em que se deve demonstrar o elemento de culpa; admitindo-se, no entanto, em algumas hipóteses específicas, a responsabilidade objetiva. Essa última decorrente da natureza da atividade de tratamento de dados pessoais, que possa ser enquadrada como atividade de risco¹⁶¹.

No que tange ao ônus da prova, ressalta-se que o Código de Processo Civil previu uma dinamicidade como exceção à regra, por meio do qual a parte mais apta à produção de prova deverá produzi-la, nos termos do §1º do seu artigo 373:

Art. 373. O ônus da prova incumbe:

I - ao autor, quanto ao fato constitutivo de seu direito;

II - ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor.

§ 1º Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas **à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova do fato contrário**, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído¹⁶². (grifo próprio)

¹⁵⁹ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 320-321.

¹⁶⁰ *Ibidem*.

¹⁶¹ *Ibidem*.

¹⁶² BRASIL. Lei nº 13.105 de 16 de março de 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2015/lei/l13105.htm>. Acesso em: 26 de novembro de 2019.

Também, o Código de Defesa do Consumidor, no seu artigo 6º, VII¹⁶³, faz a mesma previsão com semelhantes fundamentos, o que não poderia ser diferente na LGPD, uma vez que não se pode desconsiderar o que acontece na realidade, estando o titular, normalmente, em posição de desvantagem diante dos agentes de tratamento de dados. Por isso, previu expressamente a possibilidade de inversão do ônus da prova no §2º do artigo 42. Todavia, deve-se observar dois requisitos: (i) a verossimilhança da alegação do titular e (ii) a hipossuficiência ou onerosidade para fins de produção de prova¹⁶⁴. Em relação ao primeiro requisito, interessante a observação de Carlos Roberto Barbosa Moreira:

A verossimilhança se assenta num juízo de probabilidade, que resulta, por seu turno, da análise dos motivos que lhe são favoráveis (convergentes) e dos que lhe são desfavoráveis (divergentes). Se os motivos convergentes são inferiores aos divergentes, o juízo de probabilidade cresce; se os motivos divergentes são superiores aos convergentes, a probabilidade diminui¹⁶⁵.

Com isso, a LGPD assegura também no âmbito judicial uma proteção ao titular na defesa dos seus direitos.

Contudo, ainda em relação à responsabilização dos agentes de tratamento, a LGPD, em seu artigo 43, elenca hipóteses em que o *controlador* e o *operador* não serão responsabilizados:

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
 I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
 II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;
 ou
 III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro¹⁶⁶.

A primeira hipótese diz respeito à prova de que não realizaram o tratamento de dados que lhes é atribuído. O que é bastante óbvio, uma vez que não havendo nexos causal entre o dano e a ação ou omissão do agente, não haverá responsabilização. Todavia, não

¹⁶³ Art. 6º São direitos básicos do consumidor: [...] VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências [...]. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078.htm> Acesso em: 26 de novembro de 2019.

¹⁶⁴ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada – 2ª ed. rev., atual. e ampl.* – São Paulo: Thomson Reuters Brasil, 2019, p. 177-178.

¹⁶⁵ MOREIRA, Carlos Roberto Barbosa. *Notas sobre a inversão do ônus da prova em benefício do consumidor*. Revista dos Tribunais, São Paulo, n. 22, abr.-jun. 1997, p. 142.

¹⁶⁶ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 25 de novembro de 2019.

deixa de ser de grande relevância, em face da complexidade envolvida nas atividades de tratamento de dados pessoais, conforme dispõe Marcos Gomes da Silva Bruno:

[...] não é difícil que um titular demande a empresa incorreta, acreditando ser ela a responsável pelo tratamento do dado pessoal, quando não o é. Da mesma forma, é crescente a divulgação e exposição de dados pessoais que são atribuídos a incidentes de segurança de uma determinada empresa, quando não são daquela companhia, gerando inúmeros questionamentos e procedimentos, administrativos e judiciais, que são obstados justamente por essa prova, de que aquela empresa investigada/acionada não realizou o tratamento de dados pessoais que lhe foi atribuído. Exemplo dessa situação é o Inquérito Civil Público 08190.05.2296/18-50, cuja Promoção de Arquivamento foi fundamentada no fato de “que os dados pessoais supostamente obtidos durante o ataque são oriundos de outra fonte”¹⁶⁷.

A segunda hipótese de exclusão de responsabilidade já parte do princípio de que houve tratamento de dados, mas que ocorreu dentro da Lei, o que afasta a ilicitude do ato e, conseqüentemente, o dever de indenizar. Por fim, a terceira hipótese trata da culpa exclusiva do titular ou de terceiros, afastando o nexo causal entre a ação do agente e o dano suportado pela vítima. Dessa forma, a primeira parte da exceção de responsabilidade fundamenta-se na culpa exclusiva do titular dos dados pessoais¹⁶⁸, assemelhando-se ao artigo 14 do CDC, que dispõe:

Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
 § 1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
 I - o modo de seu fornecimento;
 II - o resultado e os riscos que razoavelmente dele se esperam;
 III - a época em que foi fornecido.
 § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas.
 § 3º O fornecedor de serviços só não será responsabilizado quando provar:
 I - que, tendo prestado o serviço, o defeito inexiste;
 II - a culpa exclusiva do consumidor ou de terceiro.
 § 4º A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa¹⁶⁹.

¹⁶⁷ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 324-325.

¹⁶⁸ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada – 2ª ed. rev., atual. e ampl.* – São Paulo: Thomson Reuters Brasil, 2019, p. 179.

¹⁶⁹ BRASIL. Lei nº 8.078 de 11 de setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm> Acesso em: 26 de novembro de 2019.

Assim, compreende-se que titular deu causa do dano, no caso concreto, quando, por exemplo, fornece seus dados a *sites* claramente falsos, ou quando não guarda em segurança seus documentos de identificação.

No entanto, a segunda parte da exceção, qual seja, a de culpa exclusiva de terceiros, não se faz tão clara. Questiona-se, aqui, se a invasão a um sistema que armazena dados pessoais por um agente mal intencionado, que utiliza posteriormente tais informações de forma danosa, enquadrar-se-ia como culpa de terceiro. Assim, considerando-se que é impossível haver um sistema perfeito, sem falhas, uma vez que a tecnologia de invasão evolui, muitas vezes, ainda mais rápido, costuma-se concluir que *caso a invasão resulte de táticas inovadoras, comprovada a adoção de medidas de segurança eficientes e razoáveis, admite-se a excludente de responsabilidade por fato de terceiro*¹⁷⁰, é possível que se exonere integralmente a responsabilidade, como já decidido pelo Tribunal de Justiça de São Paulo¹⁷¹:

Não se pode fechar os olhos a uma dura e triste realidade: os sistemas computacionais não são 100% indevassáveis. Aí estão os hackers para demonstrar que a muralha digital, inclusive aquela erguida nos grandes centros tecnológicos mundiais, ostenta um certo grau de vulnerabilidade.

Em semelhante cenário, que coonest a asserção da apelante de que terceiros, inspirada na ideia da régua lésbica da equidade proposta por Aristóteles, é a divisão, pela metade, dos prejuízos decorrentes da emissão fraudulenta de passagens (TJSP, Apelação 1083389-32.2015.8.26.0100, Rel. Des. Antônio Nascimento, j. 25.08.2016).

Portanto, mediante comprovação de que os sistemas envolvidos no caso concreto são efetivamente seguros, ou que se utilizou de todas as medidas de segurança cabíveis, é possível que ocorra o afastamento da responsabilidade dos agentes de tratamento por culpa de terceiro, prevista no artigo 43, III, da LGPD, através de uma análise subjetiva do julgador.

Por fim, o Capítulo VI da LGPD traz, em seu artigo 45, uma última ressalva a respeito da responsabilidade dos agentes de tratamento de dados pessoais. Dispondo da seguinte forma: “As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”. Ou seja, sempre que o titular dos dados pessoais objeto do incidente danoso

¹⁷⁰ LAGO JÚNIOR, Antônio. *Responsabilidade civil por atos ilícitos na Internet*. São Paulo: Ed. LTr, 2001 apud MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 325.

¹⁷¹ *Ibidem*.

tiver adquirido produto ou serviço como destinatário final¹⁷², poderá invocar a seu favor o sistema de responsabilização previsto no CDC. Portanto, “o artigo 45 positiva o entendimento de que o microsistema de proteção e defesa do consumidor presente na legislação brasileira se aplica à Lei Geral de Proteção de Dados, especialmente no tocante às regras de responsabilidade”¹⁷³.

4.4 Princípios da Segurança e da Prevenção

Através da leitura dos artigos da LGPD referentes aos Capítulos VI e VII, conclui-se que os agentes de tratamento têm o dever de adotar medidas de segurança e prevenção em qualquer atividade de processamento de dados pessoais. Tal comando encontra-se principalmente no artigo 46 da referida Lei:

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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução¹⁷⁴.

Ademais, a nova legislação geral traz também uma previsão de *irregularidade* no tratamento dos dados pessoais quando tais medidas não são adotadas, como se pode observar:

Art. 44. O tratamento de dados pessoais será **irregular** quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

- I - o modo pelo qual é realizado;
- II - o resultado e os riscos que razoavelmente dele se esperam;

¹⁷² Art. 2º do Código de Defesa do Consumidor - Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.

Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078.htm>. Acesso em: 26 de novembro de 2019.

¹⁷³ MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018, p. 327.

¹⁷⁴ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 26 de novembro de 2019.

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano¹⁷⁵. (grifo próprio)

Dessa forma, ainda que o tratamento dos dados seja realizado conforme enquadramento em uma base legal – como já visto nos capítulos anteriores –, será considerado irregular se não fornecer a segurança que o titular deles espera.

Portanto, depreende-se da leitura dos referidos artigos que todos aqueles que realizam atividades de processamento de dados pessoais devem implementar medidas de segurança e prevenção necessárias à proteção aos dados pessoais. A LGPD, em seu artigo 6º, inciso VII e VIII, ao indicar tais princípios como fundamentais às atividades de tratamento de dados, os define como:

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;

Todavia, os princípios de segurança e prevenção estabelecidos pela LGPD vão muito além de medidas técnicas e administrativas, envolvendo também aquelas relacionadas à segurança física e organizacional, criando uma mudança de *mindset* em todo o ambiente de trabalho do agente de tratamento¹⁷⁶, assim dispendo Paulo Marcos Brancher:

Ao pensar em segurança dos dados, não existe uma solução *tamanho único*. As medidas adequadas são aquelas que levam em consideração as circunstâncias de cada atividade de tratamento e os riscos que elas podem trazer à organização. Nesse sentido, devem ser considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os demais princípios previstos no *caput* do art. 6º da LGPD. Por essa razão, antes de decidir quais medidas adotar, o agente de tratamento deve fazer uma análise detalhada de risco de seu negócio, revendo, por exemplo, o acervo de dados que é processado, a finalidade da atividade, a extensão e qualidade dos sistemas de computador, o número de funcionários e o tipo de acesso

¹⁷⁵ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 26 de novembro de 2019.

¹⁷⁶ BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia (coord.). *Proteção de Dados Pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018*. Belo Horizonte: Fórum, 2019, p. 80.

que eles têm aos dados pessoais e empresas prestadoras de serviços com quem os dados são compartilhados¹⁷⁷.

Portanto, como se pode concluir a partir da leitura do parágrafo acima, os agentes de tratamento sujeitam-se a todos os princípios previstos no art. 6º da LGPD, mas a fim de tornar a leitura do presente trabalho mais agradável, preferiu-se destacar os referidos princípios de segurança e prevenção, uma vez que têm o condão de abarcar todos os demais ao se tratar os dados pessoais de modo seguro e preventivo.

Além disso, é importante destacar que o legislador também se preocupou em disciplinar um plano de contingência a ser adotado pelos agentes de tratamento, caso haja algum incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados, disposição presente no artigo 48 da Lei. Logo, toda organização que processe dados pessoais deve atentar-se a possíveis danos ou violações, visando mitigar os prejuízos de tais atos¹⁷⁸.

Por fim, em razão da inobservância de tais princípios e, portanto, da infração às normas previstas na LGPD, os agentes de tratamento ficam sujeitos a sanções administrativas, como se pode observar:

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

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

¹⁷⁷ BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia (coord.). *Proteção de Dados Pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018*. Belo Horizonte: Fórum, 2019, p. 80.

¹⁷⁸ *Ibidem*.

- VI - o grau do dano;
- VII - a cooperação do infrator;
- VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
- IX - a adoção de política de boas práticas e governança;
- X - a pronta adoção de medidas corretivas; e
- XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção. [...] ¹⁷⁹.

O artigo 52 é, portanto, claro ao estabelecer que as sanções são aplicadas “em razão das infrações cometidas às normas previstas nesta Lei”. Ou seja, não havendo qualquer distinção entre essas infrações, conclui-se que a inobservância dos princípios é capaz de submeter o infrator às sanções previstas. Além disso, ao prever a aplicação das referidas sanções aos “agentes de tratamento”, destaca-se que o *encarregado* não está, portanto, sujeito a elas, uma vez que estes agentes são apenas o *controlador* e o *operador*, conforme já verificado ao longo do trabalho. Não se confundindo, entretanto, a responsabilização administrativa com a responsabilização civil do empregado – caso aja com dolo – e com uma possível responsabilização penal, conforme já disposto no presente trabalho ao analisar o artigo 42 da LGPD.

¹⁷⁹ BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm>. Acesso em: 26 de novembro de 2019.

5 Conclusão

Conforme pode ser verificado ao longo dos capítulos dessa monografia, o tema da proteção de dados pessoais tornou-se fundamental para a proteção do indivíduo, diante de um mundo *hiperconectado*, em que os dados pessoais são o insumo para diversas atividades econômicas e, também, indispensáveis à atuação do setor público. Dessa forma, a fim de suprir a carência do ordenamento jurídico brasileiro, no que tange a uma legislação geral a respeito do tema, desenvolveu-se, através da Lei Geral de Proteção de Dados Pessoais, um sistema de normas que envolve procedimentos, princípios e direitos, limitando o tratamento de dados pessoais e empoderando o cidadão, no que diz respeito ao controle de suas informações.

Dessa forma, adentrando-se em tal tema e a fim de responder os questionamentos propostos pela presente monografia, que se atentou às figuras dos agentes de tratamento de dados pessoais da referida Lei, chegou-se a algumas conclusões, quais sejam:

- a) Os “dados pessoais” constituem-se de qualquer registro a respeito de um indivíduo; possuindo, todavia, algumas classificações especiais, dentre as quais merece destaque a dos “dados sensíveis”, que possuem disposição semelhante na LGPD e no novo Regulamento Europeu a respeito do tratamento de dados, uma vez que demandam tratamento especial.
- b) A proteção dos dados pessoais tem como base a proteção do indivíduo, e não dos dados *per se*, uma vez que a inadequada divulgação e utilização de informações referentes a um indivíduo pode violar a sua personalidade.
- c) O direito à proteção dos dados pessoais configura-se como um direito de personalidade autônomo, uma vez que está diretamente ligado aos aspectos morais do indivíduo, embora originário do direito à privacidade.
- d) A proteção legal dos dados pessoais iniciou-se, principalmente, através do advento da tecnologia, tendo como principal exemplo a internet, de modo que o primeiro regulamento europeu a respeito do tema se deu na década seguinte ao seu surgimento, ou seja, na década de 70.
- e) O regramento europeu a respeito do tema tem a sua maior força com o surgimento da “General Data Protection Regulation” (GDPR), que se desenvolveu através das inúmeras diretivas e convenções anteriores a respeito da proteção de dados, entrando em vigor em junho de 2018 e sendo diretamente aplicável a cada Estado membro da UE.

- f) A proteção de dados pessoais, embora seja evidente o seu caráter fundamental, carece de disposição expressa na Constituição Federal Brasileira, estando amparada, atualmente, nos fundamentos da Carta que dizem respeito à tutela da personalidade (art. 1º, III, e art. 5º, §2º). Motivo pelo qual foi Proposta de Emenda à Constituição n. 17 de 2019, que objetiva tornar a proteção de dados como um direito fundamental expresso.
- g) O tema da proteção de dados possui legislação esparsa em nosso ordenamento, estando presente, por exemplo, no Código Civil, no Código de Defesa do Consumidor, na Lei de Acesso à Informação e no Marco Civil da Internet, por exemplo. Assim, com o advento da LGPD, deve haver uma interpretação sistemática de tal diploma normativo com os demais, nos moldes do diálogo das fontes, possibilitando a aplicação simultânea dos princípios e regras gerais da LGPD com as regras setoriais.
- h) A LGPD influenciou-se claramente na GDPR. Conclusão que pode ser verificada a partir da leitura de vários artigos da Lei, como, por exemplo, aqueles referentes à exigência de uma base legal para o tratamento de dados, aos princípios gerais, aos dados sensíveis, à responsabilidade do operador e do controlador – novas figuras criadas pela Lei chamadas de “agentes de tratamento” – e à portabilidade de dados, outra inovação trazida pela LGPD. Além disso, assemelha-se à legislação europeia também no que concerne à criação de uma autoridade nacional para a aplicação da Lei.
- i) A nova lei geral tem como principal linha condutora a transparência, ou seja, mesmo nas hipóteses em que não se é exigido o consentimento prévio e expresso do titular dos dados, ele deve ser transparente.
- j) A LGPD divide-se em cinco eixos principais, sendo eles: i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados e v) responsabilização dos agentes.
- k) Embora a aplicação material da Lei tenha como base a generalidade e a unidade, aplicando-se a qualquer operação de tratamento de dados pessoais que tenha ocorrido dentro do Brasil ou que possua como objetivo final o oferecimento de bens e serviços a pessoas que estejam em território nacional, excluem-se da sua

proteção as pessoas jurídicas, de modo que a proteção se estende somente às pessoas naturais.

- l) O tratamento de dados não poderá ser realizado sem que haja uma base normativa que o autorize, ou seja, só poderá ocorrer se ele estiver embasado em uma das hipóteses autorizativas previstas no art. 7º, no art. 11 – no que tange aos dados sensíveis – ou no art. 23º da LGPD.
- m) A LGPD fundamenta-se nos seguintes princípios: (i) finalidade; (ii) adequação; (iii) necessidade; (iv) livre acesso; (v) qualidade dos dados; (vi) transparência; (vii) segurança; (viii) prevenção; (ix) não discriminação e (x) responsabilização e prestação de contas.
- n) Está-se diante de uma nova era de *minimização* de dados, onde não há mais uma coleta irrestrita, mas sim uma imposição de coleta mínima, apenas para a finalidade do produto ou serviço a ser prestado.

Iniciando-se o último capítulo do trabalho, referente aos agentes de tratamento, que pretendeu responder objetivamente os questionamentos feitos, chegaram-se às seguintes conclusões:

- a) Os agentes de tratamento de dados pessoais, inovações trazidas pela nova Lei Geral de Proteção de Dados, conforme disposição do seu artigo 5º, inciso IX, constituem-se pelas figuras do *controlador* e o *operador*.
- b) Os seus papéis no tratamento dos dados pessoais permitem que não haja mais um compartilhamento dos dados do titular de modo nunca pretendido por ele.
- c) O *controlador* constitui-se como figura central quando se trata de proteger os direitos dos titulares, ou seja, é o principal tomador de decisão em relação aos dados pessoais, possuindo como função controlar a finalidade e os meios gerais de como os dados devem ser usados.
- d) O *controlador* possui suas responsabilidades dispostas ao longo da Lei, estando entre elas, por exemplo, a prestação de contas, a elaboração do relatório de impacto, a indicação do *encarregado*.
- e) O *operador*, responsável por tratar os dados por ordem do *controlador*, tem como responsabilidade fornecer garantias para implementar “medidas técnicas e organizacionais” adequadas, de modo que o processamento cumpra os requisitos legais e de segurança.

- f) O *encarregado* pelo tratamento dos dados, embora não seja enquadrado como agente de tratamento pela LGPD, deve permitir a comunicação entre o *controlador*, o titular dos dados e a Agência Nacional de Proteção de Dados, tendo como funções aquelas dispostas no §2º do artigo 41 da LGPD.
- g) Os agentes de tratamento são civilmente responsáveis por qualquer violação legal. No entanto, concluiu-se que a LGPD se refere, principalmente, à responsabilidade subjetiva, sendo a responsabilidade objetiva exceção, aplicando-se, por exemplo, nos casos em que o titular de dados configura-se como consumidor – podendo-se aplicar a responsabilidade objetiva prevista no Código de Defesa do Consumidor – e naqueles em que ela decorre do risco da atividade de tratamento dos dados.
- h) Os agentes de tratamento devem observar todos os princípios previstos na LGPD, com atenção especial à segurança e à prevenção, uma vez que estes têm o dom de abarcar todos os demais.

As disposições acima permitiram que se concluísse que as novas figuras dos agentes de tratamento serão fundamentais para que se chegue aos objetivos pretendidos pela Lei Geral de Proteção de Dados. Embora ainda não houvesse uma legislação geral a respeito da proteção de dados no ordenamento jurídico brasileiro, determinados regramentos, que a Lei buscou unificar e homogeneizar, poderiam ser encontrados na legislação esparsa. Todavia, a Lei trouxe inovações, estando entre elas a criação das figuras do *controlador* e do *operador*, que arrisco dizer que serão determinantes na busca pela proteção dos dados pessoais, uma vez que tais inovações permitem uma maior rigidez – que não havia nos regramentos anteriores – no processamento de dados, fazendo com que as empresas possam ser responsabilizadas civil e administrativamente, conforme disposição da LGPD. Dessa forma, o cidadão experimentará um controle dos seus dados e, conseqüentemente, o respeito à sua esfera privada, no que tange às suas informações pessoais, de modo nunca antes permitido.

Referências Bibliográficas

ALEXY, Robert. *Teoria de los derechos fundamentales*. Madrid: Centro de Estudios Constitucionales, 2007.

ANDRADE, Frederico Pupo Carrijo de. *Análise comparativa do tratamento de dados pessoais à luz do direito de personalidade*. Estudos avançados de direito digital/coordenação Cíntia Rosa Pereira Lima, Lydia Neves Bastos Telles Nunes. 1ª ed. Rio de Janeiro: Elsevier, 2014.

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

BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção de dados do consumidor*. São Paulo: Almedina, 2018.

BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Cláudia (coord.). *Proteção de Dados Pessoais no Brasil: uma nova visão a partir da Lei nº 13.709/2018*. Belo Horizonte: Fórum, 2019.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Planalto. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/Ato2015-2018/2016/Decreto/D8771.htm> Acesso em: 31 de outubro de 2019.

BRASIL. Lei nº 8.078 de 11 de setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/18078.htm>. Acesso em: 06 de novembro de 2019.

BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm>. Acesso em: 06 de novembro de 2019.

BRASIL. Lei nº 12.737 de 18 de novembro de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/2011/lei/112527.htm>. Acesso em: 06 de novembro de 2019.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/lei/112965.htm>. Acesso em: 10 de novembro de 2019.

BRASIL. Lei nº 13.105 de 16 de março de 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm>. Acesso em: 26 de novembro de 2019.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 11 de novembro de 2019.

BRASIL. Proposta de Emenda à Constituição n. 17, de 2019. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1571776978885&disposition=inline>>. Acesso em: 05 de novembro de 2019.

CASTRO, Catarina Sarmiento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. São Paulo: Thomson Reuters, 2019.

CRAVO, Daniela Copetti. *Direito à portabilidade de dados Interface entre defesa da concorrência, do consumidor e proteção de dados*. Rio de Janeiro: Lumen Juris, 2018.

DE CUSPIS, Adriano. *I diritti della personalità*. Milano: Giuffrè, 1982.

DE LA CUEVA, Pablo Lucas Murillo. *Informática y protección de datos personales*. Madrid: Centro de Estudios Constitucionales, 1993.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). *Direito & Internet III – Tomo I: Marco Civil da Internet (Lei nº 12.965/2014)*. São Paulo: Quartier Latin, 2015.

DONEDA, Danilo. *Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais*. *Âmbito Jurídico*, v. 52, 2008.

ECO, Umberto. *Como se faz uma tese*. Tradução: Gilson Cesar Cardoso de Souza. São Paulo: Perspectiva, 2012. 24ª ed.

FERREIRA, Ricardo Barreto; BRANCHER, Paulo; TALIBERTI, Camila; CUNHA, Vitor Koketu da. *Entra em vigor o Regulamento Geral de Proteção de Dados da União*

Europeia. Migalhas, 2018. Disponível em <<https://www.migalhas.com.br/dePeso/16,MI281042,81042-Entra+em+vigor+o+Regulamento+Geral+de+Protecao+de+Dados+da+Uniao>> Acesso em: 30 de outubro de 2019.

FORTES, Vinicius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet*. Rio de Janeiro: Lumen Juris, 2016.

LACOMBE, Francisco José Masset et al. *Administração: princípios e tendências*. São Paulo: Saraiva, 2003.

LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia*. São Paulo: Thomson Reuters Brasil, 2018.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). *LGPD: Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2019.

MELLO, Celso Antônio Bandeira de. *Curso de Direito Administrativo*, 27ª ed. São Paulo: Malheiros, 2010.

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

MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados*. Revista de Direito do Consumidor, vol. 120, ano 27, p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018.

MENKE, Fabiano. *Fundamentos da proteção de dados*. Inédito.

MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriana Loureiro; MORIBE, Gabriela; CAMARA, Dennys Eduardo Gonsales; GHERINI, Pamela Michelena De Marchi. *Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos*. Disponível em: <<https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf>>. Acesso em: 23 de outubro de 2019.

MOREIRA, Carlos Roberto Barbosa. *Notas sobre a inversão do ônus da prova em benefício do consumidor*. Revista dos Tribunais, São Paulo, n. 22, abr.-jun. 1997.

OLIVEIRA, Ricardo Alexandre de. *Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico*. São Paulo: Revista dos Tribunais, dezembro 2018, vol. 998, ano 107.

PINHEIRO, Patrícia Peck Garrido. *Nova Lei Brasileira de Proteção de Dados Pessoais (LGPD) e o impacto nas instituições públicas e privadas*. Revista dos Tribunais, vol. 1000, ano 108, p. 309-323. São Paulo: Ed. RT, fevereiro de 2019.

PORTUGAL. Convenção 108 de 28 de janeiro de 1981. Disponível em: <<https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>>. Acesso em: 04 de novembro de 2019.

RODOTÀ, Stefano. *A vida privada na sociedade da vigilância – A privacidade hoje*. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Yuri Gonçalves dos Santos; FERREIRA, Keila Pacheco. *A privacidade no ambiente virtual: avanços e insuficiências da Lei Geral de Proteção de Dados no Brasil (Lei 13.1709/18)*. Revista de Direito do Consumidor, vol. 122, ano 28, p. 181-202. São Paulo: Ed. RT, mar.-abr. 2019.

SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. *Lei Geral de Proteção de Dados no Brasil e os possíveis impactos*. Revista dos Tribunais, vol. 998, ano 107, p. 225-239. São Paulo: Ed. RT., dezembro de 2018.

SILVA, Carlos Bruno Ferreira da. *Proteção de dados e cooperação transnacional: teoria e prática na Alemanha, Espanha e Brasil*. Belo Horizonte: Arraes Editores, 2014.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. São Paulo: Malheiros, 2012.

SILVA, Joseane Suzart Lopes da. *A proteção de dados pessoais dos consumidores e a Lei 13.709/2018: em busca da efetividade dos direitos a privacidade, intimidade e autodeterminação*. Revista de Direito do Consumidor, vol. 121, ano 28, p. 367-418. São Paulo: Ed. RT, jan.-fev. 2019.

TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. *Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil*. Tribunal de Justiça de São Paulo, 2016. Disponível em:

<<http://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ii%204.pdf?d=636680444556135606>>. Acesso em: 30 de outubro de 2019.

ZANON, João Carlos. *Direito à proteção dos dados pessoais*. São Paulo: Revista dos Tribunais, 2013.