UNIVERSIDADE FEDERAL DO PARANÁ

HEITOR BUENO NOVELLI

A PROTEÇÃO DE DADOS NO BRASIL E NA EUROPA: UM COMPARATIVO ENTRE A LEGISLAÇÃO BRASILEIRA E O MODELO EUROPEU

CURITIBA

2017

HEITOR BUENO NOVELLI

A PROTEÇÃO DE DADOS NO BRASIL E NA EUROPA: UM COMPARATIVO ENTRE A LEGISLAÇÃO BRASILEIRA E O MODELO EUROPEU

Trabalho de conclusão de curso apresentado ao Curso de Graduação em Direito, Setor de Ciências Jurídicas da Universidade Federal do Paraná, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Cesar Antonio Serbena

CURITIBA

2017

AGRADECIMENTOS

Aos meus pais, pelo apoio durante todo período da graduação.

Ao professor orientador Cesar Serbena, pela paciência e pelos conselhos fundamentais para a conclusão deste trabalho.

À minha amiga Ana Maria Higuti Becker, pelo companheirismo durante todo o período da graduação, além das dicas que ajudaram a estruturar o tema de estudo.

Ao amigo e companheiro de trabalho Daniel Sucha Heidemann, pela revisão e pelas sugestões sobre diversos detalhes que engrandeceram este trabalho.

RESUMO

Devido ao uso cada vez maior das novas tecnologias, a proteção de dados pessoais tem sido cada vez mais relevante nos dias de hoje. Neste trabalho foram analisadas as leis brasileiras e os atos legislativos da União Europeia sobre este tema, de modo a localizar as características principais destas normas que protejam de forma efetiva os dados pessoais dos titulares. Para realizar tal intento, realizou-se um panorama histórico do direito à privacidade e suas implicações com a Internet. Em seguida, o estudo passou para a legislação brasileira partindo da Constituição até as leis infraconstitucionais, dando uma ênfase maior ao Marco Civil da Internet (Lei n° 12.965/2014). No exame da legislação europeia foi feito um histórico das legislações referentes à proteção de dados, realizando uma análise da transposição das Diretivas sobre a proteção de dados para o ordenamento português. O estudo da legislação europeia terminou com uma apresentação das principais mudanças introduzidas pelo Regulamento 2016/679, que regulará o tema na União Europeia a partir de Maio de 2018. Após a análise dos pontos fundamentais dos modelos brasileiro e europeu, este trabalho demonstrou as diferenças e semelhanças entre estas legislações, tecendo, no final, algumas considerações sobre a comparação entre os dois modelos legislativos.

Palavras-chave: Proteção de dados, Privacidade, Internet, Marco Civil da Internet.

ABSTRACT

Due to the raise use of the new technologies, the protection of personal data has been increasingly relevant nowadays. In this work, the Brazilian laws and legislative acts of the European Union were analyzed in order to locate the main characteristics of these norms that effectively protect the personal data of the holders. To carry out such attempt, a historical overview of the right to privacy and its implications for the Internet was realized. The study then moved on to Brazilian legislation from the Constitution to the infraconstitutional laws, giving emphasis to the Marco Civil da Internet (Law n° 12.965/2014). In the examination of European legislation, a history of data protection legislation was carried out, analyzing the transposition of the Data Protection Directives into the Portuguese legal system. The study of European legislation ended with a presentation of the main changes introduced by Regulation 2016/679, which will regulate the subject in the European Union on May 2018. After analyzing the fundamental points of the Brazilian and European models, this work demonstrated the differences and similarities between these legislations, arguing, at the end, some considerations about the comparison between the two legislative models.

Keywords: Data Protection, Privacy, Internet, Marco Civil da Internet.

SUMÁRIO

1 INTRODUÇÃO

O avanço da tecnologia tem gerado benefícios incontáveis para a nossa sociedade. O impacto destas mudanças tornou obsoletas certas práticas e criou outras inteiramente novas em nosso dia-a-dia. A Internet, que antes era algo reservado a um círculo pequeno de pessoas com interesses específicos por tecnologia, hoje é um segundo ambiente frequentado por boa parte da população. Neste admirável mundo novo, as mensagens trafegam de um ponto a outro do globo em frações de segundo. As compras estão a alguns cliques de distância, chegando até a sua residência carregadas por um drone em algumas horas apenas. Mas nem tudo são flores neste mundo. Junto com este avanço tecnológico surgem também novos problemas a serem resolvidos neste novo mundo *high tech*.

Um destes problemas enfrentados é na questão dos dados pessoais e sua proteção. Praticamente tudo que é feito na Internet deixa rastros, pegadas que parecem sem importância quando analisadas isoladamente, mas que quando somadas com outras pegadas conseguem traçar um perfil completo de uma determinada pessoa. Diante desta situação, a lei possui um papel fundamental em garantir a proteção dos dados dos usuários que utilizam estes novos meios de comunicação. O objetivo deste trabalho será traçar um paralelo entre as normas de proteção de dados entre o Brasil e a União Europeia, extraindo desta comparação algumas considerações sobre os aspectos mais relevantes destes modelos.

Para este intento, a discussão irá iniciar com um breve histórico da proteção à privacidade e suas primeiras manifestações legislativas na história. Em seguida, será feito um breve panorama histórico da Internet e suas implicações com a questão da privacidade.

Após a introdução de alguns conceitos básicos sobre privacidade e Internet, este estudo partirá para a análise da legislação nacional relacionada à privacidade e a proteção de dados. Partindo da Constituição Federal, passando pelas legislações infraconstitucionais, o objetivo deste capítulo será mostrar, de uma forma breve, como o tema é tratado pelo ordenamento brasileiro.

Em seguida, parte-se para uma análise de como a União Europeia tutela a questão da proteção de dados. O capítulo inicia com um breve histórico da proteção de dados no Continente, que se inicia com as primeiras legislações nacionais até o

surgimento das primeiras tentativas de uma legislação supranacional. A Diretiva 95/46/CE e a Diretiva 2002/58/CE e suas transposições para a legislação portuguesa serão o ponto seguinte deste capítulo. O estudo irá focar seu lume nos pontos principais destes atos legislativos da União Europeia e suas transposições à legislação portuguesa. Por fim, o capítulo encerrará com um exame do Regulamento 2016/679, que será o ato legislativo responsável por harmonizar o tema na União Europeia.

O penúltimo capítulo será um ensaio sobre as semelhanças e diferenças entre os modelos legislativos estudados. Neste capítulo serão demonstradas, em primeiro lugar, as semelhanças mais significativas entre o modelo brasileiro e o modelo europeu de proteção de dados. As diferenças entre os modelos serão apresentadas na sequência, focando-se nos pontos mais importantes presentes nestas legislações.

Por fim, no último capítulo, após ter sido feito um paralelo entre os ordenamentos, o estudo irá expor algumas conclusões do que foi analisado no restante do trabalho. Demonstrando algumas falhas ou ausências que poderiam ser suprimidas ou melhoradas pelas legislações examinadas, assim como outras medidas que poderiam ser implementadas no sentido de aperfeiçoar a proteção de dados no Brasil.

2 A PRIVACIDADE E A INTERNET

Há alguns anos atrás, Max Schrems[1], na época estudante de Direito da Universidade de Santa Clara, resolveu contatar os responsáveis pelo Facebook para obter os dados[2] referentes à sua conta na rede social. Depois de muita insistência por parte de Max, a empresa consentiu em enviar os dados. O resultado foi surpreendente, dados que correspondiam, caso fossem impressos, a mais de 1200 páginas. Coletados no decorrer dos três anos nos quais o estudante havia utilizado a rede social. Dentre os dados enviados, havia não só informações ainda presentes no Facebook de Max, mas também fotos e conversas que haviam sido deletadas de sua conta.

Indignado com a situação, Max ajuizou uma ação coletiva contra a empresa e criou uma ONG, “Europa versus Facebook”, para identificar abusos e falhas nas políticas de privacidade da rede social. Segundo os trabalhos desta ONG, o Facebook tem informações relacionadas a 50 tipos de dados – amizades feitas e desfeitas, status de relacionamentos e até mesmo, conforme já mencionado, mensagens apagadas. O processo movido por Max ainda aguarda julgamento por parte da Corte Europeia de Justiça

O caso suscita o debate sobre a privacidade, que hoje é ainda mais atual e importante devido à popularização da Internet pelo mundo. A proteção da privacidade deixou de ser uma preocupação de algumas poucas pessoas, como era em tempos passados, para ser uma preocupação que atinge um número expressivo de pessoas. No mundo interligado pela Internet, esta preocupação se caracteriza pela proteção dos dados que circulam pela grande rede de computadores. Os mecanismos de defesa deste direito, assim como a própria concepção do direito a privacidade e sua evolução, são, portanto, os primeiros passos para iniciar a discussão sobre a proteção de dados.

---

[1] Disponível em: http://g1.globo.com/tecnologia/noticia/2014/08/em-site-austriaco-pede-que-usuarios-do-facebook-se-unam-contra-rede.html

[2] Alguns autores colocam uma distinção entre dado e informação: “dado”, para estes autores, seria "uma informação em estado potencial, antes de ser transmitida, seria uma espécie de “pré-informação”; por outro lado, a “informação” ultrapassa o significado do dado, atingido o "limiar da cognição, e mesmo nos efeitos que esta pode representar para seu receptor" (DONEDA, 2006, p.152). Na prática esta distinção é irrelevante. Neste trabalho estes termos serão usados de forma indistinta.

Neste capítulo será feita uma conceituação histórica do direito à privacidade, assim como suas primeiras manifestações. Em seguida, o estudo irá para uma breve análise histórica do surgimento da Internet e dos desdobramentos acarretados por esta tecnologia no que tange à privacidade. O objetivo deste capítulo é estabelecer os conceitos sobre privacidade e Internet que nortearão o restante do trabalho.

2.1 O DIREITO À PRIVACIDADE

Ao traçar uma origem ao conceito de privacidade podemos encontrar seus vestígios já na Antiguidade, com as sociedades gregas e romanas. Aristóteles distinguia entre o "*oikos"* e a "*polis*", na qual a primeira dizia respeito à esfera privada do indivíduo e suas manifestações – a família, as questões biológicas e econômicas -, enquanto a segunda era relacionada às questões públicas dos cidadãos (FLORENZANO, 2001). Ao reservar um aspecto da vida do cidadão uma noção distinta da sua vida pública, a esfera do "*oikos"*, nesta divisão aristotélica, possui uma forma primitiva de um conceito de privacidade. O mesmo pode ser observado na Roma Antiga com suas normas de proteção à informação (DONEDA, 2006, p.66). Os vestígios de um direito à privacidade podem ser vistos nestas civilizações antigas, ainda que com uma função bastante distinta da surgida na modernidade.

No Iluminismo começamos a ver os primeiros contornos de um conceito de privacidade como conhecemos hoje. Este período da História possui uma ênfase na liberdade dos indivíduos, mais precisamente as chamadas liberdades negativas: a liberdade do indivíduo e da sociedade de exercerem seus direitos civis e políticos – e todos os direitos advindos destes – sem a interferência positiva estatal. Nas palavras de JOSÉ AFONSO DA SILVA:

> [...] direitos fundamentais do homem-indivíduo, que são aqueles que reconhecem autonomia aos particulares, garantindo iniciativa e independência aos indivíduos diante dos demais membros da sociedade política e do próprio Estado; por isso são reconhecidos como direitos individuais, como é de tradição do Direito Constitucional brasileiro (art. 5º), e ainda por liberdades civis e liberdades-autonomia. (DA SILVA, 2002, p.182)

Neste momento nós temos uma individualização exacerbada – o direito de ser deixado só – no qual a obra considerada como marco fundamental é o *The Right to privacy*, o famoso artigo escrito por Samuel Warren e Louis Brandeis (WARREN; BRANDEIS, 1890). Neste artigo encontra-se a definição do direito de estar só (*right*

to be alone), que seria o direito de manter-se afastado dos demais, uma necessidade para a preservação da mente e desenvolvimento da personalidade.

Assim, neste momento, temos a entrada do direito à privacidade em ordenamentos que possuíam um cunho eminentemente patrimonialista, o que fez com que a sua tutela ficasse reservada ao estrato mais alto da sociedade. Logo, os primeiros julgados sobre o tema se referem aos integrantes do escol da sociedade: artistas e nobres (DONEDA, 2006).

Com o passar do tempo, e o consequente desenvolvimento tecnológico, temos uma inversão desta tendência do direito à privacidade, como um direito reservado apenas para uma parcela pequena da população. A mudança tem como fundamentos, principalmente, a mudança do estado liberal que passa para o chamado *welfare state.* Como consequência disto, surge uma demanda maior de direitos por parte da população, tendo como resultado a positivação do direito à privacidade na Declaração Universal dos Direitos do Homem, adotada pela ONU em 1948, que estabelece:

> Artº 12º : Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei. (ONU, 1948)

Também no plano internacional, na Convenção Americana de Direitos Humanos de 1969 (Pacto de San José da Costa Rica), observa-se a guarida do direito à privacidade, conforme o seu artigo 13:

> 3. Não se pode restringir o direito de expressão por vias ou meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de frequências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de ideias e opiniões. (CONVENÇÃO AMERICANA DE DIREITOS HUMANOS, 1969)[3]

Destarte, a informação pessoal, já no fim da primeira metade do século passado, passa a não ser uma preocupação apenas para pessoas da chamada “alta sociedade”. A tecnologia nesse estado de bem-estar social demanda informações para que possa por suas políticas públicas em prática. Os dados passam a vir de uma parcela cada vez maior da sociedade, de estratos diferentes da sociedade.

[3] Disponível em: http://www.cidh.org/Basicos/Portugues/c.Convencao_Americana.htm

A justificativa para a utilização das informações pessoais por parte da administração pública são duas: o controle e a eficiência. Sobre o controle, podemos citar várias atividades desempenhadas pelo estado que podem ser potencializadas com uma quantidade maior de informações pessoais. A atividade policial, por exemplo, se torna mais fácil à medida que existe uma quantidade maior de dados sobre a população - basta ver a importância do controle da informação em países autoritários. Quanto à eficiência, torna-se muito mais simples para o Estado implementar suas políticas públicas quando seus censos e bancos de dados estão mais providos de informações pessoais (DONEDA, 2006).

Em um primeiro momento o uso destas informações fica acentuado apenas pela esfera pública. Por um problema estrutural, a esfera privada não possui, neste período, recursos financeiros suficientes para a coleta de informações como a administração pública.

A evolução da tecnologia iria alterar essa dinâmica com a popularização dos microcomputadores e o desenvolvimento da Internet. Na segunda metade do século XX ocorre o surgimento da rede mundial de computadores, que barateia e simplifica a coleta de dados. Dentro deste novo mundo virtual surgem os conceitos de *Big Data* e da chamada sociedade da Informação. Temas que necessitam de um tópico separado dentro deste trabalho.

2.2 A INTERNET E A SOCIEDADE DE INFORMAÇÃO

A origem da Internet se dá com a criação da ARPA Net por parte do exército americano. Após a Segunda Guerra Mundial, com o período da Guerra Fria, era a intenção dos militares possuir um meio de comunicação que não fosse dependente de uma entidade central e que, caso um dos pontos da rede ficasse inoperante, os outros nós da rede ainda pudessem se comunicar.

Com o passar do tempo, e com o arrefecimento dos ânimos entre as potências nucleares, a ARPA Net passou a integrar mais universidades que possuíam interesse em pesquisa nesta área de comunicação. Estas primeiras décadas são marcadas, portanto, por uma rede restrita a uma coligação entre militares e algumas universidades americanas. Desta primeira fase, destaca-se o

protocolo TCP-IP[4], que seria o protocolo padrão para a Internet a partir da década de 80.

A década de 90 marca o início da popularização da Internet. O surgimento dos chamados computadores domésticos (ou microcomputadores), possibilitado pelo barateamento da tecnologia, fez com que um número expressivo de pessoas adentrasse na rede mundial de computadores. O "*World Wide Web*"[5] e o protocolo HTTP[6], que iriam se incorporar de forma definitiva na rede, são criações do início da década de 90.

O boom da Internet viria após a virada do século XX, quando a Internet passa da casa dos milhões de usuários para a casa dos bilhões[7]. A crescente popularização dos microcomputadores, assim como as redes de banda larga com preços mais acessíveis, são os principais motivos dessa explosão de usuários na grande rede. É a partir desta década que o e-commerce e as redes sociais passam a ter uma importância relevante na vida das pessoas. É nesta década também que as discussões sobre a sociedade da informação e suas implicações econômicas passam para o plano central de discussão.

A interconexão massiva, propiciada por microcomputadores baratos ligados a uma rede economicamente acessível, levou a uma transição social centrada na informação. Esta sociedade centrada na informação, segundo MANUEL CASTELLS, é definida como:

> [...] uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microeletrônica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes. (CASTELLS, 2005, p. 20)[8]

---

[4] TCP (Protocolo de Controle de Transmissão) IP (Protocolo de Internet). O TCP/IP ficou definido como protocolo padrão da ARPA Net a partir de 1983.

[5] World Wide Web, o famoso "www" que inicia os sites da Internet foi uma criação do CERN (Organisation Européenne pour la Recherche Nucléaire) para facilitar a transferência de documentos de hipermídia. A partir de 1993 o CERN permitiu para todos o acesso ao software do "World Wide Web", o que o popularizou rapidamente ante a outros softwares proprietários.

[6] Hiper Transfer Protocol (Protocolo de Transferência de Hipertexto) é um protocolo de comunicação entre sistemas de informação que permite a transferência de dados entre redes de computadores, principalmente na World Wide Web (Internet).

[7] Disponível em: http://www.internetworldstats.com/stats.htm

[8] CASTELLS usa o termo "rede" para se referir a um aspecto mais amplo desta palavra, que vai além do conceito apenas da rede de computadores. Neste trabalho o foco é se ater apenas nas redes de computador, o uso dado pelo autor do termo para a questão da sociologia foge do campo de discussão deste estudo.

Esta estrutura gera o chamado ciberespaço, o mundo paralelo ao real em que a população passa cada vez mais tempo inserida. Em alguns casos até sobrepondo ao mundo real, ocorrendo situações que lembram o caso do personagem Mattia Pascal, no famoso romance de Luigi Pirandelo[9]. Por caminhar praticamente *pari passu* com o mundo real, o ciberespaço acaba absorvendo uma quantidade massiva de informações provenientes dos seus usuários.

Todas estas informações, que podem parecer irrelevantes quando olhadas de forma isolada, se transformam em um aglomerado conhecido como *Big Data*. Praticamente tudo que praticamos no ambiente virtual deixa pegadas, que vão sendo coletadas por meio de *cookies*[10] e outros softwares que capturam informações. Ou nós mesmos cedemos nossos dados de forma voluntária, muitas vezes sem saber como serão utilizados por quem os coleta. Estas informações, quando tratadas de forma correta, podem revelar muito de nossas preferências e nossos desejos. Transformando-se, consequentemente, em uma moeda a ser usada dentro do ciberespaço:

> Tudo o que você faz na rede produz dados. Esses dados, agregados, são extremamente valiosos, mais valiosos para o comércio do que para o governo. O governo (em circunstancias normais) apenas se importa que você obedeça a um certo conjunto de leis. O comércio, por sua vez, está interessado em descobrir como você quer gastar seu dinheiro, e os dados fazem exatamente isso. Com grandes quantidades de dados sobre você, sobre o que você faz e sobre o que você diz, torna-se cada vez mais possível comercializar você de uma maneira direta e efetiva. (LESSIG, 2006, p. 216)[11]

Não é por qualquer motivo que as empresas que controlam os *Big Datas* estão entre as mais ricas do mundo. Na economia de informação, os dados pessoais são *commodities*.

Em um ambiente como este, o controle das informações pessoais passa a ser de fundamental importância para os usuários da Internet. Levando até ao conceito

---

[9] No romance de Pirandello, o personagem Mattias Pascal é confundido com outra pessoa que cometeu suicídio e se torna um "morto" para a sociedade. A analogia aqui é na questão da importância dada para informações presentes em registros civis – ou na Internet – se sobrepondo a vida real dos seus titulares.

[10] Pequeno pacote de dados usado para rastrear as preferências dos usuários na Internet.

[11] Tradução livre de: "Everything you do on the Net produces data. That data is, in aggregate, extremely valuable, more valuable to commerce than it is to the government. The government (in normal times) really cares only that you obey some select set of laws. But commerce is keen to figure out how you want to spend your money, and data does that. With massive amounts of data about what you do and what you say, it becomes increasingly possible to market to you in a direct and effective way".

de autodeterminação informativa, que seria justamente o direito do sujeito controlar os seus próprios dados, mas não se esgotando apenas a isto. Nas palavras de FABIANO MENKE:

> Segundo o Tribunal Constitucional Federal [Alemão], a autodeterminação informativa vai além da proteção da privacidade. Ela confere ao indivíduo o poder de basicamente determinar por si próprio sobre a divulgação e a utilização de seus dados pessoais. A autodeterminação informativa complementa a proteção constitucional da liberdade comportamental e da privacidade. (RAINER ERD apud MENKE, 2015, p.218)

Voltando ao caso de Max Schrems, descrito no começo do capítulo, nota-se que muito da vida uma pessoa pode estar armazenado em um servidor localizado em algum lugar distante do globo. A proteção dos dados pessoais é, neste mundo interconectado com o ciberespaço, uma questão de fundamental importância.

Feita esta breve introdução sobre o problema atual da privacidade dentro do ciberespaço, em que foi descrito algumas das questões que permeiam o discurso sobre a proteção de dados, passa-se agora para a análise de como o ordenamento pátrio trata do tema.

3 A PROTEÇÃO DE DADOS NA LEGISLAÇÃO BRASILEIRA

O escopo deste capítulo será a analise de como o ordenamento pátrio trata da questão proteção de dados. Seguiremos o caminho lógico de partir do nível constitucional, seguir pelo Código Civil, encerrando este capítulo nas leis ordinárias.

Leis que também tratam da questão da privacidade e proteção de dados, tais como as Leis n.º 9.296/1996 e n.º 10.217/2001 (que tratam da interceptação telefônica e da gravação ambiental) não serão tratadas neste trabalho. Por uma questão de escopo da discussão – e também de espaço – o foco da discussão se restringirá aos títulos legais de maior relevância com o tema.

Quanto ao Projeto de Lei nº 5.276 de 2016, conhecido como a Lei de Proteção de Dados, por ainda não ter sido aprovado e, portanto, sem uma forma final, será feita apenas uma breve análise do conteúdo do projeto.

3.1 A PRIVACIDADE NA CONSTITUIÇÃO BRASILEIRA

O primeiro ponto quanto à questão da privacidade em nossa Carta Magna é definir em qual nomenclatura este direito está inserido. Realizar este procedimento é uma tarefa importante, uma vez que a Constituição brasileira apresenta nomenclaturas diferentes para os direitos fundamentais. Assim, o art. 4°, inciso II, apresenta em seu texto a definição “direitos humanos”. Os “direitos e garantias fundamentais” estão localizados no Título II, arts. 5° a 17° - não se limitando apenas a estes artigos. No inciso LXXI do art. 5° há os “Direitos e liberdades constitucionais”, mais a frente tem-se “direitos e garantias individuais” no art. 50, §4, IV. Além destas nomenclaturas ainda contamos no Título VII com artigos que consagram o “direito à saúde” (artigos 196 a 200), “direito à educação” (artigos 205 a 214), etc.

Embora estas nomenclaturas sejam tratadas como sinônimos pela Constituição, cabe aqui o entendimento de JOSÉ GOMES CANOTILHO, que define que a expressão direito fundamental deve ser utilizado para designar os direitos “jurídico-institucionalmente” garantidos e limitados espaço-temporalmente, “direitos objetivamente vigentes numa ordem jurídica concreta” (CANOTILHO, 2003, p.393).

Seguindo esta definição, o direito à privacidade, para nossa Carta Magna, é um direito fundamental, localizado no artigo 5° do texto constitucional. Na definição de INGO WOLFGANG SARLET:

> Os direitos fundamentais, como resultado da personalização e positivação constitucional de determinados valores básicos (daí seu conteúdo axiológico), integram, ao lado dos princípios estruturais e organizacionais (a assim denominada parte orgânica ou organizatória da Constituição), a substância propriamente dita, o núcleo substancial, formado pelas decisões fundamentais, da ordem normativa, revelando que mesmo num Estado constitucional democrático se tornam necessárias (necessidade que se fez sentir da forma mais contundente no período que sucedeu à Segunda Grande Guerra) certas vinculações de cunho material para fazer frente aos espectros da ditadura e do totalitarismo (SARLET, 2005, p.70)

A preocupação da Constituição foi além e garantiu uma amplitude de proteção maior aos direitos fundamentais. Como declara o artigo 60, §4°, inciso IV, os direitos fundamentais recebem o *status* de cláusulas pétreas.

Conforme já mencionado, em nossa Carta Magna os direitos à privacidade estão situados na área de direitos fundamentais, mais precisamente no artigo 5°, incisos X e XII, a privacidade e o sigilo das informações, respectivamente. Além destes dois incisos, a Constituição protege também alguns aspectos específicos relacionados à privacidade, tais como a proteção ao domicílio (art. 5°, XI) e a violação de correspondência (art. 5°, XII).

O inciso X da Constituição declara que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”, criando uma distinção entre intimidade e vida privada. Neste ponto cabe demonstrar o que se entende por vida privada e por intimidade da leitura feita pelos doutrinadores do texto constitucional.

A intimidade, em linhas gerais, pode ser definida como a esfera da vida do indivíduo que ele escolhe esconder do conhecimento dos demais. JOSÉ AFONSO DA SILVA define a intimidade como aquilo que “integra a esfera intima da pessoa, porque é repositório de segredos e particularidades de foro moral e intimo da pessoa”, incluindo, nesse sentido, a inviolabilidade do domicílio, o sigilo da correspondência e o segredo profissional (DA SILVA, 2002, p.207).

A distinção entre a intimidade e a vida privada não é tão simples. A leitura da nossa Constituição leva a constatação de que a vida das pessoas é compreendida por dois aspectos distintos. O primeiro aspecto é o voltado para o exterior, que trata das relações sociais entre as pessoas e suas atividades públicas. Este é aspecto o

que pode ser objeto de pesquisa e de divulgação por parte de terceiros. A vida interior, o segundo aspecto, é o que, analisado sobre a mesma pessoa, vai tratar sobre os membros de sua família, sobre seus amigos, este aspecto é o que irá integrar o conceito de vida privada (DA SILVA, 2002).

No que se refere à vida privada, a tutela constitucional tem como objetivo proteger os indivíduos de duas violações particulares: ao segredo da vida privada e à liberdade da vida privada (DA SILVA, 2002, p.208). Um dos principais atentados ao segredo da vida privada e a liberdade da vida privada é a divulgação, ou seja, levar ao conhecimento público eventos relevantes da vida pessoal e familiar. Garantir que estes direitos não sejam violados é indispensável para que a pessoa possa realizar sua vida privada, sem a perturbação de terceiros (SAMPAIO, 1998).

Analisando à luz da proteção de dados, podemos dizer que o texto constitucional abarca a disciplina como uma subespécie da privacidade. Entretanto, segundo DANILO DONEDA, em um regime de proteção de dados pessoais, a referência ao direito à privacidade a uma cláusula geral da personalidade não é e "uma operação automática nem uma opção única". Para o autor, a proteção de dados pessoais é uma garantia de caráter instrumental, que advém da tutela da privacidade, mas não limitada por esta, fazendo referência a outras garantias fundamentais presentes no nosso ordenamento (DONEDA, 2006, p. 326). Dentre estas garantias, o habeas data, que será discutido brevemente em seguida.

3.1.1 O *Habeas Data*

Ainda dentro da análise da Carta Magna, é importante destacar o instituto do *habeas data*, instrumento pioneiro nas legislações latino-americanas, originado na Constituição de 1988. O *habeas data* foi uma consequência ao término do regime ditatorial que estava presente e o período de redemocratização que vivia o país na época da elaboração do texto constitucional.

A Assembleia Constituinte criou o instituto no ordenamento brasileiro para servir de instrumento para a requisição de informações pessoais presentes nos órgãos do poder público. Como já foi citado, o Brasil estava saindo de um período de regime ditatorial e o objetivo era proporcionar ao cidadão uma forma de conhecer – ou retificar, caso fosse necessário - os dados referentes à sua própria pessoa

armazenados pelo governo. Conforme o entendimento de HELY LOPES MEIRELLES:

> *Habeas data* é o meio constitucional posto à disposição de pessoa física ou jurídica para lhe assegurar o conhecimento de registros concernentes ao postulante e constantes de repartições públicas ou particulares acessíveis ao público, para retificação de seus dados pessoais. (MEIRELLES, 2009, p. 728).

Presente no rol do artigo 5° da Constituição (artigo 5°, LXXII), o *habeas data* é uma das ações constitucionais que, junto com outros instrumentos, servem à garantia de direitos individuais e coletivos. Conforme o texto do instituto:

> LXXII - conceder-se-á habeas data:
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; (BRASIL, 1988)

No que tange à proteção de dados, a aplicação do *habeas data* seria uma forma prevista pela Constituição para a tutela deste direito. Um instrumento para que a pessoa possa ter acesso aos dados referentes à sua pessoa presentes em órgãos públicos e privados – embora o texto faça referência apenas aos órgãos do setor público, a doutrina e a jurisprudência estenderam a aplicação do instrumento, posição ratificada pelo Código de Defesa do Consumidor.

Inegavelmente uma proteção importante que foi adotada por nosso ordenamento, o *habeas data* possui algumas limitações que o tornam uma ferramenta deficitária para a questão da proteção de dados. O instrumento para poder ser invocado necessita que primeiro tenha ocorrido a tentativa de obtenção da informação pelos meios administrativos e o seu esgotamento na tentativa de aquisição (conforme o disposto pela Súmula n° 2 do STJ). Ou seja, nos casos que envolvem a Internet, como nos dias de hoje, já encontramos a dificuldade de saber sequer como iniciar essa requisição, haja vista que o dado pode fazer parte do banco de dados de uma instituição de outro país. Após o insucesso e agora apto para propor a ação, temos ainda a necessidade de um advogado para sua interposição, diferentemente do *habeas corpus*, que pode ser impetrado sem esta necessidade. Todas estas limitações fazem com que o *habeas data*, nas palavras de DONEDA, não seja um instrumento “adequado para a tutela da matéria” (DONEDA, 2006, p.337).

3.2 A PRIVACIDADE NO CÓDIGO CIVIL DE 2002

A tutela da privacidade no CÓDIGO CIVIL de 2002 está localizada no capítulo dos direitos da personalidade. O artigo que aborda a questão é o artigo 21 do referido título legal:

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. (BRASIL, 2002)

A tutela, conforme definida pelo código, pode se dar de forma preventiva, evitando a violação; ou de forma repressiva, fazendo cessar a violação que está acontecendo em relação ao direito à privacidade.

Nota-se que o legislador não se limitou a simplesmente tratar do momento patológico da violação ao direito da personalidade, ele vai um passo além ao tratar de tutelar a prevenção quando diante de uma eminência de uma violação. Diante disto, fica claro que o Direito brasileiro não abriga a chamada teoria do consentimento implícito (BORGES, 2005, p.156). Portanto, ao falarmos da tutela da personalidade, a divulgação da vida de uma pessoa depende de uma autorização prévia.

Pela teoria do consentimento implícito, uma pessoa ao frequentar um ambiente público – uma rua, por exemplo – está sujeita ao risco da publicidade, podendo acabar em um filme ou fotografia sem a necessidade de uma autorização prévia. O ordenamento brasileiro não abriga essa teoria, de modo que o fato de estar em um local público não vai significar que a pessoa tenha consentido que a sua imagem venha a se tornar pública. O mesmo se aplica na revelação de informações referentes à pessoa, tais como filiação, profissão, estado civil, etc., sem o prévio consentimento.

Ligado à questão da proteção de dados, temos o enunciado 404 da 5° JORNADA DE DIREITO CIVIL, que vai tratar da questão dos dados:

> 404 - Art. 21: A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas. (AGUIAR JR., 2012, p.69)

O enunciado traz a tutela da privacidade para as questões já levantadas anteriormente, com a preocupação especial aos problemas decorrentes de violações à privacidade dentro do ambiente dos bancos de dados.

Pertinente também para a discussão é a questão da mitigação da personalidade. O entendimento doutrinário é de que os direitos da personalidade são inerentes à pessoa humana, não estando na esfera de disponibilidade das pessoas. Entretanto, a aplicação dos direitos da personalidade, quando existe a anuência de seu titular, podem em alguns pontos sofrer uma flexibilização – lembrando sempre da impossibilidade legal do afastamento completo (MATOSAS; NEDEL, 2012, p.8). Ao navegar na Internet, principalmente ao utilizar as redes sociais, ocorre esta mitigação aos direitos da personalidade quando o titular disponibiliza suas informações pessoais.

3.3 A PROTEÇÃO DE DADOS NO CÓDIGO DE DEFESA DO CONSUMIDOR

Enquanto o Código Civil trata da privacidade em geral, não chegando a tocar detalhadamente na questão dos dados, o Código de Defesa do Consumidor, em seu artigo 43, declara uma série de direitos e garantias referentes às informações presentes em bancos de dados e em outras formas de armazenamento de dados.

Criado com o objetivo de evitar abusos cometidos nas relações de consumo, o Código de Defesa do Consumidor abarcou o problemas decorrentes de abusos no uso de informações pessoais. De modo que o consumidor tenha a possibilidade de acessar, alterar e a cancelar as informações presentes em bancos de dados das entidades abrangidas pelo Código.

Entretanto, o Código de Defesa do Consumidor já nasce com limitações intrínsecas, como esclarece DANILO DONEDA. Por ter um propósito de servir as situações caracterizadas como relações de consumo, seu grau de incidência e sua própria finalidade não conseguem – e nem seria este o objetivo – abarcar a questão do problema da proteção de dados completamente (2006, p. 340). Ainda assim, não podemos deixar de mencionar este título legal por sua importância subsidiária no tema.

3.4 A PROTEÇÃO DE DADOS NO MARCO CIVIL DA INTERNET (LEI N° 12.965/2014)

O projeto do Marco Civil da Internet tem início como uma reação ao Projeto de Lei 84/1999, de autoria do deputado LUIZ PIAUHYLINO (PSDB/PE), que buscava criar uma regulação para a Internet brasileira. O motivo do embate sobre o projeto foi a forma de controle por meio de normas criminais para regular o ambiente virtual. A situação do projeto não melhorou com a entrada do senador EDUARDO AZEREDO (PSDB/MG) como relator, que acrescentou ainda mais ideias polêmicas ao projeto – como, por exemplo, o cadastramento obrigatório dos usuários da Internet perante seu provedor de acesso. De acordo com FRANCISCO CARVALHO DE BRITO CRUZ (2015), deste confronto surgiram as ideias que fundamentariam o projeto de lei do Marco Civil[12].

Planejada para ser uma lei democrática com ampla participação da comunidade, no ano de 2009 ocorre o início do projeto com sua fase de criação dividida em duas etapas. A primeira etapa tratou de receber as sugestões da população e de demais interessados, fornecidas por meio dos mecanismos de mídia do governo, dentre os quais se destaca o blog oficial[13]. A segunda etapa foi marcada pela elaboração da minuta do anteprojeto, feita com base nas informações recolhidas na primeira etapa, e nas discussões e alterações subsequentes.

Após todas as alterações e a alguns hiatos, a lei foi finalmente promulgada em 2014. Criada para ser a chamada Constituição da Internet, a lei foi estruturada em três pilares: neutralidade, privacidade e liberdade de expressão - embora seja um conteúdo interessante, o tópico da neutralidade não será abordado neste trabalho por não fazer parte do escopo da discussão.

O estudo da lei será dividido em quatro etapas, nas quais as três primeiras vão desmembrar a lei em três pontos de discussão, enquanto a última etapa ira discorrer sobre o Decreto n° 8.771/16, responsável por regulamentar alguns pontos específicos do Marco Civil.

---

[12] O projeto de lei do deputado Luiz Piauhylino foi reformulado e se transformou na Lei n° 12.735/2012. Sua promulgação gerou alterações no Código Penal, no Código Penal Militar e na Lei n° 7.716/89, para tipificar condutas realizadas por meio de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares.

[13] Disponível em: http://culturadigital.br/marcocivil/

3.4.1 Marco Civil: privacidade e proteção de dados

Uma das principais preocupações do título legal, a privacidade e a proteção de dados encontraram guarida nos artigos 7° e 8° da lei. Seguindo o entendimento atual da relevância destes direitos, a lei foi expressa em demonstrar a importância da proteção destes direitos por meio destes dois artigos.

No artigo 7° tem-se a relação de proteções referentes à proteção de dados e a indenização pelos danos no caso de descumprimento do preceito. Assim, a lei assegura a inviolabilidade da vida privada (inciso I); garante o sigilo do fluxo de suas comunicações pela internet, com a exceção da quebra do sigilo por ordem judicial (inciso II); mantém o sigilo das comunicações privadas (inciso III), e proíbe o fornecimento a terceiros dos dados pessoais dos usuários - incluindo registros de conexão - e de acesso a aplicações de Internet, salvo os casos de consentimento livre, expresso e informado (inciso VII). A lei também declara que são direitos do usuário ter informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais (inciso VIII); e garante o direito do titular em solicitar a exclusão definitiva de seus dados das aplicações de Internet, quando encerradas as relações com o provedor de serviços (inciso X).

O inciso XIII do artigo 7° demonstra a preocupação fundamental da lei com o usuário e não com o mercado, ao determinar a aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na Internet.

Além disso, há mais uma garantia ao usuário nos incisos do artigo 8°, no que se refere a abusos praticados por parte das empresas de telecomunicação. No parágrafo único do referido dispositivo, fica declarado como nulas as cláusulas contratuais que violem a garantia do direito à privacidade e à liberdade de expressão nas comunicações - ou que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas - pela Internet.

3.4.2 Marco Civil: consentimento e transparência

Definido como o título legal protege a privacidade e a proteção de dados de forma geral, neste segundo ponto entra-se na discussão do consentimento, tema intrinsicamente ligado à privacidade e a proteção de dados.

Conforme discutido no capítulo anterior, faz parte da autodeterminação informativa o direito que cada pessoa possui de expor ou deixar de expor suas informações pessoais no mundo virtual. O Marco Civil deu guarida a este direito ao definir o consentimento livre, expresso e informado, para que possa existir a utilização dos dados pessoais (Art. 7°, IX). A lei não só impõe estas condições, como ainda garante ao usuário o direito de revogar, a qualquer momento, aquilo que foi disponibilizado.

Entende-se, com base nestes dispositivos, que a lei optou pelo modelo *opt-in* ao modelo *opt-out.* O primeiro modelo estabelece que a cessão dos dados pessoais dependa de uma manifestação clara, expressa e inequívoca; enquanto o segundo, não incorporado ao ordenamento brasileiro, pressupõe a concordância em disponibilizar tais informações, necessitando de uma declaração expressa para que isto não ocorra (CELLA e FREITAS, 2016, p.61).

Conforme o que foi explicado no tópico referente ao Código Civil, a privacidade é um direito irrenunciável, mas que pode ser mitigado (art. 11 do Código Civil). Sendo assim, o usuário pode livremente renunciar a certos aspectos do seu direito à privacidade – lembrando que está renúncia deverá ser feita de forma livre e expressa, vedando-se o consentimento presumido.

Sobre o direito à exclusão, antes do Marco Civil era nebuloso o destino dos dados fornecidos a terceiros dentro da Internet. A promulgação da lei veio para sanar este problema ao prever o direito do usuário de solicitar a exclusão de seus dados pessoais (art. 7°, X). Ressalvados os dados que a lei determina a guarda, o provedor deverá realizar a exclusão quando existir o requerimento do usuário.

Finalmente, conforme visto anteriormente, a lei determina como nulas as cláusulas nos termos de uso e privacidade que gerem ofensa ao direito de sigilo das comunicações. Aqui nota-se um diálogo com o Código de Defesa do Consumidor, em que cláusulas contratuais que causem dano ao consumidor são eivadas de nulidade. O mesmo é aplicado aqui nas cláusulas que impliquem dano a privacidade.

3.4.3 Marco Civil: sigilo e inviolabilidade das comunicações

Adentrando na questão do sigilo e da inviolabilidade das comunicações, a primeira garantia está presente ainda no capítulo referente à neutralidade da rede, no §3° do artigo 9°, que impede o bloqueio, o filtro, o monitoramento e a analise dos dados:

> Art. 9º, § 3º. Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo (BRASIL, 2014).

Partindo para o capítulo seguinte da lei, o caput do artigo 10 declara a preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas quanto à disponibilização dos registros de conexão e de acesso a aplicações de Internet.

Os dois primeiros parágrafos do artigo regulam a disponibilização de informações mediante ordem judicial. O primeiro parágrafo define a questão da concessão de informações mediante ordem judicial dos registros mencionados no caput do artigo. Ou seja, a disponibilização dos registros de conexão e de aplicações de Internet, que serão fornecidos de forma autônoma ou associados a dados pessoais, ou a outras informações que possam contribuir para a identificação do usuário ou do terminal. O parágrafo 2° trata das ordens judiciais que versem sobre as comunicações privadas. Em ambos os casos deverá ser respeitado o disposto no artigo 7°.

O parágrafo seguinte (§3°) permite que as autoridades administrativas, que detenham competência legal para realizar a requisição, possam ter acesso aos dados cadastrais que digam respeito à qualificação pessoal, filiação e endereço. Vale destacar que atualmente as autoridades policias e do Ministério Público possuem esta legitimidade para os casos no âmbito de aplicação da Lei das Organizações Criminosas e da Lei dos Crimes de Lavagem de Dinheiro.

Finalmente, o quarto parágrafo faz com que o responsável pela provisão de procedimentos de segurança e sigilo tenha que informar as medidas tomadas para o usuário de forma clara e atendendo a padrões definidos em regulamento.

No artigo 11 temos a questão da aplicação da legislação brasileira nos direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e dos registros. Segundo a definição da lei, as garantias citadas na primeira parte do caput do artigo devem ser obrigatoriamente aplicadas quando pelo menos um dos seguintes atos for realizado em território nacional: coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicação por provedores de conexão e de aplicações de internet. Ou seja, uma empresa transnacional, mesmo que só armazene e trate os dados em nosso país, terá que respeitar a legislação brasileira.

O parágrafo 1° do artigo 11 estende o disposto no caput para os dados coletados no país e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. Em caso de pessoa jurídica sediada no exterior, existindo a oferta de serviço ao público brasileiro, ou que ao menos uma integrante do mesmo grupo possua estabelecimento no país, também se aplica o disposto no caput do referido artigo (parágrafo 2). Novamente, ao ampliar o âmbito de aplicação da legislação pátria, observa-se a preocupação do legislador com o usuário em detrimento do mercado.

Quanto às sanções, o artigo 12° específica quatro tipos de penalidades – sem prejuízo das demais sanções administrativas, civis e criminais - que podem ser aplicadas de forma isolada ou cumulativamente. As sanções são: a) advertência, com indicação de prazo para medidas corretivas; b) multa de até 10% do faturamento anual do grupo econômico no país; c) suspensão temporária das atividades; d) proibição das atividades no país.

A aplicação de sanções não é um ponto pacífico dentro da discussão sobre o Marco Civil. O IDEC (Instituto Brasileiro de Defesa do Consumidor) se manifestou defendendo a liberdade de expressão, o exercício da cidadania em meios digitais e a defesa do consumidor como princípios a serem observados na aplicação das sanções (IDEC, 2015). Por outro lado, o Ministério Público defendeu a aplicação de sanções quando esgotados outros meios menos gravosos, de modo a forçar que a empresas forneçam os dados requeridos (MINISTÉRIO PÚBLICO FEDERAL, 2016).

Outra questão controversa quanto ao Marco Civil da Internet foi o artigo 13, que ordena ao administrador de sistema manter os registros de conexão pelo prazo de um ano. O argumento contrário ao dispositivo foi que manter os dados por este

período de tempo acarretaria um acréscimo no valor do serviço prestado, devido à necessidade de mais *databases* para manter os dados por um período prolongado. A lei ainda determina que a manutenção dos dados não possa ser transferida a terceiros, de modo a inibir o comércio ou o vazamento destes dados.

Quanto ao provedor de aplicações de internet, a lei determina que os registros de acesso e aplicações de internet deverão ser mantidos pelo prazo de 6 meses - mantendo o sigilo e em ambiente controlado e de segurança. Aqui temos um prazo reduzido em relação ao que é definido no artigo 13, que trata do administrador responsável pela provisão de conexão à internet.

Esta obrigatoriedade em manter os dados por um ano (para os administradores responsáveis pela provisão de conexão à internet) ou seis meses (para o provedor de aplicações de internet) também não ficou isenta de críticas. Segundo SÉRGIO AMADEUS DA SILVEIRA, a lei ao obrigar, ao invés de restringir, a guarda de logs de aplicação:

> [...] está ampliando e legalizando esse mercado de observação e análise de nossas vidas que é feito pela redução crescente da privacidade e da intimidade dos cidadãos. Mesmo restringido a obrigatoriedade de guarda das informações às pessoas jurídicas com fins econômicos, ela expandirá o mercado de vigilância. (SILVEIRA, 2014)

Outra fragilidade apresentada pelo autor, ao tratar do artigo 15, diz respeito ao uso comercial dos dados armazenados. O armazenamento destas informações, para o autor, fica fragilizado frente ao interesse das grandes corporações de segmentos políticos autoritários que ocupam o Estado. O temor não é injustificado, haja vista o valor que estas informações possuem e a possibilidade de seu uso ser desvirtuado e utilizado para fins econômicos. O autor também apresenta outra possível violação advinda do artigo 15, no que diz respeito à troca de dados entre empresas especializadas em processamento de dados, segundo SILVEIRA:

> [...] após os seis meses em que os dados devem estar “guardados sob sigilo, em ambiente controlado e de segurança”, poderá ocorrer a troca dos mesmos com empresas especializadas em processar informações de navegação e realizar cruzamentos inaceitáveis, pois comprometem completamente nossa intimidade. Repare que apesar do texto do Artigo 15 enfatizar que a segurança dos dados armazenados é fundamental, ela só seria efetiva para o cidadão se seus dados não pudessem ser reunidos e armazenados. (SILVEIRA, 2014)

Ainda que possua brechas que motivem críticas dos estudiosos do assunto, como as citadas, o Marco Civil ainda é considerado como uma das leis mais

modernas sobre o tema no mundo. O projeto de lei foi intensamente debatido, tendo a presença de setores diversos da sociedade contribuindo para o resultado final.

O objetivo deste tópico foi demonstrar os principais artigos da lei do Marco Civil no que diz respeito à privacidade a proteção de dados. Como demonstrado, embora fruto de uma participação democrática de diversos setores da sociedade, a lei ainda suscita discussões sobre alguns de seus dispositivos. Embora inegavelmente inovadora no ordenamento brasileiro, mais a frente neste estudo serão demonstradas algumas falhas presentes nesta lei quando comparada com o modelo europeu de proteção de dados.

3.4.4 O Decreto nº 8.771/2016

Após o Marco Civil da Internet ter sido promulgado, algumas lacunas começaram a serem notadas nesta lei, restando claro a insuficiência de apenas este título legal para a regulação do tema. Assim veio à luz o Decreto n° 8.771/2016, para responder algumas das questões deixadas em aberto, como, por exemplo, quais seriam as autoridades competentes para fiscalizar as situações apresentadas pelo Marco Civil.

O primeiro artigo de destaque no Decreto é uma definição mais específica do que é “dado pessoal” e “tratamento de dados pessoais”. A voz, as impressões digitais, a letra, entre outras manifestações, podem levar a identificação de uma pessoa. O que torna a mera definição de “dado pessoal” sujeita a interpretações contrárias com o objetivo da lei. O Decreto corrigiu esta deficiência esclarecendo de forma mais clara estes termos, de acordo com o artigo 14:

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
> I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e
> II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2016)

No que se refere à guarda de registros e aplicações de Internet, a regulamentação adotou uma posição um tanto quanto contraditória. No artigo 11,

§1°, o Decreto desobriga o provedor de fornecer os dados cadastrais (nome, endereço, profissão, filiação, etc.), nas situações em que estes dados não foram coletados pelo provedor. O regulamento ainda foi vago ao declarar apenas com o termo “provedor”, ao invés de “provedor de aplicação”. Este dispositivo leva a uma brecha na qual um sujeito poderia contratar um provedor de conexão a Internet sem fornecer qualquer dado pessoal (ou os dados incompletos). Além disso, tal dispositivo vai contra a Constituição Federal[14] e a própria Anatel[15]. (SCALZILLI.FMV ADVOGADOS, 2016).

Por outro lado, o próximo artigo (art. 12) estabelece a elaboração de relatórios por parte da autoridade máxima de cada órgão da administração pública federal. Estes relatórios deverão conter: (i) o número de pedidos realizados; (ii) a listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos; (iii) o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e (iv) o número de usuários afetados por tais solicitações. Aqui nota-se um mecanismo que visa a transparência por parte do Estado e das empresas provedoras de conexão e de acesso à aplicações.

Outro artigo que merece destaque nesta análise do Decreto é o artigo 13, que determina diretrizes de segurança aos provedores de conexão e de aplicação. Deste modo, entre outras medidas, o ato legislativo determina a previsão de mecanismos de autenticação de acesso aos registros (inciso II) e o uso de medidas para a inviolabilidade dos dados (inciso IV). Neste artigo ficam evidentes os conceitos da privacidade adotada na própria arquitetura dos sistemas e processos, a chamada privacidade *by design* (ALVES; VAINZOF, 2016).

Finalmente, a respeito da disponibilidade de informações nos casos de ordens judiciais, o Decreto definiu que:

> Art. 15. Os dados de que trata o art. 11 da Lei nº 12.965, de 2014, deverão ser mantidos em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 13 deste Decreto. (BRASIL, 2016)

A primeira coisa a se notar quanto a este dispositivo é sua incompatibilidade com as criptografias do tipo *end to end,* em que apenas o emissor e o receptor da mensagem possuem a chave para descriptografar as informações. A observância

[14] CF art. 5°, inciso IV
[15] Resolução nº 614 de 2013, artigo 5374; e de telefonia móvel, Resolução nº 477 de 2007, artigo 10º, XXII

deste artigo, portanto, tornaria inviável tais tipos de tecnologia de criptografia, que é usada, entre outros exemplos, pelo aplicativo *WhattsApp*.

O Decreto também determinou quais as entidades responsáveis pela transparência e fiscalização nas situações descritas pelo Marco Civil. Assim, Anatel fica responsável pela fiscalização e apuração de infrações relacionadas a telecomunicações, a Secretaria Nacional do Consumidor atuará na fiscalização e na apuração de infrações relacionadas aos direitos do consumidor, ficando as infrações à ordem econômica a cargo do Sistema Brasileiro de Defesa da Concorrência (CADE).

3.5 O PROJETO DE LEI DE PROTEÇÃO DE DADOS

Também relevante para este trabalho é o Projeto de Lei n° 5276/2016, que visa regular a proteção de dados no Brasil. Por ainda estar em fase de gestação no Congresso, a análise deste projeto será breve, atendo-se apenas em suas propostas mais relevantes.

A primeira diferença substancial no projeto é a lista de termos técnicos e suas definições. Enquanto o Decreto n° 8.771/2016 só define os termos “dado pessoal” e “tratamento de dados pessoais”, o projeto apresenta uma lista com 18 incisos cada um contendo um termo técnico e sua definição.

Ressalta-se também a incorporação de nove princípios norteadores neste projeto de lei: a) princípio da finalidade; b) princípio da adequação; c) princípio da necessidade; d) princípio do livre acesso; e) princípio da qualidade dos dados; f) princípio da transparência; g) princípio da segurança; h) princípio da prevenção; i) princípio da não discriminação.

A incorporação destes princípios é uma clara influência da Diretiva 95/46/CE, que também estabelece um rol de princípios a serem observados pelos países-membros em seu artigo 25.

No que se refere ao consentimento, o projeto estendeu a quantidade de informações que devem ser disponibilizadas ao usuário no momento em que este decide enviar seus dados pessoais. De modo que, no momento em que o titular vai fornecer o seu consentimento, ele deve ser informado de: a) finalidade específica do tratamento; b) forma e duração do tratamento; c) identificação do responsável; d) informações de contato do responsável; e) sujeitos ou categorias de sujeitos para os

quais os dados podem ser comunicados, bem como âmbito de difusão; f) responsabilidade dos agentes que realizarão o tratamento; e g) direitos do titular, com menção explícita a: (i) possibilidade de não fornecer o consentimento, com explicação sobre as consequências da negativa; (ii) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; e (iii) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei.

Outro ponto a ser destacado é quanto aos dados pessoais sensíveis. Enquanto no Marco Civil não há sequer uma referência a este tipo de dados, no projeto de lei há uma seção dedicada a defesa deste tipo de dados (artigos 12 e 13 do projeto).

Ainda assim, o texto do projeto é deficiente ao não definir uma autoridade competente para a proteção de dados, embora faça menção 34 vezes sobre um “órgão competente”, sem nunca defini-lo. (CAMARGO; CRESPO, 2015).

4 A PROTEÇÃO DE DADOS NO CONTINENTE EUROPEU

Uma parte fundamental no processo de formação da União Europeia foi a transformação das leis locais dos países-membros por leis que seguissem um modelo supranacional de ordenamento. Processo que já vem sendo desenvolvido há algumas décadas no continente, sendo o Regulamento 679/2016 o último ato legislativo na busca de uma legislação uniformizada no continente no que toca a proteção de dados.

Neste capítulo será analisada esta trajetória legislativa por parte da União Europeia. Primeiro será estabelecido um breve histórico da proteção de dados no continente por meio das legislações nacionais, convergindo para o início da União Europeia e as primeiras tentativas de uma legislação supranacional. Depois o foco será voltado principalmente para a Diretiva 95/46/CE e a Diretiva 2002/58/CE analisando-se *pari passu* com sua transposição para o ordenamento português. A escolha de Portugal como modelo de referência se deve a dois motivos: a língua, que é a mesma falada pelo Brasil (sem contar a óbvia proximidade entre os países) e por este país ter adotado todas as medidas que correspondem ao cerne destas Diretivas.

Depois de feita a análise destes atos legislativos com sua devida transposição para o modelo português, o estudo passará para o recente Regulamento 679/2016. O ato legislativo será responsável por uniformizar a legislação referente à proteção de dados em todos os países signatários da União Europeia. Com sua entrada em vigor prevista para o início de 2018, neste capítulo será tratada as diferenças introduzidas por este novo ato legislativo no cenário europeu.

Antes, porém, para que não haja confusão a respeito da finalidade de cada ato legislativo existente no bloco europeu, uma breve explicação da função de cada um deles.

4.1 DIRETIVAS, REGULAMENTOS E OUTROS ATOS LEGISLATIVOS

Os atos legislativos na União Europeia se dividem em: regulamentos, diretivas, decisões, recomendações e pareceres. Destes, dois são vinculativos (regulamentos e decisões) e três não o são (diretivas, recomendações e pareceres). O enfoque maior neste trabalho será sobre os regulamentos e as diretivas – que

serão explicados mais a frente. Então, quanto aos outros atos legislativos, parte-se para uma breve análise: a) decisões: são atos legislativos vinculativos apenas para seus destinatários específicos (por exemplo, um país-membro da União Europeia ou uma empresa), sendo-lhes diretamente aplicável; b) recomendações: a finalidade destes atos é dar o conhecimento das instituições sobre algum dos seus pontos de vista, neste caso não existe nenhuma imposição de obrigação legal aos seus destinatários; c) pareceres: outro instrumento que não é vinculativo e também não impõe uma obrigação legal sobre seus destinatários, este ato pode ser emitido pelas principais instituições da União Europeia - na elaboração de legislações estas instituições emitem esses atos para demonstrar sua opinião sobre um determinado assunto[16].

A Diretiva, nas palavras de DANILO DONEDA, tem como função básica a uniformização legislativa, de forma que, após um certo período de tempo, o país-membro tenha seu ordenamento local adaptado ao preceito definido por este instrumento normativo. O processo, que vai da Diretiva até a incorporação ao ordenamento local, é chamado de transposição. A eficácia da Diretiva está ligada ao tempo em que o país-membro a adota, podendo este ficar sujeito a responder pela mora perante a Corte Europeia de Justiça (2006, p. 224).

Por outro lado, o Regulamento é um ato legislativo vinculativo, sendo aplicado em todos os seus elementos de forma simultânea em todos os países da União Europeia. Não existindo, neste caso, a transposição, como ocorre na Diretiva. A aplicação do Regulamento não depende da vontade do país-membro em adotar a medida. Depois de promulgado e estando em vigor, este ato legislativo se torna a norma a ser seguida pelos países que fazem parte da União Europeia.

4.2 O INÍCIO DA PROTEÇÃO DE DADOS NO CONTINENTE EUROPEU

O início da proteção de dados pode ser estabelecido com a Lei de proteção de dados do *Land* de Hesse na República Federal da Alemanha, no ano de 1970. Esta primeira lei tinha um conteúdo bastante curto, apenas 17 artigos, e, segundo DANILO DONEDA, “concentrava-se em disciplinar a atividade de centros de processamento de dados geridos pelo poder público, além de instituições e sujeitos

[16] Disponível em: https://europa.eu/european-union/eu-law/legal-acts_pt

submetidos à autoridade do *Land*" (DONEDA, 2006, p.228). O exemplo da lei foi seguido por outros *Länder* alemães, surgindo em 1977 uma lei federal sobre o tema.

Na Suécia surge a primeira lei nacional (lembrando que a lei alemã de 1973 era para um *Land*) tratando da proteção de dados pessoais, de 1973, cujo enfoque era voltado para o controle de banco de dados. Em 1978 a França adota a Lei 78-17, denominada *Informatique et Libertés*, também tratando do tema. Outras iniciativas nacionais ocorreram na sequência, como nos casos da Dinamarca, Luxemburgo e Áustria.

Também em 1973 é publicada uma resolução sobre a proteção de dados pela Assembleia Consultiva do Conselho Europeu. O motivo de tal ato foi a relação do artigo 8° da Convenção Europeia para a salvaguarda dos Direitos do Homem e das Liberdades Fundamentais com a questão da coleta de dados. O objetivo da resolução era fazer com que os países adotassem os princípios mínimos na proteção dos dados.

Como resultado a estas iniciativas de leis, ficou evidente a necessidade de um enfoque internacional ao tratar o tema da proteção de dados. A salvaguarda da proteção destes dados não poderia ser garantida apenas pela legislação local, haja vista a facilidade com que essas informações poderiam ser armazenadas ou tratadas em outros locais fora do domínio local. Havia a necessidade de uma lei supranacional para uma real proteção desses dados.

Nesse primeiro momento, a preocupação principal não era com a tutela da pessoa em si, mas sim com a questão do tráfego de dados. A OCDE (Organização para a Cooperação e Desenvolvimento Econômico), notando este problema enfrentado pelos países que implementaram uma legislação de proteção de dados, criou um grupo de especialistas na questão do tráfico de dados entre fronteiras. O resultado dos esforços destes especialistas foram as chamadas *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, de 1980.

Pelo fato de não terem efeito vinculante aos países membros da OCDE, estas *Guidelines* acabaram por não surtirem um efeito tão expressivo. Estes documentos acabaram se tornando apenas um modelo de referência, haja vista, conforme mencionado, o fato dos países signatários não serem obrigados a adotarem o seu conteúdo. Além da falta de obrigatoriedade, outro fator que fez com que as *Guidelines* não obtivessem grande efetividade foi que logo em seguida, em 1981,

ocorreu a chamada Convenção de Strasbourg, também conhecida como Convenção 108.

Considerada como o ponto de referência inicial do modelo europeu de proteção de dados, a Convenção de Strasbourg foi uma iniciativa do Conselho da Europa para regular o tema da proteção de dados. Criada com o objetivo de incitar os países-membros a adotarem suas medidas, a Convenção para a Proteção de Indivíduos com Respeito ao Processamento de Dados Pessoais avançou em um ponto fundamental que não havia sido estabelecido ainda no continente: a inserção da proteção de dados na esfera dos direitos humanos.

Depois da Convenção, vários países adotaram as medidas estabelecidas em seus próprios ordenamentos internos – destes vale ressaltar o Reino Unido, que reconheceu a proteção da pessoa contra a intromissão não autorizada de sua vida privada, ao invés de um direito à privacidade propriamente falando. O próximo passo na proteção de dados, que iria criar alguma forma de padronização efetiva a proteção de dados, foi a Diretiva 95/56/CE, de 1995.

4.3 A TRANSPOSIÇÃO DA DIRETIVA 95/46/CE

No ano de sua promulgação, 1995, o continente europeu já contava com vários países cujo ordenamento já possuía, em alguma medida, alguns dos mecanismos propostos pela Convenção de Strasbourg. Portugal não era uma exceção, já contando com uma lei específica sobre o assunto, a Lei 10/91, de 29 de abril[17].

A mudança fundamental da Diretiva foi que, com o novo ato legislativo, havia agora um documento propondo um modelo a ser transposto para o direito interno dos países-membros, de forma a buscar uma uniformidade legislativa no continente e fomentar relações mais próximas entre os Estados-membros. Tal ato legislativo representa um passo lógico no avanço de um conglomerado como a União Europeia. O avanço tecnológico, que já era sentido com intensidade na década de 90, necessitava de certa uniformidade nas legislações locais.

A lei portuguesa que realizou a transposição da Diretiva 95/46/CE foi a Lei 67/98, de 26 de outubro (revogando, portanto, a Lei 10/91, de 29 de abril). Dividida

[17] Disponível em: http://portalcodgdh.min-saude.pt/index.php/Lei_n.%C2%BA_10/91_de_29_de_Abril

em sete capítulos, o âmbito de sua aplicação ficou determinado pelo artigo 4°, que delimita sua aplicação ao tratamento de dados efetuados em território português e também fora do país quando, por força do direito internacional, seja aplicada a legislação portuguesa. A lei também coloca em seu âmbito de aplicação os tratamentos de dados realizados por responsável que, não estando estabelecido em território da União Europeia, realize tratamentos de dados pessoais dentro do território de Portugal.

Ao que se refere a uma autoridade de controle para fiscalização, determinada pelo artigo 28 da Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995), o país já contava com uma autoridade administrativa independente responsável pela proteção de dados antes da existência do ato legislativo. Surgida em 1991, com fulcro no n° 2, artigo 35°, da Constituição da República Portuguesa (CRP), a Comissão Nacional de Proteção de Dados Pessoais Informatizados já estava instituída em Portugal desde 1994 – a partir de 1998 esta entidade administrativa passou a ser conhecida como Comissão Nacional de Proteção de Dados Pessoais. Com poderes de investigação e de inquérito, a CNPD tem o poder de ordenar o bloqueio, apagar ou destruir os dados, assim como proibir, de forma temporária ou definitiva, o tratamento de dados pessoais situados em território português. Segundo a página oficial da CNPD:

> É uma entidade administrativa independente, com poderes de autoridade, que funciona junto a Assembleia da República, tendo como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na CRP e na lei.[18]

Além das competências mencionadas, a CNPD ainda possui, entre outras, a seguintes competências: a) *consultiva*, ao emitir pareceres obrigatórios em relação a disposições legais de direito comunitário ou internacional (artigo 23°, n° 1); b) *decisória*, que se traduz na autorização prévia do tratamento de dados sensíveis (artigo 7°), entre outros tipos de dados especificados pela lei; c) *regulamentar*, ao poder simplificar ou isentar de notificação e ao emitir diretivas sobre alguns assuntos.

Uma das preocupações da Diretiva foi corrigir as deficiências de definição que existiam na Convenção e nas *Guidelines*. Quando estes documentos especificavam termos genéricos - como, por exemplo, não definir o que abrangeria exatamente no

[18] Disponível em: https://www.cnpd.pt/bin/cnpd/acnpd.htm

conceito de dado pessoal ou processamento de dados – abria-se um leque de interpretações possíveis para o país signatário adotar em seu ordenamento. Esta preocupação da Diretiva já fica clara logo no seu artigo 2°, em que uma lista de termos é exposta, ficando mais exato o que é abrangido pelo conceito. Assim, dados pessoais, por exemplo, recebe a definição de "qualquer informação relativa a uma pessoa singular identificada ou identificável", podendo, portanto, ser uma fotografia, registros de som, etc. A mesma preocupação em definir um rol de termos se fez presente na lei portuguesa. Também no artigo 2°, a Lei 67/98 traz a definição de nove termos que dizem respeito à proteção de dados.

Sobre os direitos fundamentais, logo no primeiro dos 34 artigos da Diretiva fica claro o objetivo do documento em assegurar "a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada", no que toca ao tratamento de dados pessoais. Nas considerações da Diretiva também fica expressada esta preocupação acrescentando-se mais elementos de proteção. Segundo o texto do documento (a segunda consideração), o respeito às liberdades e aos direitos fundamentais, nos sistemas de tratamento de dados, devem ser independentemente de "[...] nacionalidade ou da sua residência ou da sua residência, especialmente a vida privada" (UNIÃO EUROPEIA, 1995).

É importante ressaltar que o conceito de "vida privada" não deve ser interpretado de forma restritiva. O entendimento do ato legislativo é de que este conceito não deve excluir outros tipos relações como as de natureza profissional ou comercial, conforme o que dispõe a Diretiva sobre o tratamento de dados no domínio da legislação do trabalho (alínea (b), número 2°, artigo 8°), ou quando trata do marketing direto (alínea (b) do artigo 14°) [19].

No ordenamento português, em consonância com a Diretiva 95/46/CE, a Lei 67/98 prevê o conceito de dados pessoais no artigo 3°, alínea (a):

> a) «Dados pessoais»: qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social; (PORTUGAL, 1998)

[19] O conceito também está presente na tutela da proteção de dados nas condenações penais, sanções administrativas e decisões cíveis, conforme o n.º 5 do artigo 8.º.

Tanto a Diretiva quanto a lei portuguesa seguem o entendimento de que a qualificação de “dado pessoal” deve se guiar pelo princípio do reconhecimento. Este entendimento é manifestado nas considerações[20] da Diretiva 95/46/CE:

> os princípios da proteção devem aplicar-se a qualquer identificação relativa a uma pessoa identificada ou identificável; importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento seja por outra pessoa; que os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser considerada identificável (UNIÃO EUROPEIA, 1995)

No que toca ao tratamento de dados, mais especificamente quanto ao consentimento, a Diretiva determina a manifestação expressa, livre, específica e informada do titular para que seus dados possam ser objetos de tratamento. De acordo com o artigo 7° do documento, o consentimento é como um “fundamento geral de licitude e como um fundamento específico em certos contextos (artigo 8.º, n.º 2, alínea (a), e artigo 26.º, n.º 1, alínea (a)).”[21] (UNIÃO EUROPEIA, 2011)

O artigo 7° da Diretiva refere o consentimento como um dos seis fundamentos diferentes que dão legitimidade ao tratamento de dados[22]. A possibilidade do consentimento, nos casos de dados sensíveis, está presente no artigo 8°, em que o tratamento destes dados fica permitido mediante a obtenção por um grau mais elevado de autorização.

Entretanto, o consentimento não é suficiente para legitimar certos atos praticados no tratamento de dados. Desta forma, o Parecer 15/2011 do Grupo de Trabalho determina que:

> A obtenção de consentimento não exonera o responsável pelo tratamento das obrigações estabelecidas no artigo 6.º relativas à lealdade, necessidade e proporcionalidade, assim como a qualidade dos dados. (UNIÃO EUROPEIA, 2011)

---

[20] Consideração n° 26

[21] Grupo de Trabalho do artigo 29.º

[22] Os outros fundamentos estão previstos na sequência do dispositivo. São eles: b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou d) O tratamento for necessário para a proteção de interesses vitais da pessoa em causa; ou e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.

Em Portugal, ainda no que toca ao consentimento e ao tratamento de dados, a CRP garante ao titular o direito de ser informado da finalidade do uso de seus dados, devendo-se observar os princípios da Proporcionalidade e da Finalidade (n° 1°, art. 35). Vale destacar que cada finalidade receberá um tratamento distinto, que deverá ser comunicado a Comissão Nacional de Proteção de Dados, assim como as possíveis alterações que possam ocorrer. O não cumprimento do dever de comunicação leva as sanções previstas no art.º 43.º, n.º 1, alínea (a), da Lei de Proteção de Dados.

Aqui se percebe uma preocupação com a questão da interconexão de dados. Vamos supor uma determinada ferramenta na Internet que possua duas atividades distintas, o titular, ao consentir em fornecer os seus dados em cada uma das atividades, não está consentindo que estes dados sejam cruzados ou interconectados. O consentimento de fornecer os dados com finalidades distintas para o mesmo responsável - ou para dois responsáveis diferentes - não permite a interconexão dos dados, salvo quando autorizado pela CNPD[23].

Os dados sensíveis, no ordenamento português, são protegidos pelo artigo 35.º, n° 3, bem como pelo artigo 7.º da Lei n.º 67/98. O entendimento inicial destes dispositivos era de que estas informações não poderiam receber tratamento de dados. Entretanto, uma Revisão Constitucional mudou o entendimento em 1997, passando a admitir que a lei possa autorizar o tratamento destes dados, desde que cumprida as garantias de não discriminação. A mudança também permitiu o tratamento dos dados sensíveis por meio do consentimento expresso do titular.

A autodeterminação informativa está presente na Diretiva 95/46/CE em seu artigo 14, que consagra o direito do titular de opor, de modo geral, ao tratamento dos seus dados pessoais. A transposição para a lei portuguesa deste preceito está localizada no artigo 13°, n. 1°, da Lei n° 67/98:

> 1 - Qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento. (PORTUGAL, 1998)

[23] N° 2, artigo 9° da Lei de Proteção de Dados e n° 2, artigo 35 da Constituição da República Portuguesa.

Sobre a distinção entre as esferas pública e privada na Diretiva 95/46/CE, o documento não cria distinção. O que existe é uma exceção a esta regra quando o país, caso haja a real necessidade, solicitar que alguma categoria de dados pessoais seja subtraída. Neste caso deverá existir um comunicado, por parte do país, ao Conselho da Europa antes da remoção. Portugal também incorporou a indistinção entre público e privado, determinando ainda que "as entidades públicas e privadas devem prestar a sua colaboração à CNPD", de modo a fornecer "todas as informações que por esta, no exercício das suas competências, lhe forem solicitadas".[24] (PORTUGAL, 1998).

Além de proteger as pessoas na questão de como os seus dados pessoais serão tratados, a Diretiva 95/46/CE também se preocupou com a questão comercial, o que demonstra, segundo DANILO DONEDA, uma dupla faceta do documento (2006, p.236). Este viés mercantil já fica presente na segunda consideração da Diretiva, que determina aos sistemas de tratamento de dados o dever de "contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos". (UNIÃO EUROPEIA, 1995)

A consideração seguinte é ainda mais clara. Segundo o disposto, fica expressamente declarada a necessidade de que os dados pessoais possam transitar livremente de um Estado-membro para outro, para que ocorra a "livre circulação das mercadorias, das pessoas, dos serviços e dos capitais", desde que respeitados os direitos fundamentais das pessoas. (UNIÃO EUROPEIA, 1995)

A Diretiva deixa claro que esta inclusão de um viés comercial deve estar equilíbrio com a proteção da pessoa. E o critério deste equilíbrio é a referência ao homem e aos seus direitos fundamentais, definidos no documento como base e fundamento da disciplina.

O último ponto de destaque na transposição da Diretiva 95/46/CE é no que toca à transferência de dados entre países-membros da União Europeia e para países terceiros.

A transferência de dados entre Estados-membros se deu por meio do artigo 18 da Lei n° 67/98, que ratificou a posição da Diretiva. Pelo artigo da lei, a circulação de dados deve ser livre entre os países signatários da União Europeia. Este posicionamento seguiu a Convenção 108 (Convenção de Strasbourg), artigo 12.º n.º

[24] Artigo 24°, n° 1

2, cujo texto legal impede restrições a livre circulação de dados entre os países-membros.

Na comunicação de dados para países que não fazem parte da União Europeia, o ponto determinante é o nível de proteção oferecido pelo país destinatário. Para que haja a comunicação, o nível de proteção do país destino deverá ser analisado em função da natureza dos dados, a duração e a finalidade, as regras de direito gerais e setoriais, entre outras proteções. Quando não cumprido estes requisitos, a transferência poderá ser permitida pela CNPD na situação em que o titular dos dados tiver dado de forma inequívoca o seu consentimento para o efeito, ou se a transferência for necessária para as finalidades indicadas nas diferentes alíneas do n.º 1, do artigo 20.

Este também é o entendimento da legislação portuguesa, cujo artigo 19° da lei n° 67/98 elenca uma relação de aspectos a serem observados pelo país terceiro para que haja a comunicação dos dados.

4.4 A TRANSPOSIÇÃO DA DIRETIVA 2002/58/CE

Depois da Diretiva 95/46/CE, que trata da proteção de dados para pessoas singulares, a segunda Diretiva de relevância para este estudo é a referente ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas, a Diretiva 2002/58/CE.

Transposta para o ordenamento português por meio da Lei n° 41/2004, esta lei sofreu algumas alterações posteriores devido a Diretiva 2009/136/CE[25], que alterava alguns aspectos da Diretiva 2002/58/CE, e pela Lei n° 46/2012 (a lei que realizou a transposição da Diretiva 2009/136/CE).

A Lei n° 41/2004 acrescenta uma segunda entidade, a ANACOM (Autoridade Nacional de Comunicações), responsável por cuidar das questões relacionadas com a supervisão, controle do funcionamento e garantia da segurança no tratamento de dados pessoais, no âmbito das comunicações eletrônicas. A responsabilidade fica, então, compartilhada entre a CNPD e a ANACOM nas situações relacionadas à privacidade nas comunicações eletrônicas.

[25] Relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrônicas.

O primeiro ponto que precisa ser destacado da Diretiva 2002/58/CE é sua definição sobre “dados de tráfego”, definido no artigo 2°, alínea (b), como “quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrônicas ou para efeitos da faturação da mesma” (UNIÃO EUROPEIA, 2002). Além deste termo, conforme a praxe deste tipo de documento, o artigo 2° apresenta uma lista com vários outros termos abordados pelo documento.

Dados de tráfego são as informações geradas de forma automática durante a transmissão, tais como o endereço de IP, número de telefone, terminal utilizado, rede utilizada, entre outros tipos de dados. Na mesma comunicação, além dos dados de tráfego, são gerados os dados de base e os dados de conteúdo, não existindo distinção doutrinal, até o momento, entre eles[26].

Por meio dos dados de tráfego, portanto, existe a possibilidade de identificar a data, o tempo, e a frequência das ligações efetuadas. Logo, estas informações devem fazer parte da proteção ao sigilo das comunicações, haja vista que a garantia do sigilo não abrange apenas o conteúdo da comunicação.

Sendo assim, as empresas que fornecem serviços de comunicação eletrônica devem garantir a proteção destas informações, de modo que não se tornem acessíveis a terceiros. A disponibilização destes dados pode levar ao conhecimento de comportamentos do indivíduo, assim como seus contatos sociais, informações que devem respeitar o desejo do titular para serem divulgadas, de acordo com os preceitos da autodeterminação informativa.

No tocante a este direito, a Diretiva determina que estes dados de tráfego devem ser eliminados ou tornados anônimos no momento em que não existir mais a necessidade para a transmissão da comunicação, de acordo com os princípios da proporcionalidade e da conservação de dados (artigo 6°, n° 1)[27].A Lei n° 41/2004 transpôs esta determinação em seu artigo 6°, n° 4.

Uma alteração referente a este dispositivo surgiu com a Lei n° 46/2012, ao determinar o consentimento livre e expresso como requisito para o tratamento

[26] Em outra abordagem, a autora portuguesa Cristina Santos estabelece a seguinte diferenciação: a) dados de base, são “dados instrumentais da comunicação, tais como o posto e o número de acesso, a identificação do utilizador ou da sua morada ou, dizendo de outro modo os dados que permitem a ligação à rede”; b) dados de conteúdo, referem-se “a mensagem em si considerada”; c) dados de tráfego, “são aqueles que permitem a identificação da comunicação e intensidade/frequência da comunicação, ou por outra forma, os dados funcionais necessários ao estabelecimento de uma comunicação e os dados gerados pela utilização da rede de telecomunicações”. (SANTOS, 2014)

[27] A mesma determinação está presente no artigo 6.º, n.º 1 da Diretiva 95/46/CE, e artigo 5.º, al. (e), da Lei n.º 67/98.

destes dados “na medida do necessário e pelo tempo necessário à comercialização de serviços de comunicações eletrônicas ou à prestação de serviços de valor acrescentado”[28]. Segundo a Recomendação 3/99 de 7 de setembro de 1999 relativa à conservação dos dados referentes ao tráfego:

> Essa medida deve-se a sensibilidade dos dados de tráfego, que revelam perfis de comunicações individuais, incluindo fontes de informação e lugares geográficos do utilizador dos telefones, fixos ou móveis, e os riscos potenciais em termos de privacidade resultante da recolha, divulgação ou utilizações suplementares dos dados em questão. (UNIÃO EUROPEIA, 1999)

O avanço da tecnologia, por meio de equipamentos portáteis de geolocalização, permitiu acompanhar os passos de uma determinada pessoa por tempo integral. Assim, por meio de um aparelho celular ajustado para isto, é possível descobrir a localização de uma determinada pessoa a qualquer hora do dia. Existindo tal tecnologia, existe também a possibilidade de invasão de privacidade por meio do controle destes dados.

Destarte, tendo em vista os riscos à privacidade advindos da obtenção destes dados por alguém não autorizado, a Lei n° 41/2004 dedicou o artigo 7° para os dados de localização, aplicando o seu disposto aos casos “em que sejam processados dados de localização, para além dos dados de tráfego”. (PORTUGAL, 2004)

Assim, a lei determina que estes dados de localização dos assinantes ou usuários, tornem-se anônimos durante o seu tratamento, salvo o consentimento contrário dos titulares[29]. Ainda que exista este consentimento, o tratamento deve ocorrer na medida do necessário e pelo tempo necessário a prestação de um serviço de valor acrescentado. O titular dos dados de localização ainda pode suspender temporariamente o tratamento destes dados[30] - lembrando que este tipo de tratamento é permitido apenas à medida e pelo tempo necessário para a prestação dos serviços de valor acrescentado.

[28] Artigo 2°, número 4°. Disponível em: https://www.anacom.pt/render.jsp?contentId=1136073
[29] art.º 9.º da Diretiva 2002/58/CE e o art.º 7.º, n.º 1 da Lei n.º 41/2004
[30] Art 7°, número 5°, alíneas (a) e (b), Lei n° 41/2004

4.5 O REGULAMENTO 2016/679

Após mais de 20 anos de sua promulgação, a União Europeia decidiu pela promulgação de um novo ato legislativo para substituir a Diretiva 95/46/CE. No ano de 2016 surge o Regulamento 2016/679[31] do Parlamento Europeu e do Conselho, revogando a Diretiva 95/46/CE e estabelecendo um novo ordenamento para a matéria de proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais.

A rápida evolução tecnológica sentida nos últimos anos exige um novo quadro legislativo na proteção de dados pessoais. Enquanto a Diretiva 95/46/CE tinha a preocupação de estabelecer um mercado único europeu, a preocupação do Regulamento 2016/679 é com a livre circulação de dados pessoais pelo continente.

O artigo 8° da Carta dos Direitos Fundamentais da Europa determina o mesmo nível de proteção de dados em toda a União Europeia[32]. Com a Diretiva 95/46/CE a transposição dos preceitos do documento para a legislação local acabava gerando incompatibilidades entre os países-membros da União Europeia. Destarte, com a promulgação de um ato legislativo vinculativo para todos os países membros, estes defeitos de incompatibilidade seriam resolvidos por uma regra harmônica ao bloco.

Entrando na análise do ato legislativo em si, o consentimento continua uma das bases que estruturam a proteção de dados, de forma que o consentimento deva ser traduzido em uma: manifestação de vontade, livre, específica, informada e explícita, pela qual a pessoa em causa aceita, mediante uma declaração ou um ato positivo inequívoco (artigo 8°).

Este consentimento é condição para a licitude do tratamento, conforme o artigo 6°, número 1, alínea (a). O titular ainda tem o direito de revogar o seu consentimento de forma gratuita e facilitada em qualquer momento que desejar (artigo 7°, n° 3°). Quanto ao ônus da prova, cabe ao responsável demonstrar que o titular dos dados deu seu consentimento (artigo 7°, n° 1).

O Regulamento manteve os princípios presentes na Diretiva 95/46/CE, artigo 6°, e acrescentou em seu artigo 5°, alínea (f), o princípio de que os dados sejam:

---

[31] O Regulamento 2016/679 tem previsão de entrada em vigor em Maio de 2018.
[32] Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf

> f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (“integridade e confidencialidade”). (UNIÃO EUROPEIA, 2016)

Uma preocupação inovadora do ato legislativo foi com a tutela da proteção de dados nos casos das crianças. Segundo o artigo 8°, estando em causa uma oferta direta de serviços a menores, o tratamento dos respectivos dados pessoais só será lícito nos casos em que o titular tenha mais de 16 anos de idade. Nos casos em que o menor tem menos de 16 anos de idade, o tratamento dos dados só será permitido quando os pais ou responsáveis do titular dos dados tenham consentido.

Obedecendo ao princípio da não discriminação, o novo Regulamento veda o tratamento de certos tipos de dados, os denominados dados sensíveis (artigo 9°, n°1) – a regra é a vedação, entretanto o ato legislativo permite o tratamento destes dados caso respeitados os dispostos no n° 2, artigo 9°. O novo ato legislativo ampliou o rol de dos dados sensíveis previstos pela Diretiva 95/46/CE, acrescentando os “dados biométricos para identificar uma pessoa de forma inequívoca”. Além desta nova categoria de dado, continua sendo considerado dado sensível para o Regulamento: origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

O responsável pelo tratamento de dados também tem suas obrigações ampliadas em relação ao titular. Passa a ser obrigação do responsável disponibilizar para o titular as informações, entre outras, referentes à finalidade do tratamento, as categorias dos dados em questão, os destinatários ou categorias de destinatários, a identidade e os contato do responsável pelo tratamento (artigo 13°, número 1).

Se os dados forem recolhidos sem o titular estar presente no ato do recolhimento, a norma determina que o responsável deva disponibilizar todas as informações que seriam fornecidas no caso em que o titular do dado está presente. O titular ainda deve ser informado da origem destes dados pessoais (artigo 14°, n° 2, alínea (f)).

Outra novidade introduzida no ato legislativo foi o direito ao esquecimento (ou “direito a ser esquecido”) presente no artigo 17°. De acordo com o dispositivo, os dados do titular serão eliminados quando: a) os dados pessoais deixarem de ser

necessários para a finalidade que motivou o seu tratamento; b) O titular retire o consentimento em que se baseia o tratamento dos dados satisfeitos determinados pressupostos; c) O titular opõe-se ao tratamento e não existem interesses legítimos prevalecentes que justifiquem o tratamento; d) Os dados pessoais foram tratados ilicitamente.

No entendimento de NELSON ROSENVALD, este direito é uma manifestação do direito fundamental ao "tratamento dos dados pessoais como derivação do princípio da dignidade da pessoa humana em sua dupla eficácia: negativa e positiva". A dupla faceta, para o autor, é manifestada da seguinte forma:

> A dimensão negativa é tutelada com a materialização do direito à proteção em face da sociedade e órgãos estatais quanto à publicidade de dados que desconsiderem o ser humano, desrespeitando a sua honra, imagem ou vida privada. Por outro lado, a eficácia positiva da dignidade é vivificada no direito à promoção da autonomia existencial da pessoa, no sentido de que ela possa realizar o seu pleno desenvolvimento sem os entraves de dados que estejam descontextualizados ou representem situações que não mais correspondam à realidade. (ROSENVALD, 2017)

Este direito não é absoluto, a norma determina algumas situações em que este direito não poderá ser exercido. Alguns exemplos de situações são por motivos de interesse público no domínio da saúde pública e nos casos de exercício da liberdade de expressão e de informação (artigo 17°, n° 3).

O Regulamento 2016/679 inovou também ao incluir o direito à portabilidade dos dados pelo titular. Agora o titular tem o direito de solicitar ao responsável pelo tratamento uma cópia de seus dados em um formato eletrônico e estruturado que permita a sua utilização posterior (artigo 20°, n° 1). A função deste dispositivo é permitir ao titular, com a posse de seus dados pessoais, transferir estas informações para outro sistema, se assim lhe convier, de modo que o responsável não possa lhe fazer objeção. Neste mundo em que predomina o livre-mercado, em que tudo adquire um valor monetário, tal medida é, no entendimento de MARIA LEONOR DA SILVA TEIXEIRA, consequência da valorização dos dados pessoais, sendo que:

> [...] o direito de portabilidade como está configurado, apenas assegura o exercício do direito de autodeterminação informativa do titular dos dados, permitindo-lhe a utilização posterior, mas não cuida de proteger o responsável pelo tratamento dos dados de potenciais abusos na utilização de dados que recolheu, tratou e organizou. (TEIXEIRA, 2013)

Destaca-se também o previsto no artigo 21°, que permite ao titular do dado de se opor ao tratamento de seus dados por motivos relacionados às situações

descritas no artigo. Entretanto, mais a frente no mesmo artigo fica determinado que por razões imperiosas e legítimas o responsável pode se opor a esta solicitação do titular. Não fica definido no Regulamento 2016/679 o que seriam exatamente estas razões “imperiosas e legítimas”, o que leva a crer que este artigo será objeto de discussões no futuro (TEIXEIRA, 2013, p.99).

Quanto às restrições, o Regulamento estipula que elas são permitidas desde que respeitada a “essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática” (artigo 23°, n° 1). Podendo ser aplicadas nas situações que em que envolva, entre outros exemplos: a segurança do Estado; a defesa; a segurança pública; a prevenção, investigação, detecção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (artigo 23°, n° 1, alíneas (a), (b), (c) e (d)).

No que diz respeito à segurança, O Regulamento 2016/679 determina o dever de aplicar técnicas avançadas de proteção de dados no “momento de definição dos meios de tratamento como no momento do próprio tratamento” (artigo 25°, n° 1). Nota-se aqui, novamente, uma definição da chamada “privacy by design”, discutida anteriormente. O artigo 5° ainda fala da necessidade do tratamento ser realizado seguindo-se os princípios relacionados com a proteção de dados, em que se destaca o da finalidade e o de manter os dados em registro apenas pelo tempo necessário.

Dentre as inovações do ato legislativo, merece destaque também as denominadas avaliações de impacto sobre a proteção de dados e a autorização prévia. Com o Regulamento 2016/679 em vigor, sempre que existir, no tratamento de dados, a possibilidade de situações suscetíveis de “um elevado risco para os direitos e liberdades das pessoas singulares”, o responsável deverá realizar antes do tratamento uma avaliação do impacto da operação sobre aqueles dados (artigo 35°, n° 1). O número 3° do mesmo artigo estabelece algumas situações em que a avaliação de impacto deve ser feita de forma obrigatória, entre elas, os casos de “operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n° 1” (artigo 35, n°3, alínea (b)), e também os casos de “controle sistemático de zonas acessíveis ao público em grande escala” (artigo 35°, n° 3, alínea (c)).

Após a realização desta avaliação de impacto, nas situações em que fique demonstrado o risco aos dados, o responsável informa ao encarregado pela proteção de dados (artigo 36°, n° 1) para que seja realizada a consulta prévia. Destarte, a autorização prévia é a regra para as situações relacionadas no artigo 35°, n°1, em que a avaliação de impacto demonstre que o tratamento envolve elevado risco à proteção de dados.

Outra mudança do Regulamento 2016/679 foi na questão do seu âmbito de aplicação territorial, agora ampliado para abranger as empresas não instaladas na União Europeia. De acordo com o projeto de lei que levou ao Regulamento[33]:

> [...] sempre que os dados pessoais atravessam fronteiras, há um risco acrescido de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se proteger da utilização ilícita ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar seguimento as queixas ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiriço podem ser também restringidos por poderes preventivos ou de medidas de reparação insuficientes, regimes jurídicos incoerentes e obstáculos práticos, tais como a limitação de recursos. Por conseguinte, revela-se necessário promover uma cooperação mais estreita entre as autoridades de controle da proteção de dados, a fim de que possam efetuar o intercâmbio de informações e realizar investigações com as suas homólogas internacionais. (UNIÃO EUROPEIA, 2012).

Esta consideração da proposta resultou no artigo 47° do Regulamento, que trata das regras vinculativas aplicáveis as empresas.

Ainda sobre a transferência de dados para países que não são signatários do bloco europeu, continua a ser aplicado preceito de que o país destino deve possuir um nível de proteção de dados considerado apropriado pela União Europeia (artigo 45°). Dentre os elementos avaliados para que possa ocorrer a transferência de dados destaca-se “a existência e o efetivo funcionamento de uma ou mais autoridades de controle independentes no país terceiro ou às quais esteja sujeita uma organização internacional” (artigo 45°, n° 2, alínea (b)) e que o país terceiro tenha assumido compromissos internacionais sobre o tema (artigo 45°, n° 2, alínea (c)).

Não existindo qualquer decisão por parte da Comissão a respeito do país terceiro, o responsável ainda pode realizar a transferência de dados desde que

[33] Considerando 91.

apresente garantias adequadas quanto à proteção de dados, conforme o que é disposto no artigo 46° do Regulamento 2016/679.

O último ponto destacado diz respeito às sanções no novo ato legislativo. A partir da entrada em vigor da norma, prevê-se a possibilidade de as multas chegarem até 20.000.000 de Euros ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial (artigo 83°, n° 5).

5 UM ENSAIO DE COMPARAÇÃO ENTRE A LEGISLAÇÃO BRASILEIRA E A LEGISLAÇÃO EUROPEIA

Neste capítulo do trabalho será feito um comparativo entre a legislação brasileira com a legislação europeia referente ao tema da proteção de dados. O objetivo do capítulo é mostrar as diferenças e semelhanças existentes entre as leis pátrias com o ordenamento europeu. Para cumprir o intento, o capítulo se focará na Diretiva 95/46/CE e na Diretiva 2002/58/CE, assim como as leis de transposição destes atos legislativos para o ordenamento português. As inovações advindas do Regulamento 2016/679, que entrará em vigor no mês de Maio de 2018, também farão parte desta análise.

5.1 SEMELHANÇAS ENTRE O MODELO LEGISLATIVO BRASILEIRO E O MODELO LEGISLATIVO EUROPEU

A primeira semelhança que encontramos ao comparar o modelo brasileiro com o modelo europeu é na importância do consentimento nestes sistemas legislativos. O consentimento é pedra angular tanto no ordenamento brasileiro quanto na Diretiva 95/46/CE (consequentemente na lei portuguesa que realiza a transposição da Diretiva) e no novo Regulamento 2016/679.

No Marco Civil da Internet o consentimento está localizado no artigo 7°, inciso IX, em que fica determinada a necessidade do consentimento livre e expresso como condição para a “coleta, uso, armazenamento e tratamento de dados pessoais”. Na Diretiva 95/46/CE o consentimento é um dos seis fundamentos que dão legitimidade ao tratamento de dados, sendo um fundamento geral de licitude, de acordo com o artigo 7° da referida Diretiva. A Lei n° 67/98 de Portugal, responsável pela transposição da Diretiva 95/46/CE, em seu artigo 6°, estabelece que o tratamento dos dados pessoais só possa ser realizado quando o “seu titular tiver dado de forma inequívoca o seu consentimento”. O Regulamento 2016/679 manteve o consentimento como fundamento, de acordo com o artigo 8° do documento, este consentimento deve se traduzir em manifestação de vontade, livre, específica, informada e explícita, pela qual a pessoa em causa aceita, mediante uma declaração ou um ato positivo inequívoco.

Diante da importância colocada na questão do consentimento em todas estas normas, a conclusão é que o modelo adotado tanto pelo Brasil quanto pela União Europeia é do tipo *opt in.* Conforme foi visto anteriormente, este modelo necessita do consentimento, para que possa ocorrer a coleta, tratamento e armazenamento dos dados pessoais. O modelo contrário, o *opt out*, presume a concordância do titular dos dados ao utilizar um determinado sistema, sendo que, neste caso, o titular deve se manifestar para que seus dados pessoais não sejam objetos de coleta, tratamento ou armazenamento.

A autodeterminação informativa é outro elemento comum entre as normas europeias e a legislação brasileira. No Marco Civil, o artigo 7°, inciso X, estabelece ao titular o direito à "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes"[34]. A Diretiva 95/46/CE reconhece o direito do titular dos dados em obter o acesso (artigo 12°) e de se opor ao tratamento dos seus dados pessoais (artigo 14°). De acordo com a Diretiva 95/46/CE, o acesso aos dados pessoais deve ser garantido pelos Estados-membros, ficando os responsáveis por estes dados obrigados a fornecerem estas informações livremente, sem restrições, sem demora e sem custos excessivos (artigo 12°, alínea (a)). O direito à oposição é descrito no artigo 14° da Diretiva, que determina ao titular do dado o direito de se "opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de tratamento" (artigo 14, alínea (a)). Em Portugal, os direitos de acesso e oposição foram transpostos respectivamente pelos artigos 11° e 12° da Lei n° 67/98 (o direito à retificação dos dados está presente na alínea (d) do artigo 11°). O Regulamento 2016/679 deu um passo além da Diretiva 95/46/CE, estabelecendo, além dos direitos ao acesso e à oposição (artigos 15° e 18°), o direito à retificação ao apagamento dos dados (artigos 16° e 17°).

Da comparação entre o Marco Civil e as normas europeias percebe-se a autodeterminação informativa presente em algum grau em todas as normas analisadas. No Brasil este direito aparece de forma tímida com a garantia de exclusão dos dados pessoais por meio de solicitação do titular. O acesso, a retificação e a oposição ao tratamento dos dados não são citados pelo Marco Civil e

[34] O Decreto 8.771/2016 reforça esta determinação em seu artigo 13, §2°, incisos I e II.

pelo Decreto n° 8.771/2016. O Regulamento 2016/679, no quesito autodeterminação informativa, parece ser a norma mais completa neste tema, estabelecendo o direito do titular dos dados pessoais ao: acesso, retificação, oposição ao tratamento de dados, eliminação dos dados, além do direito à portabilidade.

Outro ponto comum em todas as normas é no que diz respeito à chamada *Privacy by Design*, a proteção à privacidade sendo adotada na própria estrutura dos sistemas de comunicação. Todas as normas analisadas apresentam dispositivos determinando aos responsáveis pelo tratamento de dados medidas a serem incorporadas neste sentido. No Brasil, esta preocupação fica destacada no Decreto n° 8.771/2016 – responsável por regulamentar a Lei do Marco Civil - em sua Seção II, que estabelece diretrizes a serem incorporadas nos sistemas de comunicação. A Diretiva 95/46/CE incorpora o *Privacy by Design* em forma de princípios a serem seguidos. Assim, no rol de princípios dos artigos 6° e 7°, encontram-se dispositivos referentes ao recolhimento apenas de dados suficientes para a finalidade do tratamento (Art. 6°, n° 1, al. (c)) e mantidos apenas pelo tempo estritamente necessário (Art. 6°, n° 1, al. (e)). A lei portuguesa (Lei n° 67/98), em seus artigos 5° e 6°, realizou a transposição dos princípios presentes na Diretiva em sua integralidade para o ordenamento local. A implementação do *Privacy by Desing* por meio de princípios foi mantida no Regulamento 2016/679, sendo que o artigo 5° subscreve o rol de princípios do ato legislativo anterior. O novo Regulamento ainda acrescenta condições para a licitude (artigo 6°) e para o consentimento (artigo 7°) que reforçam o conceito de privacidade aplicada em nível estrutural aos responsáveis pelo tratamento de dados.

A privacidade em nível estrutural, ou *Privacy by Desing*, é uma tese defendida por vários autores de destaque que estudam a proteção de dados. Para estes estudiosos, a forma mais eficiente de se atingir a proteção de dados é pela internalização de mecanismos de proteção por parte das entidades que realizam o tratamento de dados. Ao Estado cumpre informar, por meio de leis ou outros atos legislativos, as diretrizes a serem observadas por estas entidades. No Brasil, conforme o que foi visto, o Decreto 8.771/2016 - especialmente nos incisos do seu artigo 13 - incorporou ao ordenamento pátrio diretrizes estabelecendo autenticação dupla para acesso aos registros, encriptação dos dados, entre outras disposições,

que demonstram a preocupação do legislador em adotar medidas de proteção de dados neste nível estrutural.

Outro ponto de similaridade entre as legislações é quanto à transnacionalidade. Todas as legislações examinadas estendem, de alguma forma, a sua aplicação para fora da sua fronteira. Assim, na Diretiva 95/46/CE a questão do direito nacional aplicável é definido no artigo 4°. A transposição para o direito português manteve a integralidade do texto da Diretiva 95/46/CE, de forma que a lei portuguesa seja aplicada nos tratamento dos dados efetuados:

> a) No âmbito das atividades de estabelecimento do responsável do tratamento situado em território português;
> b) Fora do território nacional, em local onde a legislação portuguesa seja aplicável por força do direito internacional;
> c) Por responsável que, não estando estabelecido no território da União Europeia, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território português, salvo se esses meios só forem utilizados para trânsito através do território da União Europeia (PORTUGAL, 1998)

O Regulamento 2016/679, por ser vinculativo a todos os Estados-membros da União Europeia, solucionou boa parte das questões envolvendo a aplicação das leis nacionais. A partir de maio de 2018 este ato legislativo será a norma a ser observada por toda a União Europeia. O Regulamento ainda acrescentou as Empresas localizadas fora dos Estados-membros (artigo 47°), conforme foi visto no capítulo anterior.

No Brasil o Marco Civil adotou uma posição semelhante ao que já existia na União Europeia, de forma que “em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações” de dados realizados dentro do território nacional, a legislação pátria deverá ser seguida (artigo 11). O Marco Civil também estendeu sua aplicação para as entidades localizadas em outros países, de forma similar ao prescrito pelo Regulamento 2016/679, conforme o parágrafo 2° do artigo 11:

> § 2o O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. (BRASIL, 2014)

5.2 DIFERENÇAS ENTRE O MODELO LEGISLATIVO BRASILEIRO E O MODELO LEGISLATIVO EUROPEU

Após a análise das semelhanças entre os modelos legislativos do Brasil e da Europa, a discussão passa para as diferenças presentes nestes modelos. Por uma questão de espaço, a análise se aterá nas questões mais relevantes apresentadas nas legislações.

Destas diferenças, a primeira que será destacada é no que diz respeito aos chamados dados sensíveis. Conforme foi visto anteriormente, dados sensíveis são aqueles que dizem respeito à religião, sexualidade, posição política, religião, entre outras informações, que se reveladas podem estigmatizar ou gerar preconceito contra o titular.

Na Europa a preocupação com este tipo de dados aparece na Diretiva 95/46/CE, em seu artigo 8°, n° 1, que determina a proibição do tratamento destes dados por parte dos Estados-membros. A transposição para a legislação portuguesa desta garantia se deu pelo artigo 7° da Lei n° 67/98. O Regulamento 2016/679, por sua vez, seguiu o disposto na Diretiva 95/46/CE, acrescentando ao rol de dados sensíveis os dados biométricos (artigo 9°, n° 1).

A regra para todas as normas europeias analisadas é a proibição do tratamento de dados sensíveis. Entretanto, vale ressaltar, a proibição não é absoluta em nenhum destes atos legislativos. A Diretiva 95/46/CE traz um rol de exceções que permitem o tratamento deste tipo de dados nas alíneas do n° 2, artigo 8°. O mesmo ocorre na lei portuguesa que realizou a transposição da Diretiva para a lei portuguesa (artigo 7°, n° 2, 3 e 4). No Regulamento 2016/679 as exceções estão no artigo 9°, n° 2 e 3.

A necessidade das exceções ao tratamento deste tipo de dados é fundamental para a prática de certas atividades do Estado e da iniciativa privada. Os planos de saúde e os hospitais, por exemplo, precisam de informações completas sobre a saúde dos clientes e pacientes. A preocupação destas normas é estabelecer uma proteção mais rígida sobre estas informações mais delicadas.

Enquanto a Europa já possui uma imposição legislativa quanto à proteção aos dados sensíveis desde 1995, no Brasil ainda não existe um título legal que trate do tema. O Marco Civil da Internet não faz a distinção entre os tipos de dados, não existindo sequer a menção aos dados sensíveis em seu texto. O mesmo ocorre no

Decreto n° 8.771/2016, que também não entra nesta questão ao regulamentar alguns aspectos do Marco Civil. O mais próximo que o Brasil possui de uma regulamentação sobre os dados sensíveis é o projeto de Lei de Proteção de Dados (Projeto de Lei n° 5276/2016), que possui uma seção reservada a este tipo de dados[35].

Uma das novidades introduzidas pelo Regulamento 2016/679 foi quanto aos dados dos titulares menores de 16 anos. Conforme foi explicado anteriormente, a partir de maio de 2018 os dados pessoais de titulares com menos de 16 anos terão uma regra mais rígida para o consentimento (artigo 8°, n° 1). A legislação brasileira não aborda a questão dos dados pessoais de crianças e adolescentes, não existindo a distinção dos dados pessoais de adultos e de crianças/adolescentes.

A segunda diferença a ser apontada entre a legislação europeia com a legislação pátria é no que diz respeito à autoridade de controle e fiscalização. Enquanto na Europa existe uma determinação legal para a criação nos Estados-membros de uma (ou mais) autoridade central responsável pela proteção de dados, no Brasil não há nenhum dispositivo que preveja a criação deste tipo de autoridade no país. Assim, na Diretiva 95/46/CE a autoridade de controle está presente no capítulo VI, artigo 28°. Portugal, conforme foi visto, já possuía uma autoridade de controle antes da existência da Diretiva 95/46/CE, sendo uma determinação da Constituição da República de Portugal (n° 2, artigo 35°). Este artigo constitucional gerou a Comissão Nacional de Proteção de Dados (CNPD), a entidade responsável pelo controle e fiscalização da proteção de dados no país. Conforme já foi visto também, com a transposição da Diretiva 2002/58/CE pela Lei n° 41/2004, o país passou a ter a Autoridade Nacional de Comunicações (ANACOM) como segunda entidade responsável pelas questões de supervisão, controle do funcionamento e garantia da segurança no tratamento de dados pessoais, no âmbito das comunicações eletrônicas. No Regulamento 2016/679 a autoridade de controle está prevista no artigo 51°, n° 1, que reproduz o que já era disposto na Diretiva.

O Brasil, diferentemente de Portugal, não possui uma autoridade central responsável pelo controle e fiscalização das questões relacionadas à proteção de

[35] A Lei n° 12.414/2011, que regula a criação e consulta de bancos de dados para formação de histórico de crédito, possui um artigo que veda as anotações referentes a “informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas”, artigo 3°, parágrafo 3°, inciso II (BRASIL, 2011).

dados. A legislação brasileira divide a competência de controle e fiscalização para autoridades diferentes, assim, como define o Decreto n° 8.771/2016, a ANATEL fica responsável no que tange ao âmbito das telecomunicações, a Secretaria Nacional do Consumidor pelo que diz respeito às relações de consumo, e a ordem econômica ao Sistema Brasileiro de Concorrência (CADE), conforme os artigos 17, 18 e 19, do referido Decreto.

Ainda no que toca ao controle e fiscalização, outra inovação advinda do Regulamento 2016/679 e que não tem paralelo com a legislação brasileira são as avaliações de impacto. De acordo com o novo ato legislativo europeu, sempre que o tratamento dos dados envolva um elevado "risco para os direitos e liberdades das pessoas singulares", o responsável deve fazer uma avaliação dos impactos deste tratamento (artigo 35°, n° 1). De forma que, caso fique provado um risco elevado, o responsável realize novas operações para minimizar o risco ou tome outras providências para dirimir estes riscos. Controlar a realização destas avaliações de impacto é uma das atribuições do encarregado de dados, pessoa designada pelo responsável para algumas situações específicas em que existe a necessidade de um controle maior na proteção dos dados pessoais (artigo 37°, n°1).

Na legislação pátria inexiste este tipo de avaliação no tratamento de dados pessoais. Conforme foi discutido quanto aos dados sensíveis, no Brasil ainda é tímida a preocupação em proteger com mais rigor o tratamento destes tipos de dados, considerados sensíveis[36].

Os dados de tráfego são o último ponto a ser destacado nas diferenças entre o sistema legislativo brasileiro e o europeu. A preocupação com estas informações está presente na Diretiva 2002/58/CE da União Europeia (artigo 6°). O ato legislativo europeu ainda distingue os dados de localização como dados de tráfego que merecem um regime de proteção especial (artigo 9°). A lei 41/2004, que transpôs a Diretiva 2002/58/CE, repetiu o disposto na Diretiva 2002/58/CE em seus artigos 6° (dados de tráfego) e 7° (dados de localização).

Novamente não existe paralelo na legislação brasileira para a questão dos dados de tráfego. O ordenamento pátrio não desmembra os dados que fazem parte dos dados pessoais, de forma que os dados de localização, por exemplo, também não são mencionados na legislação brasileira.

[36] O projeto de Lei de Proteção de Dados possui um dispositivo tratando da avaliação de impacto em seu artigo 39°, parágrafo 2°.

6 CONCLUSÕES

A proteção de dados pessoais se tornou uma preocupação de primeiro plano na sociedade de informação em que estamos inseridos. Vazamentos de dados como nos casos da Equifax[37], em que milhões de norte-americanos tiveram suas informações bancárias roubadas, ou o caso do site de relacionamentos Ashley Madison[38], que expos 37 milhões de usuários da rede, são exemplos da importância da proteção de dados neste mundo interconectado.

Conforme foi visto no decorrer deste trabalho, a preocupação com a privacidade não é algo recente, existindo - ainda que de uma forma distinta do conceito moderno - desde os tempos da Antiguidade. Após o Iluminismo a questão da privacidade começa a se delinear ao conceito existente nos dias de hoje. A importância deste direito iria continuar crescendo na medida em que a tecnologia também se desenvolvia. No *welfare state* a proteção de dados ganha relevo pelo receio de forças autoritárias utilizarem estas informações para realizarem malfeitos contra determinados grupos da população. Na segunda metade do século XX aparecem as primeiras leis nacionais a disciplinarem a questão da privacidade de dados na União Europeia. O final do milênio fica marcado como o período em que proteção de dados pessoais passa a ser uma preocupação em nível mundial, graças ao desenvolvimento da Internet que passa a conectar todo o globo.

No que tange à análise legal do trabalho, após o exame das legislações brasileira e europeia sobre o tema, algumas conclusões parecem emergir do paralelo entre os ordenamentos. Em primeiro lugar, parece claro que a legislação brasileira, da forma que se apresenta atualmente, parece insuficiente para abarcar as garantias necessárias à proteção de dados.

A Lei n° 12.965/2014 (Marco Civil da Internet), que gerou grande polêmica na época de sua promulgação, apequena-se perto do atual Regulamento 2016/679 da União Europeia, ou até mesmo perto da Diretiva 95/46/CE. Desenvolvido para ser uma Constituição da Internet, o Marco Civil da Internet, no que se refere à proteção de dados, é demasiado sucinto e insuficiente para uma adequada proteção aos dados pessoais.

---

[37] https://br.reuters.com/article/businessNews/idBRKCN1BM2HU-OBRBS
[38] https://tecnoblog.net/184013/ashley-madison-consequencias-vazamento/

Várias garantias presentes na legislação europeia ainda não receberam proteção em nosso ordenamento pátrio. Destaca-se, por exemplo, os dados sensíveis, já presentes na legislação europeia desde a Diretiva 95/46/CE, que não recebem nenhuma menção no Marco Civil da Internet ou no Decreto n° 8.771/2016. Vazamentos recentes deste tipo de dados tem demonstrado a necessidade de uma proteção mais rígida sobre este tipo de dados pelas legislações nacionais.

Os dados de tráfego são outra preocupação presente na legislação europeia sem paralelo no Brasil. Presente na Diretiva 2002/58/CE, que disciplina a proteção de dados no setor de comunicações eletrônicas, a proteção a estas informações tendem a ganhar uma importância cada vez maior, haja vista o fato de hoje em dia, graças aos aparelhos celulares, ser possível localizar uma pessoa a qualquer momento do dia. Novamente, não existe prescrição legal sobre tais tipos de dados no ordenamento nacional.

A autodeterminação informativa é outro ponto em que o Brasil parece ficar para trás em relação à União Europeia. Enquanto o usuário europeu tem direito a se opor, acessar, retificar e excluir seus dados presentes em bancos de dados, o Marco Civil menciona apenas o direito a exclusão após solicitação do titular. Ainda neste sentido, o Regulamento 2016/679 traz o inovador direito a portabilidade dos dados, que permite ao titular dos dados obter um arquivo portável para outra entidade responsável pelo tratamento de dados, sem que a primeira possa opor objeção.

Outra inovação do Regulamento 2016/679, as avaliações de impacto, também não encontram paralelo na legislação brasileira. Tal medida se trata de uma garantia maior para evitar violações aos direitos à privacidade como as descritas no início deste capítulo.

A falta de uma autoridade de controle e fiscalização exclusivamente para estas questões parece ser outra necessidade para garantir a proteção de dados pessoais. Tal preocupação já se faz presente na União Europeia desde a Convenção de Strasbourg, tendo sido incorporada nos demais atos legislativos. O Brasil, conforme foi visto na análise do Decreto n° 8.771, divide a competência entre entidades distintas.

Demonstrada estas conclusões, reitera-se a necessidade outros instrumentos legais para a proteção de dados na legislação pátria. Embora um importante passo

para legislar o tema, o Marco Civil possui limitações que o tornam um instrumento insuficiente para a proteção de dados no país.

REFERÊNCIAS

AGUIAR JR., R. R. de (Org.). **V Jornada de Direito Civil**. Brasília: CJF, 2012, p.69. Disponível em: < http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/v-jornada-direito-civil/VJornadadireitocivil2012.pdf/at_download/file> Acesso em: 24 de Outubro de 2017.

ALVES, C. S.; VAINZOF, R. **Privacy by Design e Proteção de Dados Pessoais**. 2016. Disponível em: <https://jota.info/colunas/direito-digital/direito-digital-privacy-design-e-protecao-de-dados-pessoais-06072016> Acesso em: 23 de Outubro de 2017

ASSANGE, Julian. **Cypherpunks - Liberdade e o futuro da internet**. São Paulo: Boitempo, 2013.

BORGES, R. C. B. **Disponibilidade dos direitos de personalidade e autonomia privada**. São Paulo: Saraiva, 2005, p. 156

BRASIL. **Código civil**. 46. ed. São Paulo: Saraiva, 1995. Organização dos textos, notas remissivas e índices por Juarez de Oliveira.

CAMARGO, C. A. de A.; CRESPO, M. **A proteção aos dados pessoais no ordenamento jurídico brasileiro e o anteprojeto do Ministério da Justiça**. 2015. Disponível em: < http://www.migalhas.com.br/DireitoDigital/105,MI220187,81042-A+protecao+aos+dados+pessoais+no+ordenamento+juridico+brasileiro+e+o> Acesso em: 01 de Novembro de 2017.

_____. Constituição (1988). **Constituição**: República Federativa do Brasil. Brasília, DF: Senado Federal, 1988.

_____. Decreto n° 8.771, de 11 de Maio de 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014. **Diário Oficial da União**, Brasília, DF, 11 de mai. de 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20152018/2016/decreto/D8771.htm>. Acesso em: 24 de Outubro de 2017.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, n. 77, 24 de abr. de 2014. Seção 1, p. 1. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=24/04/2014>. Acesso em: 24 de Outubro de 2017

CANOTILHO, J. J. G. **Direito Constitucional e teoria da Constituição**. 3. ed. Coimbra: Almedina, 2003.

CASTELLS, M. A. Sociedade em Rede: do Conhecimento à Política. In: CASTELLS, M.; CARDOSO, G. **A Sociedade em Rede: Do Conhecimento à Acção Política**. Belém: Imprensa Nacional - Casa da Moeda, 2005. p. 17 – 30. Disponível em: < http://www.egov.ufsc.br/portal/sites/default/files/anexos/a_sociedade_em_rede_-_do_conhecimento_a_acao_politica.pdf>. Acesso em: 20 de Outubro de 2017.

CELLA, J. R. G.; FREITAS, C. O. A. Marco Civil da Internet: Limites da Previsão Legal de Consentimento Expresso e Inequívoco como Proteção Jurídica dos Dados Pessoais na Internet. **Revista de Direito, Governança e Novas Tecnologias**, v. 2, n. 1, p. 61-80, 2016.

CRUZ, F. C. de B. **Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet**. 2015. 138 pp. Mestrado – Faculdade de Direito, Universidade de São Paulo. 2015. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2139/tde-08042016-154010/pt-br.php>. Acesso em: 20/10/2017.

DA SILVA, J. A. **Curso de direito constitucional positivo**. 20ª ed. São Paulo: Malheiros Editores, 2002.

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

FLORENZANO, M. B. B. **Pólis e oîkos, o público e o privado na Grécia Antiga**. Publicado nos Anais do I Simpósio Regional de História Antiga, Rondonópolis, M.T. 2001. P. 113-118. Disponível em: <http://labeca.mae.usp.br/media/pdf/florenzano_polis_e_oikos.pdf>. Acesso em: 20 de Outubro de 2017

IDEC. **Nota técnica sobre decisão de bloqueio do Whatsapp**. 2015. Disponível em: <http://www.idec.org.br/pdf/nota-tecnica-bloqueio-whatsapp.pdf>. Acesso em: 01 de Novembro de 2017.

LESSIG, L. **Code and Other Laws of Cyberspace ver.2.0**. New York: Basic Books, 2006. Disponível em: < http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 20 de Outubro de 2017

MATOSAS, G. K; NEDEL, N. K. **Celebridade: um status que permite a mitigação de direitos fundamentais pela mídia?** Santa Maria, 2012, p.8. Disponível em: < http://coral.ufsm.br/congressodireito/anais/2012/15.pdf> Acesso em: 24 de Outubro de 2017.

MENKE, F. A proteção de dados e novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. In: MENDES, G. F.; SARLET, I. W.; COELHO, A. Z. (Org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 205-230. V. 1.

MEIRELLES, H. L. **Mandado de segurança e ações constitucionais**.35ª edição. São Paulo: Revista dos Tribunais, 2009.

MINISTÉRIO PÚBLICO FEDERAL. **Nota técnica sobre o descumprimento da legislação brasileira que regulamenta o uso da internet**. 2016. Disponível em: <http://www.mpf.mp.br/pgr/documentos/nota-tecnica-crimes-ciberneticos/at_download/file>. Acesso em: 01 de Novembro de 2017.

ONU. **Declaração Universal dos Direitos Humanos**. Adotada e proclamada pela Assembléia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Disponível em: <https://www.unicef.org/brazil/pt/resources_10133.htm>. Acesso em: 31 de Outubro de 2017.

PORTUGAL. **Constituição da República Portuguesa de 1976**. 02 de Abril de 1976. Disponível em: http://www.parlamento.pt/Parlamento/Documents/CRP1976.pdf. Acesso em: 25 de Outubro de 2017.

_____. Lei n.º 67/98, de 26 de outubro. **Diário da República 1ª série**. N.º 247. 26 de out. de 1998. Disponível em: <http://www.cnpd.pt/bin/legis/nacional/LPD.pdf> Acesso em: 25 de Outubro de 2017.

_____. Lei n.º 41/2004, de 18 de agosto. **Diário da República 1ª série**. N.º 167. 29 de out. de 2012. p. 4819-4826. Disponível em: <http://www.cnpd.pt/bin/legis/nacional/Lei_46_2012.pdf>. Acesso em: 01 de Novembro de 2017.

SARLET, I. W. **Dignidade da pessoa humana e direitos fundamentais na constituição federal de 1988**. 5. ed. Porto Alegre: Livraria do Advogado, 2005, p. 70.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte**. Belo Horizonte: Del Rey, 1998.

SANTOS, Cristina Máximo dos. As novas tecnologias da informação e o sigilo das telecomunicações. **Revista do Ministério Público.** N° 99. 3° trimestre de 2004. Lisboa: Sindicato dos Magistrados do Ministério Público. p. 43. Disponível em: <http://rmp.smmp.pt/ermp/rmp_99/index.html#p=46> Acesso em: 23 de Outubro de 2017.

SCALZILLI.FMV ADVOGADOS. **Marco Civil da Internet: principais efeitos do Decreto 8.771 assinado em 11 de maio de 2016**. Scalzilli.fmv Advogados, 2016. Disponível em: < http://scalzillifmv.tempsite.ws/publicacao/marco-civil-da-internet-principais-efeitos-do-decreto-8-771-assinado-em-11-de-maio-de-2016 >. Acesso em: 23 de Outubro de 2017.

SILVEIRA, S. A. da. **Marco Civil e a proteção da privacidade**. Campinas, 2014. Disponível em: <http://www.dicyt.com/viewNews.php?newsId=30983>. Acesso em: 23 de Outubro de 2017.

ROSENVALD, N. **Do direito ao esquecimento ao direito a ser esquecido**. São Paulo, 2017. Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/do-direito-ao-esquecimento-ao-direito-a-ser-esquecido/17477>. Acesso em: 25 de Outubro de 2017

TEIXEIRA, M. L. da S. A União Europeia e a Proteção de Dados Pessoais – "Uma visão futurista". **Revista do Ministério Público**. Ano 34, n.º 135. Lisboa: Sindicato dos Magistrados do Ministério Público. Julho de 2013, p. 65-106. Disponível em: <http://rmp.smmp.pt/wp-content/uploads/2013/10/5.RMP_135_MARIA_LEONOR_DA_SILVA_TEIXEIRA.pdf> . Acesso em: 25 de Outubro de 2017.

UNIÃO EUROPEIA. Conselho da Europa – **Manual da legislação Europeia sobre proteção de dados**. [S.l : s.n.] 2014. Disponível em: <http://www.cnpd.pt/bin/legis/internacional/fra-2014-handbook-data-protection-pt.pdf>. Acesso em: 01 de Novembro de 2017.

_____. Grupo de Trabalho do Artigo 29.º - **Parecer 15/2011 sobre a definição de consentimento**. Bruxelas: Grupo de trabalho, 13 de jul. de 2011. Disponível em: <http://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf>. Acesso em: 25 de Outubro de 2017.

_____. Grupo de Trabalho do Artigo 29.º – **Recomendação relativa a conservação dos dados referentes ao tráfego, por parte dos fornecedores de serviços Internet, para efeitos de aplicação da lei. Recomendação 3/99**. Bruxelas: Grupo de Proteção. 07 de set.1999. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp25pt.pdf>. Acesso em: 25 de Outubro de 2017.

_____. Jornal Oficial da União Europeia – **Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Bruxelas: Comissão Europeia. 24 de out. de 1995. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em: 01 de Novembro de 2017.

_____. Jornal Oficial da União Europeia – **Diretiva 2002/58/CE, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.** Bruxelas: Comissão Europeia. 12 de jul. de 2002. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT>. Acesso em: 01 de Novembro de 2017.

_____. Jornal Oficial da União Europeia – **Regulamento (UE) n.º 679/2016 do Parlamento Europeu e do Conselho**. Bruxelas: Comissão Europeia. 27 de abr. de 2016. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 25 de Outubro de 2017.

WARREN, S. D.; BRANDEIS, L. D. **The Right to Privacy.** 15 de Dezembro de 1890. Disponível em: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf> Acesso em: 31 de Outubro de 2017.