I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

AIRES JOSE ROVER

FABIANO HARTMANN PEIXOTO

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 integra 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.

PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS: DESENVOLVIMENTO NORMATIVO NO BRASIL E ANÁLISE CONCEITUAL

PRINCIPLES OF THE GENERAL DATA PROTECTION LAW: NORMATIVE DEVELOPMENT IN BRAZIL AND CONCEPTUAL ANALYSIS

Renata Duval Martins

Resumo

O presente artigo tem por escopo realizar o apanhado histórico das normas que precederam a redação da Lei Geral de Proteção de Dados, bem como a conceituação dos princípios que fundamentam a referida lei e dos princípios arrolados no artigo 6º desta norma. Demonstra-se a gradual construção da proteção de dados no Brasil e a importância do sistema protetivo. Ademais, expõe-se a intrínseca relação entre as normas esparsas e a recente norma específica, a Lei nº 13.709/2018, que ainda carece de profunda análise doutrinária.

Palavras-chave: Lei geral de proteção de dados, Sistema de proteção de dados, Normas nacionais, Princípios

Abstract/Resumen/Résumé

The purpose of this article is to provide a historical overview of the rules that preceded the drafting of the General Data Protection Law, as well as the conceptualization of the principles that underlie that law and the principles listed in article 6 of this standard. The gradual construction of data protection in Brazil and the importance of the protective system are demonstrated. Furthermore, the intrinsic relationship between the sparse norms and the recent specific norm, Law No. 13,709 / 2018, is exposed, which still lacks deep doctrinal analysis.

Keywords/Palabras-claves/Mots-clés: General data protection law, Data protection system, National standards, Principles

INTRODUÇÃO

O presente artigo aborda os antecedentes históricos normativos da Lei Geral de Proteção de Dados no Brasil, os princípios que fundamentam esta norma e os princípios contidos no rol exemplificativo do artigo 6º da referida lei. Analisa-se o gradual desenvolvimento do sistema de proteção de dados no Brasil ao longo de décadas, bem como a relevância da base principiológica suscitada.

Na primeira parte do trabalho, discorre-se sobre as normas esparsas relativas à proteção de dados no ordenamento jurídico brasileiro: o artigo 5º, incisos X e XII, da Constituição Federal Brasileira de 198; o Código de Defesa do Consumidor (Lei nº 8.078/1990); a Lei de Arquivos Públicos (Lei nº 8.159/1991); a Lei de Habeas Data (Lei nº 9.507/1997); o Decreto nº 6.135/2007; o Decreto nº 6.425/2008; o Decreto n. 6.523/2008; a Lei do Cadastro Positivo (Lei 12.414/11); a Lei de Acesso à Informação (Lei nº 12.527/2011); e a Lei do Marco Civil da Internet (Lei nº 12.965/2014). Na segunda parte, abordam-se os quatro princípios que fundamentam a LGPD, são eles: o Princípio da Privacidade; o Princípio da Liberdade; o Princípio da Neutralidade; e o Princípio da Autodeterminação. Por fim, na terceira parte, analisam-se os princípios de proteção de dados relacionados no artigo 6º da LGPD: Princípio da Boa Fé; Princípio da Finalidade; Princípio da Adequação; Princípio da Necessidade; Princípio do Livre Acesso; Princípio da Qualidade dos Dados; Princípio da Transparência; Princípio da Segurança; Princípio da Prevenção; Princípio da Não Discriminação; Princípio da Responsabilização e Prestação de Contas.

Desta forma, demonstra-se a importância da proteção de dados, determinante tanto para a garantia da liberdade individual quanto para a preservação da dignidade humana. Além disso, por meio da análise de cada um dos princípios, ressalta-se a relevância e qualidade do sistema de proteção de dados no Brasil, bem como se expõe novos desafios a serem superados. Logo, segue-se à primeira parte do artigo, estudando-se as normas esparsas que primeiro abordaram a temática da proteção de dados no Brasil.

1 Diálogo das fontes entre LGPD e outras normas nacionais

Inicialmente, o sistema brasileiro de proteção de dados era composto por normas esparsas que exigiam uma interpretação sistemática, ou seja, coordenada de todo o ordenamento jurídico a fim de efetivar a proteção. O referido sistema apenas foi unificado com o advento da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) colocando

um termo nas discrepâncias, lacunas e incoerências decorrentes da falta de uma norma própria reguladora da matéria. Além disso, vários direitos previstos em normas esparsas foram incluídos na LGPD genericamente em forma de princípios, como a transparência, a finalidade, o livre acesso, a qualidade dos dados.

Podem-se citar dentre as normas esparsas anteriores à LGPD as disposições do artigo 5º, incisos X e XII, da Constituição Federal Brasileira de 1988: "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"; "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". Além da Carta Maior, o Código de Defesa do Consumidor (Lei nº 8.078/1990), lei complementar que determinou às empresas o dever de informar o consumidor sobre a abertura de cadastro contendo as informações deste (artigo 43, § 2º), bem como garantiu ao consumidor o direito ao acesso às informações existentes arquivadas sobre ele e suas respectivas fontes nos cadastros das empresas (artigo 43, *caput*) e o direito de correção dos dados equivocados (artigo 43, § 3º).

Também, legislações ordinárias como a Lei de Arquivos Públicos (Lei nº 8.159/1991) e a Lei de Habeas Data (Lei nº 9.507/1997), ambas concernentes às informações dos cidadãos armazenadas pelo Estado ou terceiros. Na primeira, no artigo 4º, determinando que "Todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos", excluídas informações cujo "sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas". E na segunda, no artigo 7º, I, II e III, constando que será concedido habeas data "para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público", "para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo" e "para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável".

Ademais, atos normativos infralegais, como: o Decreto nº 6.135/2007, que regula o cadastro único para programas sociais do Governo Federal, determinando em seu artigo 8º que "Os dados de identificação das famílias do CadÚnico são sigilosos e somente poderão ser utilizados para as seguintes finalidades: I - formulação e gestão de políticas públicas; e II - realização de estudos e pesquisas"; o Decreto nº 6.425/2008, que normatiza o censo escolar,

determinando em seu artigo 6º que "Ficam assegurados o sigilo e a proteção de dados pessoais apurados no censo da educação, vedada a sua utilização para fins estranhos aos previstos na legislação educacional aplicável"; e no Decreto n. 6.523/2008, que regula o Serviço de Atendimento ao Consumidor – SAC, determinando em seu artigo 11 que "Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento".

Outras leis ordinárias como a Lei do Cadastro Positivo (Lei 12.414/11) que regula "a formação e a consulta aos bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para a formação do histórico de crédito", atribuindo ao próprio indivíduo o poder de decidir se deseja ou não fazer parte do cadastro positivo, inclusive podendo cancelar sua participação neste (artigo 5º, I, III e § 4º) – em respeito ao Princípio da Autodeterminação que será estudado no próximo item do trabalho. Além disso, a referida norma proíbe explicitamente em seu artigo 3º, § 3º, o armazenamento de dados sensíveis e informações excessivas. Também, a Lei de Acesso à Informação (Lei nº 12.527/2011) relacionada à transparência nos órgãos e entidades do poder público e, em seu artigo 8º, § 2º, determinando que "É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas" e "Para cumprimento do disposto no caput, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet)".

Por fim, a Lei do Marco Civil da Internet (Lei nº 12.965/2014) que definiu direitos e responsabilidades na utilização dos meios digitais, decorrendo seu texto de amplo debate público com contribuições da sociedade civil, da comunidade empresarial, de cidadãos comuns, bem como de representantes das áreas técnica e acadêmica. Além disso, a supracitada norma estabeleceu a edição futura de lei específica sobre a proteção de dados pessoais (artigo 19, § 2º). Também, elencou, no artigo 3º, como princípios do uso da internet no Brasil: a garantia da liberdade de expressão, comunicação e manifestação de pensamento; proteção da privacidade; a proteção dos dados pessoais; a preservação e garantia da neutralidade de rede; e a responsabilização dos agentes de acordo com suas atividades. Estes princípios claramente relacionados aos princípios contidos na própria LGPD, inclusive sendo a própria proteção dos dados pessoais um princípio jurídico.

> Além disso, ao definir a proteção dos dados pessoais como princípio do uso da internet no Brasil, a referida legislação instrumentaliza o cidadão-consumidor com a positivação do princípio da autodeterminação informativa como direito essencial ao exercício da cidadania, pois ao titular das informações é conferida a prerrogativa de vedar o fornecimento a terceiros de dados pessoais e registros de conexão, salvo mediante consentimento livre e expresso ou nas hipóteses previstas em lei, o que assegura ao cidadão-consumidor o efetivo controle e a liberdade de exercício dos seus direitos fundamentais à privacidade e sigilo das comunicações. (CATUZO; EFING)

Portanto, desta compilação normativa se verifica que o sistema de proteção de dados no Brasil percorreu décadas até chegar a sua atual forma unitária, ou seja, com uma lei específica sobre o tema, a LGPD, resultando no surgimento da disciplina de proteção de dados pessoais. Assim, segue-se para o próximo item do presente artigo, analisando-se com maior profundidade a LGPD por meio dos princípios que fundamentam a referida legislação.

2 Princípios que fundamentam a LGPD

A LGPD deve ser interpretada e aplicada em conformidade com todo o sistema anterior à edição da referida norma e que já estava em desenvolvimento décadas antes da criação da lei específica. Assim, da leitura geral das regras é possível identificar princípios que fundamentam a LGPD, são eles: o Princípio da Privacidade; o Princípio da Liberdade; o Princípio da Neutralidade; e o Princípio da Autodeterminação. Estes não se confundem com os princípios de proteção de dados relacionados no artigo 6º da LGPD, assunto que será abordado no próximo tópico do presente artigo.

Iniciando pelo Princípio da Privacidade, observa-se que este: protege os valores fundamentais da dignidade humana e igualdade política, inclusive impedindo intromissões ou controle exacerbado/nocivo do Estado sobre os indivíduos impondo determinados estilos de vida ou moral; garante o controle da circulação de informações pessoais e a autodeterminação informativa (Princípio da Autodeterminação); proíbe a captação e utilização com fins comerciais de dados pessoais dos usuários/consumidores por provedores de rede, sites e fornecedores nos contratos eletrônicos; proíbe a captação e utilização com fins comerciais ou prejudiciais de dados pessoais dos trabalhadores por empregadores nas relações trabalhistas; impõe a proteção jurídica dos dados pessoais dos usuários na internet e a proteção contra discriminação; proíbe a classificação dos indivíduos por características comuns, como perfil de consumo; obriga a observância da legislação brasileira relativa à segurança da informação

por parte de empresas estrangeiras, independentemente da localização física dos centros de armazenamentos de dados destas.

Ingressando no Princípio da Liberdade, este determina que: todas as pessoas têm igual direito de difundir informações na internet (mesmo grau de liberdades civis e políticas), pois do contrário se estaria constrangendo a liberdade individual (liberdade de expressão, comunicação e manifestação de pensamento); todas as pessoas têm o controle de suas próprias informações a fim de evitar sua sujeição a organismos públicos ou privados; o uso da internet é necessário ao desenvolvimento da personalidade e à promoção da dignidade humana; a liberdade na internet não pode ser condicionada por fatores técnicos; os dados devem receber tratamento isonômico; os conteúdos publicados necessitam de autorização do autor/titular ou de ordem judicial para que seja efetuada a sua exclusão; o próprio autor é o responsável pelo conteúdo publicado, não os provedores de acesso à rede, exceto quando estes se omitirem em tornar indisponível conteúdo considerado danoso; exista liberdade nos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios, tampouco com a lei; exista liberdade de autodeterminação (liberdade para a realização do Princípio da Autodeterminação).

Seguindo para o Princípio da Neutralidade, este é premissa para a fruição do Princípio da Liberdade, tendo em vista que nenhuma liberdade pode ser absoluta, e refere-se à neutralidade da rede, por exemplo: reforçando o Princípio da Liberdade (liberdade de expressão) e tendo o Princípio da Privacidade como limite; impedindo que as empresas de telecomunicações (provedores de acesso) estipulem cobranças diferenciadas dos usuários conforme o conteúdo acessado, sendo apenas permitidas cobranças pela velocidade de conexão; impondo a isonomia no tratamento dos dados; impedindo discriminações relacionadas ao conteúdo, à identidade do usuário, à origem e ao destino das comunicações, à política, à cultura, à religião; proibindo o bloqueio, monitoramento, filtragem ou análise dos conteúdos.

> O princípio da neutralidade da rede, em particular, determina que a rede deve tratar da mesma forma tudo aquilo que transportar, sem fazer discriminações quanto à natureza do conteúdo ou à identidade do usuário, buscando-se, assim, "garantir uma experiência integral da rede a seus usuários" (WU, 2012, p. 244). A regra deve ser, portanto, o tratamento isonômico dos pacotes de dados, sem distinção por conteúdo, origem, destino, serviço, terminal ou aplicação, havendo expressa vedação ao bloqueio, monitoramento, filtragem ou análise do conteúdo dos pacotes (art. 9º do MCI). O princípio impõe que a filtragem ou os privilégios de tráfego devam respeitar apenas e tão somente critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos ou culturais que criem

> qualquer forma de discriminação ou favorecimento. (MORAES; TEFFÉ, p. 112)

Por fim, o Princípio da Autodeterminação trata da autodeterminação informativa, esta é pessoal e relativa ao uso de seus próprios dados. Logo, pode o usuário fornecer, não fornecer, corrigir ou cancelar seus cadastros, ou seja, controlar o fluxo de seus dados pessoais, exceto em circunstâncias nas quais a lei determina o contrário. Também, verifica-se a extrema relevância da autodeterminação na medida em que impede que o indivíduo fique sujeito ao poder de organismos privados ou públicos, evitando o compartilhamento de informações que podem gerar discriminação e vulnerabilidade do usuário. Ademais, favorece que a pessoa desenvolva livremente a sua personalidade, bem como determine o âmbito da sua própria privacidade (URASHIMA, 2018, p. 186).

3 Princípios de proteção de dados

O rol de princípios constante do artigo 6º da LGPD é exemplificativo, ou seja, não exclui outros princípios "previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte" (artigo 64 da LGPD). Ademais, tal relação de princípios decorre da necessidade de se estabelecer as principais regras para aplicação e interpretação da norma, razão pela qual se verifica a sua presença ao longo dos demais dispositivos da mesma, conferindo-lhe coerência, organização e concretização. Segue-se para a análise de cada um dos princípios elencados no artigo 6º da LGPD:

Primeiramente, o Princípio da Boa Fé está previsto no artigo 6º, *caput*, da LGPD e sua aplicação nesta esfera decorre da Constituição Federal, do Código Civil (LIMA; MONTEIRO, p. 66) e do Código de Defesa do Consumidor. Trata-se de uma cláusula geral que contém um princípio, esta é a razão para a sua inserção em destaque no *caput* do artigo. Ressalta-se que, por ser ao mesmo tempo cláusula geral e princípio, impõe-se a todos os demais princípios, tendo um efeito integrador, bem como garantindo coesão na interpretação e na aplicação da LGPD.

O princípio implica nos deveres de informar, de transparência e de cooperar (MARQUES, pp. 50-51), ou seja, a "[...] Boa fé é um pensar refletido, é o pensar no outro, no mais fraco, no parceiro contratual, nas suas expectativas legítimas, é lealdade, é transparência, é informação, é cooperação, é cuidado, é visualização e respeito pelo outro [...]" (MARQUES, p. 48). Ademais, apesar de ser tratado de forma abstrata na LGPD, é de extrema importância,

pois da sua não observância pode decorrer a violação de direitos fundamentais como, por exemplo, a violação de dados sensíveis.

> Boa fé é cooperação e respeito, é conduta esperada e leal, tutelada em todas as relações sociais. A proteção da boa fé e da confiança despertada formam, a base do tráfico jurídico, a base de todas as vinculações jurídicas, o princípio máximo das relações contratuais. [...] (MARQUES, p. 50)

> [...] trata-se de diretriz orientadora não apenas no âmbito do microssistema do código de defesa do consumidor mas, na realidade, que atinge todo o sistema jurídico. [...]
>
> Judith Martins-Costa, que vê a boa-fé como cláusula geral, não deixa de reconhecer a possibilidade de que possa ocorrer a situação onde esta contenha um princípio. "Aí, sim, se poderá dizer que determinada norma é, ao mesmo tempo, princípio e cláusula geral". No tema específico da proteção ao consumidor, no Direito Brasileiro, é precisamente o que ocorre, diante do conteúdo dos incisos III, IV e V do art. 6º da Lei nº 8078/90 (Código de Defesa do Consumidor), expressões da boa-fé objetiva, entendida esta como "modelo de conduta social, arquétipo ou standard jurídico, segundo o qual 'cada pessoa deve ajustar a própria conduta a este arquétipo, obrando como obraria um homem reto: com honestidade, lealdade, probidade'." (SANTOLIM, 2004, pp. 68-69)

Por fim, cabe ressaltar que se diferencia a licitude e a lealdade da boa fé, pois do princípio da licitude e da lealdade decorre que os dados devem "ser obtidos por meios lícitos e tratados para fins legítimos [...], não podendo ser utilizados de uma forma incompatível com aqueles fins" (MAIA, pp. 462-463). Logo, a lealdade guarda similitude mais acentuada com o princípio da finalidade, bem como sua amplitude é mais restrita do que a boa-fé.

> O princípio da licitude e da lealdade estabelece que os dados pessoais devem ser obtidos e processados legítima e lealmente. Grosso modo, processamento lícito pode ser entendido como aquele que não implica a violação de uma lei de proteção de dados ou de outro requisito de ordem jurídica. Com o mesmo grau de generalidade, pode-se dizer que será leal o tratamento que não implicar deslealdade para com o titular dos dados. (SANDEN)

Ingressando no Princípio da Finalidade, este se encontra no artigo 6º, inciso I da LGPD, no qual consta que os dados devem ser tratados "para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Logo, observa-se que "qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados" (DONEDA, p. 100), ou seja, "os dados pessoais somente podem ser alvo de

tratamento compatível com as finalidades que fundamentaram a sua coleta e foram informadas ao titular" (KAMEDA; PAZELLO, p. 7).

O princípio relaciona-se à boa fé e à lealdade, pois a finalidade especificada no momento do recolhimento dos dados e para a qual estes são utilizados "deve ser legítima e estar em conformidade com o ordenamento jurídico" (CORRÊA; GEDIEL, p. 147). Ademais, a relevância prática do princípio está em fundamentar a restrição da "transferência de dados pessoais a terceiros", bem como em estruturar "um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade)" (DONEDA, p. 100).

Verifica-se que o princípio da finalidade impõe que sejam especificados os propósitos para os quais os dados serão recolhidos até no máximo a data de início do seu recolhimento. Além disso, seu uso deve ser limitado aos propósitos previamente expostos ou outros que, não sendo incompatíveis, sejam especificados na ocasião em que os propósitos sofrerem alteração (OECD).

Observa-se que o princípio da finalidade é um princípio limitador do uso dos dados, pois impõe que estes não podem ser divulgados, disponibilizados e/ou utilizados para outros fins não previamente especificados, exceto se o titular dos dados der seu consentimento ou se tal decorrer da autoridade da lei (OECD).

Exemplificativamente, cabe citar a utilização do princípio da finalidade em situações nas quais ocorre um conflito entre a proteção da privacidade dos cidadãos, em particular dos grupos mais vulneráveis, e o imperativo dos Estados em garantir a proteção dos seus cidadãos contra o terrorismo e a criminalidade organizada. Nestas circunstâncias se observa uma exceção ao princípio da finalidade, tendo em vista que se permite que os dados recolhidos para determinada finalidade sejam tratados posteriormente para fim diverso (CORREIA; JESUS, p. 21). É o caso do Eurodac: "um banco de dados da União Europeia que armazena as impressões digitais de solicitantes de proteção internacional e migrantes irregulares" (DATA PROTECTION COMMISSION). Utiliza-se o referido banco de dados para identificar, por meio da impressão digital, em qual Estado-Membro o migrante ingressou inicialmente na Europa, bem como para fazer a sua identificação posterior.

Por fim, expõe-se que o Princípio da Finalidade guarda estrita relação com os Princípios da Adequação e da Necessidade – ambos serão analisados a seguir –, bem como sua concretização está presente em vários outros artigos da LGPD que exigem sua observação, como: o artigo 7, I, no qual consta as hipóteses nas quais poderá ser realizado o tratamento de dados pessoais, determinando o inciso somente "mediante o fornecimento de

consentimento pelo titular"; o artigo 7, §3º, frisando que "O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização"; o artigo 8º, § 4º, no qual se expõe que "O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas"; o artigo 9º, §2°, afirmando que "Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade", neste caso poderá o "titular revogar o consentimento, caso discorde das alterações"; e por último, o artigo 10, no qual se saliente que "O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas".

Avançando-se na matéria, o Princípio da Adequação, também identificado como Princípio da Pertinência (MAIA, p. 463), está exposto no artigo 6º, inciso II, da LGPD, neste consta determinação de: "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento". Além disso, trata-se de um princípio limitador relativamente ao modo de coleta dos dados, determinando que "deve haver limites à coleta de dados pessoais e todos os dados devem ser obtidos por meios leais e justos, onde seja adequado, com o conhecimento ou consentimento do sujeito dos dados" (OECD). Assim, impõe-se que as informações colhidas sejam "adequadas, pertinentes e não excessivas em relação a seus fins" (MAIA, p. 463).

Seguindo-se para o Princípio da Necessidade, este está previsto no artigo 6º, inciso III, da LGPD, neste consta o dever de: "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". Logo, observa-se um aspecto quantitativo limitador e de economicidade imposto por tal princípio no tratamento de dados, ou seja, não tratar mais dados do que o necessário para os fins almejados. Além disso, ressalta-se que tal limitação deve ocorrer principalmente "quando a finalidade possa ser atingida com a utilização de dados anônimos ou com uso de meios que permitam a identificação do titular somente em caso de necessidade" (KAMEDA; PAZELLO, p. 7).

Salienta-se que para o Princípio da Necessidade também pode ser utilizada exemplificativamente a base de dados Eurodac. Assim, na análise do conflito entre a necessidade de proteção da privacidade dos cidadãos, em particular dos grupos mais vulneráveis, e o imperativo dos Estados-Membros da União Europeia em garantir a proteção dos seus cidadãos contra fenômenos globais como o terrorismo e a criminalidade organizada,

deve-se garantir que “a informação seja reunida, partilhada e processada apenas em função de necessidades concretas em matéria de segurança e tendo em conta os princípios em matéria de proteção de dados” (CORREIA; JESUS, p. 23). Evitar-se-á, desta forma, violar a privacidade dos migrantes cujos dados constam na referida base.

Por fim, frisa-se que o princípio da necessidade se encontra projetado ao longo dos dispositivos da LGPD: no artigo 10, §1º, expõe-se que “Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados”; no artigo 16, ressalta-se que “Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades”, autorizada a conservação destes apenas em casos previstos na LGPD; e no artigo 18, VI, determina-se que “O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] VI - eliminação dos dados pessoais tratados com o consentimento do titular”, exceto em hipóteses nas quais é autorizada a conservação dos dados, nos termos da LGPD.

Ingressando no Princípio do Livre Acesso, este está presente no artigo 6º, inciso IV, da LGPD e assegura a “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”. Assim, frisa-se a gratuidade inerente às consultas dos seus dados pessoais, bem como das modalidades de tratamento destes (KAMEDA; PAZELLO, p. 8).

Trata-se de princípio “pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados”. Além disso, tendo em vista o princípio da exatidão, assegura-se ao indivíduo que “as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos” (DONEDA, pp. 100-101). Ademais, observa-se que a oposição do titular dos dados pode ser total ou parcial relativamente ao tratamento de suas informações. Também, ressalta-se que, graças ao Princípio do Livre Acesso, “os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade que sua coleta e seu tratamento sejam feitos com cuidado e correção, e que sejam realizadas atualizações periódicas destes dados conforme a necessidade” (MAIA, p. 463).

Finalmente, salienta-se que o Princípio do Livre Acesso está expresso no artigo 9, caput: “O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre

acesso". Também, encontra-se o referido princípio implícito nos artigos 18, 19 e 20, sobre acesso aos dados pelo titular destes, requisições feitas pelo titular ao controlador dos dados, correção dos dados solicitada pelo titular e revisão de decisões tomadas unicamente com base em tratamento automatizado de dados.

Sobre o Princípio da Qualidade de Dados, este se encontra no artigo 6º, inciso V, da LGPD e estabelece "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento". Assim, determina que "os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade" (DONEDA, p. 100). Também, estipula que "os dados pessoais devem ser relevantes para os fins para os quais devem ser utilizados e, na medida do necessário para esses fins, devem ser precisos, completos e atualizados" (OECD). Concisamente, pode-se resumir que este princípio trata da importância da "exatidão dos dados pessoais alvo de tratamento" (KAMEDA; PAZELLO, p. 8).

Por fim, observa-se que o Princípio da Qualidade dos Dados se relaciona com outros princípios da proteção de dados, como: o princípio da legalidade, impondo a observância da lei; o princípio da boa-fé, abordando a lealdade; o princípio da adequação, relativamente à "pertinência e proporcionalidade em função da finalidade de cada tratamento" (CORRÊA; GEDIEL, p. 147); o princípio do livre acesso, assegurando ao titular a retificação, exclusão, bloqueio e atualização dos dados; e com o princípio da transparência, pois impõe o conhecimento e a correção de informações equivocadas. Ademais, verifica-se a projeção do princípio no artigo 18, inciso III: "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: III - correção de dados incompletos, inexatos ou desatualizados".

Ingressando no estudo do Princípio da Transparência, também chamado de Princípio da Publicidade, este consta no artigo 6º, inciso VI, da LGPD e assegura "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". Assim, impõe que "a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para seu funcionamento, pela notificação de sua criação a uma autoridade; ou pela divulgação de relatórios periódicos" (MAIA, p. 463). Ademais, o titular deve ser informado sobre os tratamentos de seus dados, ou seja, "toda pessoa tem direito à informação por parte do

responsável pelo tratamento de dados que lhe digam respeito, inclusive no que tange ao modo, à finalidade, período de conservação etc" (CORRÊA; GEDIEL, p. 147). Em outro aspecto, o princípio determina que:

> Deve existir uma política geral de abertura sobre desenvolvimentos, práticas e políticas com relação aos dados pessoais. Devem estar prontamente disponíveis meios para estabelecer a existência e a natureza dos dados pessoais e os principais objetivos de seu uso, bem como a identidade e a residência habitual do controlador de dados. (OECD)

Por fim, salienta-se a preponderância deste princípio nos dispositivos da LGPD, presente tanto na coleta dos dados, quanto no tratamento de destes, bem como se ressalta a sua projeção especial: no artigo 9º, no qual se determina que "O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva [...]"; no artigo 10, §2º, no qual se impõe que "O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse"; no artigo 18, I, II, VII e VIII que garante ao titular dos dados pessoais o direito de obter do controlador, mediante requisição, a confirmação da existência de tratamento de dados e o acesso a estes, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, além de informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e no artigo 20, § 1º e § 2º, nos quais se frisa o dever do controlador em "fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial", sendo que, caso tais informações não sejam prestadas em razão de segredo comercial e industrial, "a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais".

Sobre o Princípio da Segurança, também conhecido como Princípio de Salvaguardas de Segurança, este está contido no artigo 6º, inciso VII, da LGPD, determinando a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". É um princípio de segurança física e lógica, ou seja, abarca ambos os meios de proteção, devendo os dados ser protegidos por garantias razoáveis de segurança contra os riscos de seu extravio, destruição, modificação, perda, transmissão ou acesso não autorizado, e/ou divulgação de dados não permitida (DONEDA, p. 101) (OECD). Ademais, ressalta-se que, apesar da utilização do termo proteção de dados pessoais, o que se está de fato

protegendo com este princípio é a privacidade da pessoa a qual se referem os dados (MAIA, p. 464).

O presente princípio reforça "a atenção quanto à segurança no tratamento de dados, a fim de que eles não caiam em mãos desautorizadas, causando prejuízos que podem trazer impacto sobremaneira elevado", devendo tal ser realizado por meio da "adoção de medidas que visam à redução máxima da quantidade de falhas" (LIMA; MONTEIRO, pp. 68-69). Assim, por exemplo, impõe-se "aos bancos de dados (principais repositórios de informações), que precisam ser desenhados de modo a impedir a captura por terceiros não autorizados, privilegiando-se a utilização de criptografia", sendo "permitido o acesso a essas informações armazenadas nos casos expressamente permitidos" (LIMA; MONTEIRO, p. 69). Também, enquadra-se neste princípio questão relativa às grandes instituições financeiras, que por lidarem com informações que são frequentemente alvo de criminosos precisarão de estruturas de dados mais complexas do que uma pequena loja, por exemplo (LIMA; MONTEIRO, p. 69).

Adentrando-se o Princípio da Prevenção, este está previsto no artigo 6º, inciso VIII, da LGPD, neste consta a relevância de "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais". Intrinsecamente relacionado ao Princípio da Segurança, o Princípio da Prevenção determina "utilização das medidas técnicas e administrativas proporcionais ao atual estado da tecnologia, à natureza dos dados pessoais e às características específicas do tratamento", capazes de prevenir a ocorrência de danos aos dados, como "destruição, perda, alteração e difusão, tanto acidentais quanto ilícitas, bem como do acesso não autorizado" (KAMEDA; PAZELLO, p. 8).

Seguindo-se para o Princípio da Não Discriminação, este se encontra no artigo 6º, inciso IX, da LGPD e determina a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Trata-se aqui de proteger os chamados dados sensíveis, ou seja, aqueles que constam no artigo 5º, II, da LGPD, o dado de uma pessoa natural "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".

Tal decorre da possibilidade de a divulgação de dados sensíveis poder "ocasionar situações de discriminação e prejuízos às pessoas. Desse modo, o princípio da igualdade pode ser vinculado aos dados sensíveis, buscando-se uma maior proteção tanto na sua coleta como na guarda ou na utilização para os fins aos quais foram captados" (LIMBERGER, p. 150). Logo, com o Princípio da Não Discriminação se busca proteger as liberdades individuais, a

dignidade humana e o indivíduo perante a livre-iniciativa, tornando efetivo o Princípio da Igualdade dos titulares de dados, especialmente de dados sensíveis.

Ressalta-se que o consentimento para a coleta de dados não sensíveis deve ser livre, informado e inequívoco, nos casos em que a lei exigir, enquanto o consentimento para a coleta de dados sensíveis deve ser livre, informado, inequívoco, específico e destacado. No entanto, nos termos do artigo 11, inciso II, da LGPD, os dados sensíveis poderão ser tratados sem o consentimento do titular nas hipóteses em que forem indispensáveis para: "a) cumprimento de obrigação legal ou regulatória pelo controlador"; "b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos"; "c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis"; "d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)"; "e) proteção da vida ou da incolumidade física do titular ou de terceiro"; "f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária"; "ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

> Os dados de caráter pessoal contêm informação das pessoas físicas que permitem sua identificação no momento ou posteriormente. Na sociedade tecnológica, os cadastros armazenam alguns dados que possuem um conteúdo especial, e por isso são denominados dados sensíveis. Tais dados podem referir-se a questões como ideologia, religião ou crença, origem racial, saúde ou vida sexual. Exige-se que os cadastros que os armazenam contenham uma segurança especial, como forma de evitar que sejam mal utilizados. Com as cautelas especiais relativas aos dados sensíveis, seja quando são recolhidos, seja quanto à segurança em seu armazenamento, tenta-se garantir que os mesmos não sejam utilizados para outra finalidade ou de maneira equivocada. O dado pessoal é uma informação que permite identificar uma pessoa de maneira direta. A proteção do dado sensível tenta prevenir ou eliminar discriminações. Pode-se dizer que é uma nova leitura do princípio da igualdade, e sua intenção é a de que os dados armazenados não sirvam para prejudicar as pessoas. (LIMBERGER, p. 149-150)

Um exemplo de utilização prejudicial de informações é o caso em que um banco de dados que contém dados sobre a religião, sexo ou saúde os concede a determinada empresa, criando uma situação de desigualdade, como: a) gerando a não contratação de um trabalhador

de determinada religião que não pode, em virtude de suas crenças, trabalhar no sábado, e tendo em vista o conhecimento desse dado de forma antecipada por parte da empresa; b) gerando a não contratação de um portador do vírus HIV em virtude de sua condição de saúde, podendo até ser despedido aquele que já se encontra trabalhando (ressalta-se que apenas pode ser pedido o exame HIV em atividade que se for portador da enfermidade o empregado pode causar um contágio) (LIMBERGER, pp. 149-150).

Ademais, ressalta-se que o Princípio da Não Discriminação abrange a atividade daquele que coleta os dados – ao restringir o uso destes, bem como a transmissão para terceiros – e também a atividade daquele que fornece os próprios dados pessoais – trata-se aqui da autodeterminação informativa, protegendo-se no caso a liberdade da pessoa de fornecer ou não seus dados pessoais, bem como corrigir ou cancelar cadastros próprios, sem ser prejudicada por tal motivo.

Por fim, tendo em vista a já abordada relevância dos dados financeiros no estudo sobre o Princípio da Segurança, cabe questionar: os dados financeiros deveriam ser também considerados dados sensíveis? Sua divulgação pode gerar insegurança e discriminação? No presente trabalho se responde afirmativamente a estes questionamentos. Observa-se que no Brasil, por exemplo, ocorre a divulgação das remunerações recebidas por servidores públicos em portais de transparência pública, sendo possível visualizar o nome dos servidores e suas remunerações detalhadamente, inclusive com descontos e acréscimos – como empréstimos, gratificação natalina, gratificação por férias, auxílios. Obviamente, de tal divulgação decorre a exposição demasiada da intimidade do servidor, podendo colocar em risco a sua segurança e de sua família. Além disso, pode ocorrer discriminação ao servidor relacionadas à sua baixa remuneração ou endividamento.

Por último, aborda-se o Princípio da Responsabilização e Prestação de Contas, este decorre da Constituição Federal e do Código Civil (LIMA; MONTEIRO, p. 66) e está previsto no artigo 6º, inciso X, da LGPD, neste impondo a "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". Trata-se do dever de reparar os danos patrimoniais, morais, individuais ou coletivos causados aos titulares dos dados pessoais (KAMEDA; PAZELLO, p. 8).

Encerra-se salientando que o Princípio da Responsabilização e Prestação de Contas se projeta ao longo na LGPD: no artigo 31, § 2º, no qual se determina que "O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" e que

“Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido”; no artigo 32, no qual consta o rol de condutas ilícitas que ensejam a responsabilidade do agente público ou militar relacionada aos fatos previstos na LGPD; no artigo 33, no qual se trata da responsabilidade da pessoa física ou entidade privada que detiver informações em virtude de vínculo de qualquer natureza com o poder público e deixar de observar o disposto na LDPD; no artigo 34, no qual se aborda a responsabilidade dos órgãos e entidades públicas pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais; e no artigo 44, no qual se altera a Lei nº 8.112/1990, acrescendo-se à referida norma o artigo 126-A relativo à não responsabilização de servidor por dar ciência à autoridade competente para apuração de infração concernente à prática de crimes ou improbidade.

CONSIDERAÇÕES FINAIS

No presente artigo verificou-se a importância do sistema de proteção de dados no Brasil, pois este implica na proteção da liberdade individual e da dignidade humana. Também, salientou-se que o sistema é composto por normas esparsas que foram emitidas ao longo de décadas e tem como norma principal a recente Lei Geral de Proteção de Dados – LGPD.

No decorrer do estudo das normas e princípios de proteção de dados, percebe-se a progressão do sistema a cada nova norma publicada, tentando tornar o tratamento de dados mais seguro e igualitário, bem como preservando a intimidade por meio dos dados sensíveis, buscando trazer mais inclusão social por meio da neutralidade da rede, coibir abusos perpetrados pela livre iniciativa, entre tantos outros direitos aos indivíduos. No entanto, também se expôs questões ainda pendentes de análise e solução por parte do legislador e da doutrina, como a questão da inclusão de dados financeiros dos servidores públicos como dados sensíveis e, portanto, sendo descabida a ampla divulgação das remunerações em Portais de Transparência do Governo.

Desta forma, conforme demonstrado, existe um sistema de proteção de dados bastante desenvolvido no Brasil, formado por normas esparsas e por norma específica. Ademais, os princípios que fundamentam a LGPD, bem como os princípios contidos no rol exemplificativo do artigo 6º desta dão coesão ao sistema inteiro, dirimindo lacunas e garantindo a eficácia na proteção dos indivíduos.

REFERÊNCIAS

BRASIL. LEI Nº 8.159, DE 8 DE JANEIRO DE 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível na URL: http://www.planalto.gov.br/ccivil_03/Leis/L8159.htm. Acesso em 14 de set. de 2019.

BRASIL. LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível na URL: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em 14 de set. de 2019.

BRASIL. LEI Nº 12.414, DE 9 DE JUNHO DE 2011. Disciplina 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. Disponível na URL: http://www.planalto. gov.br/ccivil_03/_Ato2011- 2014/2011/Lei/L12414.htm. Acesso em 14 de set. de 2019.

BRASIL. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível na URL: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em 14 de set. de 2019.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível na URL: http://www.planalto .gov.br/CCIVIL_03/_Ato2011- 2014/2014/Lei/L12965.htm. Acesso em 14 de set. de 2019.

BRASIL. Projeto de Lei Nº 5.276, de 2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível na URL: https://www.camara.leg.br/proposicoesWeb/prop_ mostrarintegra;jsessionid=62B6CCB8D15F03BD169F7421D3CDB6EE.proposicoesWeb1?c odteor=1457971 &filename=Avulso+-PL+5276/2016. Acesso em 14 de set. de 2019.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível na URL: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 14 de set. de 2019.

CATUZO, Murilo Euller; EFING, Antônio Carlos. **A proteção jurídica dos dados pessoais na internet.** Disponível na URL: https://revistaconsinter.com/revistas/ano-ii-volume-ii/parte-3-aspectos-relevantes-no-futuro-do-direito/a-protecao-juridica-dos-dados-pessoais-na-internet /. Acesso em 25 de dez. de 2019.

CORRÊA, Adriana Espíndola; GEDIEL, José Antônio Peres. **Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o Mercado.** Disponível na URL: https://www.revistas.ufpr.br/direito/article/view/15738/10444. Acesso em 15 de set. de 2019.

CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de. **A proteção de dados pessoais no Espaço de Liberdade, de Segurança e de Justiça da União Europeia.** Disponível na URL: https://www.esteio.rs.gov.br/documents/SMSMU /Revista%20de%20Se guranca%20Publica/REVISTA%20DE%20SEGURANCA%20PUBLICA%2015.pdf#page=1 9. Acesso em 14 de set. 2019.

COSTA, Judith Martins. **O Direito Privado como um "sistema em construção" - As cláusulas gerais no Projeto do Código Civil brasileiro.** Disponível na URL: https://www2.senado.leg.br/bdsf/bitstream/handle/id/383/r139-01.pdf?sequence=4. Acesso em 18 de dez. de 2019.

CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Privado**, v. 98, p. 161-186, mar.-abr., 2019.

DATA PROTECTION COMMISSION. **Eurodac**. Disponível na URL: https://www.dataprotection.ie/en/eurodac. Acesso em 14 de set. de 2019.

DIONÍSIO, Cristiano. **Marco civil da internet, neutralidade de rede e sua relação com a liberdade como direito da personalidade.** Disponível na URL: https://revistas.utfpr.edu.br/rts/article/view/7109/5249. Acesso em 25 de dez. de 2019.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Disponível na URL: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em 14 de set. 2019.

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

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. **Revista da Faculdade de Direito UFPR**, Curitiba, n. 47, p. 141-153, 2008.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

KAMEDA, Koichi; PAZELLO, Magaly. **E-Saúde e desafios à proteção da privacidade no Brasil.** Disponível na URL: https://nupef.org.br/sites/default/files/downloads/artigo%20politics _esaude%20e%20privacidade.pdf. Acesso em 15 de set. de 2019.

LEMOS, Amanda Nunes Lopes Espiñeira. Judiciário como Ator Regulador da Internet: seu papel no esquema de forças do Estado moderno. **Journal of Law and Regulation**, v. 4, n. 1, p. 169-188, 2018.

LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite. **Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada.** Disponível na URL: https://revistas.ufpr.br/atoz/article/view/41320/25261. Acesso em 14 de set. de 2019.

LIMBERGER, Têmis. **Da evolução do direito a ser deixado em paz à proteção dos dados pessoais.** Disponível na URL: https://online.unisc.br/seer/index.php/direito/article/view/580/472. Acesso em 14 de set. de 2019.

MAIA, Luciano Soares. **A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais.** Disponível na URL: http://www.publicadireito. com.br /conpedi/manaus/arquivos/anais/bh/luciano_so ares_maia.pdf. Acesso em 15 de set. de 2019.

MARQUES, Claudia Lima. Boa-fé nos serviços bancários, financeiros de crédito e securitários e o Código de Defesa do Consumidor: informação, cooperação e renegociação?. **Revista da Faculdade de Direito**, v. 1, n. 22, p. 47-83, 2002.

MARQUES, Cláudia Lima. O "diálogo das fontes" como método da nova teoria geral do direito: um tributo à Erik Jaime. In: MARQUES, Cláudia Lima (Coord.). **Diálogo das fontes**: do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**, v. 20, n. 79, p. 45-81, 2011.

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

MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 9, p. 35-48, 2016.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. Revista de Direito do Consumidor, São Paulo, v. 120, p. 469-483, nov.-dez, 2018.

MENKE, Fabiano. A interpretação das cláusulas gerais: a subsunção e a concreção dos conceitos. **Revista de Direito do Consumidor.** vol. 50. p. 9. Abr, 2004. Doutrinas Essenciais de Direito do Consumidor. vol. 4. p. 107. Abr, 2011. DTR\2004\878

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In. MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P.. **Direito, Inovação e Tecnologia**. v. 1. São Paulo: Saraiva, 2015.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara Spadaccini de. **Redes sociais virtuais: privacidade e responsabilidade civil Análise a partir do Marco Civil da Internet.** Disponível na URL: https://periodicos.unifor.br/rpen/article/view/6272/pdf. Acesso em 25 de dez. de 2019.

OECD. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Disponível na URL: https://www.oecd.org/internet/ieconomy/ oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em 15 de set. de 2019.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. 4 ed. São Paulo: Atlas, 2008.

RODRIGUEZ, Daniel Piñeiro; RUARO, Regina Linden**. O direito à proteção de dados pessoais e a privacidade.** Disponível na URL: https://revistas.ufpr.br/ direito/article/view/30768/19876. Acesso em 14 de set. de 2019.

SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado**. Disponível na URL: http://www.teses. usp.br/teses/disponiveis/2/2138/tde-05082013-165006/en.php. Acesso em 18 de dez. de 2019.

SANTOLIM, Cesar Viterbo Matos. **A aplicação dos princípios de proteção do consumidor ao comércio eletrônico no Direito Brasileiro.** Disponível na URL: https://seer.ufrgs.br/ppgdir/article/view/50519/31559. Acesso em 18 de dez. de 2019.

SANTOLIM, Cesar Viterbo Matos. **Os princípios de proteção do consumidor e o comércio eletrônico no Direito Brasileiro.** Disponível na URL: https://lume.ufrgs.br/ bitstream/handle/ 10183/12684/000398647.pdf?sequence=1&isAllowed=y. Acesso em 18 de dez. de 2019.

SILVA, Rosane Leal da. **Contratos eletrônicos e a proteção de dados pessoais do consumidor: diálogo de fontes entre o Código de Defesa do Consumidor e o Marco Civil da Internet.** Disponível na URL: http://conpedi.danilolr.info/ publicacoes/y0ii48h0/k778x2oo/41xvoaU8rO29i9qX.pdf. Acesso em 25 de dez. de 2019.

VENTURA, Leonardo Henrique de Carvalho. Considerações sobre a nova Lei geral de proteção de dados pessoais. **Revista Síntese:** Direito Administrativo, São Paulo, v. 13, n. 155, p. 56-64, nov. 2018.

VERONESE, Alexandre; MELO, Noemy. A Proposta Brasileira de Proteção de Dados Pessoais em comparação ao novo Regulamento Europeu. **Revista de Direito Civil Contemporâneo,** São Paulo, v. 14, p. 71-99, jan.-mar., 2018.

UEHARA, Luiz Fernando; TAVARES FILHO, Paulo César. Transferência Internacional de Dados Pessoais: uma análise crítica entre o Regulamento Geral de Proteção de Dados Pessoais da União Europeia (RGPD) e a Lei Brasileira de Proteção de Dados Pessoais (LGPD). **Revista de Direito e as Novas Tecnologias**, v. 2, p. 1-15, jan.-mar., 2019.

UNIÃO EUROPEIA. Convenção 108 de 1981 do Conselho da Europa. Disponível na URL: http://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em 14 de set. 2019.

UNIÃO EUROPEIA. Diretiva 46/95/CE Disponível na URL: https://eur- lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em 14 de set. 2019.

UNIÃO EUROPEIA. Regulamento 2016/679. Disponível na URL: https://eur- lex.eu ropa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 14 de set. de 2019.

URASHIMA, Pedro Nobuyuki Carvalho. **A vigilância no Marco Civil da Internet: uma análise liberal-igualitária do armazenamento geral de dados.** Disponível na URL: https://seer.ufrgs.br/resseveraverumgaudium/article/viewFile/74133/47864. Acesso em 25 de dez. de 2019.