II ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

DANIELLE JACON AYRES PINTO

JOSÉ RENATO GAZIERO CELLA

AIRES JOSE ROVER

FABIANO HARTMANN PEIXOTO

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Danielle Jacon Ayres Pinto; Fabiano Hartmann Peixoto; José Renato Gaziero Cella – Florianópolis: CONPEDI, 2020.

Inclui bibliografia
ISBN: 978-65-5648-259-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito, pandemia e transformação digital: novos tempos, novos desafios?

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Governança. 3. Novas tecnologias. II Encontro Virtual do CONPEDI (2: 2020 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil

II ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

No II Encontro Virtual do CONPEDI, realizado de 02 a 04 dezembro de 2020, o grupo de trabalho "Direito, Governança e Novas Tecnologias I", que teve lugar na tarde de 02 de dezembro de 2020, foi o promotor dos inícios dos debates sobre esse tema tão instigante e contemporâneo. Ao longo de GT foram apresentados trabalhos de alta qualidade produzidos por doutores, pós-graduandos e graduandos. Tais estudos são fruto de pesquisa contínua e do esforço efetivo para promover a consolidação de práticas justa e democráticas frente as novas tecnologias e sua influência no mundo do direito.

Ao total foram apresentados 18 artigos com uma diversidade de temas e que promoveram um intenso debate realizados pelos coordenadores do grupo de trabalho e pelo público presente na sala virtual.

Esse rico debate demonstra a inquietude que os temas estudados despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em Direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao Direito e a toda sociedade. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva, os coordenadores do grupo de trabalho dividiram os artigos em três blocos, quais sejam a) inteligência artificial; b) pandemia de COVID-19 e novas tecnologias; e c) governo eletrônico e sociedade da informação.

O bloco inicial dedicou-se a pensar a inteligência artificial e a sociedade da informação e nele foram debatidos os seguintes temas: "a aplicação da tecnologia na resolução de disputas e o serviço amica: uma análise da recente experiência australiana de uso de i.a em mediações familiares"; "algoritmos, inteligência artificial e novas formas de interação política: uma análise da influência da ia nos processos eleitorais democráticos na contemporaneidade"; "o uso da accountability e compliance como formas de mitigar a responsabilidade civil pelos danos causados pela inteligência artificial"; "a disseminação da informação – eficácia e confiabilidade na sociedade moderna"; "instrumentos preventivos na criminalidade digital - questões constitucionais e normas técnicas internacionais"; "desestatização do dinheiro na sociedade da informação".

No segundo bloco os temas ligados a pandemia de COVID-19 e as novas tecnologias foi o mote central do debate, sendo eles: "a pandemia da desinformação: covid-19 e as mídias

sociais – do fascínio tecnológico à (auto)regulação"; "autodeterminação informativa e covid-19: a ponderação de medidas no uso de dados pessoais"; "a problemática da saúde global frente aos desafios impostos pelas corporações transnacionais"; "o brasil na sociedade da informação: remissão histórica e seu panorama atual com destaque na covid-19"; "o governo eletrônico em tempos de pandemia"; "o direito fundamental ao livre acesso à internet: a efetividade do direito à saúde por meio da telessaúde e da telemedicina".

No terceiro e derradeiro bloco, os trabalhos tiveram o intuito de debater o governo eletrônico e a sociedade da informação, e para isso os temas abordados foram: análise da evolução e proteção legal da privacidade e dados pessoais no brasil"; "função social da empresa e startups uma relação disruptiva frente ao novo marco regulatório"; "lei geral de proteção de dados pessoais: direito à autodeterminação informativa do titular dos dados"; "a interface dos direitos da personalidade e os jogos violentos"; "a sociedade da informação como instrumento para a erradicação da pobreza"; "identidade cultural cyber e identidade virtual: a construção de novos direitos da personalidade pela cibercultura"

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema "Direito, Governança e Novas Tecnologias". Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em Direito brasileira, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. Aires José Rover

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. Fabiano Hartmann Peixoto

Prof. Dr. José Renato Gaziero Cella

Nota técnica: O artigo intitulado "A PANDEMIA DA DESINFORMAÇÃO: COVID-19 E AS MÍDIAS SOCIAIS – DO FASCÍNIO TECNOLÓGICO À (AUTO)REGULAÇÃO" foi indicado pelo Programa de Pós Graduação em Direito da Faculdade de Direito de Vitória, nos termos do item 5.1 do edital do Evento.

Os artigos do Grupo de Trabalho Direito, Governança e Novas Tecnologias I apresentados no II Encontro Virtual do CONPEDI e que não constam nestes Anais, foram selecionados para publicação na Plataforma Index Law Journals (https://www.indexlaw.org/), conforme previsto no item 7.1 do edital do Evento, e podem ser encontrados na Revista de Direito, Governança e Novas Tecnologias. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: DIREITO À AUTODETERMINAÇÃO INFORMATIVA DO TITULAR DOS DADOS

BRAZILIAN GENERAL DATA PROTECTION LAW: OWNER RIGHT TO SELF-DETERMINE THE INFORMATION

Tiago Pereira Remédio [1]
Davi Pereira Remedio [2]
José Antonio Remedio [3]

Resumo

As pessoas têm na atualidade seus dados pessoais normalmente armazenados e tratados em bancos de dados, inclusive por meios digitais, sem que haja prévio conhecimento ou consentimento do titular dos dados. A pesquisa objetiva analisar o direito à autodeterminação informativa da pessoa em relação a seus dados pessoais com base na Lei Geral de Proteção de Dados Pessoais. O método da pesquisa é o hipotético-dedutivo, com fundamento na legislação, doutrina e jurisprudência. Conclui que a Lei Geral de Proteção de Dados Pessoais assegura ao titular dos dados o direito à autodeterminação informativa, preservando, entre outros, seu direito fundamental à privacidade.

Palavras-chave: Autodeterminação informativa, Banco de dados, Dados pessoais, Lei geral de proteção de dados pessoais, Direito à privacidade

Abstract/Resumen/Résumé

In the current days people have their personal data stored and analyzed in databases, including digital ones, without previous knowledge or consent from the owner of such data. The research aims to analyze the right to a person's self determination regarding his personal data based on the Brazilian General Data Protection Law. The method used is the hypothetical deductive, based on legislation, doctrine and jurisprudence. It is concluded that the Brazilian General Data Protection Law ensures the data owner the right to self-determine the information, preserving, among other things, its right to privacy.

Keywords/Palabras-claves/Mots-clés: Informational self-determination, Database, Personal data, Brazilian general data protection law, Right to privacy

[1] Mestre em Ciência da Computação pela UNESP. Professor do Centro Universitário Hermínio Ometto de Araras (UNIARARAS). Professor do Centro Universitário Adventista de São Paulo (UNASP). ensino@tiagoremedio.com.br

[2] Mestre em Direito pela Universidade Metodista de Piracicaba (UNIMEP). Professor de Graduação em Direito do Centro Universitário de Araras Dr. Edmundo Ulson (UNAR). Advogado. advocaciaremedio@hotmail.com

[3] Pós-Doutor em Direito pela UENP. Doutor em Direito pela PUCSP. Mestre em Direito pela UNIMEP. Professor de Pós-Graduação em Direito da UNIMEP e de Graduação em Direito do UNASP. jaremedio@yahoo.com.br

1 INTRODUÇÃO

O mundo atual está envolto no desenvolvimento de novas e inimagináveis tecnologias nas mais diversas áreas do conhecimento, em especial as relacionadas à informática e à *internet*, com a criação de *softwares* extremamente sofisticados e de altíssima *performance*.

O desenvolvimento tecnológico, com ampla aplicação no âmbito da *internet*, tem revolucionado as áreas da informação, comunicação e economia, em particular por meio da coleta, armazenamento, tratamento e divulgação de dados pessoais, principalmente através de empresas e corporações, sem que haja efetivos instrumentos de controle por parte do titular dos dados.

A economia moderna, qualquer que seja o ramo de atividade, setor empresarial ou modelo de negócio adotado, transformou-se em uma economia estruturada em dados, sendo que a "utilização de dados pessoais ou não, representa hoje um dos principais elementos de crescimento da atividade econômica e de inovação, inclusive nas atividades do Poder Público" (LEONARDI, 2019, p. 71).

Além da importância relacionada à economia digital, no atual contexto da evolução tecnológica, a *internet* "expõe a vulnerabilidade dos pessoais dos indivíduos, e, por consequência, da intimidade e da vida privada, na medida em que o acesso não autorizado a esses dados sensíveis é crescente e notório" (GRESSLER; BACHINSKI; SILVA, 2019, p. 7).

O ambiente social no qual se concretiza a ideia de privacidade informacional na sociedade governada por dados, passa a ser qualificado pela proteção dos direitos da pessoa em manter o controle sobre seus dados, por meio de sua autodeterminação informativa, no caso a liberdade, objetivando a não-discriminação, ou a igualdade (MULHOLLAND, 2019, p. 53).

Os dados interconectados, oriundos da tecnologia informacional, "podem oferecer riscos a direitos constitucionais dos usuários, como privacidade e segurança, podendo expô-los a prejuízos dos quais não têm ainda plena consciência" (MAGRANI; OLIVEIRA, 2019, p. 82).

A título de exemplo, em 2012, no Brasil, conforme referido pelo Instituto Telecom, a empresa OI teria compartilhado informações pessoais e dados cadastrais de seus quase seis milhões de clientes de banda larga em todo o país, como nomes, telefones, informações bancárias e CPF – Cadastro de Pessoa Física, sem que houvesse autorização dos respetivos clientes (INSTITUTO, 2013).

A coleta, armazenagem, tratamento e compartilhamento dos dados pessoais estão disciplinados no Brasil por meio da Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais, que entrará em vigor em 03.05.2021, conforme previsto pela Medida Provisória 959/2020.

A pesquisa ter por objeto analisar o direito à autodeterminação informativa da pessoa em relação a seus dados pessoais, com base na Lei Geral de Proteção de Dados Pessoais.

No que se refere à estrutura, a pesquisa tem início com a abordagem do direito à informação na sociedade da informação. Em seguida trata do direito à privacidade da tutela jurídica de dados pessoais. A seguir enfoca aspectos gerais da Lei 13.709/2018. Por fim, analisa o direito à autodeterminação informativa do titular dos dados.

O método utilizado é o hipotético-dedutivo, com base na legislação, doutrina e jurisprudência.

Tem-se, como hipótese, que a Lei 13.709/2018 atribui à pessoa o direito fundamental à autodeterminação informativa, relativamente à coleta, armazenamento e tratamento de seus dados pessoais por pessoas físicas, jurídicas ou entes governamentais.

2 O DIREITO À INFORMAÇÃO NA SOCIEDADE DA INFORMAÇÃO

As expressões “era da informação” e “sociedade da informação” são utilizadas na atualidade para descrever e representar o desenvolvimento e os impactos da revolução tecnológica em curso no âmbito das sociedades, inclusive das sociedades estatais.

O século XXI nasce sob a égide da “era da informação”, dando ensejo ao surgimento da “sociedade em rede”, na qual os avanços da tecnologia da informação e comunicação geram importantes reflexos sociais (REMEDIO; SILVA, 2017, p. 673).

Os reflexos decorrentes dos avanços da tecnologia da informação são incomensuráveis, como ocorre, por exemplo, em relação à economia moderna, em especial à economia digital.

A economia digital, por meio do uso da *internet* e da inteligência artificial, tem conduzido à obtenção de lucros bastante expressivos em favor das empresas e corporações, entre outras formas, a partir do intenso uso de dados pessoais para a formação de perfis informacionais, “que permitirão identificar os hábitos, preferências, características pessoais, bem como as escolhas políticas e existenciais dos titulares dos dados, quase sempre em completo desvirtuamento da finalidade para a qual foram coletados” (CUEVA, 2019, p. 134).

A obtenção de informações sobre os consumidores na economia customizada é condição necessária para a adaptação e diversificação dos produtos e serviços para diferentes segmentos de clientes, sendo que "a oferta de volumes menores de produtos especializados, altamente qualificados e segmentados, permite a manutenção de alto grau de lucratividade e estabilidade comercial" (MENDES, 2014, p. 90).

Todavia, a economia digital, pautada pela coleta e tratamento dos dados pessoais para o funcionamento do sistema econômico produtivo, acaba expondo a riscos expressivos os indivíduos titulares dos dados pessoais, em especial no que se refere aos direitos de personalidade e privacidade (MENDES, 2014, p. 92).

O aumento expressivo da capacidade de se produzir dados pelas novas tecnologias, com a ampliação e expansão do acesso à *internet*, possibilitou a multiplicação de forma inimaginável do potencial de difusão do volume de dados produzidos, fenômeno que passou a ser amplamente debatido por meio da utilização da expressão *Big Data*.

O *Big Data* é explicado e conceituado por França, Faria, Rangel, Farias e Oliveira (2014, p. 8) nos seguintes termos:

> Os dados das redes sociais *online* podem ser usados para extrair informações sobre padrões de interações interpessoais e opiniões. Esses dados podem auxiliar no entendimento de fenômenos, na previsão de um evento ou na tomada de decisões. Com a ampla adoção dessas redes, esses dados aumentaram em volume, variedade e precisam de processamento rápido, exigindo, por esse motivo, que novas abordagens no tratamento sejam empregadas. Aos dados que possuem tais características (volume, variedade e necessidade de velocidade em seu tratamento), chamamo-los de *Big Data*.

O Comitê Gestor da Internet no Brasil (COMITÊ, 2013) define o *Big Data* como "um conjunto de dados estruturados e não estruturados, disponíveis em grandes quantidades, sendo, por sua vez, necessárias ferramentas especialmente preparadas para encontrar, analisar, tratar e aproveitar toda e qualquer informação contida nesse emaranhado de dados".

O *Big Data* possibilita "o acompanhamento de comportamentos humanos em tempo real e de maneira massificada e agregada, e, ao mesmo tempo, destacar seguimentos a partir dos próprios comportamentos" (REMEDIO; SILVA, 2017, p. 682).

No que se refere à sociedade da informação, segundo Siqueira Junior (2009, p. 215):

> A sociedade da informação é aquela em que o desenvolvimento encontra-se calcado em bens imateriais, como os dados, informação e conhecimento. O conceito de sociedade da informação é amplo, e não se reduz ao aspecto tecnológico, abrangendo qualquer tratamento e transmissão da informação, que passa a possuir valor econômico.

O ponto central da sociedade da informação é o compartilhamento de dados.

O compartilhamento da informação "é fenômeno social estimulado, numa perspectiva de que a coletividade em rede possibilita a redução espacial e de tempo para que as interações sociais possam ocorrer em maior quantidade e, preferencialmente, com melhor qualidade" (LISBOA, 2019, p. 76).

A coleta e a utilização maciça de dados deu ensejo à "constituição de uma nova forma de capitalismo, fundado na vigilância constante e no controle disperso sobre os cidadãos, a fim de possibilitar geração crescente de dados e aplicações" (FRAZÃO, 2019, p. 33-34).

Entretanto, mesmo em face da era da informação ou da sociedade da informação, a coleta, tratamento e compartilhamento da informação precisam ser delimitados e controlados, de forma a preservar os direitos dos titulares e usuários dos dados, em especial o direito fundamental à privacidade.

3 DIREITO À PRIVACIDADE E TUTELA JURÍDICA DE DADOS PESSOAIS

Os avançados sistemas de informação, de acordo com Silva (2015, p. 218), deram ensejo a verdadeira devassa na vida das pessoas, inclusive privada, de forma que "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 o seu consentimento".

Ponderando que se deve ter a consciência de que a proibição de acesso a dados pessoais implicará na efetiva exclusão social do indivíduo, com prejuízo efetivo a seu desenvolvimento social, Miranda (2018, p. 28) apresenta uma proposta de convergência entre os interesses em conflito, nos seguintes termos:

> os Estados devem buscar por meio das legislações próprias e acordos internacionais a harmonização dos interesses públicos, econômicos e privados, estimulando o uso racional e eficaz das informações, balanceando direitos e preservando as garantias fundamentais do cidadão, sem, contudo, criar antagonismos entre os interesses sociais e econômicos, posto que tais interesses são complementares.

O direito à privacidade, para fins do presente estudo, é compreendido como gênero, pois engloba todas as manifestações da esfera íntima, privada e da personalidade das pessoas, sendo o direito à intimidade compreendido como uma espécie da privacidade (SPALER; REIS, 2018).

A tutela jurídica de dados pessoais é corolário do direito à privacidade, que engloba o direito à intimidade e à vida privada e veda o tratamento de dados sem o consentimento expresso do titular (GRESSLER; BACHINSKI; SILVA, 2019, p. 14).

Todavia, a doutrina não é pacífica quanto à relação existente entre os termos privacidade e intimidade. Alguns pensadores, como Ferraz Júnior (1993, p. 442), asseveram que os termos possuem conceituações distintas, enquanto outros, como Silva (2015, p. 208), consideram que os termos são sinônimos.

O direito à privacidade ou intimidade ganhou força no âmbito internacional, ao ser referido por meio da Declaração Universal dos Direitos do Homem (ONU, 1948), nos seguintes termos: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

O indivíduo, pelo direito da privacidade, "pode desenvolver sua individualidade, inclusive e especialmente no sentido da garantia de um espaço para seu recolhimento e reflexão sem que seja compelido a determinados comportamentos socialmente esperados" (REMEDIO; REIS, 2018, p. 113).

A Carta dos Direitos Fundamentais da União Europeia de 2000 garante tanto o direito à proteção dos dados pessoais como direito fundamental autônomo (art. 8º), como o direito à privacidade (art. 7º) (LIMA, 2019, p. 61).

O direito à proteção de dados pessoais possui afinidade com o direito à privacidade, embora não possa ser reduzido a um mero aspecto seu, isso porque há condutas que são irrelevantes para o direito à privacidade, mas não para o direito da proteção de dados pessoais. O contrário também é verdadeiro, pois, "embora haja muita sobreposição no âmbito de proteção desses direitos, o direito à proteção de dados não está totalmente subsumido ao direito à privacidade" (QUEIROZ, 2019, p. 15).

O tratamento jurídico utilizado na proteção de dados pessoais não é uniforme no âmbito dos Estados modernos, inclusive havendo diversas distinções no que se refere aos sistemas da *common law* e da *civil law*.

Nesse sentido, de acordo com Danilo Doneda (2019, p. 186-187):

> A diversidade entre os sistemas de *common law* e *civil law* certamente exerceu influência no desenvolvimento de diferentes regimes de proteção de dados pessoais, sendo que uma certa resistência de países da esfera do *common law* em vincular a matéria aos direitos fundamentais ou a modelos como o da tutela da dignidade pode ser mencionada como sintomática da diferença entre enfoques.

Nos países em que o direito à privacidade e o direito à proteção de dados foram fixados legalmente, como em alguns países da Europa, os contornos desses direitos foram estabelecidos com maior clareza, ao passo que, onde essa tarefa coube à elaboração doutrinária e judicial, como nos Estados Unidos da América, os contornos são menos nítidos (QUEIROZ, 2019, p. 15-16).

Nos Estados Unidos da América, os mentores da articulação da ideia de um direito à privacidade, com instrumentos jurídicos coibirem para sua violação, foram os advogados Samuel Warren e Louis Brandeis, em artigo acadêmico publicado no final do século XIX, direito que "iria além da proteção de uma pessoa e suas propriedades, para abranger um direito de ser deixado em paz, garantindo a possibilidade de uma separação entre si e o mundo exterior (QUEIROZ, 2019, p. 16). Na ausência de disposição constitucional expressa ou legislação federal que uniformizasse a proteção legal à vida privada e aos dados pessoais, "procedeu-se a uma construção conceitual e argumentativa, inclusive no âmbito judicial, para se extrair, inicialmente, um direito à privacidade e, em seguida, um direito à proteção de dados a partir dele" (QUEIROZ, 2019, p. 17).

Na Europa, diferentemente do ocorrido nos Estados Unidos da América, vigia desde 1953 a Convenção Europeia dos Direitos Humanos (CEDH), que no art. 8º previu o direito a uma vida privada e familiar.

A Europa movimentou-se "para atingir a padronização jurídica da proteção de dados pessoais em poder dos setores públicos e privados", como se deu com a Convenção 108/1981, com a Diretiva 95/46/EC de 1995 e com o Regulamento Geral para Proteção de Dados (GDPR) – Regulamento 2016/679, implementado em 2018 (QUEIROZ, 2019, p. 18-19).

A Lei Geral de Proteção de Dados Pessoais brasileira, inspirada no Regulamento Geral para Proteção de Dados europeu, adota as premissas e os fundamentos necessários para que a proteção dos dados seja efetivo instrumento de preservação dos direitos fundamentais. Nesse sentido, "devem ser compreendidos os direitos básicos dos titulares de dados previstos no art. 18 da Lei 13.709/2018, sempre de forma consentânea com os fundamentos, os princípios e as preocupações que fazem necessária a regulação de dados" (FRAZÃO, 2019, p. 46).

4 ASPECTOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS BRASILEIRA

A atual legislação brasileira disciplina tanto a proteção do direito à privacidade como do direito à informação.

A proteção do direito à privacidade e do direito à informação está prevista em suas linhas básicas no art. 5º da Constituição Federal, nos seguintes termos (BRASIL, 1998):

> 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;
> 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;
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

Até o advento da Lei 13.709/2018 algumas normas infraconstitucionais brasileiras tratavam, com maior ou menor amplitude, da matéria concernente à proteção de dados pessoais, como o Código de Defesa do Consumidor (Lei 8.078/1990), a Lei do Cadastro Positivo (Lei 12.414/2011), a Lei do Acesso à Informação (Lei 12.527/2011), a Lei Carolina Dieckmann (Lei 12.737/2012) e o Marco Civil da Internet (Lei 12.965/2014).

O Marco Civil da Internet (Lei 12.965/2014) não só estabeleceu princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil, mas também fixou as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

A Lei 12.965/2014 previu um microssistema de proteção de dados pessoais no ambiente *on-line*, tendo como um dos principais fundamentos para o tratamento de dados pessoais o consentimento, que deve ser livre, expresso e informado, inclusive destacado das demais cláusulas contratuais (RIELLI, 2019, p. 10).

Todavia, embora existissem diversas leis tratando esparsamente da proteção de dados pessoais, o marco comum "para o início do debate sobre uma lei geral de proteção de dados no Brasil é a submissão do primeiro anteprojeto de lei do Poder Executivo à consulta pública em dezembro de 2010" (RIELLI, 2019, p. 8).

O diagnóstico que informou o anteprojeto da lei foi a ausência de uma regulação geral de proteção de dados pessoais, que colocava o Brasil em uma posição de descompasso com outros países, além de desproteger o cidadão contra o uso abusivo de seus dados pessoais e de criar um cenário de insegurança jurídica pela ausência de regras padronizadas para os diversos setores que tratam dados. O anteprojeto baseou-se em um rol de princípios de proteção de dados pessoais extraídos das práticas da regulação internacional, como "finalidade,

necessidade, proporcionalidade, qualidade, transparência, segurança e livre acesso", com especial destaque à questão da base legal do consentimento (RIELLI, 2019, p. 8).

A Lei 13.709/2018, intitulada Lei Geral de Proteção de Dados Pessoais (LGPD), que atualmente disciplina a matéria, deve ser observada pela União, Estados, Distrito Federal e Municípios, e dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o fim de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A Lei Geral de Proteção de Dados Pessoais possui como fundamentos (BRASIL, 2018a): o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

O principal objetivo da Lei 13.709/2018 foi conferir ampla proteção ao cidadão quanto ao tratamento de dados, podendo-se até mesmo afirmar "que a proteção de dados corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsicamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante (FRAZÃO, 2019, p. 34).

No tocante aos princípios retores da LGPD, as atividades de tratamento de dados pessoais estão disciplinadas no art. 6º da Lei 13.709/2018, que, além do respeito à boa-fé, exige também a observâncias dos seguintes princípios (BRASIL, 2018a):

a) finalidade: o tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

b) adequação: deve haver compatibilidade entre o tratamento e com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) necessidade: o tratamento deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d) livre acesso: deve haver garantia aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

e) qualidade dos dados: aos titulares deve haver garantia de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
f) transparência: deve haver garantia aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
g) segurança: devem ser utilizadas 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;
h) prevenção: corresponde à adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
i) não discriminação: implica na impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
j) responsabilização e prestação de contas: corresponde à demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Os princípios norteadores da LGPD buscam principalmente impedir "a redução dos dados pessoais a aspecto meramente patrimonial, uma vez que priorizou claramente a sua dimensão existencial e impôs uma série de cuidados e restrições ao tratamento de dados", como se constata dos princípios previstos no art. 6º da referida lei, que não podem ser afastados nem mesmo pelo consentimento do titular (FRAZÃO, 2019, p. 35)

O consentimento do titular dos dados, no ambiente *on-line*, conforme previsão na Lei 13.709/2018, insere-se entre os principais fundamentos para o tratamento dos dados pessoais, no que se refere à proteção dos referidos dados.

Em face de sua natureza, o termo consentimento "representa aquiescência, assentimento, manifestação de vontade com vistas à produção de efeitos obrigacionais" (MULHOLLAND, 2019, p. 50).

Mesmo antes da Lei Geral de Proteção de Dados Pessoais, o consentimento do usuário era tido como um dos nortes que lastreavam legalmente a coleta, uso, armazenamento e tratamento de dados pessoais.

Nesse sentido, o art. 7º, inciso IX, da Lei 12.965/2014, ao tratar do acesso à *internet* como instrumento essencial ao exercício da cidadania, já assegurava ao usuário o "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais" (BRASIL, 2014).

O consentimento é definido no inciso XII do art. 5º da Lei 13.709/2018 como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018a).

Segundo Mulholland (2019, p. 50), "será permitido o tratamento de dados pessoais em havendo manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

O consentimento é "a base legal que tem o condão de legitimar a comunicação, difusão, interconexão e o tratamento compartilhado de dados pessoais existentes em bases públicas por entes privados, sendo, porém, dispensado nas hipóteses dos incisos I a III" do artigo 7º da Lei 13.709/2018 (TASSO, 2019, p. 114). Para compartilhamento de dados pessoais, o consentimento "deve ser específico para essa finalidade, não bastando ao controlador tê-lo colhido para outras modalidades de tratamento (art. 7º, § 5º, da LGPD)" (TASSO, 2019, p. 114).

Somente em caráter excepcional o consentimento poderá ser dispensado, como ocorre em relação aos dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na Lei 13.709/2018, conforme previsto no art. 7º, § 4º, da referida Lei.

Os dados sensíveis possuem tratamento diferenciado no âmbito da Lei Geral de Proteção de Dados Pessoais, inclusive quanto ao consentimento do titular dos dados.

A Lei 13.709/2018 define o dado pessoal sensível no art. 5º, inciso II, como o 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" (BRASIL, 2018a).

Em relação aos dados sensíveis, o art. 11, inciso I, da Lei 13.709/2018, prevê a necessidade de que o consentimento seja realizado de forma específica e destacada, inclusive para finalidades singulares. A tônica da proteção dos dados sensíveis está em se permitir uma igualdade substancial no tratamento dos dados, coibindo a discriminação e o abuso que dele podem decorrer (MULHOLLAND, 2019, p. 51).

O fundamento do consentimento qualificado para o tratamento de dados sensíveis deve-se principalmente à natureza existencial e fundamental dos conteúdos a que os dados se referem (MULHOLLAND, 2019, p. 51).

Na prática, entretanto, o modelo de consentimento do usuário previsto como regra no art. 7º, inciso I, da Lei 13.709/2018, como elemento básico para a permissão do uso de seus

dados pessoais, tem-se mostrado ineficaz, como se observa dos constantes abusos contidos nos termos de uso dos provedores e sua desconformidade com os direitos humanos (MAGRANI; OLIVEIRA, 2019, p. 83).

O Poder Público, inclusive em face do disposto na Lei 13.709/2018, exerce importantes funções em relação aos dados pessoais, seja como ente controlador, seja na coleta e tratamento dos dados.

Assim, o uso compartilhado de dados pessoais pelo Poder Público e seu compartilhamento com o ente privado "são questões de crucial importância no contexto em que o Estado, na condição de controlador, tem o dever legal de garantir a segurança aos direitos fundamentais dos titulares de dados pessoais e, em específico, o direito à privacidade como liberdade positiva" (TASSO, 2019, p. 109).

O tratamento de dados pessoais pelo Poder Público é tratado em capítulo próprio na Lei Geral de Proteção de Dados Pessoais, especificamente nos artigos 23 a 32.

5 DIREITO À AUTODETERMINAÇÃO INFORMATIVA DO TITULAR DOS DADOS

O caráter de fundamentalidade do direito à proteção de dados pessoais é destacado por Sarlet, Marinoni e Mitidiero (2013, p. 434-435), por meio do reconhecimento de diversos direitos que o integram, como o:

> direito de acesso e conhecimento dos dados pessoais existentes em registros (banco de dados) públicos e privados; o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; o direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; o direito ao conhecimento da finalidade da coleta e eventual utilização dos dados; o direito à retificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados.

O art. 17 da Lei 13.709/2018, ao dispor sobre os direitos do titular de dados pessoais, estatui que "toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade" (BRASIL, 2018a).

Diversos direitos básicos dos titulares de dados pessoais estão contemplados no art. 18 da Lei Geral de Proteção de Dados Pessoais, sem prejuízo de outros direitos que decorram do texto constitucional e do ordenamento jurídico infraconstitucional, entre os quais (BRASIL, 2018a): confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados

desnecessários, excessivos ou tratados em desconformidade com a Lei 13.709/2018; portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei 13.709/2018; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; e informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e revogação do consentimento, nos termos do § 5º do art. 8º da Lei 13.709/2018.

O direito à autodeterminação informativa, também chamado de direito à privacidade informacional, corresponde a um desdobramento do direito à privacidade (VIEIRA, 2007, p. 27).

Entre as alterações mais relevantes da Lei Geral de Proteção de Dados Pessoais, está o reconhecimento da autodeterminação informativa e da privacidade como fundamentos de proteção de dados pessoais, em especial no ambiente digital (GRESSLER; BACHINSKI; SILVA, 2019, p. 14).

Na verdade, a Lei Geral de Proteção de Dados Pessoais tem como principal objetivo "resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa" (FRAZÃO, 2019, p. 34).

No que se refere ao consentimento do titular dos dados pessoais, o direito à autodeterminação informativa, previsto no inciso II do art. 2º da Lei 13.709/2018, identifica-se como um direito e uma garantia fundamental, "na medida em que é crucial para o pleno desenvolvimento do ser humano no contexto da sociedade informacional, caracterizada pela geração, pelo processamento e pela transmissão da informação como fontes da produtividade e de poder, haja vista as novas tecnologias" (LIMA, 2019, p. 64).

Em essência, a Lei 13.709/2018 "vem assegurar ao cidadão o *direito à autodeterminação informativa* em relação a dados pessoais fornecidos a terceiros, sejam eles empresas, órgãos governamentais, partidos políticos, associações, sindicatos e até mesmo pessoas naturais" (RAMOS; NAVARRO, 2020).

Quanto aos direitos à intimidade e à vida privada relacionados à utilização de dados pessoais, o Superior Tribunal de Justiça, quando do julgamento dos Embargos de Declaração no Recurso Especial 1.630.659-DF, sufragou o seguinte entendimento a respeito da autodeterminação informativa (BRASIL, 2018b):

> os direitos à intimidade e à proteção da vida privada, diretamente relacionados à utilização de dados pessoais por bancos de dados de proteção ao crédito, consagram o direito à autodeterminação informativa e encontram guarida constitucional no art. 5º, X, da Carta Magna, que deve ser aplicado nas relações entre particulares por força de sua eficácia horizontal e privilegiado por imposição do princípio da máxima efetividade dos direitos fundamentais.

Baseada "nas ideias do princípio da dignidade da pessoa humana e dos direitos de personalidade, a noção de autodeterminação informativa deve estar muito mais atrelada ao ser humano do que ao controle da informação em si" (RUARO, 2015, p. 45).

Inter-relacionadas à autodeterminação informativa estão a liberdade e privacidade contextuais.

A liberdade contextual, segundo Lisboa (2019, p. 79), pode ser vista como como "um direito da personalidade, desdobramento do direito à privacidade e do direito à intimidade, conferindo-se ao seu titular, em tempos de sociedade da informação, o exercício de sua autodeterminação informacional".

O titular dos dados pessoais, com base no direito à privacidade contextual, tem "a confiança de que as suas informações serão eventualmente utilizadas ou, até mesmo, tratadas em conformidade com as suas legítimas expectativas, em razão da esfera social de seu relacionamento pregresso" (LISBOA, 2019, p.78).

A aplicação do princípio da finalidade previsto na Lei 13.709/2018, que vincula o tratamento de dados pessoais ao objetivo que motivou e justificou a sua coleta, "visa garantir a privacidade contextual, evitando que os dados sejam utilizados posteriormente para finalidades incompatíveis com aquela que primeiro permitiu sua coleta" (MENDES, 2019, p. 3).

Em síntese, a autodeterminação informativa, enquanto direito fundamental, "resguarda o titular dos dados contra a utilização indevida de suas informações, coibindo discriminações e controles sociais calcados em bancos de dados que não são de conhecimento do titular, tudo como corolário ao princípio da dignidade da pessoa humana" (RUARO, 2015, p. 47).

Tamanha é a importância da autodeterminação informativa, que o art. 52 da Lei Geral de Proteção de Dados Pessoais prevê a aplicação das seguintes sanções administrativas aos agentes de tratamento de dados, por infrações cometidas às normas previstas na própria lei, aplicáveis pela autoridade nacional de forma gradativa, isolada ou cumulativa, sem prejuízo da aplicação das sanções administrativas, civis ou penais previstas na Lei 8.078/1990 – Código de Defesa do Consumidor (BRASIL, 2018a):

a) advertência, com indicação de prazo para adoção de medidas corretivas;

b) 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;
c) multa diária, observado o limite total a que se refere a letra "b" acima;
d) publicização da infração após devidamente apurada e confirmada a sua ocorrência;
e) bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
f) eliminação dos dados pessoais a que se refere a infração;
g) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
h) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
i) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

O controle do tratamento dos dados e da defesa da autodeterminação informativa, além de poder ser exercido por instrumentos de tutela judicial individual, também pode ser realizado por meio de instrumentos judiciais de tutela coletiva.

A coletivização da proteção de dados pessoais, em especial através de instrumentos jurídicos de tutela coletiva, pode ser descrita por quatro elementos básicos (ZANATTA, 2019, p. 203):
a) a crescente importância da linguagem dos direitos difusos e coletivos, fazendo com que os casos sejam avaliados por uma perspectiva de violação aos valores da sociedade;
b) a forma de proteção desses direitos, que sai de uma chave clássica liberal individual de defesa dos próprios direitos, e passa a ser feita cada vez mais por entidades civis especializadas que possuem legitimidade ativa para a proposição de ações civis públicas;
c) a ampliação das obrigações relativas à proteção do ambiente informacional em uma perspectiva preventiva;
d) a redefinição das estruturas administrativas de defesa do consumidor, que passam a tratar da proteção de dados pessoais como uma questão coletiva de defesa do consumidor.

A Lei Geral de Proteção de Dados Pessoais possui profunda conexão com o Código de Defesa do Consumidor (Lei 8.078/1990) e o sistema de tutela coletiva, tendo absorvido parte da tradição da tutela coletiva no Brasil, "abrindo espaço para que a proteção dos direitos assegurados na legislação seja feita de forma coletiva, ao lado das múltiplas formas de proteção individual dos direitos" (ZANATTA, 2019, p. 205).

Ao tratar dados direitos do titular dos dados, o art. 22 da Lei 13.709/2018 dispõe que "a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva" (BRASIL, 2018a).

No que se refere à responsabilidade e ao ressarcimento de danos pelos agentes de tratamento de dados pessoais, a Lei 13.709/2018 prevê que o controlador ou o operador que, em decorrência do exercício de atividade de tratamento de dados pessoais, acarretar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (art. 42, *caput*), e que as ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* do art. 42, podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente (art. 42, § 3º) (BRASIL, 2018a).

A partir da leitura conjunta do art. 22 e do art. 42 da Lei Geral de Proteção de Dados Pessoais, de forma íntegra ao sistema jurídico brasileiro, pode-se afirmar que a legislação brasileira (ZANATTA, 2019, p. 206): permitirá em nível administrativo uma atuação repressiva, para a tutela da proteção de dados pessoais, valendo-se para tanto do microssistema de proteção dos direitos difusos; fomentará a atuação de entidades civis especializadas e do Ministério Público na tutela judicial dos direitos difusos de proteção de dados pessoais; e possibilitará o uso de instrumentos do processo civil brasileiro para interrupção de violações de direitos assegurados na Lei 13.709/2018.

6 CONCLUSÃO

A atualidade mostra o mundo envolto no desenvolvimento de novas e inimagináveis tecnologias, em especial as relacionadas à informática e à *internet*, com a criação de *softwares* bastante sofisticados e de altíssima *performance*.

O desenvolvimento tecnológico tem revolucionado as áreas da informação, comunicação e economia, em particular por meio da coleta, armazenamento, tratamento e divulgação de dados das pessoas, principalmente por empresas e corporações.

Os reflexos dos avanços da tecnologia da informação e do desenvolvimento da *internet* são incomensuráveis, como ocorre em relação à economia, em especial no tocante à economia digital.

As pessoas passaram a ter seus dados pessoais normalmente armazenados e tratados em bancos de dados, inclusive por meios digitais, sem que haja prévio conhecimento ou consentimento do titular dos dados sobre referidas atividades.

Todavia, a coleta, tratamento e compartilhamento sem limites dos dados pessoais acaba expondo a riscos os indivíduos titulares dos dados, em especial no que se refere ao direito à privacidade.

Objetivando a preservação do direito fundamental à privacidade, o ambiente social no qual se concretiza a ideia de privacidade informacional deve contemplar instrumentos para efetiva proteção dos direitos da pessoa em manter o controle sobre seus dados, por meio de sua autodeterminação informativa.

No Brasil, a Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018, inspirada no Regulamento Geral para Proteção de Dados europeu, adota as premissas e fundamentos necessários para que a proteção dos dados seja efetivo instrumento de preservação dos direitos fundamentais.

A Lei 13.709/2018, que deve ser observada pela União, Estados, Distrito Federal e Municípios, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o fim de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Ao tratar dos direitos do titular de dados pessoais, o art. 17 da Lei 13.709/2018 estabelece que toda pessoa natural tem assegurada a titularidade de seus dados pessoais, assim como garantidos os direitos fundamentais de liberdade, intimidade e privacidade.

O direito à autodeterminação informativa, também conhecido como direito à privacidade informacional, constitui um dos fundamentos da Lei Geral de Proteção de Dados Pessoais.

A autodeterminação informativa, como direito fundamental, resguarda o titular dos dados contra a utilização indevida de suas informações, vedando discriminações e controles baseados em bancos de dados que não sejam do conhecimento ou que não tenham sido consentidos pelo respectivo titular.

Tem-se, em conclusão, que restou comprovada a hipótese inicial, no sentido de que a Lei 13.709/2018 atribui à pessoa o direito fundamental à autodeterminação informativa, relativamente à coleta, armazenamento e tratamento de seus dados pessoais por pessoas físicas, jurídicas ou entes governamentais.

REFERÊNCIAS

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 abr. 2020.

BRASIL. **Lei 13.709, de 14 de agosto de 2018a**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 24 abr. 2020.

BRASIL. Superior Tribunal de Justiça. Embargos de Declaração no Recurso Especial 1.630.659-DF. Relatora Ministra Nancy Andrighi. Brasília: **DJe**, 06 dez. 2018b. Disponível em: https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=90337964&tipo=5&nreg=201602636727&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20181206&formato=PDF&salvar=false. Acesso em: 24 ago. 2020.

COMITÊ GESTOR DA INTERNET NO BRASIL. O que é big data? **Revista.br**, Brasília, ano 4, n. 5, p. 22, nov. 2013. Disponível em: https://www.cgi.br/media/docs/publicacoes/3/cgibr-revistabr-ed5.pdf. Acesso em: 25 abr. 2020.

CUEVA, Ricardo Villas Bôas. Proteção de dados pessoais no Judiciário. **Revista do Advogado**, São Paulo, n. 144, p. 134-139, nov. 2019.

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

FRAZÃO, Ana. Direitos básicos dos titulares de dados pessoais. **Revista do Advogado**, São Paulo, n. 144, p. 33-46, nov. 2019.

GRESSLER, Igor Costa; BACHINSKI, Fabiane Leitemberger; SILVA, Rosane Leal da. A divulgação indevida de informações pessoais em site de universidade gaúcha: resposta jurisdicional entre a óptica constitucional e os princípios da Lei n. 13.709/2018. **Anais do 5º Congresso Internacional de Direito e Contemporaneidade**, Santa Maria, UFSM, p. 1-16, set. 2019.

INSTITUTO TELECOM. Ministério Público Federal: OI tem de interromper vazamento de dados sigilosos de consumidores. Disponível em: http://www.institutotelecom.com.br/ministerio-publico-federal-oi-tem-de-interromper-vazamento-de-dados-sigilosos-de-consumidores/. Acesso em: 24 ago. 2020.

LEONARDI, Marcel. Legítimo interesse. **Revista do Advogado**, São Paulo, n. 144, p. 67-73, nov. 2019.

LIMA, Cíntia Rosa Pereira de. Consentimento inequívoco *versus* expresso: o que muda com a LGPD? **Revista do Advogado**, São Paulo, n. 144, p. 60-66, nov. 2019.

LISBOA, Roberto Senise. Boa-fé e confiança na Lei Geral de Proteção de Dados brasileira. **Revista do Advogado**, São Paulo, n. 144, p. 74-79, nov. 2019.

MAGRANI, Eduardo; OLIVEIRA, Renan Medeiros de. A internet das coisas e a Lei Geral de Proteção de Dados: reflexões sobre os desafios do consentimento e do direito à explicação. **Revista do Advogado**, São Paulo, n. 144, p. 80-89, nov. 2019.

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

MENDES, Laura Schertel. Privacidade e dados pessoais: proteção de dados pessoais: fundamento, conceitos e modelos de aplicação. **Panorama Setorial da Internet**, n. 2, ano 11, p. 1-7, jun. 2019.

MIRANDA, Leandro Alvarenga. **A proteção de dados pessoais e o paradigma da privacidade**. São Paulo: All Print Editora, 2018.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**, São Paulo, n. 144, p. 47-53, nov. 2019.

ONU. **Declaração Universal dos Direitos Humanos - 1948**. Disponível em: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 23 abr. 2020.

QUEIROZ, Rafael Mafei Rabelo. Direito à privacidade e proteção de dados pessoais: aproximações e distinções. **Revista do Advogado**, São Paulo, n. 144, p. 15-21, nov. 2019.

RAMOS, Gustavo; NAVARRO, Luiz. **A LGPD no Brasil e o direito à autodeterminação informativa na era digital**. Disponível em: https://www.conjur.com.br/2020-abr-07/entrada-vigor-lgpd-brasil-direito-autodeterminacao-informativa-digital. Acesso em: 31 ago. 2020.

REMEDIO, José Antonio; REIS, Jordana. Direito à intimidade versus direito à liberdade de expressão: publicação não autorizada de biografia de pessoa pública ou famosa. **Meritum**, Belo Horizonte, v. 13, n. 2, p. 109-130, jul./dez. 2018.

REMEDIO, José Antonio; SILVA, Marcelo Rodrigues da. O uso monopolista do Big Data por empresas de aplicativos: políticas públicas para um desenvolvimento sustentável em cidades inteligentes em um cenário de economia criativa e de livre concorrência. **Revista Brasileira de Políticas Públicas**, Brasília, v. 77, n. 3, p. 671-693, 2017.

RIELLI, Mariana Marques. O processo de construção e aprovação da Lei Geral de Dados Pessoais: bases legais para tratamento de dados em um debate multissetorial. **Revista do Advogado**, São Paulo, n. 144, p. 7-14, nov. 2019.

RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina, v. 2, n. 1, p. 41-60, jan./jun. 2015.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIEIRO, Daniel. **Curso de direito constitucional**. 2. ed. São Paulo: Revista dos Tribunais, 2013.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: Malheiros, 2017.

SIQUEIRA JUNIOR. Paulo Hamilton. **Teoria do direito**. São Paulo: Saraiva, 2009.

SPALER, Mayara Guibor; REIS, Rafael Almeida Oliveira. Limites do direito fundamental à privacidade frente a uma sociedade conectada. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, Curitiba, a. 3, n. 3, dez. 2018. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista_esa_8_11.pdf. Acesso em: 24 ago. 2020

TASSO, Fernando Antonio. Compartilhamento de dados entre o setor público e privado: possibilidades e limites. **Revista do Advogado**, São Paulo, n. 144, p. 107-116, nov. 2019.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre: Sergio Antonio Fabris Editor, 2007.

ZANATTA, Rafael A. F. A tutela coletiva na proteção de dados pessoais. **Revista do Advogado**, São Paulo, n. 144, p. 201-208, nov. 2019.