UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

FACULDADE DE DIREITO

DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

Rafael Moori Pinto

O INSTITUTO DO CONSENTIMENTO NO TRATAMENTO DE DADOS PESSOAIS NA INTERNET

Porto Alegre

2018

RAFAEL MOORI PINTO

O INSTITUTO DO CONSENTIMENTO NO TRATAMENTO DE DADOS PESSOAIS NA INTERNET

Trabalho de conclusão de curso apresentado à Faculdade de Direito da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Dr. Rafael de Freitas Valle Dresch

Porto Alegre

2018

AGRADECIMENTOS

Agradeço a todos os meus amigos e, especialmente, aos meus colegas, Aline, Aylton, Fábio, Gustavo, Laura e Ulisses, que me acompanharam nessa jornada, compartilhando os eventuais sucessos e recorrentes frustrações da vida acadêmica.

Agradeço aos profissionais da Advocacia-Geral da União e da Justiça Federal do Rio Grande do Sul, com quem tive a oportunidade e a honra de estagiar, por toda a paciência, aprendizado e por serem exemplos de profissionais.

Agradeço ao Prof. Rafael Dresch, pela confiança depositada em mim ao aceitar a orientação e por sempre se mostrar acessível e disposto a auxiliar no que fosse necessário.

Agradeço, por fim, aos meus pais, Carlos Eduardo e Elisa Meiko, pelos valores passados a mim, pelo carinho e amor incondicionais, pelo apoio e suporte constantes e por sempre confiarem em mim, mesmo (e principalmente) quando eu mesmo não confiava. Sem vocês, esta conquista não seria possível e, a tudo que já fizeram por mim, jamais serei capaz de agradecer o suficiente.

RESUMO

Este trabalho é dedicado ao estudo do instituto do consentimento no contexto das contratações eletrônicas referentes ao tratamento de dados pessoais. O desenvolvimento de tecnologias de processamento de dados modificou a compreensão do direito à privacidade, que abandona a concepção clássica de um direito a estar só e passa a ter como conteúdo a possibilidade de controle dos dados pessoais e das informações que dizem respeito a cada indivíduo. Assim, na primeira parte, faz-se uma análise do direito à privacidade, identificando-se seus fundamentos legais e a evolução de suas definições. Na segunda parte, examina-se o direito à proteção de dados pessoais por meio do desenvolvimento geracional das normas europeias, dos seus princípios relativos à matéria e da abordagem deste direito pelo ordenamento jurídico brasileiro. Por último, na terceira parte, trata-se do instituto do consentimento, verificando-se seus requisitos de validade, obstáculos relativos à sua eficácia para garantia da privacidade nas contratações eletrônicas e possíveis alternativas a tais problemas.

Palavras-chave: consentimento; proteção de dados; autodeterminação informativa; privacidade.

ABSTRACT

This paper examines the consent relative to the processing of personal data disclosed in electronic contracts. The development of data processing technologies changed what we comprehend by the right to privacy, which abandons the classical idea of a right to be let alone and now translates as the possibility of controlling ones personal data and information. Therefore, in its first part, this paper analyzes the right to privacy, identifying its legal grounds and the evolution of its concepts. In its second part, this research examines the right to personal data protection through the generational law development in Europe, the data protection principles and the approach by the Brazilian law. Lastly, in the third part, it is adressed the consent mechanism, verifying its legal requirements, obstacles regarding its efficiency for the protection of personal data and possible alternatives to such challenges.

Keywords: consent; data protection; informational self-determination; privacy.

SUMÁRIO

INTRODUÇÃO

O atual modelo social, marcado pelo protagonismo da informação, prescinde de uma utilização cada vez mais ampla de dados pessoais para as mais variadas atividades a fim de que os indivíduos possam se desenvolver com autonomia e liberdade. Contudo, o tratamento de dados pessoais, em particular por processos automatizados, é uma atividade de risco, que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de tais dados (DONEDA, 2011, p. 92). Assim, para a garantia de uma efetiva tutela da privacidade e da autodeterminação informativa, é imprescindível um estudo do direito à proteção de dados pessoais, em especial no que tange ao papel do usuário quanto ao consentimento e legitimidade no processo de tratamento destes dados.

A atenção mundial voltou-se para os riscos das tecnologias relacionadas à informação quando o ex-analista de segurança da NSA (*National Security Agency*), Edward Snowden, trouxe ao conhecimento geral a existência de diversos sistemas de monitoramento telemático: PRISM, Upstream e XKeyscore, entre outros. Esses sistemas revelaram a capacidade dos Estados de interceptação, armazenamento e catálogo do tráfego mundial da internet (MORAIS e NETO, 2014, p. 418), fragilizando qualquer senso de segurança que ainda restava em relação às informações na Rede.

Não obstante, a vigilância estatal está longe de ser a única preocupação, no tocante à segurança das informações e à privacidade. Nesse sentido, Laura Mendes ressalta os riscos à privacidade dos consumidores ao longo do processo de tratamento de dados realizado pelas empresas nas relações comerciais celebradas na internet (MENDES, 2014, p. 94). Assim, chama a atenção às tecnologias de controle na internet - como *cookies* e *spywares* (Idem, p. 100) - bem como às técnicas de extração de informações a partir de dados coletados - como *Datawarehousing*, *Data mining*, *Online Analytical Processing* (OLAP), Construção de Perfil (*profiling*) e Sistema de Avaliação (*scoring*) (Idem, p. 108).

Mais recentemente, o escândalo envolvendo a empresa Cambridge Analytica e o Facebook fez com que os holofotes fossem direcionados novamente à questão da insegurança dos dados na internet, em especial nas redes sociais. O caso envolveu a coleta de informações pessoalmente identificáveis de até 87 milhões de usuários do Facebook, a partir de 2014, que foram utilizados para influenciar a opinião dos eleitores no processo eleitoral norte-americano. A coleta dos dados pessoais foi realizada por meio de um aplicativo chamado

thisisyourdigitallife, que coletou as informações não só dos usuários que fizeram o seu download e aceitaram participar da pesquisa do aplicativo, como também de diversas pessoas conectadas a esses usuários na rede social.

Assim, resta evidente a necessidade de regulação do direito à proteção dos dados pessoais, a fim de proteger os indivíduos contra tratamentos abusivos ou não autorizados de seus dados. No entanto, salienta-se que o que se busca não é um controle absoluto das pessoas sobre todas as informações que lhe digam respeito, visto que é desejável, em alguma medida, a utilização de dados pessoais por parte das empresas e do Estados. Pelas empresas, no tocante às maiores comodidades na oferta de produtos e serviços. E, por parte do Estado, tanto no que se refere ao interesse público à segurança e viabilidade das investigações criminais, quanto em relação às coletas de informações, por meio de Censos, para que sejam elaboradas políticas públicas adequadas.

Nesse sentido, o instituto do consentimento vem sendo utilizado como a principal ferramenta para a garantia da autodeterminação informativa. O instituto se tornou a peça central das legislações de proteção de dados pessoais e, mesmo na legislação brasileira, já se percebe o seu papel estrutural no tocante à legitimidade no tratamento de dados. Contudo, a experiência de diversos países, no que se refere à tutela dos dados pessoais na internet, demonstra que a garantia do consentimento do usuário, por si só, não é suficiente para assegurar a inviolabilidade de sua privacidade. Isto porque não só existe uma disparidade informacional entre os usuários e as empresas detentoras dos dados – de maneira que os indivíduos não possuem a capacidade de dimensionar os efeitos da autorização ao tratamento de dados pessoais –, com também há a problemática do desinteresse e descuido dos usuários quanto a essa tomada de decisão.

Portanto, no primeiro capítulo, será analisado o direito constitucional à intimidade e vida privada, porquanto consiste no pressuposto jurídico para o desenvolvimento de um direito à proteção de dados pessoais. Será abordada a dicotomia entre as noções de espaço público e o privado, a fim de identificar uma dimensão possível ao reconhecimento daquilo que é íntimo e privado ao indivíduo e, pois, necessário ao desenvolvimento de sua personalidade. Com isso, será analisada a evolução do conceito de privacidade, desde sua concepção clássica como "direito de ser deixado em paz" até às suas concepções mais modernas e funcionais, referentes à possibilidade do indivíduo controlar e interromper o fluxo de seus dados no contexto da sociedade da informação.

Adiante, frente aos perigos que as novas tecnologias apresentam à tutela da privacidade, serão analisadas a forma como os dados vêm sendo tratados e processados, bem como as soluções jurídicas no que tange ao direito à proteção de dados pessoais. Dessa forma, será examinado o desenvolvimento geracional das normas de proteção dos dados pessoais, culminando na faceta mais recente deste direito, traduzido no direito à autodeterminação informativa. Além disso, investigar-se-ão os princípios deste novo direito e seu recente reconhecimento enquanto direito fundamental.

Também no segundo capítulo, será analisada a legislação vigente no País, na qual é possível identificar o direito à proteção de dados pessoais, bem como a maneira como a matéria vem sendo recepcionada pela jurisprudência brasileira. Assim, serão investigados principalmente o Código de Defesa do Consumidor e o Marco Civil da Internet, que consistem na principal base legislativa para a tutela da proteção de dados pessoais. Ademais, será examinado brevemente o anteprojeto da Lei de Proteção de Dados Pessoais.

Por fim, no terceiro capítulo, será abordado o instituto do consentimento enquanto principal ferramenta para a garantia da autodeterminação informativa. Para isso, serão investigados os contratos eletrônicos e os mecanismos pelos quais ocorrem as contratações eletrônicas, por meio das quais comumente se autoriza o uso, coleta, armazenamento e transmissão dos dados pessoais na internet. Neste contexto, imprescindível a análise da problemática em torno do dever de informação aos usuários da internet, tendo em vista consistir em requisito indispensável à legitimidade no tratamento de dados pessoais.

Verificar-se-á que existem problemas quanto à tentativa de estruturação do direito à proteção de dados pessoais por meio do consentimento. Isto se demonstra no momento em que o não consentimento e, pois, o exercício do poder de autodeterminação de não revelar os dados pessoais implica, no mais das vezes, a renúncia ao acesso a um determinado bem ou serviço. Além disso, os efeitos do consentimento nem sempre se mostram nítidos ao usuário, de maneira que sua exigência para o tratamento de dados pessoais acaba por se tornar um procedimento inócuo (DONEDA, 2006, p. 373). Em razão destes problemas, bem como do excessivo número de situações em que o consentimento seria exigido nas relações de consumo pela internet, surge a tendência do desinteresse e consequente descuido dos usuários quanto à tomada de decisões acerca do consentimento ao uso de seus dados.

Desse modo, também será investigada no terceiro capítulo a suficiência do instituto do consentimento a fim de garantir o direito à autodeterminação informativa e a tutela à

privacidade. Analisar-se-á a experiência europeia na regulação da matéria, bem como as soluções atualmente apresentadas à problemática do consentimento.

Assim, o presente trabalho visa a responder aos seguintes questionamentos: quais os requisitos para um tratamento legítimo dos dados pessoais dos usuários de internet? O ordenamento jurídico brasileiro oferece a devida proteção à privacidade dos usuários? O instituto do consentimento é suficiente para a garantia da autodeterminação informativa e da privacidade na internet? Tais questões serão investigadas por meio de revisão bibliográfica, jurisprudencial e legislativa da matéria.

1. A TUTELA À PRIVACIDADE NA INTERNET

O surgimento da sociedade da informação – e, em específico, da internet – representou avanços tecnológicos inéditos, bem como uma saturação de informações, entretenimento e serviços. O advento da internet atuou como catalizador dos efeitos da globalização, trazendo significativas modificações para as relações de consumo, como a massificação do consumo, prevalência dos contratos de adesão e dificuldade de dar adequada proteção ao lado mais fraco da relação de consumo (CANTO, 2015, p. 11-14). Além disso, apaga-se a fronteira entre os espaços de convivência públicos e privados, "permitindo que as tecnologias móveis e cada vez mais portáteis adentrem na esfera doméstica" (Ibidem, p. 21).

Sob essa ótica, é inegável que um dos principais afetados por esta nova realidade é o direito à privacidade. As novas tecnologias de coleta eletrônica de dados, empregadas na internet, "propiciam novos riscos, em situações em que há atentado à privacidade dos indivíduos por meios antes inimagináveis", como nos casos de rastreamento digital das informações acessadas (MARTINS, 2014, p. 265), de modo que "cada movimento no ambiente virtual é capturado e armazenado em volumosos bancos de dados, perdendo-se o controle de quais informações estão sendo comercializadas" (CANTO, 2015, p. 23).

Em decorrência deste constante intercâmbio de informações, o direito à privacidade não mais é contemplado na sua concepção inicial, relacionada com ao isolamento do indivíduo e a proteção da vida íntima. A garantia da privacidade hoje deve abranger também "o direito da pessoa humana de manter o controle sobre os seus dados pessoais" (SCHREIBER, 2014, p. 137-138).

Frente a este contexto, o presente capítulo objetiva buscar uma delimitação do âmbito de proteção da privacidade em sua face atual, traduzida na proteção de dados pessoais. Para tanto, em um primeiro momento, será realizada uma análise terminológica da intimidade, vida privada e outros termos que se relacionam à privacidade, assim como dos diferentes pontos de vista doutrinários referentes à concepção da privacidade. Tal análise é relevante, pois o consenso a respeito do conteúdo dos valores do direito à intimidade e à vida privada importa na delimitação dos bens a serem tutelados (ROBL FILHO, 2009, p. 266). Destarte, a necessidade de delimitação de um espaço privado, em contraposição ao público, não decorre de um reconhecimento de que a liberdade em algum destes campos seria mais importante, mas sim

porque a proteção de cada um enseja tratamentos jurídicos distintos (CACHAPUZ, 2006, p. 105-106).

Ademais, a fim de contextualizar a problemática da privacidade na internet, será realizada uma análise da evolução histórica do conceito. Verificar-se-á a noção de privacidade desde sua concepção inicial, como um direito de estar só (*the right to be let alone)*, inovado na doutrina norte-americana do final do século XIX, até a concepção mais adequada à atualidade, identificável no direito fundamental à autodeterminação informativa.

1.1 TERMINOLOGIA E DEFINIÇÃO DA PRIVACIDADE

O termo "privacidade" é apontado por alguns doutrinadores como um anglicismo, derivado de *privacy*, de modo que o termo adequado seria "privatividade". Tal entendimento decorre do fato de que o "desenvolvimento do termo *privacy* na língua inglesa não teve paralelo em idiomas latinos" (DONEDA, 2006, p. 107). Contudo, afirma Leonardi (2011, p. 45) que tais críticas não procedem, já que "a palavra *privacy* tem raiz no latim, decorrente de *privare*, com a forma adjetiva *privatus*, afirmando inclusive que a expressão "privacidade" é usada pela Constituição de Portugal".

A expressão "privacidade" tornou-se uma "palavra-camaleão", utilizada para abranger uma ampla gama de interesses distintos, que vão da confidencialidade das informações pessoais à autonomia reprodutiva (LEONARDI, 2011, p. 46). Nesse sentido, a ambiguidade do termo "privacidade" traz dificuldades para a resolução de conflitos e, conforme destaca Demócrito Ramos Reinaldo Filho (2002, apud LEONARDI, 2011, p. 47-48):

> Como não se tem um indicativo constitucional ou legal da extensão desse direito, pode haver um tratamento diferenciado pelas cortes judiciárias, variando largamente de acordo com o contexto social e político em que se discutam questões ligadas à privacidade; como as circunstâncias em que esse tema está implicado podem variar largamente, fica difícil prever o resultado das lides judiciais em cada caso concreto, sendo, ao contrário, fácil prognosticar uma tendência ao desencontro de decisões judiciais, um obstáculo frente à harmonização jurisprudencial

Parece, então, que o único consenso a respeito da definição da privacidade é justamente a sua falta de clareza. A própria Corte Europeia de Direitos Humanos, na análise do caso

Niemietz v. Alemanha, não considerou possível ou necessária a tentativa de definição exaustiva da noção de "vida privada".[1]

Vale salientar que a Constituição Federal de 1988 não utiliza a expressão privacidade; o art 5º, X, da CF, declara 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". Do mesmo modo, o Código Civil de 2002 declara a inviolabilidade da vida privada, não existindo qualquer menção à privacidade no diploma legal. Contudo, não é possível extrair uma definição objetiva dos referidos termos de qualquer um dos diplomas legais.

Cabe referir que, ainda que a honra e a imagem estejam listadas ao lado da inviolabilidade da intimidade e da vida privada, tais direitos não se confundem. Predomina o entendimento de que a honra e a imagem constituem direitos autônomos. Pode haver lesão à honra sem que exista violação da intimidade ou da vida privada, e o mesmo é válido para o direito de imagem (ZANON, 2013, p.34)

Destaca-se que, ainda que alguns autores de língua espanhola, tal qual Ricardo Luiz Lorenzetti, compreendam a intimidade e a vida privada como sinônimos, é possível delimitar a cada um destes direitos uma esfera autônoma. Nesse sentido, José Adércio Leite Sampaio (1998 apud ROBL FILHO, 2009, p. 267) explica que a vida privada consiste em uma esfera mais abrangente, da qual a intimidade faria parte. Assim, fazem parte da vida privada a liberdade sexual, a liberdade da vida familiar e a intimidade, bem como outros aspectos de intersecção com outros bens ou atributos da personalidade. Por sua vez, a intimidade estaria mais diretamente relacionada à autodeterminação informativa, cuidando da projeção da vida privada no âmbito das informações pessoais e do relacionamento do ser com os demais.

Não se desconhece que uma parcela significativa de autores, entre os quais se destaca Paulo José da Costa Júnior, René Ariel Dotti, Tércio Sampaio Ferraz Júnior e Alexandre de Moraes, distingue o direito à intimidade do direito à privacidade. Nesta linha, associam este último à vida privada, que teria um âmbito de proteção mais amplo que a intimidade. No que tange aos bens jurídicos a serem protegidos, a vida privada abrangeria os comportamentos e acontecimentos relativos aos relacionamentos pessoais, em geral (incluindo relações comerciais e profissionais) que o indivíduo não deseja que se tornem públicos; por sua vez, a intimidade

[1] Tradução livre. Refere a Corte, na seção 29 do Acórdão: "*The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life*".

buscaria a proteção de uma esfera mais restrita, atinente àquilo que diz respeito somente ao indivíduo (ZANON, 2013, p. 35)

Refere Ferraz Júnior (1993, p. 442) que, dentre os direitos que integram o campo da privacidade, a intimidade é o mais exclusivo e consiste no "âmbito exclusivo que alguém reserva para si". Nesse sentido, diferencia também a intimidade da vida privada, compreendendo um caráter menos exclusivo nesta última, uma vez que "por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum)". Portanto, o atributo básico da intimidade é o estar-só, ao passo que a vida privada trata de situações em que a comunicação é inevitável, de maneira que sua proteção diz respeito a formas exclusivas de convivência.

Nesse sentido, para Ferraz Júnior, a privacidade é compreendida como um direito subjetivo fundamental e manifesta uma estrutura, cujos elementos são o sujeito, o conteúdo e o objeto. Conforme se extrai do nosso ordenamento jurídico, o sujeito, titular do direito, é toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira residente (ou transeunte) no Brasil. Seu conteúdo, por sua vez, é a faculdade específica atribuída ao sujeito; no caso dos direitos pessoais, será a faculdade de constranger os outros ou resistir-lhes, enquanto que, no caso dos direitos reais, a faculdade será de dispor, gozar e usufruir. Por fim, o objeto da privacidade é o bem protegido, qual seja, a própria integridade moral do sujeito (FERRAZ JÚNIOR, 1993, p. 439-440).

Da análise da construção doutrinária de Paulo José da Costa Júnior, extrai-se que o autor associa a esfera individual à proteção da personalidade do indivíduo dentro da vida pública, ao passo que, na esfera privada, tem-se a inviolabilidade da personalidade do indivíduo "dentro de seu retiro" (COSTA JÚNIOR, 1995, p. 30). Assim, o autor relaciona a esfera individual com a proteção da honra, enquanto a esfera privada estaria ligada à proteção contra a indiscrição (Ibidem, p.31).

Nesse sentido, Costa Júnior recorre à doutrina italiana, associando o *diritto al rispetto della vita privata* (direito de ver respeitada a vida privada) ao *diritto alla segretezza*, que consistiria no "direito de impedir que a atividade de terceiro venha a conhecer, ou descobrir, as particularidades da vida privada alheia" (COSTA JÚNIOR, 1995, p. 32). Em suma, este seria um direito do indivíduo em seu isolamento moral de impedir interferências alheias. Diferente deste seria o direito à intimidade (*diritto alla riservatezza)*, que já pressupõe uma interferência na vida privada. Esta seria a situação de um terceiro que adquire legitimamente os segredos que

lhe foram confiados (portanto, sem violação da vida privada), mas, em momento posterior, abusa da confiança, divulgando as intimidades reveladas (COSTA JÚNIOR, 1995, p. 33).

Percebe-se, assim, que a opção constitucional pela diferenciação da intimidade e da vida privada acompanha o desenvolvimento doutrinário, mais especificamente a Teoria das Esferas. Ora referida como teoria dos círculos concêntricos, esta teoria foi desenvolvida inicialmente por Henrich Hubmann e Heinrich Heinkel e, posteriormente, adotada pelo Tribunal Constitucional Alemão. A esfera mais interior consistiria no âmbito nuclear e mais íntimo da liberdade humana, razão pela qual gozaria de proteção absoluta. Em seguida, a esfera privada ampliada incluiria o âmbito privado não pertencente à esfera íntima, gozando de proteção menor. Por último, a esfera social, a qual incluiria todo o restante não englobado pela esfera privada ampliada (ALEXY, 2006, p. 360-361).

Contudo, conforme refere Danilo Doneda (2006, p. 108-109), esta teoria possui limitações quanto à sua aplicação em matéria de proteção de dados pessoais. Por isso, desde a célebre decisão de 1983, do Tribunal Constitucional Alemão, que reconheceu o direito fundamental à autodeterminação informativa, esta teoria não seria mais adequada à definição da privacidade.

Neste ponto, considerando a multiplicidade de sentidos atribuídos, é interessante a análise de João Carlos Zanon acerca dos contornos do direito à privacidade. Sem a pretensão de exaurir o tema, o autor identifica quatro contornos do conceito de privacidade: (i) a proteção da integridade psíquica; (ii) a inviolabilidade (ou liberdade de negação); (iii) conceito legal indeterminado; e (iv) como um direito limitado.

Primeiramente, a privacidade enquanto proteção da integridade psíquica estaria associada ao princípio da exclusividade. Este princípio, idealizado por Hannah Arendt (em contraposição aos princípios da igualdade e diferenciação, que caracterizariam, respectivamente, a vida política e a vida social) é o que rege o âmbito da privacidade (ARENDT, 1959, p. 51-52). Nesse sentido, ele comporta três atributos principais: a solidão; o segredo; e a autonomia (FERRAZ JÚNIOR, 1993, p. 441-442). Desse modo, conforme refere Maria Cláudia Cachapuz (2006, p. 122), permite o reconhecimento de um espaço que possibilita ao indivíduo "viver aquilo que o diferencia dos demais em sua intensidade mais severa, justamente porque assegura, pela atuação de um direito de livre desenvolvimento da personalidade, o espaço de reserva não compartilhado com os demais". Identifica-se a proteção da integridade psíquica da pessoa como bem jurídico tutelado pelo direito à privacidade também

na diferenciação entre intimidade interior e exterior, feita por Costa Júnior (1995, p. 12), em que a interior "é aquela de que o indivíduo goza materialmente, apartado de seus semelhantes", ao passo que a exterior seria "aquela de natureza psíquica"

Por sua vez, também seria identificável na raiz do direito à privacidade "sua função de fixar uma esfera exclusiva e reservada ao indivíduo, com o propósito de livrá-lo da ingerência e da curiosidade alheias" (ZANON, 2013, p. 39-40), traduzida na inviolabilidade e nas liberdades negativas. Com esse sentido se identifica o conceito à privacidade como um direito de estar só (*the right to be let alone)* elaborado na doutrina norte-americana no final do século XIX. Assim concluíram os autores Louis Brandeis e Samuel Warren (1890, p. 205), ao afirmarem que o princípio que protege a publicação indesejada de escritos não é relativo à propriedade privada, mas sim à inviolabilidade pessoal. Aqui, proclama-se, pela primeira vez, "a autonomia e o fundamento primacial do direito à privacidade: um direito à inviolabilidade da pessoa, como expressão de um mais abrangente direito da personalidade" (ZANON, 2013, p. 41). E esta concepção de privacidade a compreende como um direito de "excluir razoavelmente da informação alheia ideias, fatos e dados pertinentes ao sujeito" (FERNANDES, 1977, apud ZANON, 2013, p.43). Assim, atribui-se à pessoa o poder jurídico de se opor à divulgação de sua vida privada e a uma investigação nesta; poder este que se contrapõe a um dever dos demais à não divulgação da intimidade alheia.

Cumpre destacar que esta concepção de privacidade enquanto inviolabilidade pode ser vislumbrada em algumas cartas de direito internacional. Consta no art. 12, da Declaração Universal dos Direitos Humanas, de 1948, que "ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques"[2]. Igualmente, a Declaração Americana dos Direitos e Deveres do Homem prevê que "toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar"[3]. Ainda, a Convenção Americana de Direitos do Humanos – conhecida como Pacto de San José da Costa Rica e internalizada no direito brasileiro por meio do Decreto 678/1992 – quando versa sobre a proteção da honra e dignidade, prevê, em seu art. 11 (2), que "ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de

[2] Redação do art. 12, da Declaração Universal dos Direitos Humanos, adotada e proclamada pela resolução 217 A (III) da Assembléia Geral das Nações Unidas, em 10 de dezembro de 1948.

[3] Redação do art. 5º, da Declaração Americana dos Direitos e Deveres do Homem, proclamada pela resolução XXX, Ata Final, aprovada na IX Conferência Internacional Americana, em Bogotá, em abril de 1948.

ofensas ilegais à sua honra ou reputação", sendo que no art. 11 (3) estabelece o direito à proteção contra tais ingerências.

Em análise da redação da Constituição Federal de 1988, percebe-se que também contempla a inviolabilidade dos direitos relativos à privacidade. Dentro do já mencionado art. 5º, X, declara "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas", assegurando direito de indenização pelo dano decorrente da violação. Observa-se que abrange, sob o conceito de inviolabilidade da privacidade, a casa do indivíduo (art. 5º XI), bem como "o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas" (art. 5º, XII).

Por sua vez, o terceiro contorno do direito à privacidade, levantado por João Carlos Zanon (2013, p. 45) compreende este direito como um conceito legal indeterminado, motivo pelo qual sua delimitação precisa seria tão difícil. Justamente em razão dessa natureza da privacidade como conceito legal indeterminado, seu conteúdo seria altamente vago, impreciso e genérico, de modo que o conceito seria propositalmente abstrato e lacunoso. Desse modo, os conceitos legais indeterminados permitem a preservação da estabilidade do ordenamento jurídico ao mesmo tempo que proporcionam flexibilidade à norma, para que acompanhe as transformações da vida social. Diante destes conceitos, pois, cabe ao julgador preencher as lacunas e determinar a aplicabilidade da norma no caso concreto. Assim, "ao lado das cláusulas gerais e dos princípios gerais de direito, os conceitos legais indeterminados têm a função de dotar o sistema jurídico de certa mobilidade" (Ibidem, p. 46). Portanto, a privacidade – em suas esferas de vida privada e intimidade – seria um desses conceitos elásticos, de maneira que sua concreção depende da análise de casos concretos. Assim, "a tutela jurídica da privacidade relaciona-se com construtos *a posteriori*, e não *a priori*" (Ibidem, p. 49), motivo pelo qual a tarefa de definição exaustiva do conceito estaria fadada ao fracasso.

Por último, constitui um dos contornos à privacidade a própria limitação do direito, uma vez que, como todos os direitos fundamentais, comporta limitações próprias da vida em comunidade e da convivência com outros valores de ordem constitucional (ZANON, 2013, p. 49). Consoante a lição de Ricardo Lorenzetti (1998, p. 393), as próprias normas fundamentais estabelecem limites aos direitos fundamentais. Ademais, o próprio consentimento do indivíduo exerce um papel primordial no que tange à escolha de expor situações íntimas (ZANON, 2013, p. 51); nesse sentido, o próprio titular do direito constrói os limites, pois uma pessoa pode ser mais ou menos reservada quanto a publicação de informações que lhe dizem respeito (LORENZETTI,1998, p. 494).

Conforme ressalta Zanon (2013, p. 52), no caso dos sigilos bancário e fiscal, o próprio dispositivo constitucional que oferece a proteção (art. 5º, XII, da CF/1998) prevê as restrições ao direito, o qual pode ser excepcionado em caso de investigação criminal ou instrução processual penal, ou ainda em caso de estado de defesa (art. 136, §1º, 1, b e c, da CF/1998) e de estado de sítio (art. 139, III, da CF/1998). De modo similar, inviolabilidade à intimidade e vida privada apresenta limites referentes aos direitos de acesso à informação (art. 5º, XIV, da CF); à livre manifestação do pensamento (art. 5º, IV, da CF) e à livre expressão da atividade de comunicação (art. 5º, IV, da CF). O art. 220, §1º, da Constituição Federal, também oferece desafios ao intérprete, ao prever que "nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação", estabelecendo como limites os incisos IV, V, X, XIII e XIV do art. 5º da CF/1998. Ademais, a própria defesa do interesse público pode conferir legitimidade à intromissão sobre a intimidade e vida privada (LORENZETTI, 1998, p. 495).

É relevante o esforço de Marcel Leonardi quanto à interpretação do direito à privacidade na contemporaneidade (LEONARDI, 2011, p. 52 e ss). A fim de ilustrar a problemática que envolve a conceituação da privacidade, Leonardi reúne conceitos unitários produzidos pela doutrina e jurisprudência, separando-os em quatro categorias: (i) direito de ser deixado só; (ii) direito de resguardo contra interferências alheias; (iii) direito ao segredo ou sigilo; e (iv) direito de controle sobre informações pessoais.

Considerando a exposição feita até o momento, é perceptível que esta discussão terminológica possui relevância, porquanto serve para delimitar o âmbito de proteção do direito à privacidade. É incontestável, pois, que a multiplicidade de sentidos associados à proteção da privacidade constitui um problema de difícil solução ao jurista, principalmente quando considerada o contexto atual referente à proteção de dados pessoais.

Sem ignorar todas as construções doutrinárias referidas, as quais trazem importantes distinções à intimidade, sigilo e vida privada, entende-se que, para a presente pesquisa, a adoção do termo privacidade de forma ampla é mais adequada. Entende-se que "o termo é específico o suficiente para distinguir-se de outras locuções com as quais eventualmente deve medir-se, como a imagem, honra ou a identidade pessoal; e também é claro o bastante para especificar seu conteúdo, um efeito da atualidade" (DONEDA, 2006, p. 112). Portanto, a fim de tratar da proteção de dados pessoais no contexto de uma sociedade digitalizada, a unificação dos valores expressos na intimidade e vida privada, mediante adoção do termo privacidade, cumpre melhor os propósitos deste trabalho.

1.2 EVOLUÇÃO DA PRIVACIDADE

O desenvolvimento tecnológico alterou radicalmente a concepção da privacidade, fazendo surgir uma definição mais funcional, relativa à possibilidade de um indivíduo conhecer, controlar, endereçar ou interromper o fluxo das informações que lhe dizem respeito (MARTINS, 2014, p. 285). Assim, para uma devida compreensão acerca da problemática atual que rege a proteção da privacidade na internet, é imprescindível a realização de uma breve análise da evolução do direito à privacidade.

De início, destaca-se que, ainda que uma doutrina própria da privacidade só tenha surgido no século XIX, a diferenciação entre os espaços públicos e privados remonta ao período da antiguidade. Nesse sentido, Hannah Arendt (2007, p. 48) refere que hoje é chamado de privado é um círculo de intimidade cujas características somente são observáveis a partir da era moderna, ainda que suas raízes possam ser observadas nos períodos últimos da civilização romana.

Já na Grécia Antiga era verificável uma diferenciação entre o espaço privado, cujo centro era constituído pela casa (*oikia*) e pela família, e o espaço público, destinado à organização política. A partir do surgimento das cidades-estado e da *bios politikos*, o cidadão pertencia a duas ordens distintas de existência: uma relativa ao que lhe era próprio e outra ao que lhe era comum em relação aos demais (Ibidem, p. 33). Desse modo, as duas esferas possuíam características contrastantes e até mesmo opostas. Enquanto a vida política era marcada pelos discursos, retórica e persuasão, associava-se à vida em família a violência típica ao modelo de vida pré-político (Ibidem, p.36). O domínio absoluto e inconteste, exercido pelo chefe da casa, típico da vida privada era, pois, incompatível com a vida política, identificável com a esfera pública (Ibidem, p. 37).

Contudo, refere Sampaio Ferraz Jr. que esta distinção entre as esferas pública e privada, que era clara na antiguidade clássica, para os romanos e gregos, perde a nitidez com o advento da era moderna e o surgimento da esfera social. Com isso, surgem duas novas dicotomias que estão na raiz dos direitos humanos modernos: Estado e sociedade, sociedade e indivíduo. Nesta senda, emergem as concepções de social-público, que diz respeito à área política, e social-privado, referente à área econômica, do mercado. E é justamente em contraposição a essa presença "abrangente e avassaladora do mercado que nivela homens à mercadoria" que se

coloca a privacidade do indivíduo. Em análise desse fenômeno, Sampaio Ferraz Jr. reconhece que o âmbito social-público (político) é dominado pelos princípios da transparência e igualdade; o social-privado (mercado), pelo da diferenciação; e, por fim, o âmbito da individualidade privativa é regido pelo princípio da exclusividade (FERRAZ JÚNIOR, 1993, p. 441). Nesse sentido proclama Hannah Arendt, ao dizer que:

> "[...] a sociedade de massas não apenas destrói a esfera pública e a esfera privada: priva ainda os homens não só do seu lugar no mundo, mas também do seu lar privado, no qual antes eles se sentiam resguardados contra o mundo e onde, de qualquer forma, até mesmo os que eram excluídos do mundo podiam encontrar-lhe o substituto no calor do lar e na realidade da vida em família" (ARENDT, 2007, p. 68).

Portanto, ainda que existisse alguma delimitação de espaços público e privado na antiguidade, a preocupação com a privacidade só emerge com o surgimento da esfera social. Isto porque só há de se falar em privacidade onde há risco de violação do isolamento de uma pessoa ou grupo de indivíduos. Somente pode existir privacidade onde há uma alternativa à privacidade, ou seja, onde há uma possibilidade de divulgação ou retenção de ações ou palavras. Assim, a privacidade pressupõe a existência de uma interação entre pessoas em um espaço de convivência em comum. (SHILLS, 1966, p. 282).

Costuma-se apontar que o primeiro reconhecimento judicial do direito à privacidade remonta a um julgado do Tribunal Civil do Sena de 16 de junho de 1858. Tratou-se de caso em que foram contratados dois artistas para desenhar uma famosa artista da época em seu leito de morte, a pedido da irmã. Posteriormente, sem o devido consentimento, o desenho foi exposto e colocado à venda em estabelecimento comercial. O Tribunal determinou a apreensão do desenho e de suas várias provas fotográficas. Conforme aponta Paulo José da Costa Júnior, a importância da decisão diz respeito justamente ao reconhecimento de uma distinção entre a vida privada e a pública, mesmo no momento da morte, independentemente do quão grande ou famosa fosse a pessoa quando viva (COSTA JÚNIOR, 1995, p. 13)

Mas foi nos Estados Unidos, em fins do século XIX, que o direito à privacidade começou a tomar corpo. Thomas McIntyre Cooley, jurista norte-americano que foi presidente da Suprema Corte de Michigan, dedicando-se em primeiro lugar ao tema, foi quem cunhou, em 1888, a expressão *the right to be let alone* (o direito de estar só).

Posteriormente, na pioneira obra *The Right to Privacy*, os juristas Brandeis e Warren partem dos princípios da vida, integridade física e propriedade, reconhecidamente assegurados pela common law, para delimitar o direito à privacidade.

1.2.1 A privacidade enquanto *right to be let alone*

A doutrina da privacidade tem início em 1890, com o pioneiro artigo publicado por Samuel Warren e Louis D. Brandeis na *Harvard Law Review*: *The Right to Privacy*. O texto foi motivado por casos recentes de violação à privacidade por meio de tecnologias da época. Os autores norte-americanos abordaram a insuficiência do instituto da propriedade para a proteção dos sentimentos, emoções e pensamentos expressos por meio da escrita ou da arte, já que a prevenção da publicação seria apenas um dos aspectos de um direito mais geral: o direito de ser deixado em paz (*the right of the individual to be let alone*) (BRANDEIS e WARREN, 1890, p. 205). Assim, a proteção de escritos e outras formas de produção pessoal contra uma publicação indesejada não decorre de um princípio de proteção da propriedade privada, mas sim da inviolabilidade da pessoa.

Os doutrinadores analisam decisões em que as Cortes sustentam a proibição da publicação de cartas e escritos pessoais com base na quebra da confiança ou outras obrigações contratuais. Contudo, ressaltam que a partir do momento em que os aparatos tecnológicos modernos proporcionam mais oportunidades a violações sem qualquer participação da parte afetada, deve ser estabelecida uma base principiológica mais extensa a fim de garantir a proteção legal.[4]

Da análise do referido artigo, observa-se que os advogados concluem que o conteúdo do direito à privacidade era extraível da *common law*. Nesse sentido, a essência da privacidade estaria não na propriedade privada, mas na inviolabilidade da pessoa. Contudo, insta registrar que os autores não foram responsáveis por cunhar o termo *the right to be let alone*. Conforme referem no mencionado artigo (1890, p. 195), a expressão foi elaborada pelo Juiz Thomas Cooley, sendo que os autores não associam expressamente o conteúdo do direito à privacidade a este direito de ser deixado em paz (DONEDA, 2006, p. 105-106).

Em verdade, Warren e Brandeis não elaboram propriamente uma definição da privacidade, apenas referem que a *common law* garante o direito individual de determinar em que medida os pensamentos, sentimentos e emoções serão comunicados aos outros. Então esse

[4] Tradução livre: "*[...] now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation*". Ibidem. p. 211.

right to be let alone seria um direito geral à imunidade da pessoa, o direito à própria personalidade (LEONARDI, 2011, p. 53). Dessa maneira, em que pese o mérito dos norte-americanos quanto à inovação de uma doutrina da privacidade, o referido direito de estar só não indica os limites da privacidade, ou seja, não aponta em quais circunstâncias, no caso concreto, devemos ser deixados em paz (LEONARDI, 2011, p. 54).

Segundo esta concepção, a privacidade é compreendida como uma *zero-relationship*, no sentido de que é constituída pela ausência de interação, comunicação ou percepção dentro de contextos em que esta interação, comunicação ou percepção são viáveis (SHILS, 1966, p. 281).

Por este motivo, a concepção da privacidade como um direito de estar só recebe críticas, pois, não só é marcado por um individualismo exacerbado, que visa a proteger a ausência de interação, mas também se torna um conceito amplo demais, de modo que não serve para delimitar o âmbito de proteção da privacidade (LEONARDI, 2011, p. 54).

Neste sentido se manifestou a Corte Europeia de Direitos Humanos, no caso Niemietz v. Alemanha, referindo que o respeito à vida privada deve compreender também, em alguma medida, o direito de estabelecer e desenvolver relações com outros indivíduos. Por isso, seria restritivo demais limitar a noção de privacidade a um círculo íntimo dentro do qual o indivíduo poderia viver sua vida privada da maneira que quisesse, excluindo completamente o mundo exterior não englobado por este círculo.[5]

1.2.2 A privacidade na era da internet

Pode-se estabelecer a Revolução Industrial como "o momento a partir do qual a tecnologia passou a ocupar um lugar de maior destaque na dinâmica social" (DONEDA, 2006, p. 34), fenômeno este que se perpetua até os dias atuais. O campo jurídico, por sua vez, não foi imune a essas influências, de maneira que se percebe, desde o início, a tecnologia como um vetor do interesse jurídico sobre a proteção da privacidade.

Em um primeiro momento, o surgimento de aparatos capazes de interferir na vida privada das pessoas, como por meio da fotografia, impulsionou o estabelecimento do direito à

[5] Tradução livre. Seção 29. Disponível em <http://www.refworld.org/cases,ECHR,3f32560b4.html>. Acesso em 16/05/2018.

privacy, que se sustentava nos clássicos direitos de liberdade e propriedade, a fim de defender o direito de ser deixado em paz (*the right to be let alone*). Mas, da mesma forma que as inovações tecnológicas desenharam esta primeira concepção de privacidade, o contínuo desenvolvimento tecnológico deu ensejo à necessidade de surgimento de outros conceitos, que se adequassem melhor ao estado da técnica atual.

O surgimento de computadores, bancos de dados e o início do tratamento automatizado de dados modificou substancialmente o perfil deste direito, transformando-o em uma disciplina mais funcional: a proteção de dados pessoais. Assim, pode-se dizer que a proteção de dados pessoais conta com pressupostos ontológicos idênticos aos da própria proteção da privacidade, sendo uma "continuação por outros meios" (DONEDA, 2006, p. 27). Com isso, a privacidade não mais se identifica com a noção de *zero-relationship* e a estruturação em torno do eixo "pessoa-informação-segredo", mas sim em um eixo "pessoa-informação-circulação-controle". (Ibidem, p. 23). Nesse sentido, refere Guilherme Martins que "voltam-se as atenções para o controle, por indivíduos e grupos, do exercício dos poderes fundados na disponibilidade de informações, contribuindo para um equilíbrio sociopolítico mais adequado" (MARTINS, 2014, p. 264).

A associação do direito à privacidade não com o isolamento do indivíduo, mas sim com a proteção de dados pessoais, fica mais evidente a partir da década de 1970, em que cada vez mais a privacidade foi ligada a casos de informações armazenadas em bancos de dados. Ademais, não é coincidência que a primeira legislação norte-americana sobre *privacy* é o *Fair Credit Reporting Act*, de 1970 (DONEDA, 2006, p. 141).

O desenvolvimento das tecnologias da informação representou um aumento na capacidade de processamento de dados e, com isso, o surgimento de novas ameaças. Mais recentemente, a popularização da internet trouxe ainda mais possibilidades de intrusões indesejadas. Diferentemente do que se pensou em um primeiro momento, os perigos da atualidade não residem mais na figura dos grandes bancos de dados, controlados pelo Estado, mas sim nas diversas atividades que ocorrem diariamente na rede. Nesse sentido, Simson Garfinkel, em analogia à literatura Orwelliana, refere que o futuro ao qual nos encaminhamos

não é com um “Grande Irmão”, que vigia e grava cada instante, mas sim com centenas de “pequenos irmãos”, que constantemente vigiam e interrompem nossa vida diária.[6]

Neste contexto de constantes ameaças à privacidade advindas de processos automatizados de tratamento de dados pessoais, o reconhecimento do direito à autodeterminação informativa constituiu um marco importante para garantia do desenvolvimento do indivíduo. O direito fundamental à autodeterminação informativa foi primeiramente reconhecido na pioneira decisão da Corte Constitucional Alemã, em 1983. A decisão será analisada em maiores detalhes posteriormente, no segundo capítulo, mas merece destaque que a referida decisão reconheceu a proteção de dados pessoais não como um fim em si mesma, mas como um meio para o exercício dos direitos básicos e fundamentais ao desenvolvimento do indivíduo. Assim, foi reconhecida a necessidade de proteção da capacidade individual de decidir por si, no que tange às informações que lhe dizem respeito (ROUVROY e POULLET, 2009, p. 52). No mesmo sentido refere Lorenzetti, ao afirmar que a autodeterminação informativa “inclui a faculdade do indivíduo de dispor e revelar dados referentes a sua vida privada e sua livre disposição em todas as fases da elaboração e uso dos dados, ou seja, sua acumulação, sua transmissão, sua modificação e seu cancelamento” (LORENZETTI, 2004, p. 90).

Contudo, diferentemente do contexto que deu origem ao direito fundamental à autodeterminação informativa, no qual o governo representava a principal ameaça a proteção de dados pessoais, hoje o comércio pela Internet é o que oferece maiores perigos à privacidade (PAESANI, 2014, p. 37).

A Internet pode ser compreendida como uma “rede internacional de computadores conectados entre si” e constitui um “meio de comunicação que possibilita o intercâmbio de informações de toda natureza, em escala global, com um nível de interatividade jamais visto anteriormente” (LEONARDI, 2005). Por esse motivo, a Internet representa um aumento na possibilidade de coleta eletrônica de dados, a qual tem como riscos inerentes (MARTINS, 2014, p. 265): “a maior quantidade de informações disponíveis, a enorme facilidade e a maior escala de intercâmbio de informações, os efeitos potencializados das informações errôneas e a duração perpétua dos registros”.

[6] Tradução livre: “The future we're rushing towards isn't one where our every move is watched and recorded by some all-knowing "Big Brother." It is instead a future of a hundred kid brothers that constantly watch and interrupt our daily lives”. GARFINKEL, Simson. Database Nation: the death of privacy in the 21st century.

Dentre as principais tecnologias de tratamento de dados pessoais que oferecem perigos à privacidade dos usuários, merecem menção as técnicas de coleta de dados, como os *cookies* e *spyware*, além de técnicas de processamento dos dados pessoais, como o *data mining, Online Analytical Processing (OLAP),* a construção de perfil (*profiling).* As técnicas referidas não esgotam as possibilidades de coleta e processamento de dados, mas já permitem uma análise dos riscos oferecidos à privacidade dos usuários no contexto social atual.

Os *cookies* são marcadores digitais que consistem em "arquivos de texto oriundos de um *website*, que são gravados no disco rígido de determinado computador e utilizados por seu programa navegador", de maneira que podem tornar mais conveniente a navegação na Internet, evitando que certos dados precisem ser fornecidos a cada vez que uma determinada página é visitada (LEONARDI, 2012, p. 418). Os perigos oferecidos pelos *cookies* são mínimos, considerando que são lidos somente pelo servidor que os criou, além de não possuírem habilidade de vasculhar o conteúdo do disco rígido (Ibidem, p. 420). Contudo, eles possibilitam o rastreamento do comportamento do usuário em diversos sites, quando inseridos por um longo período de tempo (MENDES, 2014, p. 103), motivo pelo qual é essencial que o usuário não só seja notificado, mas também aceite a utilização dos *cookies*.

Diferentemente dos *cookies*, os *spyware* oferecem riscos maiores aos usuários. Eles consistem em um *software* que tem como objetivo "monitorar atividades de um sistema e enviar as informações coletadas para terceiros, podendo comprometer a privacidade do usuário e a segurança do computador" (MENDES, 2014, p. 104). Esse monitoramento pode ser referente a URL acessadas, podendo até mesmo capturar senhas bancárias e números de cartões de crédito. Em razão deste alto potencial invasivo e consequente oferecimento de riscos à personalidade dos cidadãos, a legitimidade da utilização do *spyware* é bastante questionável.

No tocante às tecnologias de processamento de dados, são essencialmente técnicas responsáveis por lapidar os dados, transformando-os em informações úteis para o interessado (MENDES, 2014, p. 95). Uma das principais técnicas é a de *data mining* (ou mineração de dados), que consiste em um "processo pelo qual dados de difícil compreensão são transformados em informações úteis e valiosas para a empresa, por meio de técnica informática de combinação de dados e de estatística" (Ibidem, p. 109). Para que a mineração de dados seja possível, costuma-se utilizar a técnica de *data warehousing*, a fim de agregar e organizar as informações coletadas a partir de diferentes bancos de dados (ZARSKY, 2003, p. 8).

De modo similar, o *Online Analytical Processing (OLAP)* também possibilita a análise de dados a partir dos dados presentes em um *data warehouse.* A técnica foi desenvolvida com a finalidade de aperfeiçoar a mineração de dados, de maneira que, por meio desta, as empresas podem realizar "a previsão de tendências e prognósticos, a partir de uma determinada base de dados" (MENDES, 2014, p. 111).

Por sua vez, uma das técnicas mais utilizadas para o processamento de dados é a de *profiling* (construção de perfil). Mireille Hildebrandt (2008, p. 18) afirma que o *profiling* automatizado é resultado de um processo de mineração de dados, que indicam padrões e relações entre os dados coletados. Assim, identifica-se um padrão comportamental, mediante o qual se podem prever comportamentos futuros. Por este motivo, Laura Mendes (2014, p. 111) refere que esta técnica "possibilita a tomada de importantes decisões a respeito dos consumidores, trabalhadores e cidadãos em geral, afetando diretamente a sua vida e influenciando o seu acesso a oportunidades sociais".

Contudo, em que pese todos os riscos à privacidade presentes nas tecnologias referidas, há de se destacar que o uso dessas técnicas não é necessariamente ilegítimo. Um exemplo seria o da publicidade dirigida, que somente é possível mediante tratamento de dados pessoais e possui um papel essencial no fornecimento de serviços e informações na Internet, até mesmo porque uma quantia considerável dos usuários prefere o oferecimento de serviços aparentemente gratuitos, em troca de dados pessoais, do que a cobrança em dinheiro pelos mesmos serviços. Assim, o pagamento com dados é uma escolha válida e deve ser respeitada pelo ordenamento jurídico (LEONARDI, 2012, p. 417-418), principalmente considerando a própria possibilidade de o indivíduo decidir a respeito do uso de suas informações.

Sob essa ótica, o consentimento do usuário de Internet recebe um papel instrumental como mecanismo de exercício da autodeterminação informativa, pois ele que consiste no principal meio de garantia da legitimidade do tratamento de dados na Internet. Por esse motivo, a tutela da privacidade na Internet não é contemplada pelo direito de estar só, pois compreende "um problema de comunicação, no tocante aos dados utilizados sem consentimento para construir um perfil do sujeito" (MARTINS, 2014, p. 266).

2. O DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Conforme se extrai da explanação realizada até aqui, o direito à privacidade hoje assumiu um sentido mais amplo, que não se limita à proteção da intimidade. "Não se limita ao direito de cada um de ser 'deixado só' ou de impedir a intromissão alheia na sua vida íntima e particular" (SCHREIBER, 2014, p. 139). O desenvolvimento tecnológico e consequente multiplicação de mecanismos automatizados para tratamento de informações estimularam um aumento significativo no fluxo de dados na sociedade contemporânea (Ibidem, p. 137). Em razão disso, prevalecem hoje definições mais funcionais da privacidade, referentes à proteção de dados pessoais e "à possibilidade de um sujeito conhecer, controlar, endereçar ou interromper o fluxo das informações que lhe dizem respeito" (MARTINS, 2014, p. 264).

Sendo assim, o presente capítulo tem como escopo uma compreensão melhor desta face atual do direito à privacidade. Para isso, serão analisadas as normas de proteção de dados pessoais, conforme o desenvolvimento geracional proposto por Viktor Mayer-Schönberger. Em um segundo momento, serão examinados os princípios associados à proteção de dados pessoais. Ademais, será verificado o ordenamento brasileiro no que tange à construção legal da proteção de dados pessoais, a fim de examinar se é oferecida proteção suficiente aos dados pessoais, em nosso País. Por fim, serão estudados especificamente os requisitos para a legitimidade do tratamento de dados pessoais, mediante análise não só do ordenamento brasileiro, mas também da regulação europeia, para que restem evidentes as condições para que não exista violação à privacidade.

Vale acrescentar que a legislação brasileira não traz uma definição de dados pessoais, mas, para a presente pesquisa, considera-se dado pessoal "qualquer informação relativa a uma pessoa singular identificada ou identificável" (MENDES, 2014, p. 56). Não se ignora que, doutrinariamente, são tecidas diferenciações quanto aos conceitos de dados e informações pessoais. O termo "dado" apresentaria uma conotação mais primitiva e fragmentada, "como uma informação em estado potencial, antes de ser transmitida", isto é, uma "pré-informação". Por outro lado, a informação "alude a algo além da representação contida no dado" (DONEDA, 2006, p. 152). É cabível a diferenciação também dos chamados "dados sensíveis", tendo em vista que possuem uma "potencialidade maior de causar ofensa aos direitos fundamentais", motivo pelo qual demandam proteção especial (LIMBERGER, 2007, p. 203). São dados relativos à "origem racial ou étnica, às opiniões políticas, às convicções religiosas ou

filosóficas, à filiação sindical ou associativa, bem como os relativos à saúde ou sexualidade" (Ibidem).

2.1 O DESENVOLVIMENTO GERACIONAL DAS NORMAS DE PROTEÇÃO DE DADOS PESSOAIS

2.1.1 O Estado social e a centralização da informação: a primeira geração de normas

O século XX trouxe uma série de mudanças que contribuíram para o abandono da concepção da privacidade enquanto *zero relationship*. Dentre os vários motivos, tem-se a mudança de um modelo de estado liberal para o Estado de bem-estar social (*welfare state*); a mudança de relacionamento entre cidadão e Estado; o desenvolvimento tecnológico - ao qual correspondia uma capacidade técnica cada vez maior de recolher, processar e utilizar a informação; e o consequente aumento do fluxo de informações (DONEDA, 2006, p. 12).

O surgimento do *Welfare State* trouxe uma demanda cada vez maior de informações a respeito dos cidadãos, uma vez que um conhecimento profundo da população é indispensável para a instituição de políticas públicas. Além disso, nesta época a utilização de informações em larga escala era realizada primordialmente pelo Estado. Isso porque as empresas privadas não tinham poder econômico suficiente para tornar atrativa a coleta e tratamento de dados.

Este período foi marcado pela centralização das informações e dados pessoais em gigantescos bancos de dados, controlados pela Administração Pública. Preocupações com o monopólio estatal das informações e o consequente fim da privacidade são perceptíveis na literatura da época, na qual se destaca a obra de George Orwell, "1984". Por meio da figura do "Grande Irmão", a icônica obra expôs os perigos da vigilância estatal.

Como uma reação a este contexto, a primeira geração de normas de proteção de dados pessoais surgiu com o escopo de regular estes gigantescos bancos de dados, sob controle dos Estados e de grandes empresas, bem como de enfrentar as pretensões de centralização dos dados em grandes bancos de dados nacionais, que surgiram nas décadas de 1960 e 1970. São legislações que representam essa primeira geração de normas: a Lei de proteção de dados do Estado Alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de

Dados do Estado Alemão de *Rheinland-Pfalz* (1973), as diversas propostas legislativas alemãs de proteção de dados, as propostas da Áustria de uma Lei de Proteção de Dados (1974), bem como a Lei Federal de Proteção de Dados da Alemanha, de 1977 (MAYER-SCHÖNBERGER, 1997, p. 221).

Explica Viktor Mayer-Schönberger (1997, p. 222) que o desenvolvimento dos computadores e da tecnologia de coleta e armazenamento de dados surgiu no contexto do Estado Social. O aumento dos deveres estatais, que passava a ser responsável por massivas reformas sociais, gerou uma necessidade de sistemas mais sofisticados de planejamento e burocracia, para os quais a obtenção de informação da população era indispensável. Sem computadores, portanto, o Estado Social seria inviável.

Este interesse governamental na centralização da informação é perceptível na proposta legislativa da Suécia, no fim da década de 1960, que visava à fusão de dados tributários, cadastros de registros civis e dados de censo em um único banco de dados nacional. Igualmente, na Alemanha, o Estado da Bavária tinha interesse no aproveitamento dos computadores lá instalados para as Olimpíadas de 1972, a fim de centralizar as informações em um grande sistema. Além disso, na esfera federal, a Alemanha criou um comitê especial para coordenar a união dos pretendidos bancos de dados municipais, estaduais e federais (Ibidem).

As críticas a essas propostas de criação de bancos de dados nacionais, motivadas principalmente pelo medo da vigilância estatal por meio da tecnologia, sedimentaram o cenário de criação da primeira geração de normas de proteção de dados. Estas primeiras leis não tinham como foco a proteção individual da privacidade, mas sim a função do processamento de dados na sociedade (MAYER-SCHÖNBERGER, 1997, p. 223). Refere Doneda (2011, p. 96) que "o núcleo dessas leis girava em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle a posteriori por órgãos públicos". Consequentemente, nessas primeiras regulações não existia a previsão de direitos subjetivos quanto à conformidade com o tratamento de dados. Em vez disso, foram criadas instituições para supervisionar a devida obediência às normas de proteção de dados (MAYER-SCHÖNBERGER, 1997, p. 224). A primeira geração de normas estabelecia princípios gerais e abstratos de proteção, focalizados essencialmente na atividade de processamento de dados (DONEDA, 2011, p. 96). Sua linguagem era marcada pela priorização de jargão técnico, utilizando termos como "bancos de dados", "registros de dados", "arquivos", e não propriamente à "privacidade", "proteção da intimidade" e "informação".

Contudo, a não concretização dos temidos bancos de dados nacionais, o desenvolvimento tecnológico - que, a partir da diminuição do tamanho dos computadores, permitiu a descentralização dos centros de processamento - bem como os anseios populacionais por uma proteção com enfoque na privacidade, fizeram com que estas primeiras normas de proteção de dados se tornassem ultrapassadas (MAYER-SCHÖNBERGER, 1997, p. 225).

2.1.2 A segunda geração e a proteção da privacidade

A segunda geração de normas de proteção de dados tinha como enfoque a proteção da privacidade e não mais somente o estabelecimento de procedimentos. Assim, a tutela do indivíduo volta a uma posição de destaque, porquanto a estrutura da proteção de dados passa a ser sustentada pelo direito à privacidade e às liberdades negativas.

São exemplos de legislações deste período a Lei Francesa de Proteção de Dados Pessoais de 1978 (*Informatique et Libertées*) e os Estatutos de Proteção de Dados da Áustria, Dinamarca e Noruega. Além disso, também merecem destaque as Constituições da Áustria, da Espanha e de Portugal que passaram a garantir a privacidade informacional.

Ainda que as normas de primeira geração incluíssem alguns direitos individuais no que tange ao acesso e correção de suas informações pessoais, estes eram interpretados funcionalmente, de maneira a dar suporte à precisão dos dados pessoais processados e armazenados. Ou seja, não se falava em direito individual de decidir a respeito do processamento dos dados, apenas de retificar informações errôneas. A partir da segunda geração, o consentimento do indivíduo ganhou espaço como precondição ao processamento de dados. Não se tratava mais de direito meramente de acesso e retificação de informações, mas sim de uma garantia de escolha individual quanto à autorização do uso dos dados pessoais. Isso é perceptível na legislação norueguesa de proteção de dados, de 1978, que, em seus §7º e §33, concedia aos indivíduos o direito de recusa do processamento de dados para fins de marketing direto ou pesquisa de marketing (MAYER-SCHÖNBERGER, 1997, p. 227).

Todavia, as tentativas de regular a tecnologia e garantir a proteção dos dados por meio das liberdades negativas e escolha individual mostraram-se um otimismo ingênuo, uma vez que a participação no Estado Social pressupunha um fornecimento de informações constante. Diferentemente do contexto social no Estado Liberal, quando tais valores foram idealizados, o

funcionamento da burocracia do *Welfare State* dependia do fluxo de dados pessoais, de maneira que a interrupção ou mesmo o questionamento deste pelo cidadão frequentemente implicava a sua exclusão de algum aspecto da vida social (DONEDA, 2011, p. 97). Percebe-se, então, que essas leis também apresentavam seus problemas, pois a exclusão da vida social era um custo alto demais a se pagar pela proteção dos dados pessoais.

2.1.3 A autodeterminação informativa e a terceira geração de normas

A terceira geração de normas de proteção de dados é marcada pelo reconhecimento do direito à autodeterminação informativa, que se tornou um marco na evolução do conceito de privacidade e no direito à proteção de dados pessoais, "radicalizando a ideia do controle do indivíduo no processamento de seus dados" (MENDES, 2014, p. 41).

O direito fundamental à autodeterminação informativa foi reconhecido em decisão do Tribunal Constitucional Alemão, em 25 de março de 1983, no histórico julgamento da Lei do Censo (*Volkszählungsgesetz*). Essa lei visava a fornecer informações à Administração Pública no que tange ao crescimento populacional, distribuição espacial da população pelo território e atividades econômicas realizadas no país, sendo feita a coleta de dados dos cidadãos por meio de uma série de questionamentos versando sobre profissão, moradia e local de trabalho (MENDES, 2014, p. 30). A lei também previa uma multa àqueles que se recusassem a responder.

Assim, frente às insurgências no tocante à inconstitucionalidade da referida lei, o Tribunal Constitucional Alemão declarou nulos os dispositivos que determinavam a comparação dos dados coletados e a sua transferência para outros órgãos da administração, reconhecendo a constitucionalidade da lei em geral (MENDES, 2014, p. 31). Nesta senda, declarou a Corte Alemã que:

> Dado o contexto do processamento de dados na modernidade, a proteção de indivíduos em face da coleta, armazenamento, uso e transferência ilimitados de seus dados pessoais está integrada ao direito geral da personalidade, previsto no artigo 2.1 em conjunto com o artigo 1.1 da Lei Fundamental (*Grundgesetz* - GG). Nesse sentido, esse direito fundamental garante aos indivíduos o poder de decidir acerca da divulgação e uso de seus dados pessoais.[7]

[7] Tradução livre da redação em inglês *"Given the context of modern data processing, the protection of individuals against unlimited collection, storage, use and transfer of their personal data is subsumed under the general right of personality governed by Article 2.1 in conjunction with Article 1.1 of the Basic Law (Grundgesetz*

A decisão da Corte Alemã produziu efeitos em toda estrutura da proteção de dados da Lei Geral Alemã, declarando que todas as fases do processamento de informação, desde a coleta até a transmissão, estariam sujeitos a limitações constitucionais. Consequentemente, diferentemente da previsão legislativa das normas de segunda geração, determinou-se que o indivíduo deveria estar envolvido continuamente em todas as etapas do processamento de dados (MAYER-SCHÖNBERGER, 1997, p. 229-230)

As normas da terceira geração, portanto, tinham ênfase na participação do indivíduo, ao longo do processamento de dados, e na garantia do direito individual à autodeterminação informativa. Contudo, em que pese o número de garantias asseguradas pela terceira geração de normas, a realidade é que os indivíduos raramente faziam uso de seus direitos. Isto porque, além dos custos e inconveniências de buscar tutela judicial constantemente, tornou-se frequente a previsão de cláusulas contratuais que acarretavam a cessão desses direitos de autodeterminação informativa. Em suma, a autodeterminação informativa tornara-se um privilégio de uma minoria (Ibidem, p. 232).

2.1.4 A quarta geração de normas

As normas da quarta geração surgiram com a finalidade de solucionar os problemas relativos à ineficácia do modelo existente na época, no que tange à autodeterminação informativa. Assim, as novas legislações propuseram duas abordagens distintas, a fim de solucionar os obstáculos citados.

Em primeiro lugar, os legisladores visaram a fortalecer a posição do indivíduo, equilibrando a relação em face das entidades responsáveis pelo processamento dos dados. Com isso, estes esforços preservavam a crença na autodeterminação informativa e na importância da escolha individual, mas reconheciam a necessidade de reequilibrar estas relações. Nesse sentido, destaca-se emendas da Lei Federal de Proteção de Dados da Alemanha, que introduziram o sistema de compensação sem necessidade de demonstração de culpa (*no-fault compensation*) nas reclamações individuais em matéria de proteção de dados, expandindo o

- *GG). In that regard, this fundamental right guarantees in principle the power of individuals to make their own decisions as regards the disclosure and use of their personal data.”*, disponível em <https://freiheitsfoo.de/files/2013/10/Census-Act.pdf>. Acesso em 14/03/2018. Texto original, em alemão, disponível em <http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintText&Name=bv065001>.

modelo já existente na Noruega quanto a reivindicações frente a órgãos de proteção de crédito (MAYER-SCHÖNBERGER, 1997, p. 233).

Por outro lado, os legisladores reduziram a esfera de controle do indivíduo, reconhecendo que determinados assuntos seriam tão importantes que deveriam ser passíveis de proteção absoluta, motivo pelo qual não poderiam estar na esfera de disposição individual (Ibidem). Tal proteção é observável na tutela dos dados sensíveis, cujo processamento tornou-se proibido em diversos países. Isto é observável nas legislações de proteção de dados pessoais da Noruega, Finlândia, Dinamarca, Bélgica, França e Inglaterra. As leis da Alemanha e da Suíça, por sua vez, não proibiam expressamente o processamento de dados sensíveis, mas restringiam fortemente a disposição do indivíduo no tocante a estas informações, de maneira que sua autodeterminação informativa limitava-se ao acesso, correção e exclusão destes dados (Ibidem). De modo similar, a Diretiva Europeia de 1995 permitia o tratamento de dados sensíveis somente em casos excepcionais.

Além disso, as normas de quarta geração são marcadas pela "disseminação do modelo das autoridades independentes para a atuação da lei" (DONEDA, 2011, p. 98), bem como pelo surgimento de normas setoriais específicas, a fim de suplementar as leis gerais de proteção de dados. O modelo de regulação setorial de proteção de dados foi inicialmente implantado nos países nórdicos e foi sendo incorporado mesmo em países com tradição de Leis Gerais de Proteção de Dados - como a Alemanha e da Áustria. Tal modelo de regulação setorial suplementar também foi incorporado expressamente na Diretiva Europeia 95/46/CE. (MAYER-SCHÖNBERGER, 1997, p. 234).

2.2 PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

O desenvolvimento geracional das normas de proteção de dados pessoais demonstra uma evolução na concepção de privacidade, tendendo a uma garantia de maior controle dos dados pessoais, por parte dos indivíduos, bem como à criação de uma estrutura normativa que facilite a responsabilização das entidades que detêm os dados. Nesse sentido, ao longo dessa evolução normativa é possível delinear objetivos e linhas de atuação em torno de princípios em comum, nos quais se observa uma forte convergência de soluções legislativas sobre a matéria (DONEDA, 2006, p. 214).

Esse rol em comum de princípios passou a ser conhecido como "*Fair Information Principles*" e sua origem remonta ao fim da década de 1960 e início dos anos 70, tanto nos EUA quanto na Europa (BENNETT, 2008, p. 7). Refere Doneda (2006, p. 214) que alguns destes princípios já estavam presentes nas leis de primeira e segunda geração, mas a origem desse rol parece se reportar às discussões que acompanharam a tentativa de estabelecimento do *Nacional Data Center*, nos EUA.

Em 1972, foi designada pelo Secretário do Departamento de Saúde, Educação e Bem-Estar dos EUA um comitê consultivo de sistemas automatizados de dados pessoais ("*Advisory Committee on Automated Personal Data Systems*") para estudo do tema. (MENDES, 2014, p. 68). No ano seguinte, foi divulgado um relatório sobre "Registros, Computadores e Direitos do Cidadão", no qual se propunha a redefinição do conceito de privacidade - associando-a com o tratamento de dados pessoais - além de estabelecer cinco princípios fundamentais que todo processamento de dados deveria seguir: (a) não deve existir sistema de armazenamento de dados pessoais secreto; (b) deve existir um meio pelo qual o indivíduo pode ter conhecimento a respeito de quais informações suas estão registradas e como são utilizadas; (c) deve existir um meio para um indivíduo prevenir que informações coletadas com um propósito específico sejam utilizadas ou disponibilizadas para outros fins, sem o seu consentimento; (d) deve existir um meio pelo qual o indivíduo possa corrigir ou retificar um registro de informação a seu respeito; (e) qualquer organização que crie, mantenha, use ou dissemine registros de informações pessoalmente identificáveis deve assegurar que os dados sejam utilizados para o fim pretendido e deve tomar as devidas precauções para evitar o abuso destes dados.[8]

2.2.1 Princípio da finalidade

O princípio da finalidade é fundamental a todas atividades de processamento de dados e prevê a necessidade de correlação entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados. A relevância prática deste princípio é evidente, já que, com base nele, fundamenta-se a restrição de transferência de dados pessoais a terceiros. Do mesmo modo, a partir deste princípio são criados parâmetros para verificar a razoabilidade

[8] EUA, HEW, "*Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems*". Julho, 1973, tradução livre. Disponível em <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em 06/05/2018.

da utilização de determinados dados pessoais para uma certa finalidade, fora da qual estaria configurado o abuso (DONEDA, 2006, p. 216). Assim, este princípio exige que a finalidade do tratamento de dados seja estabelecida de forma expressa e limitada pelo responsável por este tratamento, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidade amplas ou genéricas (MENDES, 2014, p. 71).

2.2.2 Princípio da transparência (ou publicidade)

Este princípio reza que a existência de um banco de dados, contendo dados pessoais, seja de conhecimento público (DONEDA, 2006, p.216). Refere Laura Mendes que este princípio reafirma o preceito democrático, segundo o qual não podem existir dados sigilosos, e centra-se na noção de que a transparência consiste em uma das principais formas de se combater os abusos (MENDES, 2014, p. 71).

Neste aspecto, o princípio da transparência está diretamente relacionado à participação do indivíduo no procedimento de tratamento de dados pessoais, uma vez que, para que esta participação seja efetiva, é preciso, antes de tudo, que o indivíduo tenha acesso às informações acerca da coleta, armazenamento e uso de dados pessoais.[9] Além do mais, este princípio serve de base para o dever dos bancos de dados de publicar seu nome, sede e conteúdo em registros públicos, diários oficiais ou meios de grande circulação, sob pena de ineficácia deste direito, de maneira que a transparência pode ser vista como uma condição essencial à *accountability* dos bancos de dados. Nesta senda, em alguns países, exige-se autorização estatal prévia ou notificação ao órgão de supervisão como pressuposto para o funcionamento dos bancos de dados (MENDES, 2014, p. 71).

2.2.3 Princípio do consentimento

O princípio do consentimento, por sua vez, está diretamente relacionado à garantia da autodeterminação informativa, pois o exercício da liberdade de controle de dados pessoais se baseia no consentimento do titular. Consoante este princípio, o consentimento deve ser sempre

[9] OECD Guidelines. p. 43.

livre, específico e informado, salvo em casos específicos, previstos em lei, nos quais será justificado o processamento de dados sem o prévio consentimento do seu titular (Ibidem).

2.2.4 Princípio da qualidade dos dados

O princípio da qualidade dos dados relaciona-se diretamente com a necessidades de que os dados sejam objeto de tratamento leal e lícito, não excedendo a finalidade declarada. Além disso, o princípio é associado à exatidão dos dados pessoais, de maneira que as informações constantes em bancos de dados estejam sempre fiéis à realidade. Assim, a coleta e tratamento dos dados devem ser feitos sempre com cuidado e correção, de modo que sejam realizadas atualizações periódicas dos dados, a fim de impedir que estejam ultrapassados, com o passar do tempo. Além do mais, é fundamental a garantia dos direitos de acesso, retificação e cancelamento dos dados, a fim de que seja garantida a efetividade deste princípio (MENDES, 2014, p. 72).

2.2.5 Princípio da segurança física e lógica

Este princípio, por sua vez, prevê a necessidade de que os dados sejam protegidos contra "os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado" (DONEDA, 2006, p. 217). Destaca-se que as questões relativas à privacidade e segurança não se confundem; contudo, as limitações ao uso e distribuição dos dados devem ser reforçadas por medidas de segurança adequadas.

2.3 A PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

Conforme exposto até o momento, a proteção à intimidade e à vida privada tem amparo constitucional, a qual se depreende do art. 5º, X. Outrossim, o Código Civil de 2002, em seu

art. 21, dentro do capítulo referente aos direitos da personalidade, reitera a proteção conferida pela Carta Magna.

Reconhecida a proteção constitucional à privacidade, cabe examinar se a legislação ordinária contempla a proteção específica aos dados pessoais. Destaca-se que não se pretende investigar exaustivamente a legislação brasileira no tocante à proteção conferida aos dados, mas somente verificar se é identificável um direito à proteção de dados suficiente para garantia da autodeterminação informativa. Assim, serão analisados o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Cadastro Positivo e o Marco Civil da Internet. Considerando o impacto que das regulamentações europeias na concepção deste direito, será feita uma breve pesquisa da *General Data Protection Regulation,* a qual entrou em vigor na União Europeia recentemente. Além disso, será estudado sucintamente o Projeto de Lei da Câmara 53/18, porquanto pode se tornar a primeira lei brasileira específica sobre a proteção de dados pessoais.

2.3.1 O Código de Defesa do Consumidor

O Código de Defesa do consumidor foi a primeira legislação do nosso ordenamento jurídico que tratou da proteção de dados e da privacidade de forma moderna e com objetivo de lidar com as novas tecnologias de processamento de dados. (MENDES, 2014, p. 141). Em específico, do art. 43, do CDC, que regula os bancos de dados e cadastros de consumidores, extraem-se importantes princípios e garantias em matéria de proteção de dados pessoais. Vale menção que a redação deste dispositivo recebeu influência direta do *National Consumer Act* e do *Fair Credit Reporting Act*, estando de acordo com importantes princípios internacionais de proteção de dados pessoais (MENDES, 2014, p. 143).

No caput do referido artigo já é possível destacar a garantia do direito de acesso às informações constantes em arquivos de consumo e bancos de dados, sem prejuízo da possibilidade de utilização de habeas data. Tal direito também é aspecto essencial ao exercício do direito de autodeterminação informativa, uma vez que o exercício de controle sobre os dados só é possível se garantido o acesso a eles. Além disso, a garantia de acesso aos dados também é fundamental para que o interessado possa, futuramente, demandar a retificação das informações relativas a sua pessoa (BESSA, 2003, p.189).

Por sua vez, o art, 43, §1º, ao dispor que "os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão", contempla o princípio da qualidade dos dados. A exigência de utilização de linguagem de fácil compreensão relaciona-se diretamente com o direito de acesso, pois, para que este possa ser exercido, o interessado deve ser capaz de compreender exatamente o conteúdo e significado da inscrição. Assim, veda-se o uso de informações codificadas, linguagem técnica, prolixa e utilização de idioma estrangeiro. A determinação de utilização de informação clara, por sua vez, está relacionada à veracidade das informações, que devem ser precisas e completas, a fim de que o destinatário dos dados possa efetivamente analisar o grau de solvência da pessoa interessada na obtenção do crédito (BESSA, 2003, p. 184). Complementa Leonardo Bessa que "a clareza é fundamental para uma correta avaliação dos riscos do crédito". Por seu turno, a exigência de objetividade nas informações refere-se à vedação de juízo de valor ou análise subjetiva da situação financeira do consumidor. Nesse sentido, no tocante aos bancos de dados de proteção ao crédito, "a valoração das informações é tarefa a ser realizada pelo destinatário das informações, pelo consulente dos arquivos, e não pelas entidades de proteção ao crédito (BESSA, 2003, p. 183).

Da análise do §2º do referido artigo, por outro lado, extrai-se a previsão do princípio da transparência. Na disposição de que o "cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele", assegura-se o direito à comunicação, sendo que o dever de comunicar refere-se a qualquer novo registro no banco de dados (BESSA, 2003, 194).

Já o art. 43, §3º traz a garantia ao direito de retificação aos dados, sendo que o dispositivo indica prazo de 5 dias para a comunicação da alteração das informações incorretas aos eventuais destinatários. Insta ressaltar que, em vista da importância deste direito, o art. 73 do CDC prevê pena de detenção de um a seis meses ou multa em razão de "deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata".

Extrai-se também do art. 43, em seus §§ 1º e 5º, a previsão de limites temporais. Enquanto o §1º faz referência a informações negativas, o §5º refere-se a informações que possam impedir ou dificultar a obtenção de crédito. Há outra distinção na redação dos dois dispositivos, porquanto o §1º determina que os bancos de dados não podem conter informações negativas, ao passo que o art. 5º estabelece que "não serão fornecidas informações", uma vez que consumada a prescrição. Contudo, ressalta Leonardo Bessa que tal distinção não implica necessariamente na possibilidade de os bancos de dados reterem as informações pessoais, na

hipótese do art. 43, §5º, destacando que "por questão de segurança é melhor que toda informação que extrapole seu limite temporal, seja em decorrência do §1º ou do §5º, seja definitivamente excluída dos arquivos dos bancos de dados" (BESSA, 2003, p. 209). Vale mencionar que a previsão de limites temporais para o armazenamento de dados é também associada com a garantia do princípio do esquecimento (MENDES, 2014, p. 143).

2.3.2 Lei do Cadastro Positivo

A Lei n. 12.414/2011, também chamada de Lei do Cadastro Positivo, disciplina a formação e consulta a bancos de dados com informações de adimplemento. Esta lei tem como principal característica o aumento da possibilidade de fluxo de dados no mercado com a regulação de bancos de dados com informações de adimplemento, mas também com o estabelecimento de regras de proteção à privacidade e métodos de controle e fiscalização dessa atividade (MENDES, 2014, p. 145). Desse modo, interessa ao presente trabalho a análise da legislação no que se refere à tutela da privacidade e dados pessoais.

Em seu art. 3º, §1º, a Lei do Cadastro Positivo prevê que somente poderão ser armazenadas, para a formação do cadastro, "informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado". De início, então, percebe-se que o dispositivo mencionado contempla o princípio da qualidade dos dados. Ademais, o art. 5º, nos incisos II e III, prevê, respectivamente, o direitos de acesso do cadastrado às suas informações, bem como de correção e cancelamento das informações cadastradas erroneamente. Além disso, o art. 7º da Lei n. 12.414/11 estipula a finalidade das informações disponibilizadas nos bancos de dados, que somente poderão ser utilizadas para: (i) realização de análise de risco de crédito do cadastrado, e (ii) subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.

Por sua vez, o princípio do consentimento é garantido pelo artigo 4º, da Lei do Cadastro Positivo, que prevê a necessidade de autorização mediante consentimento informado do interessado, mediante assinatura em instrumento específico ou em cláusula apartada, para que seja realizada a abertura do cadastro. De maneira similar, a legislação também contempla o referido princípio ao garantir o cancelamento do cadastro, quando solicitado pelo cadastrado

(art. 5º, I), e ao prever que o compartilhamento de informação de adimplemento será permitido somente mediante autorização expressa do cadastrado (art. 9º).

Destarte, mediante essas garantias de controle do indivíduo sobre seus dados, inclusive com a atribuição de poder de decisão acerca do seu interesse na formação do cadastro positivo, permitindo até mesmo o cancelamento deste, a Lei 12.414/11 "consolida a evolução de um conceito de autodeterminação informativa no nosso ordenamento" (MENDES, 2014, p. 146).

2.3.3 Lei de Acesso à Informação

A fim de compreender a maneira como o ordenamento jurídico brasileiro rege o tratamento de dados pessoais, é importante também a análise da Lei de Acesso à Informação (Lei n. 12.527/2011). Esta legislação é de suma importância, dentro do contexto da proteção dos dados pessoais, no que se refere à garantia de maior transparência na Administração Pública e, consequentemente, na efetivação da autodeterminação informativa dos cidadãos.

Vale dizer que esta lei visa a regulamentar o art. 5º, XXXIII, da CF, o qual garante a todos o direito de receber "informações de seu interesse particular, ou de interesse coletivo ou geral", salvo "aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado". Desse modo, tendo em vista que as informações e dados pessoais dizem respeito à privacidade do indivíduo e, com isso, são de seu interesse particular, extrai-se que a Lei de Acesso à Informação possibilita o acesso de informações pessoais do indivíduo que estão mantidas pelo Poder Público (MENDES, 2014, p. 150).

Observa-se que, em seu art. 3º, inciso I, a lei prevê a publicidade como preceito geral, de modo a possibilitar o amplo acesso às informações constantes em bancos de dados públicos. Ademais, em que pese o objetivo de garantir maior transparência, a legislação não ignora as garantias constitucionais de privacidade, referindo no seu art. 31 que o tratamento de informações pessoais deverá ser realizado com "respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais". [10]

[10] "Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. "

Desse modo, a Lei de Acesso à Informação contribui para a difícil tarefa de garantir os princípios de transparência e publicidade sem ignorar as proteções próprias da esfera privada. Nesse sentido, reconhece-se que não há antagonismo entre proteção de dados pessoais e acesso à informação, mas sim uma "relação mútua entre a construção de espaços ao privado e ao público na perspectiva de estabelecimento de uma autodeterminação informativa" (CACHAPUZ e CARELLO, 2017, p. 7).

2.3.4 O Marco Civil da Internet

Merece destaque também a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, que, dentre os direitos e garantias dos usuários, prevê a proteção da privacidade e dos dados pessoais na Internet.

Elenca o Marco Civil, em seu art. 3º, incisos II e II, dentre os princípios relativos ao uso da internet, a proteção da privacidade e dos dados pessoais, respectivamente. Outrossim, o art. 7º da referida lei traz os direitos dos usuários, dentre os quais se destaca a inviolabilidade da intimidade e da vida privada; a inviolabilidade e sigilo do fluxo de suas comunicações pela internet e a inviolabilidade e sigilo de suas comunicações privadas armazenadas. Além disso, fica evidente a posição central do consentimento no inciso VII, que prevê 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. Igualmente, o inciso IX estabelece que o consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais deverá ocorrer de forma destacada das demais cláusulas contratuais.

Ademais, extrai-se do art. 10 do Marco Civil que, além da proteção conferida aos dados pessoais, também devem atender à preservação da intimidade e vida privada a guarda dos registros de conexão e de acesso a aplicações de internet. No §1º, o dispositivo prevê que o provedor responsável pela guarda destes registros eletrônicos somente deverá disponibilizá-los mediante ordem judicial, evidenciando que a regra é a proteção dessas informações (LIMA, 2014, p. 156). Insta observar a exceção prevista no §3º, do art. 10, no qual se contempla a possibilidade de acesso aos dados cadastrais referente à qualificação pessoal, filiação e endereço, por autoridades administrativas com competência legal para tal requisição. No ponto, o Marco Civil não detalha quais as autoridades administrativas seriam competentes para a

referida requisição dos dados cadastrais, mas a interpretação do dispositivo em conjunto com o art. 15 da Lei nº 12.850/2013 permite a conclusão de que as autoridades seriam o Delegado de Polícia e os membros do Ministério Público.

Neste aspecto, vale lembrar que a regra do art. 10, §3º do Marco Civil da Internet deve ser interpretada em cotejo com as garantias de privacidade e proteção dos dados pessoais, constantes na lei. Assim, o pedido da autoridade administrativa também deve obedecer fundamentos fáticos e legais. Tal entendimento é corroborado pela leitura do art. 50, da Lei nº 9.784, que dispõe acerca da necessidade de que os atos administrativos tenham motivação clara, explícita e congruente, de modo que não se justifica o envio indiscriminado dos dados pessoais do usuário. Além disso, o referido dispositivo se limita aos "dados cadastrais que informem qualificação pessoal, filiação e endereço", não abrangendo endereço de IP e registros de conexão (LIMA, 2014, p. 157).

Contudo, em que pese o mérito do Marco Civil da Internet em dispor acerca da proteção da privacidade e dos dados pessoais, há que se destacar que o diploma legal não traz uma definição dos dados pessoais, sendo necessária uma interpretação sistemática do ordenamento jurídico, em cotejo com as definições trazidas pela doutrina, a fim de se delimitar o conceito de dados pessoais. Do mesmo modo, não faz distinção entre dados pessoais e dados sensíveis, motivo pelo qual se entende que a Lei quis trazer proteção mais ampla, abrangendo os dois termos (LIMA, 2014, p. 155).

2.3.5 *General Data Protection Regulation*

Para o presente trabalho é importante a análise da nova regulação europeia em matéria de proteção de dados pessoais, a *General Data Protection Regulation* (GDPR), em vigência desde maio de 2018. A análise desta legislação torna-se relevante principalmente quando se observa que a proposta de lei brasileira para a matéria se espelha no modelo europeu de proteção dos dados pessoais. Contudo, aqui não se busca um exame exaustivo da regulação supracitada, mas sim uma análise de seus aspectos gerais e inovações relevantes, em relação à norma que vigia anteriormente na Europa.

A GDPR, cuja criação foi aprovada pelo Parlamento Europeu em maio de 2016, entrou em vigor em maio de 2018, substituindo a Diretiva Europeia 95/46/CE. Em suma, a nova

legislação tem como escopo aprimorar a proteção da privacidade dos dados dos indivíduos, bem como facilitar a atuação das empresas por meio de maior clareza nas suas regras, que contam com requerimentos concretos e até mesmo instruções diretas para a implementação das determinações legais (MARKKULA et al, 2017). Nesse sentido, diferentemente da Diretiva Europeia, cuja efetividade dependia da internalização a ser feita pelos países europeus, a GDPR já é aplicável diretamente a todos os países integrantes da União Europeia. Além disso, estão sujeitos à legislação todas as empresas responsáveis pelo tratamento de dados pessoais de cidadãos da União Europeia, independentemente do local da sede da empresa, de modo que as companhias internacionais deverão sujeitar-se à GDPR também.

Nos artigos 1 a 11 da GDPR constam regras gerais e princípios da disciplina, incluindo definições de termos presentes na Regulação, como dados pessoais, processamento, entre outros (art. 4), alcance material (art. 2) e territorial (art. 3), bem como os objetivos da legislação (art. 1). Destaca-se que o alcance territorial da legislação foi ampliado, em comparação com a Diretiva Europeia 95/46, a fim de aplicar a nova regra também para empresas localizadas fora da Europa. No que tange aos princípios, o art. 5º (2) inclui um novo princípio de *accountability*, segundo o qual o responsável pelo tratamento de dados deverá demonstrar a observância dos demais princípios elencados no dispositivo. Além disso, enquanto a Diretiva 95/46 estipulava que a proteção de dados pessoais deveria ser adequada, relevante e não excessiva, no tocante aos propósitos da coleta e processamento, a GDPR introduz o princípio da minimização dos dados (*data minimization)*, o qual exige limitação dos dados pessoais aos mínimos necessários para os propósitos do tratamento, e isto somente se estes propósitos não puderem ser alcançados sem o tratamento de dados pessoais (MARKKULA et al, 2017, p. 6).

Ademais, a GDPR traz modificações no tocante aos requisitos de validade do consentimento, para fins de legitimidade no tratamento de dados. Enquanto na Diretiva Europeia existia uma exigência de consentimento inequívoco, a GDPR exige não só um consentimento livre, específico e informado, com indicações expressas da vontade do usuário, mas também prevê que é ônus do responsável pelo tratamento dos dados a comprovação da ocorrência deste consentimento (Ibidem).

A *General Data Protection Regulation*, em seus arts. 40 a 43, também atualiza as previsões referentes aos códigos de conduta. Assim, há o encorajamento da elaboração de códigos de condutas a fim de melhor aplicar as regras da Regulação, considerando as necessidades específicas de cada setor e empresa. Nesse sentido, há uma simplificação do procedimento, em comparação à legislação anterior, permitindo-se que códigos de conduta de

aplicação nacional sejam aprovados diretamente pelas autoridades de supervisão competentes no País (Ibidem, p. 11). Também são previstas novas formas para as empresas demonstrarem observância à GDPR, quais sejam mecanismos de certificação de proteção de dados, selos e marcas.

Além disso, é interessante observar que, a fim de garantir a eficácia deste sistema de responsabilização das empresas e devida prestação de contas, a GDPR prevê a possibilidade de aplicação de sanções administrativas a serem impostas pela autoridade responsável. No que se refere à aplicação de multa administrativa, o art. 83 (2) da regulação elenca uma série de circunstâncias a serem observadas na determinação do valor da multa, tais quais a gravidade da infração, a intencionalidade, o grau de responsabilidade, as categorias de dados pessoais violados, entre outras.

Portanto, de um modo geral, observa-se que a GDPR busca maior eficiência na tutela dos dados pessoais e da privacidade na Internet, tentando equilibrar este direito com o desenvolvimento econômico. Em comparação com a legislação anterior, a GDPR não só unifica o direito vigente na União Europeia, mas também oferece meios concretos de garantir a observância das normas. Assim, conta com regras mais protetivas no tocante ao consentimento dos consumidores bem como com a atuação de autoridades administrativas, responsáveis pela fiscalização e aplicação da legislação.

2.3.6 Projeto de Lei da Câmara nº 53/2018

Já não é recente a menção à necessidade de criação de uma lei específica sobre a matéria de proteção de dados pessoais do Brasil. Neste ponto, há um significativo atraso do País, considerando que a maioria dos Países, não só na América Latina, mas no mundo inteiro já contam com leis específicas sobre a matéria. A existência de uma lei geral sobre a matéria é imprescindível para uma tutela adequada, pois ela não só traz delimitações a respeito do bem jurídico a ser protegido, mas também constrói uma arquitetura regulatória, consolidando a proteção de dados como um setor de políticas públicas. Neste ponto, o modelo de lei geral garante a implementação da legislação e eficiência na tutela por meio de criação de instrumentos estatutários, sancionatórios, bem como pela criação de um órgão administrativo, responsável pela implementação e aplicação da legislação (MENDES, 2014, p. 49).

Em nosso ordenamento jurídico, embora seja possível extrair algum conteúdo jurídico relativo à proteção de dados pessoais, a proteção existente é insuficiente. Há de se mencionar que a primeira legislação que buscou regular o uso da Internet e expressamente trouxe o direito à proteção de dados pessoais dos usuários – o Marco Civil da Internet – apresenta uma grande lacuna, a qual não condiz com as suas pretensões: a inexistência de definições de dados pessoais e dados sensíveis. Desse modo, é natural que fique prejudicada a proteção conferida pela lei, pois ela própria não é suficiente para delimitação do direito que visa a tutelar.

Por estas razões, é importante a análise do Projeto de Lei da Câmara nº 53/2018, porquanto pode se tornar a primeira legislação brasileira específica sobre a proteção de dados pessoais.

De início, em seu art. 5º, a PLC 53/18, traz algumas definições importantes. Seu inciso I menciona que dados pessoais são quaisquer informações relacionadas à pessoa natural identificada ou identificável, diferenciando-os dos dados sensíveis, que são dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (inciso II). Por sua vez, a legislação visa a regular o tratamento de dados pessoais, o qual é definido, no inciso X, como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração", percebendo-se uma intenção do legislador de proteger quaisquer operações relativas aos dados pessoais. Inclui definições importantes como sobre bancos de dados (inciso IV), titular dos dados (inciso V), responsável (inciso VI), agentes do tratamento (inciso IX), bem como diversas outras relevantes para a disciplina.

Em seu artigo 6º, o projeto de lei elenca os princípios a serem observados na realização das atividades de tratamento de dados pessoais, quais sejam a finalidade; adequação; necessidade; livre acesso; qualidade de dados; transparência; segurança; prevenção; não discriminação e responsabilização e prestação de contas. Com isso, observa-se que o PLC 53/18 segue a tendência europeia, que prevê como regra geral a minimização do tratamento de dados pessoais, a fim de que seja feito somente quando necessário, bem como a priorização a uma proteção preventiva (como, por exemplo, por meio da *privacy by design*, a qual será melhor explicada posteriormente). Além disso, por meio dos princípios da responsabilização e

prestação de contas, o PLC reflete os institutos da *accountability* e *compliance*, trazidos pela regulação europeia, a qual será analisada em maior detalhe em seguida.

A proposta legislativa também elenca, em seu art. 18, direitos dos titulares dos dados, dentre os quais se destacam as garantias de acesso; correção; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou em desconformidade com a lei (o que evidencia o princípio legislativo referente a minimização no tratamento de dados); eliminação dos dados tratados com o consentimento do usuário; e a possibilidade de revogação do consentimento, além de outros direitos listados no dispositivo.

Ademais, no capítulo IV do PLC 53/2018 são previstas regras referentes ao tratamento de dados pessoais pelo poder público – nos termos do art. 1º da Lei 12.527/2011 – que deverá "ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público"[11]. Ressalta-se que o art. 24 indica que tais regras não são aplicáveis às empresas públicas e as sociedades de economia mista, as quais receberão mesmo tratamento das pessoas jurídicas de direito privado particulares. No tocante à responsabilização dos órgãos públicos por violação no tratamento de dados pessoais, o PLC limita-se a indicar que a autoridade administrativa poderá solicitar aos agentes do poder público um "relatório de impacto à proteção de dados pessoais" e, eventualmente, sugerir a adoção de "padrões e boas práticas aos tratamentos de dados pelo poder público".

Por sua vez, consoante se extrai do seu art. 42, o projeto de lei prevê a responsabilização do operador (solidariamente) e do responsável pelo tratamento na hipótese de "dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais", sendo obrigatória a reparação do dano. Nesse sentido, a regularidade do tratamento de dados relaciona-se também com a segurança e sigilo dos dados, os quais deverão ser observados pelos responsáveis (art. 44).

[11] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011, deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I – sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; II – sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, no âmbito da Lei nº 12.527, de 18 de novembro de 2011, vedado seu compartilhamento no âmbito do poder público e com pessoas jurídicas de direito privado; e III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.

Além disso, similarmente às normas europeias referentes à prevenção de danos e padrões de conduta, o PLC prevê regras gerais de boas práticas e governança, estabelecendo condições de organização, procedimentos, padrões técnicos, mecanismos internos de supervisão e mitigação de riscos, além de outros aspectos relativos ao tratamento de dados pessoais. Neste âmbito, o §2º, I, a, do mesmo dispositivo, reflete o sistema de *compliance* previsto na GDPR, de modo que os responsáveis pelo tratamento poderão implementar um programa de governança em privacidade que "demonstre o comprometimento do responsável em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais". Vale destacar que estas regras referentes à iniciativa das empresas são importantes pois facilitam a fiscalização dos órgãos responsáveis e, com isso, garantem maior observância aos ditames legais.

Destarte, ainda que sejam cabíveis críticas a aspectos pontuais do referido projeto de lei, tem-se que a legislação em trâmite no Senado Federal adequa-se aos modelos mais recentes de proteção de dados pessoais. O Projeto de Lei da Câmara 53/2018 prevê não só direitos individuais dos usuários titulares de dados, mas também regula a criação de órgãos responsáveis pela aplicação e observância da legislação. Assim, entende-se que a aprovação deste projeto representa um primeiro passo à efetiva tutela da privacidade dos dados pessoais no Brasil.

2.4 A LEGITIMIDADE NO TRATAMENTO DE DADOS PESSOAIS

O estudo das condições de legitimidade no tratamento de dados pessoas é central para a compreensão das situações em que não há violação da privacidade dos indivíduos. Apesar de todos os mencionados riscos apresentados pelo tratamento automatizado de dados pessoais, há de se reconhecer que os dados pessoais possuem um papel significativo no mercado. Isto porque "tanto as empresas quanto os governos justificam a coleta de informações como fator preponderante para o fornecimento de melhores serviços" (LEONARDI, 2007, apud MARTINS, 2014, p. 273). Por isso, o papel do direito deve ser justamente buscar equilíbrio, compatibilizando a privacidade com os demais interesses relativos ao tratamento de dados pessoais.

Segundo se extrai da legislação supracitada, o consentimento do indivíduo costuma ser o requisito para o uso, coleta, processamento ou transferência de dados pessoais. No entanto, não se visa a uma garantia de direito absoluto no que tange ao exercício da autodeterminação

informativa, pois o consentimento pode ser excepcionado sem que haja, com isso, uma violação ao direito da privacidade da pessoa. Conforme é referido por Marcel Leonardi "não se nega que a privacidade deva ceder, dentro de limites constitucionais, ao interesse público, notadamente no que tange às informações judiciais, criminais, tributárias, de saúde pública e afins" (LEONARDI, 2007, apud MARTINS, 2014, p. 274).

Observa-se, na análise do art. 31, §1º, II, da Lei de Acesso à Informação, o consentimento expresso da pessoa é um dos mecanismos autorizadores à divulgação ou acesso por terceiros das informações pessoais. Contudo, o §3º do referido artigo já enumera situações em que ele pode ser dispensado:

> § 3º O consentimento referido no inciso II do § 1o não será exigido quando as informações forem necessárias:
> I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
> II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
> III - ao cumprimento de ordem judicial;
> IV - à defesa de direitos humanos; ou
> V - à proteção do interesse público e geral preponderante.

Por sua vez, no caso específico da internet, o "consentimento livre, expresso e informado" do usuário é a regra geral para a permissão do fornecimento de dados pessoais a terceiros, consoante o art. 7º, VII do Marco Civil da Internet. Contudo, o sopesamento da privacidade em face do interesse público é observável na legislação ao estabelecer, em seu art. 7º, incisos II e III, a garantia da inviolabilidade e sigilo das comunicações pela internet, salvo mediante ordem judicial. Conforme notam Fábio Kujawski e Alan Thomaz, no que tange à possibilidade de quebra de sigilo nas comunicações privadas, o Poder Judiciário vem manifestando-se pela admissibilidade de pedidos de quebra de sigilo de contas de e-mail em processos criminais, aplicando o parágrafo único da art. 1º da Lei nº 9.296/96, em que pese as controvérsias doutrinárias a respeito da constitucionalidade deste dispositivo (KUJAWSKI e THOMAZ, 2014, p. 684).

Neste ponto, é relevante a análise do Projeto de Lei da Câmara nº 53/2018, em trâmite no Senado Federal, que dispõe sobre a proteção de dados pessoais. O art. 7º do referido Projeto versa sobre os requisitos para o tratamento de dados pessoais e prevê que este poderá ser realizado mediante fornecimento de consentimento pelo titular dos dados ou ainda: (a) para o cumprimento de obrigação legal ou regulatória pelo responsável; (b) pela administração pública, para tratamento e uso compartilhado de dados necessários à execução de políticas

públicas; (c) para a realização de estudos por órgão de pesquisa, garantindo-se a anonimização dos dados pessoais, sempre que possível; (d) quando necessário para a execução de contrato ou procedimentos preliminares relacionados a contrato do qual é parte o titular, a pedido do titular de dados; (e) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (f) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (g) para a tutela da saúde; (h) quando necessário para atender aos interesses legítimos do responsável ou de terceiro; e, por fim, (i) para a proteção do crédito, de acordo com o art. 43 do Código de Defesa do Consumidor.

Percebe-se então que o PLC 53/18 enumera um extenso número de situações nas quais é possível um tratamento legítimo dos dados pessoais sem que seja necessário o consentimento do titular. Assim, a proteção proposta pelo referido Projeto se assemelha à regulação europeia da matéria. Conforme o art 6º da *General Data Protection Regulation* (GDPR), em vigor na europa desde maio de 2018, além da hipótese de consentimento do usuário, o tratamento de dados será legítimo se necessário: (a) à execução de contrato do qual o titular dos dados é parte ou ainda para realização de procedimentos contratuais preliminares do qual é parte o titular; (b) cumprimento de obrigação legal à qual o responsável pelos dados é sujeito; (c) para proteção de interesses vitais do usuário ou terceiro; (d) para execução de uma incumbência de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento; (e) para dar continuidade a interesses legítimos do responsável pelo tratamento ou de terceiros, salvo em caso de prevalência de interesses ou de direitos e liberdades fundamentais do usuário que requeiram proteção dos dados pessoais, em particular se o usuário for criança[12].

Destaca-se, pois, que a nova regulamentação europeia não traz alterações significativas, sendo sua redação quase idêntica à do art. 7º da Diretiva Europeia 95/46/CE[13]. Insta registrar

[12] Tradução livre: *"Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

[13] *Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the*

que a Diretiva Europeia já recebia críticas no que tange os requisitos autorizadores à legitimidade do tratamento de dados. Conforme menciona Gabriela Zanfir (2014, p. 239), não obstante a posição central do consentimento do usuário – frequentemente mencionado na doutrina como indispensável para um tratamento legítimo dos dados pessoais e para a garantia da autodeterminação informativa – a enumeração legal indica que o tratamento de dados pessoais seria possível, na maioria dos casos, sem o seu consentimento. Ou seja, as exceções seriam mais frequentes do que a regra geral.

controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed , except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

3 O CONSENTIMENTO AO TRATAMENTO DE DADOS PESSOAIS NA INTERNET

Conforme se extrai da análise feita até o momento, o direito de proteção de dados pessoais ampara-se na garantia do poder e capacidade do indivíduo para controlar livremente a revelação e utilização de seus dados, preservando, com isso, sua capacidade de livre desenvolvimento de sua personalidade. Em razão disso, a maioria das legislações acerca da proteção de dados pessoais tem o consentimento como figura central na legitimação ao tratamento de dados. Ainda que não possua uma lei geral de proteção de dados pessoais, o ordenamento brasileiro não é exceção, visto que o próprio Marco Civil da Internet exige o consentimento do usuário a fim de que sejam legítimas a coleta e transferência de dados pessoais.

Destarte, neste capítulo será analisado o instituto do consentimento a fim de identificar não só a sua função, mas também os requisitos para sua validade. Por último, verificar-se-á se a garantia do consentimento do usuário é suficiente para a proteção da privacidade dos usuários da internet.

3.1 BREVES CONSIDERAÇÕES SOBRE AS CONTRATAÇÕES NO COMÉRCIO ELETRÔNICO

Para uma melhor compreensão acerca do contexto em que ocorre o tratamento de dados pessoais na internet, é útil um exame a respeito do comércio eletrônico e dos contratos eletrônicos de adesão.

Consoante a lição de Ricardo Lorenzetti (2004, p. 285-287), o contrato eletrônico existe quando for utilizado o meio digital para celebrar, cumprir ou executar um acordo. Na hipótese de celebração digital, pode tanto ocorrer a elaboração e envio das declarações de vontade das partes eletronicamente, quanto a elaboração pode acontecer fisicamente, sendo realizado somente o envio por meio digital. No caso do cumprimento eletrônico, transfere-se um bem digitalizado e paga-se com moeda digital (comprimento total), ou a remessa de bem físico é feita por transporte convencional e paga-se a partir de transferência eletrônica de dinheiro (cumprimento parcial). Por fim, os remédios para o descumprimento também podem ser

eletrônicos, como em caso de contrato com garantias autoliquidáveis, mediante transferência eletrônica de dinheiro.

Nas palavras de Cláudia Lima Marques (2004, p. 35):

> É o 'comércio clássico' de atos negociais entre empresários e clientes para vender produtos e serviços, agora realizado através de contratações à distância, conduzidas por meios eletrônicos (*e-mail*, mensagens de texto etc.), por Internet (*on-line)* ou por meios de telecomunicações de massa (telefones fixos, televisão a cabo, telefones celulares etc.).

Nesta senda, as contratações eletrônicas à distância, em especial no caso dos contratos de consumo, apresentam uma série de desafios à regulação jurídica, quais sejam: (a) a despersonalização; (b) a desmaterialização; (c) a desterritorialização e a atemporalidade; e (d) a desconfiança dos consumidores no comércio eletrônico (MARQUES, 2004, p. 63). Nestes contratos pós-modernos, são revisados elementos tradicionais de contratação; a impessoalidade torna-se a regra geral e, além disso, "todas as técnicas de contratação de massa se reúnem: do contrato de adesão, e das condições gerais contratuais, ao *marketing* agressivo, à catividade do cliente, à internacionalidade intrínseca entre consumidor e fornecedor" (Ibidem, p. 65).

As contratações eletrônicas também apresentam peculiaridades no que tange à declaração de vontade das partes. A intermediação da negociação por meio de computadores pode levar à problemas na comprovação da imputabilidade da declaração. Em virtude de tais limitações, Lorenzetti (2004, p. 293) enuncia que, em regra, "aquele que utiliza o meio eletrônico e cria uma aparência de que este pertence a sua esfera de interesses, arca com os riscos e os ônus de demonstrar o contrário". Esta regra geral seria complementada por deveres anexos impostos às partes, tais quais o dever de informação e o de utilizar um meio seguro. Também merece menção a hipótese de declaração de vontade emitida automaticamente por um computador. Neste caso, "é de fundamental importância o comportamento concludente da parte que instala um sistema informático automatizado para relacionar-se com terceiros, pois cria, a partir destes, uma aparência jurídica clara de que responderá pelas ações da máquina" (Ibidem, p. 296).

Como regra geral, a aceitação da contratação é uma declaração unilateral de vontade que, quando em confluência com a oferta, configura o consentimento no contrato eletrônico (LORENZETTI, 2004, p. 305). Destaca-se que as manifestações virtuais de vontade negocial dos fornecedores – tais quais anúncios em *sites, links, e-mails*, a publicidade, *spams*, entre outras formas de manifestação – contêm os elementos da oferta e despertam a confiança dos

consumidores, motivo pelo qual seriam compreendidos como mais do que meros "convites públicos à oferta" (MARQUES, 2004, p. 261). Quanto à aceitação, os consumidores podem manifestar sua vontade de forma expressa, por palavras, ou ainda por atos (tocar símbolos, ícones, *clicks* – como no caso de *point and click agreements* ou *click-wrap agreements* – condutas sociais típicas etc.), mas não pode ser presumida do silêncio (Ibidem, p. 271).

Assim sendo, nos meios eletrônicos, o consentimento pode ser formado tanto por declaração de vontade formulada por correio eletrônico ou meios similares – nos quais o consumidor poderá se manifestar utilizando linguagem escrita – como também poderá se dar por declaração de vontade expressa via página da Internet, hipótese na qual o usuário, mediante um *click*, aceita a contratação. Ressalta-se que, neste último caso, os atos de execução do contrato que concretizam a aceitação da oferta aperfeiçoam a contratação, em que pese o silêncio e a não aceitação formal (SCHERKERKEWITZ, 2014, p. 82-83).

Percebe-se que o último caso, em que a declaração de vontade é expressa via página da *web*, é o que há de mais frequente nas contratações eletrônicas da atualidade. Assim, apontam-se dois modelos de consentimento, por meio dos quais o usuário manifestaria sua vontade de contratar: o modelo *opt-in* e o *opt-out.*

O modelo *opt-in* exige uma postura ativa do usuário, declarando sua vontade de submeter seus dados pessoais a um tratamento qualquer (MENDES, 2014, p. 205). Um exemplo disso seria uma caixa na qual o usuário deve assinalar a fim de manifestar que está ciente e concorda com os termos de serviço e políticas de privacidade. A outra possibilidade é a obtenção do consentimento por meio do modelo *opt-out*, o qual se apoia em uma postura mais passiva do usuário, cuja inércia implica a concordância com os termos propostos. Este seria o caso de uma cláusula de autorização ao tratamento de dados em contrato de adesão, sem o devido destaque, ou ainda de uma caixa previamente assinalada, no sentido de que o usuário deve se manifestar apenas se não estiver de acordo com o conteúdo.

A discussão sobre o modelo utilizado é de grande relevância, pois este pode exercer influência sobre a consciência do usuário quanto à sua tomada de decisão. A utilização de caixas previamente assinaladas pode mascarar a percepção dos usuários quanto ao fato de que estão consentindo a políticas de privacidade, além de contribuir para a trivialização do consentimento (ROGOSCH e HOHL, 2012, p. 39).

Vale acrescentar, no que se refere à oferta de serviço, que o art. 3º, §2º, do Código de Defesa do Consumidor, exige remuneração pela atividade para que esteja caracterizada

propriamente a contratação de consumo. Sob esta ótica, muitas contratações na *web* poderiam ensejar dúvidas a respeito da aplicabilidade do CDC; contudo, segundo Cláudia Lima Marques (2004, p. 253), não há óbice à aplicação da legislação consumerista neste tipo de contratação. Isto porque:

> A 'gratuidade' no mercado de consumo é muitas vezes ilusória, pois há remuneração indireta (e por vezes direta e conexa) do fornecedor pela prestação daquele 'serviço' na sociedade de informação. É justamente o movimento da análise econômica nos Estados Unidos que nos alerta para a falácia 'econômica' dos chamados 'serviços', 'utilidades' ou promessas 'gratuitas', o que não passaria de uma superada ficção jurídica. O que parece juridicamente gratuito, alertam-nos mesmo os conservadores e radicais autores desse movimento de Chicago, é economicamente baseado na remuneração indireta, na interdependência de prestares futuros e atuais (sinalagma escondido), no estado de catividade e de dependência a que um dos parceiros fica reduzido e no lucro direto e indireto do outro.

Neste contexto de contratação gratuita com provedores de serviços na internet, surge um novo instrumento de pagamento e troca – uma nova moeda – que consiste, diretamente, nas informações pessoais e econômicas dos consumidores e, indiretamente, em seu poder aquisitivo, contribuindo para aumentar a capacidade de penetração das empresas no mercado (MARTINS, 2014, p. 73 e 74). Por este motivo, a tutela à privacidade dos indivíduos torna-se um desafio ao Direito, que deve buscá-la em equilíbrio com a garantia do desenvolvimento econômico e tecnológico.

3.2 MODALIDADES DE TUTELA DO DIREITO DE PROTEÇÃO DE DADOS PESSOAIS

O reconhecimento do direito fundamental à proteção de dados pessoais acompanha, desde o princípio, discussões a respeito de sua eficácia. Neste ponto, é útil fazer menção às modalidades de tutela para os dados pessoais identificados por Doneda, quais sejam a tutela proprietária e a tutela aquiliana (DONEDA, 2006, p. 362).

Na primeira modalidade, são utilizados instrumentos de tutela da propriedade para a definição do estatuto jurídico da informação pessoal. Assim, reconhece-se ao interessado a faculdade do interessado "de ser o exclusivo árbitro do destino dos dados que lhe digam respeito" (DONEDA, 2006, p. 363).

Vale salientar que a tentativa de aplicação análoga de institutos jurídicos tradicionais, tal qual a propriedade, não se limita a matéria de proteção de dados pessoais. Desde o surgimento da internet, há doutrinadores que defendem que os problemas enfrentados na Rede poderiam ser resolvidos por meio da analogia. Assim, para resolução de controvérsias na Internet seriam aplicados os princípios extraídos da norma já existente para casos outros que não os expressamente contemplados, "mas cuja diferença em relação a estes não seja essencial" (LEONARDI, 2011, p. 140).

Sobre essa abordagem, surgem divergências no que se refere à natureza dos dados pessoais e, com isso, sobre o reconhecimento dos dados pessoais como bens jurídicos ou não. Argumenta-se que uma tutela proprietária dos dados pessoais seria incongruente com o próprio reconhecimento do caráter de direito fundamental, em razão da "incompatibilidade entre os meios de tutela e o exercício de um direito real sobre os dados pessoais" (DONEDA, 2006, p. 364).

Nesse sentido, ao tratar sobre a questão que envolve a propriedade dos dados, Fabiano Menke destaca que o direito à proteção de dados não consiste em um direito regulatório da propriedade, pois não é adequado falar em propriedade de um indivíduo sobre os dados relativos a sua pessoa. Este direito consiste num ordenamento sobre a informação e a comunicação relacionada aos dados, determinando quem, em qual relação e em qual situação, está autorizado a lidar com os dados de um indivíduo de uma determinada maneira (MENKE, 2015, p. 213).

Por sua vez, à tutela aquiliana também recaem críticas no tocante à uma abordagem predominantemente patrimonialista do problema (DONEDA, 2006, p. 364). Além disso, também existiria uma crítica quanto ao uso da responsabilidade civil na solução das questões relativas à proteção de dados pessoais, uma vez que esta modalidade de tutela pode incentivar o estabelecimento de um padrão comportamental e o uso da responsabilidade civil, na maioria dos casos, não seria um caminho encorajador (DONEDA, 2006, p. 365). Explica Doneda que a responsabilidade civil pode integrar-se à disciplina de modo auxiliar, principalmente em casos de responsabilidade objetiva, tendo em vista a dificuldade de demonstração do dano em situações de violação da privacidade.

Também seria uma possibilidade de tutela a auto-regulamentação, na hipótese de regramento advindo de fontes não-estatais, como códigos de conduta adotados por associações de classe ou grupos de empresa. Contudo, vale referir a problemática em torno de encarregar a proteção de dados a regras não vinculantes, surgidas fora do âmbito do Estado, justamente em

função de se tratar de um direito fundamental. Relaciona-se a este problema a falta de poder coercitivo destas normas não-estatais, de maneira que não atingiriam todos destinatários de forma igual (DONEDA, 2006, p. 366).

Ademais, vem sendo reconhecida como propícia a garantia da privacidade dos usuários na Internet à tutela por meios técnicos, como no caso das chamadas *Privacy Enhancing Technologies* (PETs). Esta tutela consiste na utilização da própria tecnologia para a proteção dos dados pessoais, atuando diretamente na "arquitetura da privacidade" (DONEDA, 2006, p. 368). Ainda que não se possa construir uma tutela da privacidade na Internet somente com base nestas tecnologias, elas consistem em uma importante ferramenta para auxiliar a proteção jurídica, uma vez que podem limitar ou impossibilitar o tratamento de dados pessoais. Neste ponto, refere Danilo Doneda que:

> Evidentemente, a tecnologia não pode, por si só, ser tomada como um possível meio de tutela e sequer pode ser qualificável juridicamente de forma plenamente satisfatória. Porém, na medida em que ela pode interferir na arquitetura sobre a qual situam-se os dados pessoais, ela pode ter consequências para a configuração jurídica do problema, assim como pode ser o instrumento de atuação de políticas públicas na área, por exemplo.

Portanto, frente às limitações inerentes às mencionadas formas de tutela, bem como às dificuldades no que tange à proposta de solução para a proteção de dados pessoais, é cabível o estudo dos institutos centrais nesta problemática da proteção de dados pessoais e privacidade na internet. O estudo de tais institutos permite ao intérprete do direito o estabelecimento de critérios para o balanceamento dos interesses em jogo (DONEDA, 2006, p. 371), quais sejam a proteção da privacidade e o desenvolvimento tecnológico e econômico. Neste âmbito, a análise do consentimento do indivíduo envolvido no tratamento de dados pessoais é imprescindível, mormente por se tratar de um dos pilares na maioria das legislações específicas sobre esta matéria.

3.3 REQUISITOS DO CONSENTIMENTO

No âmbito das contratações eletrônicas e das relações de consumo da Internet, o consentimento apresenta-se como o principal instrumento por meio do qual o usuário pode manifestar sua vontade a respeito da permissão ou não do tratamento de dados pessoais. Em análise do consentimento e da autonomia individual, Heidi Hurd (1996, p. 123) identifica como

função primordial do consentimento a transformação da moralidade de um ato, isto é, reconhece-se a moralidade de uma conduta que, em sua ausência, seria vedada (por exemplo, a partir do consentimento, uma invasão transforma-se em uma visita). Considerando, então, que a permissibilidade de um comportamento se apoia principalmente na autonomia do indivíduo, de maneira que ele mesmo gerencie sua privacidade, há um grande esforço legislativo no sentido de garantir a validade do ato por meio do qual a pessoa consente o tratamento de dados pessoais.

Refere Laura Schertel Mendes que o consentimento é o instituto jurídico por meio do qual um indivíduo exerce seu poder de autodeterminação informativa e, assim, expressa sua vontade de autorizar ou não o processamento de dados pessoais (MENDES, 2014, p. 60). Mendes (Ibidem, p.61) ainda elenca como pressupostos de um consentimento válido: (i) a emissão do consentimento por livre vontade do titular dos dados; (ii) que o consentimento seja voltado a uma finalidade específica; (iii) que o titular seja informado acerca do objetivo da coleta, do processamento e do uso dos dados, assim como das consequências de não consentir com o tratamento. Portanto, não basta uma mera aceitação ou assinatura do interessado (ou ainda um *click*, no caso dos usuários de internet) para que esteja configurado o consentimento, é preciso que ele seja suficientemente livre e informado (BEYLEVELD e BROWNSWORD, 2007, p. 7).

3.3.1 Liberdade e especificidade

Não se ignora o fato de que a discussão a respeito da liberdade para consentir traz consigo profundos debates acerca da autonomia do indivíduo, liberdade de escolha, entre outras questões que podem ocupar também a filosofia do direito. Contudo, a presente pesquisa tem como foco uma análise mais funcional a respeito desta verificação de liberdade no consentimento.

Sob essa ótica, a garantia de um consentimento livre está diretamente relacionada ao princípio da finalidade e, pois, com a determinação de que o tratamento de dados pessoais seja voltado a uma finalidade específica. Nesse sentido, para verificar se existe liberdade da pessoa para consentir ao tratamento de seus dados pessoais, cabe verificar: (i) se este foi condicionado à aquisição de algum serviço essencial; (ii) se foi dado em uma relação contínua de

dependência, como em um contrato cativo de longa duração; e (iii) se for exigido em um contrato de adesão e não puder ser separado das demais cláusulas (MENDES, 2014, p. 207)

Sobre este último ponto, é interessante a análise da possibilidade de consentimento parcial em contratações realizadas com provedores de serviço da internet. Tal possibilidade é relevante, uma vez que sua privação poderia acarretar uma limitação à liberdade de escolha dos usuários. Contudo, segundo uma pesquisa realizada por Patrícia Rogosch e Erik Hohl, a maioria dos provedores de serviço não oferece possibilidade de concessão parcial do consentimento[14]. De acordo com os pesquisadores, a ausência de possibilidade de concessão parcial do consentimento decorre da dificuldade de oferecer um serviço com diferentes graus de consentimento para múltiplos usuários. Além disso, essa possibilidade não seria do interesse dos provedores do ponto de vista financeiro, considerando o risco de usuários não garantirem consentimento para anúncios de publicidade pessoais, atingindo com isso uma das maiores fontes de rendas dos sites.

Conforme apontado na referida pesquisa, o não consentimento do usuário às políticas de privacidade tem como consequência, no mais das vezes, a impossibilidade completa de acesso aos serviços ofertados[15]. Com isso, o obstáculo apresentado aos usuários (que não podem gozar dos serviços, sequer parcialmente, na hipótese de não consentimento) torna-se um mecanismo de pressão à aceitação dos termos dos sites. Os usuários frequentemente se veem forçados a escolher entre consentir integralmente aos termos apresentados ou enfrentar um isolamento social (esta consequência é mais visível quando no caso das redes sociais, nas quais a não adesão implica na impossibilidade de o usuário interagir com seu círculo social).

Conforme se extrai da nova regulamentação da União Europeia acerca da proteção de dados pessoais, para verificar se o consentimento foi suficientemente livre, em uma dada contratação, cabe observar se a execução do contrato tem como requisito o consentimento ao uso de dados pessoais que não sejam necessários para a finalidade declarada[16]. Desta forma,

[14] De acordo com a pesquisa, dos 140 sites pesquisados, somente 3 sites (2%) permitiam o consentimento parcial, 126 não o possibilitavam (90%), ao passo que 11 não requeriam o consentimento do usuário (8%). HOHL, Erik; ROGOSCH, Patricia. *Data protection and Facebook: an empirical analysis of the role of consent in social networks*. Berlin: LIT Verlag, 2012. p. 21-22.

[15] 104 dos 140 (74%) serviços pesquisados impediam totalmente o uso do serviço na hipótese de não ser dado o consentimento; 16 dos 140 (11%) permitiam o acesso parcial aos serviços; e somente 9 dos 140 (6%) não estabeleciam restrições à recusa do consentimento das políticas de privacidade. Ibidem. p. 23.

[16] Art. 7 (4) da GDPR: "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".

em uma situação com múltiplas finalidades, será necessário o consentimento a cada uma delas separadamente.

3.3.2 Informação suficiente

O processo de tomada de decisão também depende de informações claras e suficientes para que, com isso, o indivíduo possa declarar sua vontade de forma autônoma e sem restrições. Surge assim o questionamento: quão informado deve estar o indivíduo a fim de que esteja suficientemente informado? Sobre esse ponto, Roger Brownsword (2009, p. 101) afirma que o consentimento será suficientemente informado quando o indivíduo entende que o consentimento é uma opção (portanto, não há penalidade para a recusa) e que, na hipótese da concessão do consentimento (e somente para essa finalidade a qual se consentiu), será concedido o direito de agir de maneira que, caso contrário, violariam os direitos do interessado.

Outrossim, dever de informação possui conexão com o princípio da finalidade, porquanto o interessado deve ter completa consciência sobre o destino de seus dados pessoais, caso forneça o consentimento para seu tratamento. Ou seja, o indivíduo deverá ser informado a respeito da finalidade do tratamento dos dados, a quem esses dados se destinam, por quanto tempo, quem terá acesso aos dados, se poderão ser transferidos a terceiros, bem como quaisquer outros detalhes necessários para a formação da convicção livre e consciente do interessado, para que este realize o ato de autodeterminação (DONEDA, 2006, p. 383).

Não obstante, deve-se prezar não só pela quantidade de informações oferecidas, mas também por sua qualidade. Informações relevantes para a tomada de decisão incluem as possíveis consequências do consentimento e, eventualmente, de sua não concessão. Ademais, a clareza com que são dadas as informações ocupa um papel importante, pois este processo de escolha depende da capacidade do consumidor de compreender adequadamente as informações oferecidas. Para ser capaz de deliberar racionalmente, deve-se compreender os fatos relevantes bem como as circunstâncias que regem esta tomada de decisão, a fim de que seja possível discernir a melhor opção (MCLEAN, 2009, p. 45-47).

Nesse sentido, Laura Mendes (2014, p. 207) ressalta a importância de que o interessado seja informado de todas as condições do tratamento de dados, trazendo como exemplo o

disposto nos arts. 4º, caput, e 5º, V, da Lei do Cadastro Positivo (Lei nº 12.414/11)[17]. Os referidos dispositivos preveem, para a abertura do cadastro, a exigência do consentimento informado do potencial cadastrado, devendo este "ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento". Além disso, tratando-se de relação de consumo, o consentimento não será válido se for baseado em informações enganosas veiculadas pelo fornecedor, conforme dispõe o art. 37, §1º, do CDC.

Tratando-se dos usuários da internet enquanto consumidores, é relevante também a proteção conferida pelo art. 6º, III, do CDC, segundo o qual é direito básico do consumidor a "informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem". Considerando que não é especificado o meio pelo qual o contrato deva ser celebrado a fim de que o consumidor goze deste direito, entende-se que o dispositivo é aplicável a contratações de consumo celebradas em qualquer meio, inclusive na internet (MARQUES e KLEE, 2014, p. 506).

Por sua vez, o Marco Civil da Internet, em seu art. 7º, VIII, complementa o direito do usuário, assegurando a estes o direito a "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais". O inciso VII, do mesmo artigo, por sua vez, expande esta garantia no tocante às transferências de dados, prevendo o direito ao não fornecimento dos dados a terceiros "salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei".

3.3.3 Revogação do consentimento

Além do exposto, é imprescindível a garantia da possibilidade de revogação do consentimento, a fim de que esteja configurado o consentimento válido. Isto porque, sendo o consentimento um meio pelo qual o indivíduo exerce não só um controle preventivo, mas

[17] "Art. 4º: A abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada".

"Art. 5º: São direitos do cadastrado: V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento".

também posterior, na hipótese de avaliar que o tratamento de dados pessoais não seja adequado ou não atenda mais aos seus interesses (MENDES, 2014, p. 64). Nesse sentido, também destacando a essencialidade da revogação do consentimento, relata Danilo Doneda (2006, p. 380) que "a ideia da revogabilidade incondicional deste tipo de consentimento encontra fundamento no fato de que se está protegendo a própria personalidade, entre cujos atributos estaria a indisponibilidade"

A importância desta garantia pode ser extraída da análise de diversos ordenamentos de proteção de dados pessoais. A *General Data Protection Regulation* (GDPR), já em vigência na Europa, prevê em seu art. 7 (3) a possibilidade de revogação do consentimento (ainda que sem efeitos retroativos), sendo que a revogação do consentimento deve ser tão fácil de ser exercida quanto foi a sua concessão.[18] De maneira similar, a *Ley Orgánica* 15/1999, que rege a proteção de dados pessoais na Espanha prevê a possibilidade de revogação do consentimento, fazendo diferenciação quanto às revogabilidades em hipóteses de tratamento de dados ou de cessão. Em seu art. 6º, 3, a lei espanhola reconhece a possibilidade de revogação do consentimento para o tratamento dos dados pessoais, exigindo uma causa justificada e sem efeitos retroativos[19]. Enquanto isso, o art. 11º, 4, que versa sobre a cessão de dados, não se menciona o condicionamento de uma causa para a revogação[20]. Tal diferença se justifica porque a circulação dos dados pessoais pode acarretar uma ameaça maior à personalidade do cidadão (MENDES, 2014, p. 64)

Ademais, observa-se que a revogabilidade do consentimento possui conexão direta com o direito ao esquecimento, ainda que não o esgote. Do exame do art. 17 da GDPR percebe-se que a revogação do consentimento se encontra entre as condições para que o indivíduo tenha reconhecido seu direito à exclusão de seus dados pessoais.[21]

Em decorrência da importância desta garantia, é cabível uma análise empírica acerca da possibilidade de revogação do consentimento, bem como suas eventuais consequências.

---

[18] *(1) The data subject shall have the right to withdraw his or her consent at any time. (2)The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. (3) Prior to giving consent, the data subject shall be informed thereof. (4) It shall be as easy to withdraw as to give consent.*

[19] *"Art. 6. 3. El consentimento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos."*

[20] *"Art. 11. 4. El consentimento para la comunicación de los datos de carácter personal tiene también um carácter de revocable."*

[21] *Art. 17 (1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing.*

Segundo Rogosch e Hohl (2012, p. 25), uma minoria dos sites expressamente garante a possibilidade de revogação do consentimento inicial, enquanto que muitos destes não oferecem informações acerca dessa possibilidade. Por sua vez, alguns provedores permitem que os usuários excluam suas contas, mas não revelam as consequências desta exclusão no tocante aos dados pessoais ligados a estas. Nesse sentido, após a revogação do consentimento, a tendência majoritária é a exclusão da conta do usuário, de maneira a impossibilitar o uso do serviço (Ibidem, p. 28-29). E quanto à possibilidade de revogação parcial do consentimento, uma parcela dos sites analisados permitiam a possibilidade de revogação parcial do consentimento ao tratamento de dados pessoais, mas esta revogabilidade estava relacionada principalmente ao envio de e-mails promocionais e a anúncios personalizados (Ibidem, p. 26).

Portanto, quaisquer que sejam os motivos pelos quais os usuários tenham consentido inicialmente às políticas de privacidade de um determinado provedor de serviço na internet, somente existirá garantia da autodeterminação informativa se houver a possibilidade de revogação deste consentimento.

3.4 A INSUFICIÊNCIA DO CONSENTIMENTO

Da análise feita, pois, percebe-se que o consentimento do usuário consiste em um dos pilares centrais à autorização do tratamento de dados na internet. Ademais, para que ele seja válido e, com isso, efetivamente garanta legitimidade ao tratamento, são necessários os preenchimentos de uma série de requisitos. Esta exigência rigorosa, no que diz respeito à conferência de validade do consentimento, justifica-se na medida em que se busca garantir, de forma plena e com autonomia máxima, a autodeterminação informativa do indivíduo.

3.4.1 Problemas de um controle centrado no consentimento individual

Apesar da reconhecida importância da garantia de controle individual sobre os dados pessoais, a inserção do consentimento como peça estrutural nas legislações de proteção de dados pessoais levanta uma nova gama de problemas. Há um descompasso, portanto, entre a teoria legal e a realidade do comércio na internet. Diferente do que pressupõe o Direito, o

consentimento não costuma decorrer de decisões conscientes de um usuário racional e bem informado. O que efetivamente ocorre na prática do comércio eletrônico é o oposto: consumidores consentem a quaisquer tratamentos de dados, sem o devido cuidado com a leitura de termos de uso e política de privacidade (SCHERMER et al, 2014, p. 171).

Os efeitos práticos do rigor exigido para a validade do consentimento podem ser resumidos a partir das noções de *consent transaction overload* (sobrecarga transacional do consentimento), *information overload* (sobrecarga de informação) e *absence of meaningful choice* (ausência de uma opção significativa) (Ibidem, p. 176-178). O primeiro efeito diz respeito ao excessivo número de situações em que o consentimento seria requerido. A exigência de um consentimento expresso do usuário, no mais das vezes, implicaria um excesso de notificações e *pop-ups* solicitando sua autorização, gerando um efeito de desgaste na atenção dos consumidores (ao contrário do que se deseja, que é a maior atenção). Por sua vez, a exigência de que o usuário esteja suficientemente informado, para que o consentimento seja válido, tem como efeito uma sobrecarga informacional a estes. Isto porque, considerando a natureza complexa do tratamento de dados pessoais, bem como as demandas legais por transparência e notificação, os termos de uso e políticas de privacidade costumam ser extensos, repletos de linguagem técnica e, com isso, de difícil compreensão. Consequentemente, os consumidores confrontam-se com uma escolha entre uma gratificação instantânea (como contratação de um produto ou serviço desejados) ou, por outro lado, um risco abstrato relativo ao abuso dos dados pessoais, os quais frequentemente não são compreendidos plenamente. Por fim, tendo em vista a forma como são realizadas as contratações na Internet, raramente é oferecida uma margem de negociação significativa aos consumidores. Isso decorre não só das características inerentes às contratações de adesão, mas também do fato de que os provedores de serviços *online* necessitam de meios rápidos e eficientes de contratação para não perder clientes em potencial. Assim, quanto mais opções – ou *clicks* – forem necessárias para o uso do serviço, maior a chance de o consumidor desistir da contratação. Consequentemente, os consumidores deparam-se com um cenário de "usar ou largar", o que gerou uma cultura em que frequentemente são ignoradas as "caixas de diálogo" dos *sites* a fim de prosseguir com a contratação, independentemente do conteúdo das políticas de privacidade.

De maneira parecida, Bygrave e Schartum (2009, p. 160-161) resumiram os problemas decorrentes de uma proteção da privacidade na Internet centrada no consentimento do usuário. O primeiro seria no que tange à interpretação do que consistiria em um consentimento suficientemente informado. O segundo problema seria referente à limitação do poder de escolha

dos indivíduos no que se refere a produtos e serviços oferecidos por empresas detentoras de dados em situação de monopólio. Em terceiro lugar, existe a disparidade informacional entre o usuário e a empresa que detém seus dados. Salientam os autores que, mesmo na hipótese de as informações estarem suficientemente providas pelos responsáveis pelo tratamento dos dados pessoais, muitos indivíduos ainda carecem da capacidade de avaliar o valor de suas informações no mercado, ou ainda de aferir as consequências de longo prazo do consentimento. Por fim, a falta de cuidado (e interesse) dos usuários quanto à tomada de decisão acerca do consentimento ao uso de seus dados.

Outrossim, Paul Schwartz (1999, p. 821-822) elenca alguns desafios ao controle da privacidade que também podem significar a ineficácia de um controle por meio do consentimento do indivíduo e, com isso, da própria autodeterminação informativa. Neste contexto, um dos problemas destacados pelo autor é o da "armadilha da autonomia" (*autonomy trap)*, que se refere a um conjunto de consequências ligadas ao paradigma do controle dos dados pessoais na internet. Nesse sentido, alude a limitações à autodeterminação informativa, principalmente no que diz respeito à falta de conhecimento técnico de grande parte dos usuários da internet. Isto porque "a maioria dos usuários sequer está ciente de que os sites que visita coletam informações pessoais e, mesmo se sabem dessa possibilidade, os usuários tem pouco conhecimento sobre como esses dados pessoais podem ser processados" (NETANEL, 2000, p. 476).[22]

Além do mais, existem tecnologias que apresentam risco à efetividade do consentimento informado, sendo uma das principais destas a técnica de construção de perfis (*profiling).* Por perfil se compreende "um registro sobre uma pessoa que expressa uma completa e abrangente imagem sobre sua personalidade"; de modo que a construção de perfil "compreende a reunião de inúmeros dados sobre uma pessoa, com a finalidade de se obter uma imagem detalhada de comportamento, de gostos, hábitos de consumo e preferências do consumidor" (MENDES, 2014, p. 111). Assim, o *profiling* traz visibilidade a padrões não cognoscíveis por aqueles que tem seu perfil construído, já que o padrão só é perceptível pelos responsáveis pela construção do perfil. Por conta disso, uma das principais consequências desta técnica é a de que os consumidores são forçados a tomar decisões sem que tenham conhecimento pleno acerca das informações mantidas pela empresa que coleta e utiliza seus dados, trazendo, com isso,

[22] Tradução livre: "[...] most users are not even aware that the web sites they visit collect user information, and even if they are cognizant of that possibility, they have little conception of how personal data might be processed"

implicações profundas ao consentimento (HILDEBRANDT, 2009, p. 242). No caso específico do *profiling* em grupo, a construção do perfil é realizada a partir da correlação de dados de diversos indivíduos, a fim de identificar uma série de atributos em comum e, com isso, constituir grupos (Idem, 2008, p. 20). Por consequência disso, o indivíduo não tem meios de antecipar as consequências da aplicação dos perfis decorrentes dos dados de outras pessoas, de maneira que o consentimento informado fica prejudicado.

Neste âmbito, também é pertinente a análise da "falácia da suficiência" do consentimento (*falacy of sufficiency)*, referida por Roger Browsword e Deryck Beyleveld (p. 356-357). Segundo os autores, assim como não se ignora a existência de situações em que o consentimento é dispensável, sem que isso acarrete em uma violação dos direitos de um indivíduo, há de se reconhecer que nem sempre o consentimento significa a legitimidade de um ato. Para os autores, ainda que o consentimento seja suficiente para justificar a prática de ato entre privados, nada impede que este ato viole, em alguma medida, interesses públicos. Assim, seria uma falácia entender que a ausência de violação entre privados necessariamente implica na compatibilidade com a ordem jurídica.

3.4.2 Opt-in e Opt-out: o problema do consentimento implícito

Ao se reconhecer a necessidade de que o consentimento seja expresso, a fim de que seja válido, cabe o questionamento acerca da forma que deve assumir. Neste contexto, conforme referido anteriormente, existem dois modelos pelos quais um usuário pode consentir em uma determinada contratação realizada na internet: o *opt-in* e o *opt-out*.

Considerando que, por vezes, um dos requisitos para a validade do consentimento é justamente que este seja expresso, é preciso que a declaração de vontade seja clara e expressa, vedando-se a declaração oculta, subentendida ou implícita. Por este motivo, o modelo *opt-in* parece proporcionar maior validade ao consentimento, tornando legítimo o tratamento de dados (MENDES, 2014, p. 205).

Em que pese a unanimidade do reconhecimento do modelo *opt-in* como o que melhor garante a validade do consentimento, muitos provedores de serviço ainda implementam um modelo de consentimento implícito, no qual o usuário estará concordando com as cláusulas das políticas de privacidade ao clicar no botão para registrar-se no site. Este modelo costuma ser

tão usado quanto o método *opt-in* no qual se exige que o usuário assinale uma caixa para consentir aos termos, sendo que este último modelo se encontra mais presente em países nos quais a proteção aos consumidores é mais rigorosa (ROGOSH e HOHL, 2012, p. 40).

Contudo, se existe algum equilíbrio quanto à adoção dos modelos *opt-in* e *opt-out* quando do consentimento inicial, esta situação muda drasticamente em casos de emenda ou modificação das políticas de privacidade. Não só muitos provedores de serviço não notificam os usuários sobre modificações em suas políticas de privacidade (indicando uma falta de interesse em informar os consumidores), como também o modelo *opt-out* costuma ser adotado na maioria destes casos (Ibidem, p. 59-62). Segundo os dados trazidos por Patrícia Rogosch e Erik Hohl, somente uma minoria dos sites pesquisados – 8 dos 140 (6%) – utilizam um modelo no qual o usuário deve se manifestar ativamente para consentir às mudanças. Alguns provedores que utilizam o método *opt-out* oportunizam um período de tempo, que costuma variar entre duas a seis semanas, a fim de que os usuários possam se manifestar quanto à discordância das modificações. Após este período, pressupõem o consentimento do usuário quanto às mudanças. Contudo, considerando que muitos sites sequer informam devidamente os usuários acerca dessas modificações nas políticas de privacidade, dificilmente existe uma real chance de exercício da autonomia, nestes casos.

3.5 ALTERNATIVAS AO CONSENTIMENTO PARA A REGULAÇÃO DA PROTEÇÃO DOS DADOS PESSOAIS

Conforme visto, um controle da privacidade na internet centrado no consentimento do usuário apresenta uma série de obstáculos que podem comprometer sua eficiência. De acordo com Danilo Doneda (2006, p. 399):

> A impossibilidade de uma autodeterminação informativa baseada na ação singular de seu interessado é patente em vista da desproporção entre sua vontade e a existência de estruturas destinadas à coleta de seus dados e preparadas a excluí-lo de certas vantagens, caso decida por não fornecê-los.

Por este motivo, não só a doutrina vem trazendo soluções para os problemas decorrentes do consentimento do usuário, mas também as legislações de proteção de dados pessoais trazem alternativas para garantir a legitimidade no tratamento de dados pessoais. Dentre as alternativas apontadas, a presente pesquisa identifica três soluções que possuem potencial para garantia de uma tutela mais eficiente aos dados pessoais: (a) a flexibilização nos critérios de validade do

consentimento dos usuários; (b) atuação de autoridades independentes; e (c) implementação de tecnologias que complementem a proteção da privacidade na Internet.

Consoante foi apontado, a exigência de um consentimento expresso por meio do modelo *opt-in*, a fim de que este seja válido, é presente não só na doutrina, mas também nas legislações recentes em matéria de proteção de dados pessoais. No entanto, esta exigência, quando aplicada nas relações de consumo da Internet, tem como efeito uma dessensibilização do consentimento, de modo que os usuários não mais fazem escolhas racionais e bem informadas, mas sim apenas autorizam qualquer tratamento que solicite o consentimento, quaisquer que sejam seus termos (SCHERMER et al, 2014, p. 179). Nesse sentido, há uma inversão de raciocínio jurídico, pois o maior rigor normativo não equivale a uma maior proteção, motivo pelo qual uma das soluções apontadas se refere justamente à maior flexibilização nos critérios de validade do consentimento.

Desse modo, a autorização do consentimento implícito talvez seja necessária para que os consumidores não sejam sobrecarregados com informações e requerimentos de consentimento a todo momento. Assim, seria cabível uma distinção entre os dados pessoais de menor relevância e aqueles que carregam maior potencial de infringir direitos individuais, tais quais os dados sensíveis. Para estes últimos, que demandam uma proteção mais cuidadosa, não existiria óbice a exigência de rigor maior para a validade do consentimento. Para os demais, no entanto, seria exigível somente um consentimento inequívoco, seja ele expresso ativamente ou de forma implícita. Isto significa que, mesmo que o consumidor não se manifeste ativamente quanto à aprovação de um determinado tratamento de seus dados pessoais, poderá estar configurado o consentimento na hipótese de ele agir de maneira a indicar que estava ciente (por exemplo, prosseguindo na contratação, ou ainda não impedindo a utilização de *cookies* nas configurações de seu navegador de Internet). Neste modelo, diminuindo a exigência de manifestações ativas dos usuários, seria possível concentrar a atenção dos usuários ao tratamento daqueles dados que justamente são mais importantes.

Ademais, um dos principais meios de garantia da proteção dos dados pessoais na internet é por meio do estabelecimento de uma autoridade independente que poderá fiscalizar o cumprimento às normas, independentemente do consentimento dos usuários ao tratamento de dados. Neste contexto, vale destacar a regulação proposta pela GDPR. No novo regulamento europeu, são reforçadas as competências das Autoridades de Proteção de Dados, dentre as quais se destaca: a especificação de sanções a serem impostas aos responsáveis por tratamento de dados, em caso de violação das regras da GDPR; a responsabilização do responsável pelo

tratamento de dados; e a obrigação de notificação de violações de segurança de dados (GUIDI, 2018).

Estes órgãos independentes atuam de modo a aproximar as esferas do Estado, do mercado e dos cidadãos, agindo em contextos demasiadamente complexos e especializados para serem efetivamente regulados pelas instituições tradicionais (DONEDA, 2006, p. 387). Por este motivo, as autoridades independentes não só são indispensáveis no modelo europeu de proteção de dados pessoais, como também estão presentes em países como Argentina, Austrália, Canadá, Japão, Israel, Hong Kong, Nova Zelândia e Taiwan. Até mesmo nos Estados Unidos da América foi implementada a *Federal Trade Comission* (FTC) que, embora se diferencie dos órgãos presentes nos modelos citados, tem o encargo de fiscalizar a utilização de dados pessoais em relações de consumo (Ibidem, p. 386).

Estas autoridades – que recebem nomenclaturas diversas, como agências, autoridades independentes, comissários, *comissions*, conselhos, entre outras – podem ser definidas como:

> Entes ou órgãos públicos dotados de substancial independência do governo, caracterizados pela sua autonomia de organização, financiamento e contabilidade; da falta de controle e sujeição ao poder Executivo, dotadas de garantias de autonomia através da nomeação de seus membros, dos requisitos para esta nomeação e da duração de seus mandatos; e tendo função de tutela de interesses constitucionais em campos socialmente relevantes (CARINGELLA e GAROFOLI, 2000, apud DONEDA, 2006, p. 388).

É relevante mencionar que, no ordenamento jurídico brasileiro, já se fazem presentes organismos com características similares, que buscam maior eficiência na regulação de aspectos críticos do mercado e gozam de independência para atingir suas finalidades, tais quais o Instituto Brasileiro do Café ou o Instituto do Açúcar e do Álcool. (Ibidem, p. 389).

Assim, diferentes configurações são possíveis, para a implementação destes órgãos. Podem ser criados como órgãos funcionalmente independentes da estrutura estatal, nos moldes das agências; pode o próprio Ministério Público ficar responsável por tais atribuições; bem como podem ser constituídos estruturalmente ligados ao poder executivo, como no modelo Argentino, cuja *Dirección Nacional de Protección de Datos Personales* (DPDP) é parte do Ministério da Justiça do país. Em todo caso, é imprescindível a garantia de independência à atuação do órgão em relação a qualquer um dos poderes, pois suas finalidades pressupõem uma neutralidade em face dos interesses políticos e Estatais (Ibidem, p. 401).

Por último, merece menção a possibilidade de controle da privacidade por meio das próprias tecnologias adotadas pelas empresas para o tratamento de dados pessoais. Nesse sentido, a GDPR consolida os conceitos de *privacy by default* e *privacy by design*, incluindo-os dentre as obrigações do responsável pelo tratamento dos dados (GUIDI, 2018). Sob essa ótica, também é possível a garantia da privacidade por meio das já mencionadas *Privacy Enhancing Technologies.*

Menciona Daniel Le Métayer (2010, p. 323-324) que *privacy by design* consiste essencialmente em uma adequação das tecnologias de comunicação e informação à privacidade, de maneira que o *designer* destas tecnologias deverá levar em conta os princípios relativos à proteção de dados pessoais ao criá-las. Assim, é uma estrutura que visa a embutir a proteção da privacidade no desenvolvimento tecnológico desde o início do processo criativo. (ORRÙ, 2017, p. 107). Ademais, guarda similaridades à noção de *privacy by default*, também prevista na GDPR, em seu art. 25, a qual, igualmente, prevê a necessidade do responsável pelo tratamento adotar as medidas técnicas e organizacionais necessárias para que sejam utilizados somente dados pessoais específicos a finalidade de cada tratamento. Isso diz respeito à quantidade de dados coletados, à extensão do tratamento, ao tempo de armazenamento bem como à acessibilidade das informações.

Relacionada a estes princípios, existem as já mencionadas P*rivacy-Enhancing Technologies* (PETs), as quais dizem respeitos a conceitos técnico-organizacionais que buscam a proteção da identidade e privacidade de usuários. Costumeiramente, envolvem o uso de criptografia, assinaturas digitais, pseudônimos digitais, entre outras técnicas. Cabe salientar que estas PETs não se confundem com tecnologias ligadas à segurança dos dados, pois estas últimas têm como escopo um tratamento de dados seguro, independentemente da legitimidade deste, enquanto as PETs relacionam-se diretamente com a proteção da privacidade dos usuários, garantindo maior controle sobre os dados (BURKERT, 1997, p. 125). Estas PETs podem ser diferenciadas em função de suas orientações, isto é, se são relativas: ao sujeito, ao objeto, à transmissão ou ao sistema[23]. As PETs com orientação subjetiva visam a eliminar ou reduzir a capacidade de identificação do sujeito a cujos dados o tratamento diz respeito. As relativas ao objeto visam a eliminação de vestígios eventualmente ligados ao objeto de uma transação informacional (um exemplo seria a de dados pessoais ligados a um pagamento por serviço, hipótese na qual as tecnologias tentariam, sem eliminar o próprio pagamento, liberar as

[23] Tradução livre. Herbert Burker utiliza a nomenclatura *subject-oriented concepts, object-oriented concepts, transaction-oriented concepts e system-oriented concepts.* Ibidem, p. 125-128.

informações pessoais deste). As que atuam diretamente sobre a transação buscariam a eliminação de informações relativas ao processo de tratamento dos dados pessoais sem atingir propriamente o objeto ou sujeito (por exemplo, a exclusão do próprio registro da transação após a decorrência de um período predeterminado). Por fim, as PETs que atuam sobre o sistema como um todo abrangeriam os demais conceitos.

No entanto, há de se destacar que um modelo de proteção de dados pessoais não pode se apoiar somente nestas tecnologias, porquanto elas também apresentam limitações. Essencialmente, as *Privacy-Enhancing Technologies* não passam de instrumentos que podem auxiliar a tutela da privacidade dos usuários, mas ainda dependem de decisões normativas relativas ao modo de sua implementação. Assim, o ordenamento jurídico é responsável por decidir a maneira como devem ser aplicadas, quais partes merecem proteção e em que grau será concedida tal proteção (BURKERT, 1997, p. 130). Desse modo, ainda que as técnicas em si possam ser consideradas neutras, as autoridades que as implementam não o são.

CONSIDERAÇÕES FINAIS

Conforme visto, o desenvolvimento das tecnologias da informação, ao longo do século XX, demandou o surgimento da uma nova compreensão do direito à privacidade. O tratamento de dados pessoais, especialmente por processos automatizados, fez aumentar a preocupação com a proteção destes. Com isso, o direito à privacidade não mais se identifica com as liberdades negativas e com o *right to be let alone*, cujas finalidades consistiam em guardar o indivíduo de interferências alheias indesejadas. Hoje, a proteção da privacidade é compreendida de maneira mais funcional, refletida na proteção dos dados pessoais. Desse modo, a proteção de dados pessoais compreende os mesmos pressupostos ontológicos da proteção da privacidade, consistindo em um direito cuja proteção é indispensável à garantia da dignidade e desenvolvimento da personalidade dos indivíduos.

O direito à proteção de dados pessoais, desde sua primeira recepção nos ordenamentos jurídicos europeus, passou por uma série de modificações quanto ao seu sentido e sua esfera de proteção. Desde seu princípio, progresso econômico, social e tecnológico moldaram o direito à proteção de dados pessoais, de modo que as legislações sempre refletiram tais mudanças.

As primeiras normas foram criadas no contexto geral do *Welfare State*, que passou a demandar uma utilização de informações cada vez maior para o bom funcionamento da burocracia e, pois, para o devido planejamento das políticas públicas. Com isso, diversos Estados idealizaram a criação de gigantescos bancos de dados informatizados nacionais e, em decorrência deste cenário, foram criadas legislações com o escopo de controlar esse uso de dados pessoais por parte do Estado. Os anseios gerais centravam o tratamento informacional por parte dos Estados e não propriamente em uma proteção dos indivíduos.

Em consequência da proteção conferida por essas primeiras normas, que priorizavam regulamentação de procedimentos em detrimento de direitos, surgiu a segunda geração de normas. Estas, por sua vez, afastaram-se do fenômeno computacional, resgatando tutela da privacidade e dos dados pessoais como liberdades negativas. Contudo, estas regulações também apresentaram problemas, porquanto o fornecimento de dados pessoais pelos cidadãos tornara-se um requisito importante para a participação na sociedade, de maneira que uma proteção centrada na não concessão de informações implicava no isolamento da vida social.

Concomitantemente com a icônica decisão do Tribunal Constitucional Alemão, de 1983, na qual foi declarada a inconstitucionalidade parcial da Lei de Censeamento, surge o

reconhecimento do direito fundamental à autodeterminação informativa. A partir do reconhecimento da autodeterminação informativa, há uma radicalização da noção de controle individual sobre os dados e, pois, do próprio conteúdo do direito à proteção de dados pessoais. A tutela dos dados não mais dizia respeito somente à liberdade para fornecer ou não, passando a abranger também a garantia da efetividade desta liberdade sem excluir o indivíduo da participação em sociedade.

A partir de então, a autodeterminação informativa continua sendo uma constante no que se refere à proteção de dados pessoais, de modo que as normas posteriores – de quarta geração – somente visaram ampliar o alcance de fato destas garantias. Estas novas legislações já reconhecem o desequilíbrio existente na relação entre os titulares dos dados e aqueles responsáveis pelo tratamento, buscando fortalecer a posição do indivíduo. Ademais, disseminaram também o modelo de regulação e fiscalização por meio de autoridades independentes, bem como a existência de normas setoriais para campos específicos.

Portanto, percebe-se que o reconhecimento da tutela dos dados pessoais já se encontra bastante consolidada. Nesse sentido, identifica-se uma convergência dentre os diversos ordenamentos jurídicos existentes sobre esta matéria no que se refere aos princípios de proteção de dados pessoais, dos quais se extraem os principais objetivos e linhas de atuação. Ainda que possam existir divergências pontuais, é uníssono o reconhecimento de uma série de princípios, quais sejam o da finalidade, da transparência (ou publicidade), da exatidão, do consentimento, da qualidade dos dados e da segurança física e lógica.

A uniformidade existente na regulação desta matéria, bem como a sua reconhecida importância, torna imprescindível a análise acerca da existência deste direito no ordenamento jurídico brasileiro. Isto porque, como já mencionado no presente trabalho, o direito brasileiro não conta com uma lei geral sobre a matéria de proteção de dados pessoais. Destarte, cabe o exame dos instrumentos existentes para a tutela dos dados.

A Constituição Federal contempla a inviolabilidade da vida privada e da intimidade. Nesse sentido, não se ignora que a previsão constitucional reflete debates doutrinários, os quais identificam esferas de proteção distintas à intimidade (identificada com uma esfera mais interior e particular do indivíduo) e à vida privada (que pressupõe uma interferência maior do que à esfera íntima); contudo, entende-se que tais diferenciações semânticas não frutíferas para a compreensão do direito à proteção de dados pessoais. Ainda que a Constituição tenha previsto de forma diferenciada os dois termos, há de se reconhecer que ambos possuem um grau de

subjetividade significativo, uma vez que seus sentidos não podem ser preenchidos se não com auxílio da doutrina e jurisprudência. Com isso, tendo em vista que a preocupação maior do ordenamento é a própria proteção à dignidade e desenvolvimento da personalidade, a utilização do termo geral "privacidade" em nada fere o dispositivo constitucional e, além disso, é suficiente para abarcar a tutela dos dados pessoais.

Nesta senda, a proteção de dados pessoais é identificável na legislação infraconstitucional, principalmente no Código de Defesa do Consumidor, na Lei de Acesso à Informação, na Lei do Cadastro Positivo e no Marco Civil da Internet. O Código de Defesa do Consumidor (Lei 8.078/90) foi a primeira legislação do nosso ordenamento jurídico a tratar de proteção de dados e da privacidade de forma moderna, com objetivo de lidar com as novas tecnologias de processamento de dados. Assim, em seu art. 43, o CDC regula os bancos de cadastro de consumidores e, com isso, abriga os principais princípios identificados com a proteção de dados pessoais. Além disso, o CDC é imprescindível para regular as contratações de consumo celebradas na Internet, as quais frequentemente versam sobre tratamento de dados pessoais. Por sua vez, a Lei do Cadastro Positivo (Lei 12.414/2011), disciplina a formação e consulta a bancos de dados com informações de adimplemento e, tal qual o CDC, contempla alguns dos princípios associados à proteção de dados pessoais, buscando equilibrar a proteção da privacidade com o fluxo de dados no mercado e formação de históricos de crédito. Ademais, a Lei de Acesso à Informação também foi importante para a garantia da autodeterminação informativa, equilibrando uma maior transparência em relação às informações públicas com respeito à intimidade, vida privada, honra e imagem das pessoas e às liberdades e garantias individuais, nos casos das informações pessoais. Por fim, o Marco Civil da Internet (Lei 12.965/2014) expressamente garantiu a proteção à privacidade e aos dados pessoais como princípios regentes da lei. No entanto, ainda que seja identificável uma garantia legal à proteção dos dados pessoais na legislação brasileira, a ausência de uma lei geral que regule a matéria é prejudicial.

Do que se extrai do ordenamento analisado, portanto, o consentimento do interessado costuma ser a regra geral para fins de autorização do tratamento de dados pessoais. Salvo em hipóteses que possa ser dispensado, como na prevalência de interesse público, o consentimento livre, expresso e informado é indispensável para a legitimidade no tratamento dos dados, motivo pelo qual a legislação preocupa-se em garantir sua validade.

A legislação atual apoia-se principalmente no instituto do consentimento a fim de legitimar o tratamento de dados. Com isso, para que não exista violação da privacidade dos

indivíduos, é importante garantir que seus requisitos de validade sejam preenchidos, isto é, ele deve ser livre, expresso, informado e relativo à finalidade declarada. Para que um indivíduo possa exercer sua vontade de contratar de forma autônoma, pois, é necessário que esteja suficientemente informado quanto a aspectos relevantes à tomada de decisão (a serem verificados no caso concreto), não esteja condicionado a aceitação de tratamento de dados pessoais sobre finalidades outras que aquela desejada e, além do mais, que esta manifestação de vontade seja expressa (por meio de um consentimento *opt-in*).

Esta proteção centrada no consentimento do indivíduo apresenta problemas que afetam sua eficiência da tutela à privacidade. O desequilíbrio inerente às relações de consumo implica em uma falta de capacidade dos usuários compreenderem plenamente as informações relativas às políticas de privacidade. Tal realidade é agravada pelo caráter altamente técnico do tratamento de dados pessoais. Com isso, mesmo aqueles com conhecimento da matéria de proteção de dados pessoais carecem de capacidade de compreensão plena sobre todos os efeitos do tratamento. Além do mais, diferentemente do que pressupõe a legislação, o consentimento não costuma ser uma manifestação de vontade sobre o qual o consumidor dedica reflexão suficiente. Pelo contrário, a tendência das relações de consumo na Internet é a de que os consumidores autorizam o tratamento de dados pessoais sempre que for exigido, até mesmo porque a não utilização de determinados serviços *on-line* pode acarretar em um isolamento social da pessoa.

Neste contexto, o ordenamento jurídico brasileiro não oferece proteção suficiente à privacidade dos consumidores nas contratações eletrônicas, pois os instrumentos atualmente empregados não levam em conta a complexidade das relações na Internet. Por esta razão, é imprescindível a existência de uma lei geral de proteção de dados pessoais capaz de proporcionar uma estrutura mais segura aos usuários e consumidores na Rede. Em vez de sustentar a legitimidade do tratamento de dados pessoais majoritariamente no consentimento dos consumidores, é necessária a criação de autoridades independentes para a regulamentação da matéria e fiscalização do comportamento dos responsáveis, verificando a observância das normas. Ademais, uma lei geral é capaz de assegurar padrões técnicos mínimos, no que tange à garantia da privacidade, a serem observados na elaboração de novos produtos e serviços. O emprego deste conjunto de mecanismos é mais apto à proteção dos dados pessoais, em comparação a um regime que dependa excessivamente da declaração de vontade dos indivíduos.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros Editores Ltda., 2008.

ARENDT, Hannah. **A condição humana**. 10. ed. Rio de Janeiro: Forense Universitária, 2007.

_____. ***Reflections on little rock.*** Nova York, *Dissent*, 6 (1), dez–fev , 1959.

BENNETT, Colin J. ***The Privacy Advocates: resisting the spread of surveillance***. The MIT Press, 2008.

BESSA, Leonardo Roscoe. **Os limites dos bancos de dados de proteção ao crédito**. São Paulo: Editora Revista dos Tribunais, 2003.

BEYLEVELD, Deryck; BROWNSWORD, Roger. ***Consent in the law: legal theory today***. Portland: Hart Publishing, 2007.

BRANDEIS, Louis D.; WARREN, Samuel D. ***The right to privacy***. *Harvard Law Review*, v. IV, n. 5, 1890. p. 193-220.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 27 jun. 2018.

_____. Lei 8.078 de 11 de setembro de 1990. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/l8078.htm>. Acesso em: 27 jun. 2018.

_____. Lei 12.414 de 09 de junho de 2011. Planalto. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/L12414.htm>. Acesso em: 27 jun. 2018.

_____. Lei 12.527 de 18 de novembro de 2011. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 27 jun. 2018.

_____. Lei 12.965 de 23 de abril de 2014. Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 jun. de 2018.

_____. Projeto de Lei da Câmara 53 de 2018. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 27 jun. 2018.

BROWNSWORD, Roger. *Consent in data protection law: privacy, fair processing and confidentiality*. In: DE HERT, Paul; GUTWIRTH, Serge; NOUWT, Sjaak; POULLET, Yves; TERWANGNE, Cécile de (eds.). ***Reinventing Data Protection?***. Netherlands: Springer, 2009. p. 83-110.

BURKERT, Herbert. *Privacy-Enhancing Technologies: typology, critique, vision.* In: AGRE, Philip E.; ROTENBERG, Marc. (eds.). ***Technology and Privacy: the new landscape***. Cambridge: MIT Press, 1997.

BYGRAVE, Lee A.; SCHARTUM, Dag Wiese. *Consent, proportionality and collective power.* In: DE HERT, Paul; GUTWIRTH, Serge; NOUWT, Sjaak; POULLET, Yves; TERWANGNE, Cécile de (eds.). ***Reinventing Data Protection?***. Netherlands: Springer, 2009. p. 157-174.

CACHAPUZ, Maria Cláudia. **Intimidade e vida privada no novo Código Civil Brasileiro: uma leitura orientada no discurso jurídico**. Porto Alegre: Sergio Antonio Fabris Ed., 2006.

_____; CARELLO, Clarissa Pereira. Tratamento à informação, dados nominativos e a interpretação possível à lei de acesso à informação. In: **Direito, governança e novas tecnologias**. ANDRADE, Francisco António Carneiro Pacheco de; CELLA, José Renato Gaziero; FREITAS, Pedro Miguel Fernandes. Florianópolis: CONPEDI, 2017.

CANTO, Rodrigo Eidelvein do. **A vulnerabilidade dos consumidores no comércio eletrônico: a reconstrução da confiança na atualização do código de defesa do consumidor**. São Paulo: Editora Revista dos Tribunais, 2015.

COSTA JÚNIOR, Paulo José da. **O direito de estar só: tutela penal da intimidade**. 2. ed. editada, revista e atualizada. São Paulo: Editora Revista dos Tribunais Ltda., 1995

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

_____. A proteção de dados pessoais como um direito fundamental. Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

ESPANHA. ***Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal***. Disponível em: <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>. Acesso em: 27 jun. 2018.

ESTADOS UNIDOS DA AMÉRICA. *Department of Health, Education & Welfare*. *Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Julho, 1973.

FERRAZ JÚNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**.

GARFINKEL, Simson. ***Database Nation: the death of privacy in the 21st century***. EUA: O'Reilley & Associates, Inc., 2000.

GUIDI, Guilherme Berti de Campos. Modelos Regulatórios para Proteção de Dados Pessoais. In: Sérgio Branco; Chiara de Teffé. (Org.). **Privacidade em Perspectivas**. 1. ed. Rio de Janeiro: Lumen Juris, 2018, v. , p. 85-109.

HILDEBRANDT, Mireille. *Who is profiling who? Invisible visibility*. In: DE HERT, Paul; GUTWIRTH, Serge; NOUWT, Sjaak; POULLET, Yves; TERWANGNE, Cécile de (eds.). ***Reinventing Data Protection?***. Netherlands: Springer, 2009. p. 239-252.

HOHL, Erik; ROGOSCH, Patricia. ***Data protection and Facebook: an empirical analysis of the role of consent in social networks***. Berlin: LIT Verlag, 2012.

HURD, Heidi M. The moral magic of consent. In: ***Legal theory today***. vol. 2. Cambridge: Cambridge University Press, 1996. p. 121-146.

KLEE, Antonia Espíndola; MARQUES, Cláudia Lima. Os direitos do consumidor e a regulamentação do uso da internet no brasil: convergência no direito às informações claras e completas nos contratos de prestação de serviços de internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 469-517.

LIMA, Caio César Carvalho. Garantia da privacidade e dados pessoais à luz do marco civil da internet. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet.** São Paulo: Atlas, 2014. p. 148-164.

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

LE MÉTAYER, Daniel. *Privacy by design: a matter of choice*. In: GUTWIRTH, Serge; DE HERT, Paul; POULLET, Yves. ***Data protection in a profiled world***. Springer, 2010.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Editora Saraiva, 2011.

LORENZETTI, Ricardo Luis. **Fundamentos do direito privado**. São Paulo: Editora Revista dos Tribunais, 1998.

_____. **Comércio Eletrônico**. São Paulo: Editora Revista dos Tribunais, 2004.

MARKKULA, Jouni; ROHUNEN, Anna; TIKKINEN-PIRI, Christina. *EU General Data Protection Regulation: changes and implications for personal data collecting companies*. In: **Computer Law & Security Review**. Elsevier, 2017.

MARTINS, Guilherme Magalhães. O direito ao esquecimento na internet. In: _____ (coord.). **Direito Privado e Internet**. São Paulo: Atlas, 2014. p. 3-28.

MAYER-SCHÖNBERGER, Viktor. *Generational development of data protection in Europe*. In: AGRE, Philip E.; ROTENBERG, Marc. (eds.). ***Technology and Privacy: the new landscape***. Cambridge: MIT Press, 1997.

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

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. (Org.). **Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2015. p. 205-230. V. 1.

MORAIS, José Luis Bolzan de; NETO, Elias Jacob de Menezes. A insuficiência do Marco Civil da Internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da *surveillance*. In: LEITE, George Salomão; LEMOS, Ronaldo (coord.). **Marco Civil da Internet**. São Paulo: Atlas, 2014. p. 417-439.

NETANEL, Neil Weinstock. *Cyberspace self-governance: a skeptical view from liberal democratic theory*. Berkeley, California Law Review, v. 88, p. 395-498, mai. 2000.

PARLAMENTO EUROPEU. **Diretiva 95/46/CE**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 27 jun. 2018.

_____. ***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)***. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1530135586767&uri=CELEX:32016R0679>. Acesso em: 27 jun. 2018.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 7. ed. São Paulo: Atlas, 2014.

ROBL FILHO, Ilton Norberto. Direito, intimidade e vida privada: uma perspectiva histórico-política para uma delimitação contemporânea. In: CORTIANO JUNIOR, Eroulths; MEIRELLES, Jussaria Maria Leal de; FACHIN, Luiz Edson; NALIN, Paulo (coord.). **Apontamentos críticos para o direito civil brasileiro contemporâneo**. Curitiba: Juruá Editora, 2009. p. 263-280.

SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone. ***Crisis of consent: how stronger legal protection may lead to weaker consent in data protection.*** Dordrecht: Springer, 2014. p. 171-182.

SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

SCHWARTZ, Paul M. *Internet privacy and the state.* Connecticut *Law Review*, 1999. v. 32. p. 815-859.

SHILLS, Edward. ***Privacy: its constitution and vicissitudes. Law and contemporary problems***, Durham: N.C. School of Law, Duke University, Privacy, v. 31, n. 2, 1966. p. 281-306.

ZANFIR, Gabriela. *Forgetting about consent. why the focus should be on "suitable safeguards" in data protection law*. In: GUTWIRTH, Serge; DE HERT, Paul; LEENES, Ronald. (eds.). ***Reloading data protection: multidisciplinar insights and contemporary challenges***. Dordrecht: Springer, 2014. p. 237-258.

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