

I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

AIRES JOSE ROVER

FABIANO HARTMANN PEIXOTO

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Napolini - UNIVEM/FMU - São Paulo

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade - UNIMAR/FEPODI - São Paulo

Conselho Fiscal:

Prof. Dr. Caio Augusto Souza Lara - ESDHC - Minas Gerais

Prof. Dr. João Marcelo de Lima Assafim - UCAM - Rio de Janeiro

Prof. Dr. José Filomeno de Moraes Filho - Ceará

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Prof. Dr. Valter Moura do Carmo - UNIMAR - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Daniela Marques De Moraes - UNB - Distrito Federal

Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM - São Paulo

Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie - São Paulo

Comunicação:

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - Paraíba

Prof. Dr. Matheus Felipe de Castro - UNOESC - Santa Catarina

Relações Internacionais para o Continente Americano:

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Relações Internacionais para os demais Continentes:

Prof. Dr. José Barroso Filho - ENAJUM

Prof. Dr. Rubens Beçak - USP - São Paulo

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - Paraná

Eventos:

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - Minas Gerais

Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC - Paraná

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - Mato Grosso do Sul

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UMICAP - Pernambuco

D597

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

Coordenadores: Danielle Jacon Ayres Pinto

Aires Jose Rover

Fabiano Hartmann Peixoto – Florianópolis: CONPEDI, 2020.

Inclui bibliografia

ISBN: 978-65-5648-086-2

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, cidades e crise

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. I Encontro Virtual do CONPEDI (1: 2020 : Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O I ENCONTRO VIRTUAL DO CONPEDI, ocorrido entre os dias 23 e 30 de junho de 2020, foi realizado exclusivamente a partir da utilização das novas tecnologias de informação e comunicação. Foi o maior sucesso nesses tempos de pandemia. Mais do que nunca se viu a tecnologia servindo como instrumento de ação no campo do conhecimento e da aprendizagem, o que este GT sempre defendeu e esteve atento discutindo os limites e vantagens dessa utilização. Os artigos apresentados, como não podia deixar de ser, mostraram que os temas relacionados às novas tecnologias estão cada vez mais inseridos na realidade jurídica brasileira e mundial. Diversos fenômenos do cenário digital foram abordados ao longo dos trabalhos e demonstraram que a busca por soluções nessa esfera só pode ser pensada de forma multidisciplinar.

Assim, vejamos as principais temáticas tratadas, em sua sequência de apresentação no sumário e apresentação no GT. No primeiro bloco temático temos:

- marco civil da internet no brasil
- proteção de dados pessoais do trabalhador
- governança de dados aplicada a big data analytics
- consentimento do titular dos dados
- princípios da lei geral de proteção de dados
- blockchain e LGPD

No segundo bloco:

- inteligência artificial, bots e sexismo
- inteligência artificial para melhoria do judiciário
- danos causados por veículos autônomos

- implicações éticas
- direitos da personalidade
- reconhecimento facial

No terceiro bloco:

- Peter Häberlee a democracia digital
- constitucionalismo digital
- inclusão digital e inclusão social
- democracia participativa

No quarto e último bloco:

- deepweb e a (in)segurança dos cidadãos
- criptoativos e soberania tradicional
- fakenews e direito à saúde
- intimações judiciais na internet
- aplicativo uber

Com esses estudos de excelência os coordenadores desse grupo de trabalho convidam a todos para a leitura na íntegra dos artigos.

Aires José Rover –UFSC

Fabiano Hartmann Peixoto - Universidade de Brasília

Danielle Jacon Ayres Pinto – IMM/ECEME e UFSC

Nota técnica: O artigo intitulado “Marco civil da internet no Brasil: conquistas e desafios” foi indicado pelo PPGD/UNIVEM, nos termos do item 5.1 do edital do Evento.

Os artigos do Grupo de Trabalho Direito, Governança e Novas Tecnologias II apresentados no I 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 8.1 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 (LEI 13.709/2018): O
CONSENTIMENTO DO TITULAR DOS DADOS PARA O TRATAMENTO DE
SEUS DADOS PESSOAIS**

**NATIONAL LAW OF DATA PROTECTION (LAW 13.709/2018): THE CONSENT
OF THE DATA OWNER FOR THE MANIPULATION OF HIS PERSONAL DATA**

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

Resumo

Os dados pessoais dos usuários da internet são normalmente armazenados em bancos de dados, inclusive para fins de comercialização dos dados, sem seu prévio conhecimento ou consentimento. A pesquisa tem por objeto analisar a necessidade de exigência de consentimento pelo titular para o tratamento de seus dados pessoais, com fundamento na Lei Geral de Proteção de Dados Pessoais. O método utilizado é o hipotético-dedutivo, com base na legislação, doutrina e jurisprudência. Conclui que o consentimento do titular dos dados, exceto nos casos previstos na legislação, é condição necessária para a validade do tratamento de seus dados pessoais.

Palavras-chave: Banco de dados, Dados pessoais, Lei geral de proteção de dados, Proteção de dados pessoais, Tratamento de dados pessoais

Abstract/Resumen/Résumé

Internet users personal data are usually stored in online databased, including for the purpose of marketing, without their prior knowledge or consent. The research aims to analyze the need of expressly consent by the owner for the manipulation of his personal data, based on the National Law of Data Protection. The method used is the hypothetical-deductive, based on legislation, doctrine and jurisprudence. It is concluded that the owner consent, except in cases provided for in the legislation, is a necessary condition for the validity of the manipulation of his personal data.

Keywords/Palabras-claves/Mots-clés: Database, Personal data, National law of data protection, Personal data protection, Personal data manipulation

¹ 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

² Mestre em Ciência da Computação pela UNESP. Professor do Centro Universitário Hermínio Ometto de Araras. Professor do Centro Universitário Adventista de São Paulo. ensino@tiagoremedio.com.br

³ 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

INTRODUÇÃO

Os avanços tecnológicos obtidos em âmbito planetário no século XX, o crescente processo de globalização do planeta e o desenvolvimento de instrumentos como a internet, possibilitaram a difusão da informação e da comunicação de forma generalizada, como jamais se poderia imaginar em tempos pretéritos.

O século XXI, que nasce sob a égide da era da informação, apresenta o surgimento de uma sociedade em rede, na qual os avanços da tecnologia da informação e comunicação geram importantes reflexos sociais (REMEDIO; SILVA, 2017, p. 673).

Marcada pelo aumento expressivo da capacidade de produzir dados dos mais variados tipos, com a ampliação e expansão do acesso à internet, a era da informação multiplicou de forma inimaginável o potencial de difusão do volume de conteúdo de dados produzidos, fenômeno esse que passou a ser amplamente debatido, em especial pela mídia especializada em tecnologia, por meio da utilização da expressão *Big Data*.

O compartilhamento da informação, ínsito à era 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).

Todavia, apesar de indispensável à sociedade da informação, o compartilhamento de dados precisa ser delimitado, havendo para tanto diversas ordens de razões, dentre as quais, as humanas (como a preservação do direito à privacidade) e as econômicas (pois a falta de limites do compartilhamento de dados implicaria numa menos valia da informação) (LISBOA, 2019, p.76).

A evolução tecnológica atual, se, de um lado, amplia as possibilidades de desenvolvimento para o indivíduo, de outro lado, também implica em enormes riscos para a pessoa, em especial no tocante a seu direito de privacidade e intimidade.

Os avançados sistemas de informação 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” (SILVA, 2015, p. 218).

Nesse contexto, os dados dos diversos dispositivos 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 tem ainda plena consciência” (MAGRANI; OLIVEIRA, 2019, p. 82).

No Brasil, em 2018 foi promulgada a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), dispondo sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Ao tratar dos direitos do titular de dados pessoais, o art. 17 da Lei 13.1709/2018 dispõe 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 termos da própria lei (BRASIL, 2018a).

A Lei Geral de Proteção de Dados Pessoais dá especial ênfase à necessidade de consentimento dos usuários para a coleta, uso e tratamento dos dados pessoais coletados pelos sistemas de informação.

Como problema, indaga-se se é possível a convivência com a evolução tecnológica, no que se refere ao tratamento dos dados pessoais, e a preservação dos direitos do titular dos dados, no tocante à preservação de seus direitos, como a privacidade e a intimidade.

A pesquisa tem por objeto analisar a necessidade de exigência de consentimento pelo titular dos dados para o tratamento de seus dados pessoais, com fundamento na Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

No que concerne à estrutura, a pesquisa tem início com a análise da evolução legislativa da proteção do tratamento dos dados pessoais no Brasil e do direito à privacidade. Em seguida, trata da coleta e tratamento de dados pessoais com base na Lei 13.709/2018. Por fim, analisa o consentimento do titular dos dados no tratamento de seus dados pessoais, conforme previsto na Lei Geral de Proteção de Dados Pessoais.

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

Tem-se, como hipótese, que o consentimento do titular dos dados, exceto nos casos previstos na legislação, é condição necessária para a validade do tratamento de seus dados pessoais e preservação de seus direitos constitucionais.

1 EVOLUÇÃO LEGISLATIVA DA PROTEÇÃO DOS DADOS PESSOAIS E DIREITO À PRIVACIDADE

A legislação brasileira, tanto constitucional como infraconstitucional, é bastante expressiva no tocante à proteção dos direitos à privacidade e à informação.

A proteção do direito à privacidade, à intimidade e à informação está prevista de forma bastante ampla na Constituição Federal de 1988, como se constata, entre outros, nos seguintes dispositivos normativos (BRASIL, 1988):

Art. 5º (...)

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;

XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

LXXII - conceder-se-á habeas data:

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

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

Na órbita infraconstitucional, mesmo antes do advento da Lei Geral de Proteção de Dados Pessoais (LGPD), diversas leis especiais tratavam e ainda tratam da questão relativa à proteção de dados pessoais, como o Código de Defesa do Consumidor – CDC (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 - MCI (Lei 12.965/2014).

Nesse sentido, o Código de Defesa do Consumidor possui uma seção específica para disciplinar a matéria concernente aos bancos de dados e cadastros de consumidores. Em conformidade com o disposto no art. 43 do Código de Defesa do Consumidor (Lei 8.078/1990), o consumidor, sem prejuízo do disposto no art. 86 da própria lei, 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 (BRASIL, 1990).

A Lei do Cadastro Positivo (Lei 12.414/2011), sem prejuízo do disposto na Lei 8.078/1990, dispõe sobre a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

A Lei 12.527/2011 disciplina os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, objetivando garantir o acesso a informações previsto no inciso XXXIII do art. 5º, inciso II do § 3º do art. 37 e § 2º do art. 216 da Constituição Federal. O tratamento das informações pessoais está disciplinado em Seção própria da Lei

12.527/2011 e, nos termos do art. 31 da referida lei, deve ser feito de forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais, observando-se, em relação às informações pessoais relativas à intimidade, vida privada honra e imagem, o seguinte (BRASIL, 2011):

- a) terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos, a contar da data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem;
- b) poderão ter autorizada sua divulgação ou acesso por terceiros em face de previsão legal ou consentimento expresso da pessoa a que elas se referirem, não se exigindo o consentimento quando as informações forem necessárias.
- c) aquele que obtiver acesso às informações será responsabilizado por seu uso indevido.

A Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, dispõe sobre a tipificação criminal de delitos informáticos, tendo inserido no Código Penal diversos tipos penais inerentes à matéria.

Por sua vez, o Marco Civil da Internet (Lei 12.965/2014) 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 matéria.

O Marco Civil da Internet contempla um “microssistema de proteção de dados pessoais” no ambiente *on-line*, tendo como principal base legal 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). Trata-se a Lei 12.965/2014 “de um verdadeiro *miniestatuto-microssistema* que estabelece, por vezes de maneira detalhada, regras que governam fluxo de informações pessoais no ambiente eletrônico” (BIONI, 2019, p. 223).

A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como, dentre outros fundamentos, a proteção dos dados pessoais, na forma da lei, conforme disposto no art. 2º, inciso III, da Lei 12.965/2014. A lei em questão, no art. 7º, inciso VII, inclui entre os direitos e garantias dos usuários, o “não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei” (BRASIL, 2015).

Ainda, o Marco Civil da Internet, sem prejuízo de outras referências no texto legal, trata em seção própria (Seção II, arts. 10 a 17), da proteção aos registros, aos dados pessoais e às comunicações privadas.

Assim, como visto, diversas leis brasileiras foram editadas e ainda estão em vigor, embora sem caráter geral, objetivando o controle e o tratamento de dados, inclusive pessoais, como as Leis 8.078/1990, 12.414/2011, 12.527/2011, 12.737/2012 e 12.965/2014.

O marco comum para o início do debate sobre uma lei geral de proteção de dados no Brasil foi a submissão do primeiro anteprojeto de lei do Poder Executivo à consulta pública, fato esse que se verificou em dezembro de 2010. O diagnóstico que informou o anteprojeto foi a que “a ausência de uma regulação geral de proteção de dados pessoais, além de colocar o Brasil em uma posição de completo descompasso com outros países, causava um duplo efeito: a um só tempo, desprotegia o cidadão contra o uso abusivo de seus dados pessoais e criava um cenário de insegurança jurídica pela ausência de regras padronizadas para os mais diversos setores que tratam dados” (RIELLI, 2019, p. 8). 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).

Em 2012 foi proposto o Projeto de Lei 4.060/2012. Em 2014 foram apresentados dois novos projetos de lei, ambos do Senado Federal, ou seja, os Projetos de Lei 131/2014 e 330/2013.

Em 2016, quando foi apresentado o Projeto de Lei 5.276/2016, que deu origem à Lei 13.709/2018, o texto consolidado do Poder Executivo estava assentado em nove bases legais, com destaques ao consentimento e ao legítimo interesse (RIELLI, 2019, p. 11).

A Lei 13.709/2018, intitulada Lei Geral de Proteção de Dados Pessoais (LGPD), cuja *vacatio legis* foi prorrogada até 3 maio de 2021 pela Medida Provisória 959/2020, possui caráter de norma geral, de interesse nacional, 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 (BRASIL, 2018a).

No que se refere à liberdade, embora inexista uniformidade de pensamento a respeito, o conceito de liberdade humana “consiste na possibilidade de coordenação consciente dos meios necessários à realização da felicidade pessoal” (SILVA, 2015, p. 235).

O direito à privacidade, por sua vez, corresponde ao direito de ser deixado em paz, ou seja, implica na proteção de uma esfera autônoma da vida privada (SARLET; MARINONI; MITIDIERO, 2013, p. 456).

A Constituição Federal de 1988 consagrou o direito à privacidade, “tomada essa expressão em sentido amplo para abranger todas as manifestações da esfera íntima, privada e da personalidade das pessoas” (CUNHA JÚNIOR, 2009, p. 678).

O Superior Tribunal de Justiça, ao julgar os Embargos de Declaração no Recurso Especial 1.630.659-DF, sufragou o entendimento no sentido de que (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.

O direito à proteção de dados, segundo Cíntia Rosa Pereira de Lima (2019, p. 61), decorre do direito geral de personalidade (CF, art. 1º, III, e CC/2002, art. 11), ou seja, é “caracterizado como um direito autônomo que garante ao seu titular exercer o controle sobre a coleta, o armazenamento, o tratamento e o compartilhamento de seus dados”.

2 COLETA E TRATAMENTO DE DADOS PESSOAIS NA LEI 13.709/2018

Os sistemas de inteligência artificial que movem a economia digital “são programados para produzirem inferências e previsões, com as quais se pode classificar as pessoas e, a partir daí, determinar os seus destinos, acessos a direitos e oportunidades”, embora referidas modificações não se restrinjam à economia, pois também implicam em consequências para a política, a sociedade e as próprias dimensões existenciais dos cidadãos (FRAZÃO, 2019, p. 34).

A economia moderna, independentemente de ramo de atividade, setor empresarial ou de modelos de negócios específicos, transformou-se em uma economia baseada 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).

Uma vez que se caminha na atualidade para uma sociedade governada por dados, o ambiente social no qual se concretiza a ideia de privacidade informacional “passa a ser qualificado pela proteção dos direitos da pessoa de manter o controle sobre seus dados, por meio de sua autodeterminação informativa (liberdade), visando à não discriminação” ou igualdade (MULHOLLAND, 2019, p. 53).

O potencial vulnerante aos direitos fundamentais do indivíduo que o inadequado tratamento de dados pode ocasionar, é o propulsor do surgimento das diversas regulações protetivas no que concerne ao tratamento de dados pessoais por entes públicos e privados (TASSO, 2019, p. 116).

Especialmente quanto ao desenvolvimento europeu, a legislação acabou definindo com maior precisão tanto o objetivo específico do direito à proteção de dados como os direitos conferidos ao respectivo titular de dados. O objeto relevante do direito à proteção de dados é o “dado pessoal”, ou seja, “qualquer informação relacionada à pessoa natural identificada ou identificável, processada em bancos de dados ou cadastro, ainda que ela não seja particularmente sensível à privacidade desta pessoa” (QUEIROZ, 2019, p. 19).

Inspirada no Regulamento Geral Europeu de Proteção de Dados (GDPR), a Lei Geral de Proteção de Dados Pessoais Brasileira (Lei 13.709/2018) “busca, em poucas palavras, garantir a um só tempo o reconhecimento de direito fundamental à proteção dos dados pessoais e a regulação do tratamento destes dados pelos mais diversos agentes” (MULHOLLAND, 2019, p. 48).

No Brasil, a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, objetivando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, e estatui que a disciplina da proteção de dados pessoais tem 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.

A Lei Geral de Proteção de Dados Pessoais possui natureza jurídica essencialmente principiológica e conceitual, tendo o art. 5º da referida lei especificado diversos conceitos necessários para a compreensão dos termos nela expressados (MULHOLLAND, 2019, p. 48).

O art. 5º da Lei 13.709/2018 apresenta uma série de conceitos e atribuições de responsabilidades das organizações que atuam na coleta e uso de dados pessoais digitais, dentre os quais, os conceitos de dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, controlador, operador, anonimização, consentimento e uso compartilhado de dados (BRASIL, 2018a).

A Lei Geral de Proteção de Dados Pessoais teve como objetivo central resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa. Seu objetivo foi conferir ampla proteção ao cidadão no tocante ao tratamento de dados, podendo-se afirmar, inclusive, “que a proteção de dados corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante (FRAZÃO, 2019, p. 34).

Para Patrícia Peck Pinheiro (2018, p. 16):

O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis.

As atividades de tratamento de dados pessoais, conforme previsto no art. 6º da Lei Geral de Proteção dos Dados Pessoais, devem observar a boa-fé e também os 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.

A prevenção também se insere entre os princípios norteadores da Lei Geral de Proteção de Dados Pessoais, em especial quanto à proteção da privacidade. Nesse sentido, de acordo com Viviane Maldonado e Renato Ópice Blum (2019, p. 158):

A prevenção esperada no princípio ora analisado deve ser pautada no conceito *Privacy by Design (PbD)*, de Ann Cavoukian, pelo qual a proteção à privacidade advém da trilogia (i) sistemas de tecnologia da informação (*IT system*); (ii) práticas negociais responsáveis (*accountable business practices*); e (iii) *design* físico e infraestrutura de rede (*physical and network infrastructure*).

Todavia, importante destacar que a existência de diversos princípios que regem as atividades de tratamento de dados pessoais não infirma a assertiva no sentido de que referidos dados também são vistos como bens jurídicos, assim como não implica em negar que há desdobramentos patrimoniais dos dados, que, inclusive, podem ser objeto de negociação. O que os princípios da Lei Geral de Proteção de Dados Pessoais buscam impedir “é 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).

Ao tratar dos direitos do titular de dados pessoais, o art. 17 da Lei 13.709/2018 dispõe 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).

Por sua vez, o art. 18 da Lei 13.709/2018 prevê uma série de direitos básicos dos titulares de dados pessoais, sem prejuízo de outros que decorrem do texto constitucional e do ordenamento jurídico infraconstitucional, dentre os quais (BRASIL, 2018a): confirmação da existência de tratamento; o acesso aos dados; correção de dados incompletos, inexatos ou

desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; 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 LGPD; 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 LGPD.

O direito à autodeterminação informacional previsto no art. 2º, II, da Lei 13.709/2018, consubstanciado no consentimento do titular dos dados pessoais, ressalvadas as hipóteses legais de dispensa, é considerado um direito e 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).

3. O CONSENTIMENTO DO TITULAR PARA O TRATAMENTO DE SEUS DADOS PESSOAIS

O termo consentimento “representa aquiescência, assentimento, manifestação de vontade com vistas à produção de efeitos obrigacionais” (MULHOLLAND, 2019, p. 50).

O consentimento do titular dos dados é um dos instrumentos que fundamentam legalmente a coleta, uso e tratamento de dados pessoais, nos termos da Lei Geral de Proteção de Dados Pessoais.

Todavia, mesmo antes da Lei 13.709/2018, o Marco Civil da Internet (Lei 12.965/2014), ao disciplinar o acesso à internet como instrumento essencial ao exercício da cidadania, já assegurava ao usuário, no art. 7º, inciso IX, 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 art. 5º, inciso XII, da Lei 13.709/2018 (LGPD) define o consentimento 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).

A comparação entre as leis citadas, ao menos numa análise preliminar, permite concluir que há aparente conflito de normas, uma vez que, enquanto o Marco Civil da Internet

refere-se no art. 7º, inciso IX, a “consentimento expresso”, a Lei Geral de Proteção de Dados Pessoais refere-se no art. 5º, inciso XII, a “manifestação livre, informada e inequívoca”.

Entretanto, o conflito em questão é apenas aparente, uma vez que a Lei 13.709/2018, como norma posterior e especial em relação ao tratamento dos dados pessoais, prevalece em relação ao Marco Civil da Internet, norma essa anterior e de caráter mais geral, que trata dos princípios, garantias, direitos e deveres para o uso da internet no Brasil (LIMA, 2019, p. 63).

A fim de que o tratamento de dados pessoais possa ser realizado, é imprescindível que haja uma finalidade determinada, uma justificativa, as razões pelas quais o dado precisa ser coletado, armazenado e qual a sua necessidade, pois, além de serem protegidos, é necessário que haja o consentimento do titular dos dados, que por sua vez terá acesso a qualquer dado existente a seu respeito, bem como poderá solicitar sua exclusão (GREGORI, 2020, p. 7).

Contudo, a LGPD, no art. 5º, inciso XII, exige, como regra geral, expressiva fundamentação no consentimento do titular de dados para admitir o tratamento dos dados pessoais, isso significando “que 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” (MULHOLLAND, 2019, p. 50).

A premissa estabelecida na Lei Geral de Proteção de Dados Pessoais segue a tendência de exigir o consentimento livre, informado e inequívoco do titular para o tratamento de seus dados pessoais, como se vislumbra no art. 2º, inciso II e no art. 5º, inciso XII, ambos da Lei 13.709/2018 (MOURA; ANDRADE, 2019, p. 122).

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 LGPD (TASSO, 2019, p. 114).

No que toca ao 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).

Embora em regra o consentimento do usuário seja condição necessária para a coleta, uso e tratamento dos dados pessoais, a Lei Brasileira de Proteção de Dados Pessoais prevê algumas exceções em relação à sua exigência.

Nesse sentido, o consentimento do titular dos dados pode ser dispensado nas hipóteses previstas no art. 7º, incisos II a X, da Lei Geral de Proteção de Dados Pessoais, como para a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII), para a tutela

da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (inciso VIII).

Por outro lado, os dados sensíveis são tratados de forma diferenciada na Lei Geral de Proteção de Dados Pessoais, inclusive no que concerne ao consentimento pelo titular dos dados.

O dado pessoal sensível é definido no inciso II do art. 5º da LGPD 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).

Contudo, importante destacar que a definição legal de dado pessoal sensível é meramente exemplificativa, e não taxativa ou exaustiva, uma vez que a lei enumera apenas algumas das hipóteses em que serão identificados os dados pessoais que tenham natureza considerada sensível (MULHOLLAND, 2019, p. 48).

No que se refere aos dados sensíveis, o art. 11, inciso I, da Lei 13.709/2018 estabelece a necessidade de que o consentimento seja realizado de forma específica e destacada, inclusive para finalidades específicas.

A tônica da proteção dos dados sensíveis está em permitir uma igualdade substancial no tratamento dos dados, proibindo a discriminação e o abuso que dele podem decorrer. O fundamento do consentimento qualificado para o tratamento de dados sensíveis deve-se sobretudo à natureza existencial e fundamental dos conteúdos a que se referem (MULHOLLAND, 2019, p. 51).

Importante o consentimento seja extremamente importante no que concerne ao tratamento dos dados pessoais, destacam Eduardo Magrani e Renan Medeiros de Oliveira (2019, p. 83), que o modelo de consentimento do usuário previsto como regra no art. 7º, inciso I, da Lei 13.709/2018, como elemento central para a permissão do uso de seus dados pessoais, tem-se mostrado ineficaz na prática ou realidade, como se constata de recorrentes abusos contidos nos termos de uso dos provedores e sua desconformidade com os direitos humanos.

CONCLUSÃO

A era da informação, característica marcante do início do século XXI, é identificada pelo surgimento de uma sociedade em rede, em que os avanços da tecnologia da informação e comunicação geram importantes reflexos para o indivíduo, a sociedade e o Estado.

A ampliação, expansão e desenvolvimento do acesso à internet ampliaram de forma inimaginável a celeridade e o potencial de difusão do volume de conteúdo de dados produzidos em nível nacional e internacional.

A evolução tecnológica das últimas décadas, se, de um lado, significa a ampliação das possibilidades de desenvolvimento para o indivíduo, de outro lado, implica em enormes riscos para a pessoa titular dos dados pessoais, em especial quanto a seu direito à privacidade e à intimidade.

O compartilhamento da informação, inerente à era da informação e oriundo da tecnologia informacional, embora apresente riscos a direitos dos usuários, como privacidade e intimidade, também é bastante estimulado, uma vez a coletividade em rede permite a redução espacial e temporal de interações sociais.

O fenômeno relacionado ao tratamento e controle dos dados dos titulares dos dados não é apenas brasileiro, mas também abrange todo o planeta.

Especificamente no Brasil, em 2018 foi promulgada a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), dispondo sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A Lei 13.709/2018, ao tratar dos direitos do titular de dados pessoais, estatui que toda pessoa natural tem assegurada a titularidade de seus dados pessoais, bem como garantidos os direitos fundamentais de liberdade, intimidade e privacidade.

O consentimento dos usuários para a coleta, uso e tratamento de seus dados pessoais coletados pelos sistemas de informação constitui uma exigência expressamente prevista na Lei Geral de Proteção de Dados Pessoais, somente excepcionado nos casos previstos na própria lei.

A Lei 13.709/2018, ao tratar dos princípios e direitos e direitos dos titulares dos dados, e ao estabelecer uma série de limites em relação ao tratamento dos dados, torna possível a convivência entre a evolução tecnológica consubstanciada no tratamento de dados pessoais e a preservação dos direitos do titular dos dados no que tange à preservação de seus direitos, como a privacidade e a intimidade

Tem-se, em conclusão, que o consentimento do titular dos dados previsto na Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), exceto nos casos previstos na legislação, é condição necessária para a validade do tratamento de seus dados pessoais e preservação de seus direitos constitucionais, em especial os direitos fundamentais à privacidade e à intimidade.

REFERÊNCIAS

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

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 30 abr. 2020.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078.htm. Acesso em: 30 abr. 2020.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 30 abr. 2020.

BRASIL. **Lei n. 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/112965.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**, 6 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 abr. 2020.

CUNHA JÚNIOR. Dirley da. **Curso de direito constitucional positivo**. 3. ed. Salvador: JusPodvim, 2009.

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

GREGORI, Maria Stella. Os impactos da Lei Geral de Proteção de Dados Pessoais na saúde suplementar. **Revista de Direito do Consumidor**, v. 127, jan./fev. 2020, p. 171-196.

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

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

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

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, nov. 2019, p. 80-89.

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

MOURA, Plínio Rebouças de; ANDRADE, Diogo de Calasans Melo. **Revista de Direito, Governança e Novas Tecnologias**, Goiânia, v. 5, n. 1, p. 110-133, jan./jun. 2019.

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

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018.

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

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, 2017, p. 671-693.

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, nov. 2019, p. 7-14.

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**. 38. ed. São Paulo: Malheiros, 2015.

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