Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil

Letícia Antunes Tavares[1]
Juíza de Direito no Estado de São Paulo

Bruna Acosta Alvarez
Juíza de Direito no Estado de São Paulo

1. Dados pessoais — conceito, importância e proteção

O episódio envolvendo o website "tudosobretodos.se" intensificou o debate acerca da proteção aos dados pessoais. De acordo com as reportagens sobre o assunto[2], o referido site divulgou e disponibilizou à venda, sem prévia autorização, dados sobre pessoas físicas, incluindo endereço, dados sobre vizinhos etc. Ainda, no mês de novembro de 2015, foi divulgada matéria pelo programa Fantástico[3] a respeito de uma investigação encabeçada pelo Ministério Público do Estado de São Paulo, envolvendo o *website* "cartório virtual", que, supostamente, estaria divulgando dados pessoais, inclusive de autoridades públicas, tais como endereço, números de identificação, dados telefônicos etc., sem prévio consentimento da pessoa envolvida[4].

Estes são, apenas, dois exemplos recentes do uso indevido de dados pessoais e servem para ilustrar a vulnerabilidade da privacidade dos cidadãos, na sociedade atual. E são acontecimentos como tais que despertam os indivíduos para a necessidade de um marco legal, já que

---

[1] Especialista em Direito Público pela Escola Paulista de Magistratura. Mestranda em Direito Comparado pela *Samford University*.

[2] Disponível em: <http://info.abril.com.br/noticias/internet/2015/07/seu-nome-cpf-e-endereco-completos-podem-estar-disponiveis-neste-site-sem-que-voce-saiba-disso.shtml>. Acesso em: 8 nov. 2015.

[3] Programa jornalístico veiculado pela Rede Globo de televisão.

[4] Disponível em: <http://g1.globo.com/fantastico/noticia/2015/11/mp-sp-acusa-grupo-que-age-na-internet-de-vender-dados-sigilosos.html>. Acesso em: 8 nov. 2015.

o Brasil, diferentemente da Europa e de alguns países da América Latina (Chile, Colômbia, Peru e Argentina)[5], possui tímidas menções à proteção de dados pessoais em legislações esparsas, não possuindo lei específica sobre o assunto, até o presente momento. Não à toa que, em 2010, o Ministério da Justiça iniciou um debate público a respeito da proteção de dados pessoais[6], visando à regulamentação do tema, sendo que a versão final do anteprojeto de lei foi, finalmente, apresentada em outubro de 2015[7].

Paralelamente, em 13 de junho de 2012, foi apresentado à Câmara dos Deputados o Projeto de Lei Federal n. 4060/12[8], projeto este que foi recentemente desarquivado e que, hoje, está em trâmite na Comissão de Ciência e Tecnologia, Comunicação e Informática. Do mesmo modo, no Senado Federal tramita projeto de lei tratando do tema (Projeto de Lei n. 330 de 2013), sendo que o substitutivo fora recentemente aprovado pela Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática[9].

Mas, o que seriam dados pessoais e qual seria o motivo de tamanha preocupação?

1.1. Conceituação

Dados poderiam ser definidos como "um conjunto de registros sobre fatos, passíveis de serem ordenados, analisados e estudados para se alcançar conclusões". Estes dados, quando "organizados e ordenados de forma coerente e significativa para fins de compreensão e análise", são chamados de informação.[10] E, quando se adiciona a palavra "pessoais" ao termo "dados", há uma personalização do conceito, de modo que os "dados pessoais" seriam um conjunto de registros referentes a um indivíduo.

---

[5] Data Protection Laws of the World. Disponível em: <http://dlapiperdataprotection.com/#handbook/world-map-section>. Acesso em: 27 set. 2015.

[6] Disponível em: <http://participacao.mj.gov.br/dadospessoais/>. Acesso em: 8 nov. 2015.

[7] Disponível em: <https://www.justica.gov.br/noticias/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais>. Acesso em: 9 jan. 2016.

[8] Disponível em: <http://www2.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 26 jan. 2016.

[9] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 9 jan. 2016.

[10] LACOMBE, Francisco José Masset et al. *Administração* – princípios e tendências. São Paulo: Saraiva, 2003. p. 490.

Nos termos da Diretiva n. 95/46/CE da União Europeia, ainda em vigor, que trata da proteção das pessoas no que diz respeito ao tratamento de dados pessoais, a expressão "dados pessoais" pode ser definida como "qualquer informação relativa a uma pessoa singular identificada ou identificável", sendo "considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos de sua identidade física, fisiológica, psíquica, econômica, cultural ou social" (artigo 2º, "a").

Também, a citada Diretiva, em seu artigo 8º, 1, cria uma subespécie de dados pessoais, os chamados dados sensíveis, que são os "dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual".

Vale destacar que, no Brasil, não existe uma definição legal da expressão "dados pessoais".[11] Até mesmo o Marco Civil, quando trata do assunto (artigo 3º, inciso III, da Lei n. 12.965 de 2014), relega sua regulamentação à lei específica, ainda em fase de elaboração, cumprindo mencionar que os referidos projetos de lei que tratam do tema ofertaram definição para expressão "dados pessoais", inclusive "dados sensíveis" (artigo 7º, incisos I e IV, do Projeto de Lei da Câmara dos Deputados n. 4060 de 2012 e artigo 3º, incisos I e II, do Projeto de Lei do Senado Federal de 2013), com nítida inspiração na diretiva europeia, sanando omissões e alinhando-se, assim, a uma tendência internacional.

Pela própria denominação da Diretiva (relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados) ou mesmo de acordo com os objetivos dos citados projetos de lei, é possível concluir que o objeto da proteção da legislação é o indivíduo e não os seus dados em si. Isso porque tais informações dizem respeito à intimidade e privacidade do ser humano, direitos estes de caráter fundamental no Brasil, inclusive amparados pela Constituição Federal. Daí a necessidade de regulamentação do tema, especialmente, quando considerada a importância dos dados pessoais na sociedade de informação.

[11] Vale destacar que a Lei de Acesso à Informação (Lei n. 12.527 de 2011), conquanto não oferte definição à expressão "dados pessoais", define a expressão "informações pessoais", como aquela relacionada à pessoa natural identificada ou identificável.

1.2. Relevância do tema

Com efeito, a coleta e a análise de dados pessoais sempre permeou as relações intersociais, com o objetivo de melhorar a vida em sociedade, aprimorar o desenvolvimento econômico, resolver problemas etc.,[12] sendo certo que, na atualidade, na sociedade informacional, os dados pessoais galgaram posição central, em especial, no universo digital.[13]

De acordo com Manuel Castells, o informacionismo seria um novo modelo de desenvolvimento, historicamente moldado pela reestruturação do capitalismo, no final do século XX. Para o autor, nesse novo modelo de desenvolvimento,

> [a] fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos. Na verdade, o conhecimento e informação são elementos cruciais em todos os modos de desenvolvimento, visto que o processo produtivo sempre se baseia em algum grau de conhecimento e no processo de informação. Contudo, o que é específico ao modo informacional de desenvolvimento é a ação de conhecimento sobre os próprios conhecimentos como principal fonte de produtividade.[14]

Ainda, para Castells, a base tecnológica que dá forma organizacional à Era da Informação é a internet. Para o sociólogo,

> [a] influência das redes baseadas na Internet vai além do número de seus usuários: diz respeito também à qualidade do uso. Atividades econômicas, sociais, políticas, e culturais essenciais por

[12] Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 29 set. 2015.

[13] "No fim do segundo milênio da Era Cristã, vários acontecimentos de importância histórica transformaram o cenário social da vida humana. Uma revolução tecnológica concentrada nas tecnologias de informação começou a remodelar a base material da sociedade em ritmo acelerado" (CASTELLS, Manuel. *A sociedade em rede*. Tradução de Roneide Venancio Majer. 8. ed. Paz e Terra. v. I, p. 39.).

[14] CASTELLS, Manuel. *A sociedade em rede*. Tradução de Roneide Venancio Majer .8. ed. Paz e Terra. v. I, p. 51-54.

> todo o planeta estão sendo estruturadas pela Internet e em torno dela, como por outras redes de computadores.[15]

Conhecimento e informação, portanto, são vitais para a sociedade informacional e sua utilização mostra-se potencializada pelo uso da internet, que, hoje em dia, permeia todo o tipo de atividade, em especial a econômica e social.

Pode-se dizer, assim, que a informação seria a principal *commodity* e instrumento de poder na sociedade informacional e, por outra via, como a informação nada mais é do que o processamento de dados, é possível concluir que a utilização de tais dados, também, é essencial à Era da Informação.

Vale ressaltar, como apontado no estudo realizado pela Presidência dos Estados Unidos da América de maio de 2014[16], a coleta, o armazenamento e a análise de dados estão em uma trajetória ascendente e, aparentemente, sem limites, alimentados por um aumento no poder de transformação, pela redução dos custos de computação e de armazenamento, e pelo número crescente de tecnologias de sensor incorporadas em todos os tipos de aparelhos. E a esse universo, que reflete a capacidade tecnológica de capturar, agregar e processar um número e variedade cada vez maior de dados, é conferido o nome de "big data"[17].

Sobre o prisma governamental, de acordo com o citado estudo, enquanto o "big data" aumenta o potencial de poder do governo, por outro lado, também, aumenta a responsabilidade deste, diante da necessidade de proteção da privacidade e demais direitos do cidadão.[18]

---

[15] CASTELLS, Manuel. *A galáxia da internet:* reflexoes sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 7-8.

[16] BIG data: seizing opportunities, preserving values. p. 1-2. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 29 set. 2015.

[17] Disponível em: <https://www.privacyinternational.org/node/8>. Acesso em: 29 set. 2015.

[18] Vale lembrar que, em 2013, conforme denúncia de Edward Snowden, descobriu-se que o governo norte-americano, por meio da agência de segurança nacional (em inglês, NSA), estava espionando os cidadãos americanos e vários países da Europa e América Latina, entre eles Brasil e Alemanha. Assim, tais países, vislumbrando a necessidade de um marco civil multilateral, apresentaram à Organização das Nações Unidas (ONU) uma proposta de resolução para tratar da proteção da privacidade, incluindo dados pessoais na era digital, que foi aprovada em 2013 (Resolução 68/167) e atualizada em novembro de 2014 (Resolução 69/166) (disponível em: <http://www1.folha.uol.com.br/mundo/2014/11/1553381-onu-aprova-resolucao-proposta-por-brasil-e-alemanha-contra-espionagem.shtml>, acesso em: 9 nov. 2015).

O mesmo raciocínio se aplica às organizações empresariais. Nos dias de hoje, em que as mudanças ocorrem numa velocidade cada vez maior[19], a sobrevivência da atividade empresarial está ligada à criação de vantagens competitivas, sendo certo que o conhecimento e as informações são os principais exemplos destas vantagens, formando o chamado capital intelectual.

É sensível a dependência da atividade empresarial em relação a informações, pois quanto maior o volume de dados pessoais coletados, maiores serão as condições de competitividade, ou seja, quanto mais se conhece o consumidor, maiores são as possibilidades de venda de um produto ou serviço.

Como exemplo de prática que incrementa as condições de competitividade, pode-se citar o *profiling,* que se consubstancia na metodologia que cria um perfil do usuário da rede mundial de computadores, com base nos registros eletrônicos de hábitos de navegação associados a outras fontes de informação.[20]

Ainda, o modelo de negócio de alguns provedores de serviços depende quase que exclusivamente da monetização de dados de seus usuários. Dados estes que na sua maioria são pessoais. Uma vez que a receita das empresas se origina principalmente da publicidade oferecida através de suas plataformas, e a eficiência dessas propagandas está diretamente ligada à análise do comportamento do usuário, caso estas empresas não coletassem dados, elas simplesmente não existiriam.[21]

Além dessas organizações que auferem lucros principalmente em decorrência da publicidade on-line, existem os chamados "serviços de dados" ou, ainda, "data brokers", que englobam uma classe de empresas que coletam dados através de muitas fontes, agregando-os, analisando-os, e, então, compartilhando essas informações. Muitas dessas empresas não têm relação direta com os consumidores cujos dados são coletados, fornecendo serviços a outras organizações, incluindo comercialização.

---

[19] "A velocidade é parte da cultura que criou a internet. O típico usuário da rede mundial de computadores exige rapidez e agilidade na obtenção de qualquer informação, e a presença do fornecedor, produzindo os bens que deseja produzir, na quantidade que entende necessária, distribuindo da forma como lhe convém, por si só, já representa a pressão realizada pelo meio" (KLEE, Antonia Espíndola Longoni. *Comércio eletrônico.* São Paulo: Revista dos Tribunais, 2014. p. 64.).

[20] MONTEIRO, Renato Leite. Da Proteção aos registros, aos dados pessoais e às comunicações privadas. In: MASSO, Fabiano del et al. (Coord.). *Marco Civil da Internet*. São Paulo: Revista dos Tribunais, 2014. p. 141.

[21] Idem, p. 141.

Existem, também, alguns bancos de dados que fornecem informações sobre consumidores, para fins de realização de operações financeiras, de crédito etc. No Brasil, tais agências possuem caráter público, por imposição do parágrafo 4º do artigo 43 do Código de Defesa do Consumidor.[22]

Insta salientar que a proteção aos dados pessoais não se restringe ao âmbito digital; porém, como visto, foi a internet[23] a responsável pelo aumento do uso de dados pessoais, pois ínsito às atividades, sejam empresariais ou governamentais, na atualidade.

Na era informacional, o valor agregado da informação, ainda que personalíssima, maximizou-se. De acordo com Monteiro, "com regulação estatal ou não, dados continuarão a ser coletados e armazenados, pois o atual modelo de negócio das empresas de Internet depende dessa prática"[24].

Assim, na medida em que a internet[25] potencializou a coleta, análise, utilização e transferência de dados pessoais de forma simples e pouco custosa, também, cresceu a preocupação a respeito do nível de proteção conferido a tais dados por aquele que os possui, seja pessoa física ou mesmo pessoa jurídica de direito privado ou público.

Portanto, surge a necessidade de proteção do titular dos dados, principalmente porque o tratamento inadequado aos dados pessoais, no que se incluem os dados sensíveis (aqueles que traduzem informações relativas à origem social e étnica, à genética, à orientação sexual e às convicções políticas, religiosas e filosóficas do titular), pode violar a privacidade, intimidade e outros direitos fundamentais do indivíduo.

---

[22] Vale ressaltar que, recentemente, o C. Superior Tribunal de Justiça, quando do julgamento do Recurso Especial n. 1457199, confirmou a legalidade da prática conhecida como *credit scoring*, que atribui pontuação a consumidores, pontuação esta que é produto da análise dos dados pessoais destes, incluindo eventual inadimplência, e que influencia a decisão das empresas sobre a concessão de crédito a clientes. Todavia, a despeito da licitude do método, o respeito à privacidade do consumidor e a transparência são condicionantes. Assim, de acordo com a decisão do Egrégio Tribunal, as empresas que prestam o serviço de *scoring* devem informar ao titular da pontuação quais os dados utilizados para o cálculo do risco de crédito, a fim de evitar excessos ou até permitir eventual retificação.

[23] "A internet que viabiliza a globalização da informação, é a maior rede internacional de computadores utilizada como meio de comunicação pelos países" (KLEE, Antonia Espíndola Longoni. *Comércio eletrônico*. São Paulo: Revista dos Tribunais, 2014. p. 61.).

[24] MONTEIRO, Renato Leite. Da Proteção aos Registros, aos dados pessoais e às comunicações privadas. In: MASSO, Fabiano del et al. (Coord.). *Marco Civil da Internet*. São Paulo: Revista dos Tribunais, 2014. p. 141.

[25] Com um número estimado que supera os 3 bilhões de usuários de internet em 2015, a proteção de dados pessoais mostra-se um dos mais importantes assuntos da atualidade (disponível em: <http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx#.Vj_FqLerSUm>, acesso em: 8 nov. 2015).

Desta feita, impõe-se perquirir sobre a melhor forma de controlar e restringir os potenciais efeitos nocivos do uso indevido de dados pessoais. Isso porque, quem mais se beneficia com a regulamentação e o estabelecimento de regras claras a respeito da questão, é o cidadão.

Assim sendo, considerando a importância do tema, este trabalho terá por objetivo a análise da perspectiva brasileira a respeito da proteção de dados pessoais, bem como abordará a necessidade de estabelecimento de um marco legal sobre assunto, com estudo comparado de duas realidades regulatórias opostas: a estadunidense e a europeia. Como será estudado, a União Europeia, diferentemente dos Estados Unidos, que possui regulação híbrida, optou pela regulamentação abrangente do uso de dados pessoais[26].

1.3. Níveis de proteção dos dados pessoais: uma abordagem comparada

Existem quatro modelos para a regulamentação em termos de proteção de dados pessoais. De acordo com Moshell, tais modelos não são exclusivos, mas às vezes são complementares ou até contraditórios a depender da aplicação que lhes é dada.

Assim, para o autor, a) o modelo compreensivo estabelece leis gerais de proteção aos dados pessoais, aplicáveis tanto aos setores privado e público; b) o modelo setorial tem por alvo setores específicos que demonstraram ser lesivos à privacidade do cidadão; c) o modelo de autorregulação prevê o estabelecimento de condutas e fiscalização mútuas pelas empresas e indústrias, e d) o modelo de uso de tecnologias para proteção da privacidade pelo próprio indivíduo, permite ao cidadão gerenciar a cessão e distribuição de seus próprios dados pessoais.[27]

Neste aspecto, pode-se afirmar que a União Europeia optou pela regulamentação compreensiva, sendo que a Diretiva n. 95/46/EC, ainda em vigor, seria um exemplo de adesão estrita a este modelo. Por outro lado, os Estados Unidos da América optaram por um modelo híbrido, em geral considerado insuficiente, possuindo um aspecto setorial e outro autorregulatório.[28]

---

[26] LYNSKEY, Orla. *The foundations of EU Data Protection Law.* Oxford: Oxford University Press, 2015. p. 15

[27] MOSHELL, Ryan. And there was one: the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. Texas Tech Law Review, v. 37, p. 366-367, 2005.

[28] Idem. p. 366-367.

Para Fromholz, na União Europeia, estados-membros foram impulsionados a regular o uso de dados pessoais de forma exaustiva. Nos Estados Unidos, por outro lado, o governo absteve-se desta forma de regulação, permitindo que empresas e associações utilizassem a autorregulação, com exceção de um pequeno número de normas estritamente concebidas para determinados setores da indústria.[29]

A divergência nas abordagens americana e europeia está intimamente ligada às diferenças culturais, já que os americanos, ao contrário dos europeus, possuem maior desconfiança do governo, e maior estima ao mercado e tecnologia.[30] Além disso, Europa e Estados Unidos conferem enfoques distintos à privacidade em geral, direito do qual deriva a proteção aos dados pessoais.[31]

No direito europeu, o direito à vida privada possui caráter de direito fundamental e, além de estar disposto na Declaração Universal de Direitos Humanos de 1948 (artigo 12) e na Convenção Europeia dos Direitos Humanos de 1950 (artigo 8º), também está expresso na Carta dos Direitos Fundamentais da União Europeia (artigo 7º), que, ainda, prevê, especificamente, o direito à proteção de dados pessoais (artigo 8º), o qual passou, então, ante o caráter de fundamentalidade, a gozar de hierarquia normativa priveligiada no ordenamento jurídico da União Europeia.

Nos Estados Unidos da América, por seu turno, o direito à privacidade (*right to privacy*), não está explicitamente previsto na Constituição e decorre de interpretação jurisprudencial, possuindo, basicamente, três aspectos:

a) o direito de não interferência, ou seja, de ser deixado em paz (*right to be left alone*), desenvolvido por Warren e Brandeis[32], não possuindo status constitucional, que protege o cidadão da "obtenção e disseminação não autorizadas de informações pessoais [...]. Também se inclui nessa modalidade a vedação ao uso comercial não autorizado de aspectos da personalidade, como a imagem e o nome pessoal"[33];

---

[29] FROMHOLZ, Julia M. The European Union data privacy directive. *Berkeley Technology Law Journal*, v. 15, p. 461, 2000.

[30] O´QUINN, John C. None of your business. *Harvard Journal of Law & Technology*, v. 12, n. 3, p. 683-687, 1999.

[31] FROMHOLZ, Julia M. Op. cit., p. 462.

[32] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review,* v. 4, n. 193, 1890.

[33] SAMPAIO, José Adércio Leite. In: CANOTILHO, J. J. Gomes et al. (Coord.). *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 2013. p. 276.

b) o direito fundamental previsto na quarta emenda Constitucional, que garante ao cidadão a inviolabilidade de sua residência, de seus bens e objetos pessoais em face do Estado; e

c) "o direito de tomar decisões de caráter pessoal ou íntimo (*intimate ou fundamental decisions privacy*) – a defender o indivíduo e a família contra a intromissão estatal nas opções e decisões de natureza reservada ou personalíssima [...]"[34] (*e.g.* aborto[35]).

Esta abordagem fragmentada do direito à privacidade nos Estados Unidos é atribuída à falta de previsão expressa do direito à privacidade na Constituição norte-americana. Tal abordagem, de acordo com Moshell, culmina na inexistência de uma legislação compreensiva a respeito da proteção de dados pessoais, demonstrando a falta de apreço dos Estados Unidos pela regulação abrangente do tema.[36]

Assim, muito embora a afeição pela proteção da privacidade esteja ligada aos regimes liberais, que regra geral optam pela regulação exaustiva da proteção aos dados pessoais derivada do direito à privacidade, nos Estados Unidos – forte pelos ideais liberais – a proteção legal aos dados pessoais mostra-se insuficiente, quando comparada à proteção conferida pela União Europeia, por exemplo, o que parece ser contraditório.[37]

Para Bygrave, essa variação reflete as diferenças em relação ao quanto cada pessoa, nos respectivos países, leva a privacidade em consideração, independentemente de leis sobre o assunto, bem como as percepções das pessoas a respeito do grau de ameaça à privacidade. Segundo o autor, a natureza exaustiva da proteção aos dados pessoais na Europa estaria ligada aos traumas causados pelos relativamente recentes regimes totalitaristas que dominaram alguns de seus países, o que não ocorreu nos Estados Unidos.[38]

---

[34] SAMPAIO, José Adércio Leite. In: CANOTILHO, J. J. Gomes et al. (Coord.). *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 2013. p. 277.

[35] Em 1973, a Suprema Corte Norte-Americana, invocando o direito à privacidade da mulher, decidiu, no caso emblemático Roe versus Wade, que a lei texana que criminalizava o aborto era inconstitucional.

[36] MOSHELL, Ryan. And there was one: the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. *Texas Tech Law Review,* v. 37, p. 373, 2005.

[37] BYGRAVE, Lee A. *Privacy and data protection in an international perspective*. 2010, p. 176. Disponível em HeinOnline.

[38] Idem. p. 176.

Por outro lado, continua o autor, afirmando que outra diferenciação interessante a respeito dos dois regimes diz respeito à percepção do nível dos interesses que competem com a privacidade, tais como segurança pública e nacional, o que pode ser notado pela política regulatória norte-americana após os ataques terroristas de 11 de setembro de 2001.[39]

Ainda, o direito à privacidade na Europa mostra-se mais amplo em escopo do que nos Estados Unidos, pois reflete a necessidade de se assegurar condições necessárias para participação do cidadão na vida pública e na ordem democrática.[40]

Além disso, diferentemente dos Estados Unidos, em que o direito à privacidade é estritamente negativo, reconhece-se na Europa, também, um aspecto positivo a tal direito, de modo que o Estado tem não só o dever de se abster de intervir na privacidade do indivíduo, mas também a obrigação de assegurar tal direito na sociedade.[41]

A despeito de tais diferenciações, inegável que privacidade e proteção de dados são essenciais não apenas para os indivíduos, mas para a manutenção da sociedade civilizada, do pluralismo e da própria democracia.

Contudo, tais diferenças culturais ganham relevo quando se constata que para a União Europeia o direito fundamental à privacidade e à proteção de dados pessoais estaria mais bem protegido por meio de legislação e fiscalização abrangentes, e para os Estados Unidos, em que tais direitos não gozam de caráter fundamental expresso, a regulação setorial e a autorregulação, precipuamente, seriam utilizadas para proteção da privacidade e dos dados pessoais de seus cidadãos.[42]

Portanto, de rigor a análise comparativa de tais regimes regulatórios opostos, com o objetivo de se extrair qual espécie de regulação se amoldaria mais adequadamente à realidade brasileira, considerando as especificidades culturais do País.

---

[39] BYGRAVE, Lee A. *Privacy and data protection in an international perspective*. 2010, p. 177. Disponível em HeinOnline..

[40] Idem. p. 172.

[41] KROTOSZYNSKI, Ronald J. Reconciling privacy and speech in the era of big data: a comparative legal analysis. *William & Mary Law Review,* v. 56, n. 1279, 2015.

[42] TAN, Domingo R. Personal privacy in the information age: comparison of internet data protection regulations in the United States and the European Union. *Loy. L.A. Int'l & Comp. L. J.*, v. 21, p. 681, 1999.

2. Da proteção de dados pessoais na União Europeia

A preocupação com a proteção e confidencialidade das informações pessoais constantes de bancos de dados remonta à metade do século XX, sendo que alguns países, desde a década de 1970, já haviam aprovado leis para tratar do assunto, como, por exemplo, o "Data Protection Act" (que, em suma, proibia a abertura de registros de dados sem permissão oficial e estabelecia um conselho para proteção de dados pessoais, para supervisão de tais atividades), aprovado pelo governo sueco, em 1973, e o "Privacy Act" (que, em síntese, proibia a divulgação de informações pessoais por agências governamentais sem o prévio consentimento da pessoa envolvida) aprovado pelo governo norte-americano, em 1974. Em 1978, normas semelhantes foram adotadas por outros países europeus, como Alemanha e França.[43]

Por sua vez, os primeiros debates a respeito das implicações do desenvolvimento das novas tecnologias para a privacidade dos indivíduos ocorreram entre 1967 e 1968 durante a Assembleia do Conselho da Europa, em que houve menção à insatisfação com a proteção conferida pela legislação nacional dos estados-membros da Comunidade Europeia e destaque à insuficiência da proteção conferida pelo artigo 8º da Convenção Europeia de Direitos Humanos – que trata do direito ao respeito à vida privada – pois tal instrumento foi elaborado em 1950, quando ainda as ameaças a direitos humanos pelas novas tecnologias sequer haviam sido reconhecidas.[44]

Como conclusão destes debates, a Assembleia aprovou uma recomendação e, em 1970, foi produzido um relatório preliminar para examinar o problema, em que se concluiu pela insuficiência de proteção à privacidade em nível nacional e mesmo regional (Europa), motivo pelo qual foram elaboradas recomendações para estados-membros do Conselho da Europa relativas à regulação de bancos de dados operados por empresas privadas.

Contudo, até aquele momento, não existia nenhum instrumento que impusesse aos estados-membros uma obrigação legal de adequada proteção à privacidade dos cidadãos.

---

[43] EVANS, A. C. European Data Protection Law. *The American Journal of Comparative Law*, v. 29, p. 571, 1981.

[44] Ibidem. p. 572.

De qualquer modo, as recomendações e estudos elaborados pelo Conselho da Europa tiveram grande impacto na Comunidade Europeia, que começou a ser pressionada a tomar alguma atitude a respeito da proteção de dados pessoais, reconhecendo a importância do tema, não somente no aspecto econômico, mas também para a proteção de direitos humanos. Então, estudos sobre a possibilidade de aprovação de uma diretiva a respeito do tema começaram a ser realizados.

Sem que houvesse progresso na aprovação da diretiva, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), aprovou, em 1980, uma recomendação contendo orientações sobre proteção da privacidade dos indivíduos e sobre o fluxo transnacional de dados pessoais. Todavia, tais diretrizes não eram vinculantes e não estabeleciam um padrão de proteção mínimo.

Após, numa nova tentativa de estabelecer orientações a respeito da proteção de dados pessoais, o Conselho da Europa, em 1981, adotou a Convenção n. 108 para a proteção dos indivíduos com respeito ao processamento automático de dados pessoais, contendo princípios básicos muito similares às diretrizes da OCDE. Tal convenção foi ratificada por todos os estados-membros da Comunidade Europeia[45], contudo, o Conselho não possuía o poder de forçar os países a implementarem a convenção por meio de legislação nacional.

Apesar da não vinculação e da dificuldade de implementação, a importância desses instrumentos para a ordem jurídica foi inegável. De acordo com Doneda, tais documentos apresentaram um rol de medidas que passou a ser encontrado no núcleo de diversas normativas que vieram a tratar da proteção dos dados pessoais, medidas estas conhecidas como "Fair Information Principles". Para o autor, tais princípios formam um núcleo de questões que, necessariamente, devem ser objeto de análise por um ordenamento jurídico quando do tratamento da matéria. Vale elencar os princípios, tais como citados pelo autor[46]:

> a) Princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público,

[45] HANDBOOK on European Data Protection Law. p. 16. Disponível em: <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Handbook.pdf>. Acesso em: 14 nov. 2015.

[46] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Joaçaba,* v. 12, n. 2, p. 100-101, 2011.

> seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos"; b) Princípio da exatidão: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade; c) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade); d) Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos; e) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Portanto, foi relevante a contribuição da Convenção e das Diretrizes da OCDE, em termos de proteção de dados pessoais, sendo que suas disposições e princípios influenciaram e impulsionaram a elaboração de leis nacionais pelos estados-membros. Porém, tais normas, que continham expressões vagas, não apresentavam uniformidade, pois alguns países da União Europeia já possuíam leis que tratavam do assunto antes mesmo da aprovação da convenção e das diretrizes, inclusive, com níveis mais elevados e diferenciados de proteção.[47]

[47] EVANS, A.C. European Data Protection Law. *The American Journal of Comparative Law*, v. 29, p. 580-581, 1981.

Desta feita, considerando essa diversidade de tratamento à proteção dos dados pessoais pelos estados-membros, a harmonização tornou-se imperiosa, motivo pelo qual, em 24 de outubro de 1995, foi editada a Diretiva para Proteção de Dados Pessoais (DPD).

A diretiva, portanto, constitui o texto de referência em termos de proteção de dados pessoais, instituindo um quadro regulamentar com vistas a equilibrar os níveis de proteção da vida privada dos indivíduos e a livre circulação dos dados pessoais no âmbito da União Europeia. Ainda, a diretiva fixou limites estritos para a coleta e utilização de dados pessoais, demandando, também, a criação de uma autoridade nacional independente incumbida do controle de todas as atividades que dependam do tratamento de dados pessoais.[48]

Como todas as diretivas europeias, a DPD é vinculativa quanto aos seus objetivos, porém, como norma de caráter secundário, dependia da aprovação de leis nacionais, pelos estados-membros. No caso da citada diretiva, contudo, até 25 de outubro de 1998, todos os estados-membros haviam aprovado legislação nacional implementando as provisões constantes da norma para fins de proteção do direito à privacidade dos indivíduos e para prevenção da disseminação não autorizada de informações pessoais dos cidadãos, na União Europeia e fora dela.

Vale destacar que a aplicação da DPD se estende para além dos 28 estados-membros, abrangendo, inclusive, países que são partes da área econômica europeia, tais como, Islândia, Liechtenstein e Noruega.[49]

A DPD propõe uma normatização abrangente englobando todos os setores, sejam públicos ou privados, e todos os níveis de coleta e uso de dados pessoais. Porém, de fato, o foco da diretiva está no setor privado, pois prevê exceções generosas em relação ao setor público. Nesta esteira, a diretiva não se aplica a atividades relativas à segurança pública, defesa e segurança do Estado, bem como à esfera criminal (art. 3º, 2, da Diretiva 95/46/CE). Ainda, de acordo com o artigo 13 da citada norma, os estados-membros podem restringir sua aplicação, adotando medidas legislativas, quando tais limitações forem necessárias à proteção da segurança nacional etc.[50]

---

[48] Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:l14012>. Acesso em: 13 nov. 2015.

[49] HANDBOOK on European Data Protection Law. p. 17. Disponível em: <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Handbook.pdf>. Acesso em: 14 nov. 2015.

[50] LYNSKEY, Orla. *The foundations of EU Data Protection Law.* Oxford: Oxford University Press, 2015. pp. 20/21.

A DPD protege os direitos fundamentais e liberdades das pessoas naturais, e em particular, o direito à privacidade destas no que concerne aos dados pessoais (art. 1º, 1, da Diretiva 95/46/CE).

Nos termos da norma, a expressão dados pessoais abrange informação relacionada a uma pessoa identificada ou identificável que pode ser reconhecida, direta ou indiretamente, por referencia a um número de identificação ou um ou mais fatores específicos ligados à sua identidade social, física, mental, econômica, fisiológica, cultural ou social (art. 2º, a, da Diretiva 95/46/CE).

O processamento ou tratamento de dados pode ser definido como qualquer operação relativa a dados pessoais, ainda que não seja feita por meios automatizados, tais como coleta, gravação, organização, armazenamento, adaptação ou alteração, etc. (art. 2º, b, da Diretiva 95/46/CE).

Uma exceção importante da aplicabilidade da DPD ocorre no âmbito doméstico, pois o uso meramente particular dos dados pessoais está inserido na esfera de proteção da privacidade do indivíduo (art. 3º, 2, da Diretiva 95/46/CE).

Em suma, toda informação pessoal utilizada deve obedecer aos seguintes princípios relativos à qualidade dos dados (art. 6º, a-e, da Diretiva 95/46/CE):

> a) Dados pessoais devem ser processados de forma leal e de acordo com a lei, com a divulgação do responsável ("controller") pelo tratamento de tais dados, bem como do propósito da coleta;
>
> b) Dados pessoais devem ser coletados para fins específicos, explícitos e legítimos, vedado o processamento posterior incompatível com tais propósitos;
>
> c) Dados pessoais devem ser adequados, pertinentes e não excessivos em relação ao propósito para o qual foram coletados;
>
> d) Dados pessoais devem ser exatos e, se necessário, atualizados, apagados ou retificados;
>
> e) Dados pessoais devem ser conservados de forma a permitir a identificação dos indivíduos, apenas, pelo período necessário ao atingimento das finalidades para as quais foram recolhidos.

De acordo com a DPD, em síntese, o tratamento de dados será lícito: a) se contar de forma inequívoca com o consentimento do indivíduo; b) se o tratamento for necessário para a execução de um contrato do qual o indivíduo seja parte; c) se o tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; d) se o tratamento for necessário para a proteção de interesses vitais da pessoa em causa; e) se 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; f) se o tratamento for necessário para perseguir interesses legítimos do responsável pelo tratamento ou do terceiro a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa (art. 7º da Diretiva 95/46/CE).

De rigor ressaltar que a DPD proíbe o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual do indivíduo. Essa disposição comporta exceções, por exemplo, a casos em que haja o consentimento da pessoa ou, ainda, em que o tratamento seja necessário para proteger interesses vitais da pessoa em causa (art. 8º da Diretiva 95/46/CE).

Conforme ditam os artigos 12 e 14 da DPD, a pessoa cujos dados são tratados possui os seguintes direitos:

> a) o direito de acesso aos dados: o responsável pelo tratamento deve fornecer ao indivíduo, sem custos e em prazo razoável, informações que lhe digam respeito, como, por exemplo, a forma de tratamento, o destino e a origem dos dados pessoais;
>
> b) o direito de retificação ou eliminação de dados pessoais: todas as pessoas em causa têm o direito de obter do responsável pelo tratamento a retificação ou mesmo eliminação dos dados utilizados, quando incompletos, inexatos ou contrários às disposições da diretiva;
>
> c) o direito de oposição ao tratamento de dados: a pessoa em causa tem direito de se opor, por motivos legítimos, a que os dados que lhe digam respeito sejam objeto de tratamento. Também, possui

> direito de se opor, a seu pedido e gratuitamente, ao tratamento de dados para fins de mala-direta. Ainda, deve ser informada antes de os dados serem comunicados a terceiros e ter o direito de se opor a essa comunicação.

No que concerne à segurança, o artigo 17 da DPD determina que os estados-membros implementem medidas para proteger os dados pessoais contra "a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito". Ainda, tais medidas, devem levar em conta a natureza dos dados objeto de proteção e os riscos que o tratamento apresenta.

Com vistas à efetivação da proteção dos dados pessoais, a DPD exige que os estados-membros criem remédios judiciais para defesa do indivíduo que tenha seus direitos à privacidade violados (art. 22 da Diretiva 95/46/CE). Ainda, competirá aos estados-membros a adoção de medidas adequadas para a aplicação de sanções em caso de violação das disposições da DPD (art. 24 da Diretiva 95/46/CE).

De se ressaltar que um aspecto interessante e, potencialmente crítico da DPD, reside na questão envolvendo a transferência de dados para países que estão fora da União Europeia. De acordo com a DPD, tal transferência somente poderá ocorrer se o país recebedor da informação dispuser de um "nível adequado de proteção" (art. 25, 1, da Diretiva 95/46/CE), demandando análise casuística da questão.

Assim, o nível adequado de proteção é determinado pela Comissão Europeia, de acordo com os critérios estabelecidos na DPD, que levam em consideração fatores relativos à natureza, propósito e destinação dos dados, à duração do processamento, bem como quais os países de origem e de destino e as leis em vigor no terceiro país, a respeito do tratamento de dados pessoais (art. 25, 2, da Diretiva 95/46/CE).

Tal exigência foi objeto de crítica, por suas implicações internacionais[51] e tem grande impacto na economia global, pois não são

[51] A diretiva também traz implicações internacionais – além de meras complicações decorrentes de imposição de seus princípios – na medida em que sugere uma tentativa da União Europeia em exercer jurisdição sobre atividades estrangeiras (MOSHELL, Ryan. And there was one: the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. *Texas Tech Law Review,* v. 37, p. 462, 2005. (tradução livre)).

todos os países que dispõem de níveis adequados de proteção aos dados pessoais.

De acordo com a Comissão Europeia[52], somente Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça, Uruguai e os Estados Unidos (de acordo com os princípios do "Safe Harbour", como será visto no capítulo próprio[53]) dispõem de nível adequado de proteção, na atualidade.

O receio da proibição de transferência de dados a terceiros países que não possuem nível adequado de proteção aos dados pessoais, com grandes repercussões econômicas, encorajou países, com a Letônia e a Noruega, a adotar medidas de proteção similares às da União Europeia.[54]

Vale destacar que o artigo 26, 2, da DPD, estabelece uma exceção à exigência de adequação, possibilitando soluções *ad hoc*, por meio, por exemplo, da criação de acordos entre as partes, para fins de preencher as lacunas e assegurar a proteção integral da privacidade dos indivíduos. Nesse aspecto, a Comissão Europeia aprovou modelos de contratos para auxiliar os responsáveis pelo processamento de dados.[55]

Ainda, a DPD prevê a criação de uma autoridade supervisora pelos estados-membros, para fins de proteção dos dados pessoais, com vistas à fiscalização da aplicação de suas regras, investida, também, em poderes de intervenção nas organizações violadoras das normas de proteção, bem como de investigação, entre outros (art. 28 da Diretiva 95/46/CE).

Além dessa autoridade supervisora de abrangência interna de cada estado-membro, a União Europeia aprovou o Regulamento n. 45/2001, que criou uma autoridade supervisora independente para monitorar a

---

[52] Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>. Acesso em: 13 nov. 2015.

[53] "No dia 06 de outubro de 2015, o Tribunal de Justiça da União Europeia invalidou a decisão da Comissão Europeia sobre as relações UE – US Safe Harbour. Em 06 de novembro de 2015, então, a Comissão Europeia adotou a Comunicação sobre a transferência de dados pessoais da União Europeia para os Estados Unidos da América ao abrigo da Directiva 95/46/CE, na esteira da decisão proferida pela Corte de Justiça no caso C- 362/14 (Schrems). O objetivo é fornecer uma visão geral das ferramentas alternativas para transferências de dados transnacionais na ausência de uma decisão a respeito da adequação". Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>. Acesso em: 13 nov. 2015.

[54] MOSHELL, Ryan. And there was one: the outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection. *Texas Tech Law Review*, v. 37, p. 388-390, 2005.

[55] Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm>. Acesso em: 13 nov. 2015.

aplicação da DPD em todas as instituições da Comunidade Europeia, em nível regional.[56]

Cumpre citar que em 7 de dezembro de 2000 foi aprovada a Carta dos Direitos Fundamentais da União Europeia, que passou a ter caráter vinculante, após a assinatura do Tratado de Lisboa, em 1º de dezembro de 2009. A Carta, além da garantia de respeito à vida privada, estabeleceu o direito à proteção de dados pessoais (artigo 8º), conferindo a este a qualidade de direito fundamental, aplicável retroativamente, inclusive.[57]

De todo o exposto, é possível concluir que a DPD é o instrumento central de proteção de dados na União Europeia, com reflexos, inclusive, transnacionais. Sensível, ainda, o caráter compreensivo da legislação europeia, que estabelece regras gerais e muito estritas para o tratamento de dados pessoais, exigindo que a finalidade deste tratamento seja legítima. Além disso, as pessoas ou os órgãos responsáveis pela recolha e processamento de dados pessoais têm a obrigação de evitar que tais informações sejam utilizadas de forma incorreta, devendo respeitar os direitos relativos aos proprietários dos dados, consagrados na legislação europeia.

Ademais, a harmonização do assunto, por meio de uma regulamentação comum, evita a existência de regulamentação contraditória nos diferentes países da União Europeia, assegurando que os dados pessoais são salvaguardados por níveis de proteção elevados.

Em suma, pode-se dizer que a proteção mais abrangente dos dados pessoais visa, além de remediar injustiças dos regimes totalitaristas do passado como apontado no capítulo anterior, promover o comércio eletrônico, por meio de criação de regras uniformes e, principalmente, proteger a expectativa dos cidadãos em relação à privacidade de seus dados pessoais.

Além disso, a DPD tornou-se referência internacional. Desse modo, para garantir que as leis sejam consistentes com os padrões europeus, muitos países, como a Argentina, por exemplo, estão adotando leis baseadas nos princípios e normas da Convenção do Conselho da Europa e da Diretiva de Proteção de Dados da União Europeia, para assegurar que o comércio transnacional não seja afetado pelos requisitos da DPD.

---

[56] Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF>. Acesso em: 14 nov. 2015.

[57] HANDBOOK on European Data Protection Law. p. 21. Disponível em: <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Handbook.pdf>. Acesso em: 14 nov. 2015.

De rigor ressaltar que, em 2015, a DPD completou vinte anos e, três anos antes, em 2012, a Comissão Europeia propôs uma reforma geral das regras de proteção dos dados pessoais atualmente em vigor. Ora, a rápida evolução tecnológica das últimas décadas impôs novos desafios à proteção dos dados pessoais dos cidadãos, em especial quando se tem em conta o aumento do compartilhamento e utilização de informações, numa escala global, inclusive. Vale destacar que a integração econômica e social na era informacional, incrementada pelo uso da internet, implicou, também, no aumento da circulação transnacional de dados pessoais, devendo ser adotado um nível de proteção compatível para resguardo da privacidade dos indivíduos.

Além disso, considerando o caráter vinculante atribuído à Carta dos Direitos Fundamentais, após a assinatura do Tratado de Lisboa, em 2009, a União Europeia passou a ter base jurídica específica para adotar legislação destinada à proteção de dados pessoais, direito este de caráter fundamental.

Assim, em meados do mês de dezembro de 2015, a Comissão Europeia, atendendo a um apelo de cerca de 90% da população da Europa, chegou a um acordo sobre o tema, dando início ao chamado Mercado Único Digital, com a harmonização oficial do nível de proteção conferido aos dados pessoais, por meio da criação de uma normatização pan-europeia. O texto final do regulamento deverá ser formalmente adotado pelo Parlamento Europeu e pelo Conselho no início de 2016, e as novas regras se tornarão aplicáveis após dois anos da aguardada adoção formal.[58]

As novas normas têm por escopo reforçar a confiança dos consumidores nos serviços on-line, com o objetivo de impulsionar o crescimento, o emprego e a inovação na Europa, colocando fim à atual fragmentação e, assim, gerando redução de custos para as empresas, com a simplificação e racionalização das regras de proteção em toda a Europa.

A atualização proposta pela Comissão visa modernizar os princípios consagrados na diretiva de 1995. As principais mudanças incluem: a) um conjunto único de regras de proteção de dados, válido em toda a União Europeia, com a redução de custos administrativos; b) o aumento da responsabilidade e prestação de contas para o tratamento de dados pes-

[58] Disponível em: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>. Acesso em: 13 fev. 2016.

soais por parte das empresas; c) a sujeição das organizações a uma única autoridade nacional de proteção de dados, no país da União Europeia onde tem o seu estabelecimento principal; d) a possibilidade de o indivíduo procurar a autoridade de proteção de dados de seu país, mesmo quando os seus dados são processados por uma empresa sediada fora da União Europeia; e) o reforço da necessidade de consentimento explícito para o processamento de dados; f) fácil acesso dos indivíduos aos seus próprios dados e a possibilidade de transferência de seus dados pessoais de um prestador de serviço para outro com mais facilidade (direito à portabilidade dos dados), alavancando a concorrência entre os serviços; g) expressa previsão ao direito ao esquecimento, com o objetivo de ajudar as pessoas a gerenciar melhor os riscos de proteção de dados on-line; h) a necessidade de aplicação das regras da União Europeia aos dados pessoais tratados no exterior por empresas que atuem no mercado e ofereçam os seus serviços aos cidadãos europeus; i) o reforço dos poderes conferidos às autoridades independentes de proteção de dados nacionais, com a possibilidade de aplicação de multas elevadas àquele que violar as regras, e j) a necessidade de aplicação dos princípios e das regras de proteção de dados em geral para a cooperação judiciária em matéria penal e policial, inclusive em nível transnacional.

Como se nota a novel legislação, além de simplificar os procedimentos para as empresas, tem por objetivo primordial reforçar a proteção da privacidade do cidadão europeu, por meio de uma regulamentação ainda mais estrita do tema, de forma que não houve mudança no modelo de regulação adotado, ou seja, a União Europeia confirmou sua preferência por uma regulamentação compreensiva do tema, como forma de ampliar a proteção conferida ao cidadão.

Todavia, considerando a *vacatio* de dois anos, ou seja, considerando que a atual diretiva ainda está em vigor e foi mantida em parte substancial, bem como o fato de que os Projetos de Lei brasileiros para fins de proteção de dados pessoais, no geral, basearam-se na diretiva de 1995, ora estudada, este artigo manterá o foco nesta última legislação.

Superada esta questão referente à atualização legislativa, vale anotar que a adoção de um regime compreensivo de regulação da proteção de dados pessoais mostra-se recomendável e, da análise dos projetos de lei em trâmite, é possível dizer que o Brasil caminha nesse sentido.

Antes, porém, analisemos o regime regulatório norte-americano.

3. Da proteção de dados pessoais nos Estados Unidos da América

De início, é impositivo relembrar que, conforme já observado acima, entende-se, atualmente, que nos Estados Unidos da América, o direito à privacidade (*right to privacy*), não está explicitamente previsto na Constituição, mas decorre de interpretação jurisprudencial, revelando-se como: a) o direito de não interferência, ou seja, de ser deixado em paz (*right to be left alone*); b) o direito fundamental previsto na quarta emenda Constitucional, que garante ao cidadão a inviolabilidade de sua residência, de seus bens e objetos pessoais em face do Estado, e c) "o direito de tomar decisões de caráter pessoal ou íntimo" (*intimate ou fundamental decisions privacy*).

Para melhor compreensão do tratamento dado ao tema pelo direito norte-americano, necessário se faz delinear pequena introdução histórica acerca do direito à privacidade.

Até o ano de 1890, nenhuma corte inglesa ou americana havia reconhecido o direito de privacidade. No final desse ano, Warren e Brandeis publicaram um artigo intitulado "O direito a privacidade" (*"The Right to Privacy"*), que se tornaria clássico no tratamento jurídico do direito à privacidade nesses países. Nesse texto inaugural, o direito à privacidade seria espécie do gênero do "direito a ser deixado sozinho" (*"right to be left alone"*). Os autores indicaram que, no passado, para proteger esse gênero de direito, os tribunais valeram-se de uma combinação de diferentes doutrinas da *common law*, tais como a de difamação (*defamation*), de quebra de confiança (*breach of confidence*) e de contrato implícito (implied contract). Entretanto, os autores entenderam que essa combinação de doutrinas destinadas à proteção de outros direitos não era suficiente para as demandas criadas por inovações tecnológicas e novos modelos de negócio, que passavam a indicar a necessidade de um novo direito, a que eles deram o nome de direito à privacidade. A principal preocupação dos autores, à época, era o risco de que informações a respeito da vida privada de alguém fossem levadas ao conhecimento geral do público (*general public*) por meio da imprensa. Os autores propugnaram pela limitação do direito a privacidade a matérias que tivessem interesse público ou geral.[59]

Aqui vem à tona um tema importante na discussão do direito à privacidade no direito norte-americano. Trata-se de um potencial conflito

[59] ROSS, Anneliese. Data privacy: the American experience. *J.S.Afr. L.*, v. 264, p. 266, 1990.

de direitos, presente em qualquer sistema jurídico, mas de especial sensibilidade no direito norte-americano: de um lado, existe o direito à liberdade de discurso (*freedom of speech*), previsto pelas Emendas Primeira e Décima Quarta, e tão relevantes aos valores norte-americanos; de outro, a preservação de uma esfera privada, que não deve ser exposta, a contragosto, ao público em geral. Com efeito, todo o desenvolvimento do direito à privacidade na história norte-americana será permeado de maneira peculiar pela tensão entre estes dois valores.

A partir da obra de Warren e Brandeis, as legislações estaduais dos EUA passaram a prever o direito à privacidade e os tribunais estaduais passaram a aplicá-lo de forma autônoma, sem precisar se valer de outras doutrinas para, de maneira reflexa, proteger a privacidade por meios não pensados inicialmente para tanto.

Em 1960, a partir de um balanço da aplicação do direito à privacidade na primeira metade do século XX, realizado por Prosser, afirmou-se que a maioria das cortes norte-americanas de alguma forma admitia a existência de um direito à privacidade. Entretanto, para Prosser, emergia dessas decisões o diagnóstico de que não haveria um único ilícito civil (*tort*) de "violação ao direito de privacidade", mas, sim, um feixe de possíveis violações ao "direito de ser deixado sozinho", que quase nada mais teriam em comum do que serem tratadas pelo mesmo nome. Prosser identifica quatro diferentes ilícitos civis (*torts*) tratados sob o nome de "violação ao direito a privacidade", sendo eles: (i) invasão do isolamento voluntário de alguém; (ii) divulgação de fatos embaraçosos a respeito da vida privada de alguém; (iii) publicidade que sujeita alguém a um viés falso e negativo da opinião pública, e (iv) apropriação, com vantagem ilícita, do nome ou aparência de alguém.[60]

O refinamento do direito à privacidade, trazido por essa divisão doutrinária da violação do direito à privacidade entre quatro possíveis ilícitos civis (*torts*), foi muito festejado na academia e igualmente encontrou aplicação nos tribunais. Entretanto, o crescente desenvolvimento de novas tecnologias nas décadas seguintes, em especial a criação dos computadores pessoais e sua interligação por meio da rede mundial de computadores, passou a demonstrar que o direito à privacidade, mesmo com a sofisticação de sua divisão em diferentes ilícitos civis, não era, por si só, suficiente para responder às novas demandas. Exemplificativamente, com relação ao primeiro ilícito civil,

[60] ROSS, Anneliese. Data privacy: the American experience. *J.S.Afr. L.*, v. 264, p. 2676, 1990.

de invasão do isolamento de alguém, ele poderia ser considerado bastante próximo do ilícito praticado quando os dados pessoais de alguém são violados, como no caso da invasão de um banco de dados por um *hacker,* mas não era juridicamente admitido quando se tratava de uso pelo governo de um banco de dados adquiridos de um indivíduo. Com relação ao segundo ilícito civil, de viés negativo e falso a que um indivíduo é exposto perante a opinião pública, a preocupação com relação à proteção dos dados não diz respeito apenas à maneira como é publicada uma informação pessoal, mas vai muito além, preocupando-se com diversas outras questões, tais como, qual informação é coletada, por quem é coletada, de quem e para quê; como ela é armazenada; quem tem acesso a tal informação e sob quais condições tal acesso é garantido. Não se trata apenas da publicação da informação a um público geral, como era a preocupação de Warren e Brandeis no final do século XIX com a imprensa, mas, sim, uma preocupação mais ampla, de maneira que uma informação privada revelada, mesmo a uma única pessoa não autorizada a ter acesso àquela informação, pode ser uma violação de direito. Indo ainda mais além, pode haver violação apenas pela maneira como se armazena informações pessoais de forma não autorizada, por permitir um potencial uso de informação pessoal, ainda que nunca efetivado. Enfim, como se vê dos exemplos, uma proteção à privacidade pensada em um momento histórico pré-internet dificilmente poderia fazer frente a todos os desafios crescentemente trazidos por desenvolvimentos tecnológicos jamais cogitados nas décadas que os antecederam.[61]

Justamente reconhecendo essa necessidade de um estatuto jurídico que tratasse especificamente dos desafios trazidos pela tecnologia ao direito à privacidade, que os EUA, no ano de 1974, promulgam a Lei de Privacidade (*Privacy Act of 1974*).[62] Não se trata da primeira lei federal de proteção à privacidade individual, mas sem dúvida houve um salto de abrangência em seu escopo, especialmente com relação à proteção de dados privados, o que faz com que tal lei mereça menção especial.

Após inúmeras violações ao direito de privacidade cometidos durante a Guerra Fria, tanto pelo governo como por entidades privadas, aumentou a preocupação com a proteção dos dados privados. O estopim de toda essa preocupação foi o escândalo de Watergate, em que

[61] ROSS, Anneliese. Data privacy: the American experience. *J.S.Afr. L.*, v. 264, p. 267-268, 1990.

[62] Disponível o texto integral no site do Departamento de Justiça dos Estados Unidos, acessível pelo lynk: http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf.

cinco pessoas foram presas durante a campanha eleitoral presidencial quando tentavam fotografar documentos e instalar escutas clandestinas no escritório do Partido Democrata. O surgimento de provas de que o Presidente Nixon sabia das operações ilegais na sede do partido adversário o levou a renunciar à Presidência da República em agosto de 1974. Como efeito colateral, o Congresso norte-americano entendeu a necessidade e urgência de adotar uma legislação específica que protegesse a privacidade de dados. Ambas as casas se mobilizaram para que, antes do término da sessão legislativa de 1974, fosse aprovada essa lei.

Como a própria lei anuncia, ela visa estabelecer algumas garantias contra a invasão da privacidade pessoal (*personal privacy*). Para tanto, a lei estabelece que agências federais (*Federal agencies*) devem, a menos quando haja previsão legal específica em sentido contrário, (i) permitir a um indivíduo determinar quais dados pertencentes a ele são coletados, mantidos, usados ou divulgados por estas agências; (ii) permitir a um indivíduo evitar que dados a ele pertencentes, colhidos para determinada finalidade, sejam usados ou disponibilizados para quaisquer outras finalidade, sem seu consentimento; (iii) permitir a um indivíduo ter acesso a informação pertencente a ele nos registros das agências federais, ter cópias integrais ou parciais de tais informações, e corrigi-las ou complementá-las, se necessário. Além disso, as agências federais, pela lei de 1974, devem coletar, manter, usar ou divulgar qualquer informação pessoal identificável, de maneira que assegurem que tal ação era estritamente necessária e com propósito legal; que a informação é atual e acurada, de acordo com a finalidade buscada; e que as devidas garantias são respeitadas, a fim de evitar mau uso da informação. A própria lei admite apenas como exceções aos requisitos por ela elencados, casos em que haja uma importante política pública a fundamentar tal exceção, devidamente previstas as exceções em leis específicas. Além disso, a lei prevê a responsabilidade civil das agências federais que violarem suas disposições e causarem danos aos indivíduos que tiveram seus dados violados.

Como se nota, o âmbito de atuação da Lei de Privacidade de 1974 é bastante restrito. Ela busca proteger uma gravação (*record*) de dados de um indivíduo mantidos em um sistema de gravações (*system of records*) por uma agência federal. Se pegarmos as definições legais dos principais termos, o campo de atuação mostra-se ainda menor, devido às definições restritivas aplicadas. Por exemplo, por gravação (*record*) entende-se "uma informação sobre um indivíduo que é mantida por uma agência [...] que contenha seu nome [...] ou outra identificação

particular". Por sua vez, sistema de gravações (*system of records*) é definido como "um grupo de gravações [...] do qual informação é recuperada, pelo nome do indivíduo ou por algum outro número identificador". Desta maneira, a fim de que um indivíduo possa se valer da proteção legal da lei de 1974, para evitar uma violação de privacidade ou ressarcir-se de um dano causado por uma violação já perpetrada, é necessário que a situação se encaixe nos termos acima. Isto fez com que diversas situações permanecessem desprotegidas com relação a eventuais violações de privacidade. Para citar alguns exemplos, não é protegida pela lei de 1974 a habilidade computacional de pesquisar por atributos e fazer buscas textuais sem usar um identificador pessoal. Além disso, se a informação for acessada de forma aleatória, sem estar mantida em um sistema de gravações previamente ordenado, também sua violação não estaria protegida pela lei de 1974.

Percebe-se, dessa maneira, como, embora a Lei da Privacidade de 1974 tenha representado um inegável avanço na proteção dos dados individuais nos EUA, seu campo de atuação restrito faz com que as situações reguladas por esta lei estejam longe de responder a todos os desafios reguladores trazidos pela criação da rede mundial de computadores e o desenvolvimento exponencial da tecnologia, especialmente naqueles casos em que a ameaça de violação não vem necessariamente de órgãos estatais.

Cerca de dez anos depois do *Privacy Act,* em 1986, advém o *Electronic Communications Privacy Act* (ECPA), que é considerada a legislação de proteção de dados mais abrangente dos Estados Unidos, que salvaguarda as informações pessoais que sejam disponibilizadas na internet. O ECPA abrange todas as formas de comunicação digital, incluindo transmissões de texto e de imagens, bem como transmissão de voz. A referida lei proíbe espionagem não autorizada, tanto pelo governo como por todas as pessoas e empresas. Além disso, proíbe acesso não autorizado de mensagens armazenadas nos sistemas de computador e intercepção não autorizada de mensagens em processo de transmissão.[63]

O ECPA contém inúmeras exceções, como, por exemplo, não assegura os direitos de privacidade de mensagens armazenadas de usuários de sistemas on-line, com relação aos operadores destes sistemas, que têm capacidade para rever todas as mensagens que são transmitidas

[63] TAN, Domingo R. Personal privacy in the information age: comparison of internet data protection regulations in the United States and the European Union. *Loy. L.A. Int'l & Comp. L. J.*, v. 21, p. 671, 1999.

por meio do sistema. Contudo, é ilegal que esse operador de sistema revele as mensagens privadas ou os dados de seus usuários para outras pessoas. Por outro lado, há situações excepcionais em que as mensagens podem ser divulgadas, como, por exemplo, a mensagem enviada para o próprio operador como destinatário. Ou, ainda, as mensagens armazenadas podem ser acessadas por autoridades governamentais, quando o operador acredita que uma atividade ilegal está ocorrendo com o sistema. Mas para a interceptação ou recuperação de mensagens, as autoridades precisam de mandado judicial específico.

Para ter acesso a uma mensagem que está armazenada há menos de 180 dias, em um sistema on-line, o agente governamental precisa obter um mandado judicial. Em contraposição, para ter acesso a uma mensagem armazenada há mais de 180 dias, a autoridade governamental precisa obter apenas uma autorização administrativa. Os operadores de sistema que cooperam com agentes governamentais, que tenham mandados judiciais adequados, estão salvaguardados com relação aos usuários que tenham suas mensagens reveladas ao governo.

Sob a égide do ECPA, os operadores de sistema que violarem a privacidade de seus usuários, como, por exemplo, divulgar publicamente um e-mail privado, podem ser processados diretamente pelos seus usuários. O operador deverá remover a publicação e poderá ser responsabilizado civilmente por qualquer prejuízo material que tenha resultado dessa divulgação indevida. O ECPA ainda autoriza o reembolso de custos com advogado e com o ajuizamento do processo. Isso é principalmente importante porque os custos de se processar uma causa perante o Judiciário estadunidense são muito altos. Há ainda previsão de sanções criminais por violação à referida lei.

Além do *Privacy Act* e do *Electronic Communications Privacy Act*, que indubitavelmente são os mais relevantes na proteção de dados, há outras leis esparsas e específicas de determinados segmentos, que podem ser citadas. Tais como: a) *The Tax Reform Act*, que protege a confidencialidade de informações acerca de restituições de impostos e outros dados relacionados, limitando a disseminação de dados fiscais individuais entre agências federais; b) *Freedom of Information Act*, que regula o acesso de terceiras pessoas a registros mantidos pelo governo; c) *Right to Financial Privacy Act*, que limita o acesso governamental a registros bancários; d) *Fair Credit Reporting Act*, que regula o uso de informações creditícias por agências de crédito; e) *Cable Communications Policy Act*, que exige uma autorização judicial para que o governo possa acessar registros de comunicações via cabo;

f) *Telecommunications Act*, que salvaguarda informações mantidas pelas transmissoras de telecomunicação; g) *Telephone Consumer Protection Act*, que regula práticas de telemarketing; h) *Federal Records Act*, que regulamenta a disposição de registros federais.

Esse é o panorama legislativo da proteção de dados privados no direito norte-americano.

Assim, observa-se que, nos Estados Unidos, diferentemente do modelo europeu, o Estado absteve-se da regulação abrangente da proteção dos dados pessoais, adotando, primordialmente, o sistema da autorregulação por empresas e associações, ressalvadas algumas poucas normas estritamente concebidas para determinados setores da indústria, como aquelas acima mencionadas, optando, assim, por um modelo híbrido de regulação.

Relevante dizer, nesse tocante, que, segundo Caio César Carvalho Lima[64], as discussões mais efetivas acerca da regulamentação do uso da internet tiveram início no começo da década de 1990, exatamente nos Estados Unidos, a partir da Escola Libertária, que expôs suas ideias em Manifesto Libertário de 1994, liderado por John Perry Barlow. Esse movimento defendia que os próprios usuários traçariam as regras aplicáveis (autorregulamentação). Com o passar do tempo, o cenário foi se modificando com o crescente aumento de usuários da internet, passando a se entender que a autorregulação não seria suficiente.

Surgiu, então, a Escola do Direito do Ciberespaço, que teve seu apogeu em 1996, com a edição do livro *Law and borders*, de David Johnson e David Post, em que se defendia que a aplicação do Direito não poderia ir além das fronteiras territoriais, o que também não se mostra suficiente para a regulamentação da internet, que tem como característica a liberdade de tráfego de dados sem limites de fronteira.

Posteriormente, advieram outros movimentos, como a Escola da Arquitetura da Rede, encabeçada por Lawrence Lessing, que sustentava, em síntese, modalidades de regulamentação, entre as quais, a principal delas consistia na ideia de "que os códigos-fonte dos programas de computador (*code* em inglês) seriam aptos a estruturar a arquitetura de rede, por meio da utilização de filtros, bem como de linhas de comando que limitassem a autuação dos usuários, de acordo com as leis

[64] LIMA, Caio César Carvalho. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 149.

vigentes e os interesse dos dirigentes de dada nação".[65] Surgiram, ainda, a Escola do Direito Internacional, que considerava a internet como sendo território internacional, sem fronteiras delimitadas, bem como a Teoria da Aplicabilidade do Direito Vigente, que defende a aplicação do Direito em vigor, não se podendo distinguir o espaço virtual do físico.

Certo é que, a despeito da constante discussão pelos estudiosos do Direito, acerca da regulamentação da internet, nos Estados Unidos, a regulação e intervenção estatal sobre as questões nascidas das relações mantidas no ambiente da internet ainda é ínfima se comparada com outros países, em especial à União Europeia, prevalecendo a autorregulamentação pelos próprios operadores e usuários da internet.

Essa característica de diminuta interferência estatal nas relações nascidas na internet, como dito anteriormente, decorre da própria cultura dos norte-americanos que, em contraposição aos europeus, se qualifica por adotar maior estima ao mercado e à tecnologia.

No que tange à autorregulação, ela pode ser conceituada como o deslocamento da produção regulamentar e normativa para os próprios participantes e interessados diretos na proteção de seus direitos. Parte-se do pressuposto de que "ninguém melhor do que o próprio interessado para saber quais são as lacunas que o Direito deve proteger, quais são as situações práticas do dia a dia que estão sem proteção jurídica e que caminhos de solução viável podem ser tomados".[66]

A vantagem da autorregulação é que possibilita melhor adequação à realidade social, uma vez que as relações no Direito Digital são dinâmicas e se modificam com muita rapidez, permitindo-se, assim, em tese, maior eficácia à regulação criada.

Contudo, apesar de inúmeras empresas que atuam na internet criarem os seus próprios guias de proteção à privacidade (como os denominados "Termos de Uso"), os usuários de internet, o Estado e muitas empresas concordam que os esforços da indústria ainda não são suficientes para saber o que é necessário à efetiva proteção dos dados pessoais de seus usuários.

Essa constatação de que o tratamento jurídico adotado pelos Estados Unidos é insuficiente à proteção dos dados pessoais dos usuários

---

[65] LIMA, Caio César Carvalho. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 149-150.

[66] PINHEIRO, Patricia Peck. *Direito digital*. 5. ed. rev. atual. e ampl., de acordo com as leis 12.735 e 12.737 de 2012. São Paulo: Saraiva, 2013. p. 103.

da internet gera desconfiança na segurança da proteção de dados, principalmente, quando há colheita de dados de usuários residentes em outros países, em especial de países pertencentes à União Europeia.

Isso porque, como já ressaltado, enquanto os Estados Unidos relega a proteção de dados pessoais, primordialmente, à autorregulação, a União Europeia concebe a privacidade de dados como um direito fundamental, com abrangente proteção legislativa.

Outra característica apontada pelos europeus acerca da insuficiência quanto à proteção de dados na internet é a inexistência, nos Estados Unidos, de uma agência independente ("data protection authority" ou "privacy comissioner"), em nível federal, para supervisionar a autorregulação pelas empresas, como existe na União Europeia e em outros países.[67]

Tal diferença ideológica e de mecanismos efetivos governamentais causa, portanto, preocupação aos estados-membros quanto à proteção de dados pessoais, em especial quando há transferência destes dados entre a União Europeia e os Estados Unidos, o que é parcialmente solucionado no artigo 25 da Diretiva 95/46/CE da União Europeia, que entrou em vigor em outubro de 1998.

O referido dispositivo regula a proteção de dados transferidos para países que não façam parte da União Europeia, determinando que esta transferência somente possa ser realizada se referidos países assegurarem nível de proteção adequado, de acordo com os parâmetros estabelecidos pela Comissão Europeia e pelos estados-membros.

Para a manutenção das relações comerciais entre as empresas dos dois territórios, é inevitável que possa ocorrer a colheita e transferência de dados entre eles, já que neles se encontra grande parte da população mundial do mercado de consumo.

O Departamento de Comércio dos Estados Unidos e a Comissão da União Europeia, desde a entrada em vigor da Diretiva, em 1998, passaram a negociar um compromisso de manter a fluência de dados entre os dois territórios, havendo proposta dos Estados Unidos para que companhias americanas voluntariamente se adequem às disposições da Diretiva Europeia, acordando-se o que se denomina de "safe harbour"[68], que

[67] BYGRAVE, Lee A. *Privacy and data protection in an international perspective*. 2010. p. 176. Disponível em HeinOnline.

[68] Disponível em: <http://www.export.gov/safeharbor/>. Acesso em: 13 nov. 2015.

estabelece princípios para proteção de dados pessoais, possibilitando a autocertificação das companhias americanas para acessarem os dados de pessoas que estejam no território europeu, transferindo-os ao território americano. São os seguintes princípios:

> a) Notificação (*Notice*): os indivíduos devem ser informados de que seus dados estão sendo coletados e como serão usados;
> b) Escolha (*Choice*): os indivíduos devem ter a oportunidade de escolher como seus dados pessoais fornecidos podem ser utilizados e se podem ser transferidos para terceiros;
> c) Transferência Progressiva (*Onward Transfer*): quando houver transferência de dados a terceiros, assegura-se que estes terceiros garantem um nível adequado de segurança de proteção de dados;
> d) Segurança (*Security*): devem ser adotados esforços adequados para a prevenção de perda e colheita indevida de dados pessoais;
> e) Integridade de Dados (*Data Integrity*): os dados devem ser relevantes e confiáveis para o propósito pelo qual foram coletados;
> f) Acesso (*Access*): os indivíduos devem ter acesso às informações armazenadas sobre eles, podendo corrigi-las ou deletá-las se forem imprecisas;
> g) Execução (*Enforcement*): a proteção dos dados privados deve incluir mecanismos efetivos e adequados para o cumprimento desses princípios.

Os acordos entre Estados Unidos e União Europeia intensificaram-se nos últimos anos, havendo intenção do Estado norte-americano de maior adequação à legislação europeia. Esse interesse americano decorre, principalmente, da necessidade de se combater o terrorismo, uma das maiores preocupações dos Estados Unidos no que tange às relações internacionais, após os atentados de 11 de setembro de 2001, quando houve o ataque às torres gêmeas do *World Trade Center*, em Nova Iorque. A partir desse marco histórico, nota-se que a apreensão com a segurança nacional passou a superar a falta de interesse governamental na regulação do direito à privacidade, exigindo maior intervenção estatal na proteção dos dados pessoais.[69]

[69] BYGRAVE, Lee A. *Privacy and data protection in an international perspective*. 2010. p. 177. Disponível em HeinOnline.

Contudo, mesmo com a apreensão do governo americano em salvaguardar a segurança nacional a ensejar maior regulação, ainda persistem conflitos ideológicos dos dois territórios, por se considerar que a proteção americana aos dados pessoais permanece insuficiente à legislação abrangente e rigorosa da União Europeia.

Em setembro de 2015, foram publicadas notícias jornalísticas[70] relatando que, após anos de negociações, a União Europeia e os Estados Unidos chegaram a um novo acordo sobre os regulamentos de proteção de dados pessoais, que ainda depende de aprovação do Congresso americano. Segundo foi noticiado, caso seja aprovado, será permitido aos europeus ingressarem diretamente com processos judiciais em tribunais americanos, se houver o uso indevido de dados pessoais, equiparando-os aos cidadãos americanos, neste tocante.

Com o referido acordo, haverá regras mais rigorosas sobre a distribuição de dados a países que não façam parte da União Europeia e sobre o armazenamento excessivo de informações por muito tempo.

Entretanto, após o anúncio do acordo entre os dois territórios, mais recentemente, especificamente em 6 de outubro de 2015, foi prolatada decisão do Tribunal de Justiça Europeu, no processo C-362/14[71], que, ao julgar o caso Maximillian Schrems contra *Data Protection Commissioner* (órgão independente de proteção de dados da Irlanda), em síntese, considerou frágil a autocertificação das companhias americanas pela mera adequação aos princípios do "safe harbour", considerando inválido o referido acordo, firmado há cerca de quinze anos entre os dois territórios, exigindo um processo mais complexo de proteção de dados pessoais, para permitir a transferência dos dados para o território norte-americano.

A referida decisão, indubitavelmente, gerará impactos econômicos e políticos negativos nas empresas norte-americanas que mantêm

---

[70] G1. *UE e EUA chegam a acordo sobre proteção de dados*. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/09/ue-e-eua-chegam-acordo-sobre-protecao-de-dados.html>.
TERRA. *União Europeia e Estados Unidos alcançam acordo sobre proteção de dados*. Disponível em: <http://noticias.terra.com.br/uniao-europeia-e-estados-unidos-alcancam-acordo-sobre-protecao-de-dados,f3314dfd3fdf515dc2afb1ed1399bd4azgupRCRD.html>.

[71] Em suma, o caso teve origem com demanda proposta por Maximillian Schrems, que colocou em cheque a proteção de dados assegurada pelo Facebook, após os escândalos de Edward Snowden, ex-funcionário da Agência Nacional de Segurança (NSA) dos EUA que tornou público o fato de que a referida agência tinha acesso irrestrito a dados pessoais de diversas empresas que se autocertificavam como cumpridoras dos princípios do "safe harbour". (Disponível em: <http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=pt&type=TXT&ancre>).

clientes e usuários que residem na União Europeia, diante da impossibilidade de transferência dos dados pessoais ao território norte-americano, obrigando que as companhias mantenham servidor de dados em território europeu, o que dificultará, provavelmente, as relações comerciais entre eles.

4. Da proteção de dados pessoais no Brasil

Como apontado, o Brasil não possui uma lei específica regulamentando a proteção de dados pessoais, porém, na legislação há menções esparsas sobre o assunto, sendo certo que, de forma genérica, tal proteção pode ser extraída da nossa Lei Maior. Isso porque é inegável que a proteção aos dados pessoais está intimamente ligada ao direito à privacidade, que encontra guarida no rol dos direitos fundamentais da Constituição da República.

A Constituição Federal prevê o direito à privacidade (art. 5º, inciso X), incluindo a inviolabilidade do sigilo de comunicações, de dados e comunicações telefônicas (art. 5º, inciso XII), bem como a garantia de acesso a informações pessoais, e de retificação de dados, constantes de bancos de dados públicos por meio do *Habeas Data* (art. 5º, inciso LXXII), este regulado pela Lei n. 9.507 de 1997.

Insta salientar, contudo, que a interpretação conferida ao inciso XII da Constituição Federal, extraída da Lei n. 9.296 de 1996 não abrangeria os dados estáticos,[72] ou seja, apenas o fluxo de informações estaria protegido pelo mencionado dispositivo constitucional, de modo que a proteção aos dados pessoais estaria abarcada pela previsão genérica constante do inciso X da Constituição Federal.

De rigor mencionar, também, que o citado remédio constitucional (*Habeas Data*), pode ser impetrado somente em face de órgãos públicos e instituições privadas que prestem serviço para o público ou de interesse público.[73] Ainda, na atualidade, tal garantia tem por escopo

[72] Nesse sentido: "não se pode, todavia, confundir dados estáticos – que, aliás, sequer estão protegidos pelo dispositivo constitucional sob comento (veja-se que a Constituição alude à 'comunicação de dados') – com dados em tráfego (excepcionalmente violáveis): há que se distinguir 'banco de dados' do seu 'conteúdo', qual seja, os dados em si – cujo conteúdo se relaciona a crimes [...]" (CANOTILHO, J. J. Gomes et al. (Coord.). *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 2013. p. 293.).

[73] SILVA, José Afonso. *Curso de direito constitucional positivo*. 20. ed. São Paulo: Malheiros, 2002. p. 454.

a preservação da "privacidade e dos dados sensíveis da coletividade, pois com o desenvolvimento de modernos aparelhos tecnológicos e a disseminação da internet abrem-se múltiplas possibilidades de ocorrência de abusos"[74].

Assim, embora de caráter restrito, o referido remédio não deixa de ter relação com a proteção da privacidade e dos dados pessoais, desde que, constantes de bancos de dados governamentais ou de caráter público. É de se dizer que tal garantia seria um desdobramento do princípio insculpido no mencionado inciso X da Constituição Federal, que ora se analisa.

No Brasil, o direito à privacidade, engloba a proteção à vida privada, intimidade, honra e imagem das pessoas (art. 5º, inciso X, da Constituição Federal), sendo considerado direito conexo ao direito à vida.[75] Assim, como na Europa, o direito à privacidade no Brasil comporta interpretação ampla.

Ainda, de rigor mencionar que a Constituição faz distinção entre intimidade e vida privada, sendo a primeira de conteúdo menos abrangente, pois ligada às relações subjetivas da pessoa, no âmbito familiar e de amizades; a segunda abarcaria o conceito da primeira, incluindo, ainda, todos os relacionamentos objetivos (*e.g.* relações comerciais etc.).[76]

De acordo com José Adércio Leite Sampaio,

> [o] direito geral à vida privada desafia uma compreensão muito mais ampla, assentada na própria ideia de autonomia privada e da noção de livre desenvolvimento da personalidade, sem embargo, contida em certos desdobramentos materializantes, como a seguir veremos. Há de se ter presente que tais desdobramentos são produto de uma dada realidade social, econômica e política, percebível pelo pensamento jurídico contemporâneo e, por ele, revelado.[77]

---

[74] AGRA, Walber de Moura. In: CANOTILHO, J. J. Gomes et al. (Coord.). Comentários à Constituição do Brasil. São Paulo: Saraiva, 2013. *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 2013. p. 486.

[75] SILVA, José Afonso. *Curso de direito constitucional positivo*. 20. ed. São Paulo: Malheiros, 2002. p. 205.

[76] MORAES, Alexandre de. *Direitos humanos fundamentais* – teoria geral. 9. ed. São Paulo: Atlas, 2011. p.138.

[77] SAMPAIO, José Adércio Leite. In: CANOTILHO, J. J. Gomes et al. (Coord.). *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 2013. p. 277.

Como visto na primeira parte deste estudo, não restam dúvidas de que a privacidade de um indivíduo pode ser afetada diretamente pelo tipo de tratamento conferido aos seus dados pessoais, o que corrobora a necessidade de regulação da matéria, pois o cidadão tem o direito de ter acesso aos seus dados pessoais, o direito de retificá-los ou excluí-los, de decidir a respeito de seu destino e finalidade etc.

Assim, é possível afirmar que a sociedade da informação impôs uma nova realidade percebível pelo pensamento jurídico contemporâneo, seja do aspecto social, econômico e, inclusive, cultural, de forma que a interpretação alargada do direito à vida privada se mostra necessária, a fim de abarcar a proteção aos dados pessoais, não apenas na esfera governamental, mas também na esfera privada.

A despeito da ausência de previsão específica, é certo que a preocupação com a proteção de dados pessoais, no Brasil, remonta à década de 1980, quando aprovada a Lei n. 7.232/84, que estabeleceu a política nacional de informática.

Referida lei, conquanto limitada ao ambiente informático, em seu artigo 2º, incisos VIII e IX, estabelece como princípios da citada política: a) o "estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas"; b) o "estabelecimento de mecanismos e instrumentos para assegurar a todo cidadão o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas".

Contudo, após o estabelecimento de tais princípios, não há notícias de progresso legislativo no que toca ao assunto, até mais recentemente, como será visto. Cumpre mencionar que, em 1990, o Código de Defesa do Consumidor trouxe previsão específica sobre o direito de acesso e de retificação de dados pessoais, em seu artigo 43 e seus parágrafos. Ainda, o Decreto n. 7.962 de 2013 que regulamenta o citado diploma legal, para dispor sobre o comércio eletrônico, prevê em seu artigo 4º, inciso VI, que o fornecedor deverá utilizar mecanismos de segurança eficazes para tratamento de dados do consumidor. O avanço mais significativo, todavia, se deu com entrada em vigor do Marco Civil da Internet (Lei n. 12.965), em 23 de abril de 2014, vinte anos após a previsão principiológica contida na Lei n. 7.232/84.

Antes de adentrar no estudo dos dispositivos legais do Marco Civil que se referem à proteção da privacidade e dos dados pessoais dos

usuários da internet, é impositivo tecer alguns comentários introdutórios acerca de seu processo de elaboração e aprovação pelo Poder Legislativo.

A finalidade do Marco Civil da Internet foi estabelecer princípios, garantias, deveres e direitos dos usuários de Internet, dos prestadores de serviços e do poder público, o que configurava antiga preocupação legislativa, como se extrai dos inúmeros projetos de lei que tramitavam nas duas casas do Congresso Nacional desde meados da década de 1990. E, exatamente pelo seu conteúdo principiológico, delimitador de diretrizes gerais para a regulação das questões decorrentes da relação entre o direito e a internet, que, atualmente, é conhecido como a "Constituição da internet".

O processo de aprovação do Marco Civil demorou mais de sete anos, desde a concepção até a sua entrada em vigor, caracterizando-se por ter sido concebido em conjunto com a sociedade, com ampla participação popular por meio de debates públicos sobre o tema.[78]

De acordo com a exposição de motivos do Projeto de Lei que deu origem ao Marco Civil, ele teve inspirações no texto constitucional e no conjunto de recomendações apresentadas pelo Comitê Gestor da Internet no Brasil – CGI.br – no documento "Princípios para a governança e uso da Internet" (Resolução CGI.br/RES/2009/003/P).

Mostra-se relevante mencionar o contexto histórico que propulsionou a apreciação pelo Congresso Nacional do Projeto de Lei n. 2.126/2011, de iniciativa da Presidente da República. Extrai-se das informações relativas à tramitação legislativa obtidas junto ao site da Câmara dos Deputados[79] que a referida proposta de lei estava sem movimentação relevante naquela Casa do Congresso, quando ocorreu o escândalo envolvendo Edward Snowden e a *National Security Agency* (NSA), a partir do qual se teve conhecimento de que o Brasil foi alvo de espionagem pelo governo americano, o que ensejou à Presidência de se valer da prerrogativa do artigo 64, § 1º, da Constituição Federal, para, em setembro de 2013, apresentar requerimento de urgência no regime

[78] Os debates com a sociedade civil ocorreram, principalmente, em um blog mantido por plataforma denominada Cultura Digital, uma rede social mantida pelo Ministério da Cultura e pela Rede Nacional de Ensino e Pesquisa – RNP, antes mesmo de se tornar projeto de lei. Após a apresentação da proposta feita pela Presidente da República, o Marco Civil foi colocado novamente em discussão pública, por meio do portal e-Democracia, da Câmara dos Deputados, recebendo inúmeras contribuições.

[79] Disponível em: <http://www2.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em: 13 nov. 2015.

de tramitação do projeto de lei[80], que se tornou, posteriormente, na Lei Ordinária n. 12.965 de 23 de abril de 2014.

O requerimento de urgência na apreciação do projeto de lei foi considerado uma resposta política adequada ao referido escândalo de obtenção não autorizada de dados envolvendo a Agência de Segurança Nacional norte-americana, diante da contradição que se verificou entre o discurso dos Estados Unidos na defesa de princípios democráticos e o comportamento de violação da privacidade de dados sigilosos de países estrangeiros, entre os quais o Brasil.

Além disso, o governo brasileiro passou a defender um Marco Civil internacional, com a adoção de princípios globais para proteção de dados em nível mundial, sendo que diversos países, inspirados no Marco Civil brasileiro, adotaram em leis internas dispositivos do projeto aqui idealizado.

Quase que simultaneamente, o Brasil obteve êxito na aprovação de uma resolução proposta em conjunto com a Alemanha, no âmbito das Nações Unidas, ganhando relevante repercussão internacional, conclamando os Estados a criarem e incrementarem legislação com vistas à proteção da privacidade na era digital.[81]

Diz-se que o Marco Civil é uma lei "pró-inovação" e "pró-direitos", porque, em sua redação original, traz um rol de princípios destinados à proteção de usuários, empreendedores e a própria característica de abertura da internet. Exemplo disso são os seus dispositivos sobre a privacidade, estabelecendo regra universal no sentido de que nenhum dado do usuário pode ser acessado sem ordem judicial prévia, bem como delimitando critérios para que juízes possam autorizar ou não o acesso aos dados pessoais.[82]

De acordo com o Ministro da Justiça José Eduardo Cardozo[83], que participou da elaboração do projeto de lei, o Marco Civil é formado por três pilares: neutralidade de rede, liberdade de expressão e privacidade, sendo certo que, no presente estudo, o que nos interessa, em especial, é o último pilar. Nesse tocante, acrescenta o Ministro, que o

[80] Disponível em: <http://www2.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1132586&filename=MSC+391/2013+%3D%3E+PL+2126/2011>. Acesso em: 13 nov. 2015.

[81] Trata-se da Resolução 68/167, aprovada em 2013, posteriormente atualizada, em novembro de 2014, por meio da Resolução 69/166.

[82] LEMOS, Ronaldo. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 8.

[83] CARDOZO, José Eduardo Martins. Prefácio. In: LEITE. George Salomão; LEMOS, Ronaldo. (Coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014.

tema da proteção de dados pessoais na internet foi abordado pelo Marco Civil, que, partindo da premissa de que as pessoas são titulares de seus próprios dados pessoais, estabelece regras para o consentimento na coleta de dados, exigindo que sejam coletados apenas para a finalidade das atividades prestadas, bem como ressalta a importância da transparência nas políticas de privacidade, entre outras medidas.

Feitas essas considerações, verifica-se que a proteção à privacidade é tratada nos seguintes dispositivos legais da Lei n. 12.965/14: artigo 3º, incisos II e III; artigo 7º, incisos I, II, III, VI, VII, VIII, IX, X; artigo 8º; artigos 10 ao 12; artigo 16, inciso II; e, artigo 23.

O Marco Civil, em seu artigo 3º, incisos II e III prevê expressamente e de forma separada que a disciplina do uso da internet, no Brasil, tem por princípios a proteção da privacidade e a proteção dos dados pessoais, que se dará na forma da lei específica.

Conforme leciona Doneda[84], apesar das similaridades, a menção em separado a tais princípios sugere que a proteção de dados pessoais seria diversa, em termos de objetivos, daquela conferida à privacidade, seguindo a abordagem apresentada pela Carta de Direitos Fundamentais da União Europeia, já estudada.

Ainda, o inciso III do artigo 3º, já sinalizando o âmbito limitado de aplicação do Marco Civil da Internet em termos de proteção de dados pessoais, além de não ofertar definição terminológica a respeito do assunto, relegou à lei específica a regulação exaustiva do tema.

Por outro lado, o artigo 7º do citado diploma legal elenca os direitos dos usuários de internet. Alguns desses direitos, por estarem diretamente ligados ao tema deste estudo, merecem menção específica.

O inciso I assegura aos usuários de internet a inviolabilidade da intimidade e da vida privada, prevendo expressamente direito à indenização pelo dano material ou moral decorrente de sua violação.

O inciso II prevê a inviolabilidade e sigilo do fluxo das comunicações realizadas pela internet, salvo por ordem judicial, na forma da lei.

O inciso III, reforçando a previsão constitucional, estabelece a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial". Considerada a extensão conferida pelo artigo 10, parágrafo 2º, da lei, tal disposição elucida a divergência

[84] DONEDA, Danilo. *Privacy and data protection in the Marco Civil da Internet*. Disponível em: <http://www.privacylatam.com/?p=239>. Acesso em: 15 nov. 2015.

relativa à possibilidade de interceptação do conteúdo da comunicação e não dos dados estáticos, como estudado anteriormente. Isso porque o inciso confere à proteção aos dados armazenados o mesmo grau de proteção outrora conferido à comunicação.

O inciso VI dita que é assegurado o direito a "informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade". De acordo com Doneda,[85] tal inciso, que tem aplicação aos regulamentos de privacidade que regem os serviços ofertados pela internet, deve ser interpretado conjuntamente com o inciso VIII, de forma que as políticas de privacidade ou qualquer termo de uso aplicável a dados pessoais devem ser claros e compreensíveis. Ainda, para Monteiro[86] citado inciso deve ser interpretado em consonância com o inciso XIII, que confirma o entendimento já em vigor de que as normas para a defesa do consumidor aplicam-se às relações de consumo estabelecidas por meio da rede mundial de computadores.

O inciso VII estabelece uma garantia de "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei". Interessante notar que o inciso separa registros de conexão dos dados pessoais, conferindo-lhes âmbitos de proteção distintos, portanto. Ainda, o consentimento é apresentado como um instrumento que o indivíduo pode utilizar para decidir sobre a divulgação ou transmissão de seus dados pessoais a terceiros. Para Monteiro,

> [...] o consentimento livre, expresso e informado, será aquele em que o usuário não é forçado a concordar com os termos do contrato, e as cláusulas que discorrem sobre qualquer tipo de tratamento de dados – inclusive fornecimento a terceiros – deverão ser redigidas de forma destacada, e se possível, separadas das demais.[87]

[85] DONEDA, Danilo. *Privacy and data protection in the Marco Civil da Internet*. Disponível em: <http://www.privacylatam.com/?p=239>. Acesso em: 15 nov. 2015.

[86] MONTEIRO, Renato Leite. Da Proteção aos Registros, aos dados pessoais e às comunicações privadas. In: MASSO, Fabiano del et al. (Coord.). *Marco Civil da Internet*. São Paulo: Revista dos Tribunais, 2014. p. 146.

[87] Idem, p. 149.

O inciso VIII assegura ao indivíduo o direito a "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet". Segundo Doneda, essa disposição indica a adoção de dois princípios, o da transparência e o da finalidade. Assim, há necessidade de que as informações sejam claras e compreensíveis e, ainda, fica vedado o uso dos dados pessoais para outros fins que não aquele previamente autorizado e especificado.[88]

Por sua vez, o inciso IX dispõe a respeito da "necessidade de consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais". Assim, como já apontado o consentimento é imprescindível para o tratamento de dados pessoais e deve ser obtido de forma separada, a fim de facilitar o entendimento do indivíduo.

O inciso X prevê o direito do indivíduo de "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei".

Para Vancim e Neves, o artigo ora estudado deve ser objeto de interpretação ampliativa favorável aos usuários, constituindo "números abertos" de hipóteses inseridas aos direitos dos usuários, o que permite afirmar que outros direitos, não expressamente previstos, mas admitidos pela sistemática da norma, devem ser protegidos e preservados".[89]

De acordo com Ulisses Schwarz Viana[90], os direitos estabelecidos no artigo 7º, em seu aspecto deontológico, podem ser traduzidos como deveres recíprocos entre usuários e provedores do sistema, representando a consagração, no plano infraconstitucional, dos princípios-garantias dos incisos X e XII do artigo 5º da Constituição Federal, que se revelam como potencial fonte de conflito com o direito à liberdade de expressão, mormente diante das características da internet, em que

---

[88] DONEDA, Danilo. *Privacy and data protection in the Marco Civil da Internet*. Disponível em: <http://www.privacylatam.com/?p=239>. Acesso em: 15 nov. 2015.

[89] VANCIM, Adriano Roberto et al. *Marco Civil da Internet*. 2. ed. São Paulo: Mundo Jurídico, 2015. p. 69-70.

[90] VIANA, Ulisses Schwarz. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014. p. 135.

a disseminação de informações e de opiniões ocorre de maneira veloz e abrangente, não se limitando nem mesmo ao território nacional. Acrescenta que, diante do conflito entre o direito à privacidade e à liberdade de expressão na internet, para solucioná-lo, deve-se valer da teoria constitucional da ponderação. Por fim, sustenta que se tem percebido tendência no Supremo Tribunal Federal, à adoção da doutrina *preferred position* que reconhece à liberdade de expressão posição de vantagem quando em conflito com outros direitos fundamentais.[91]

O artigo 8º estabelece em seu *caput* que "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet". Em seu parágrafo único, estabelece-se, de maneira ampla, que são nulas de pleno direito as cláusulas contratuais que violem os direitos garantidos no *caput*, tais como aquelas estabelecidas nos incisos ("que: I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou II – em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil").

Obtempere-se, portanto, que o parágrafo único traz cláusula aberta quanto às hipóteses de nulidade de cláusulas inseridas em contratos relacionados ao acesso à internet, que sejam violadoras do direito à privacidade dos seus usuários, trazendo rol meramente exemplificativo em seus incisos, oportunizando, assim, a declaração de nulidade de outras cláusulas contratuais ofensivas à privacidade.

Os artigos 10 a 12 do Marco Civil da Internet estabelecem meios para proteção dos dados pessoais, dispondo que a guarda e disponibilização destes deve atender à preservação da vida privada, intimidade, honra e imagem das partes direta ou indiretamente envolvidas, bem como que a lei brasileira será aplicável às hipóteses em que o tratamento de dados ocorra em território nacional ou, mesmo em casos de pessoa jurídica sediada no exterior, quando o serviço é prestado ao público brasileiro. Ainda, foram previstas sanções em caso de violação

[91] De acordo com a doutrina da posição preferencial ou "preferred position", em caso de conflito de direitos fundamentais, a liberdade de expressão goza de posição de precedência. Tal teoria foi citada no voto dissidente proferido pelo Ministro Harlan F. Stone da Suprema Corte Norte-Americana, em 1942, no caso Jones versus Opelika, defendendo a posição preferencial das liberdades de expressão e religião contra quaisquer tentativas discriminatórias. No Brasil, o Ministro do Supremo Tribunal Federal, Luiz Fux, no voto proferido na ADPF 187, fez expressa menção a essa teoria, dizendo que o pensamento jurídico brasileiro acolheu tal entendimento, hoje dominante na Suprema Corte Estadunidense.

às suas disposições, sem menção, todavia, a respeito da autoridade competente para aplicá-las.

O artigo 16, por sua vez, nas relações de usuários com provedores de aplicações de internet, seja ela onerosa ou gratuita, veda expressamente a guarda: (i) dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º, e; (ii) de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Assim, sem prejuízo do consentimento do usuário para manutenção de seus dados pelo provedor de internet, não pode haver a guarda de dados além daqueles necessários à finalidade para o qual foram coletados.

Por fim, o artigo 23 estabelece que nos processos de requisição judicial de registros, compete ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar, se for o caso, segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Tais disposições inovaram no ordenamento jurídico nacional, mas ainda não esgotam o tema, principalmente porque se mostraram lacunosas, demandando regulamentação específica, que até o momento não foi objeto de elaboração pelo Poder Legislativo.

Especialmente, quando comparado com a Diretiva Europeia de 1995, que o antecedeu em quase vinte anos, o Marco Civil da Internet revela-se tímido, deixando, por exemplo, de definir o que seriam dados pessoais e sequer distinguindo tal expressão de dados sensíveis. Nem mesmo faz menção aos princípios relativos à qualidade dos dados, previstos na diretiva europeia. Além disso, o citado diploma legal não prevê direito de acesso ou de retificação de dados pessoais, não tratando das transferências internacionais de tais dados, nem dispondo a respeito da criação de uma autoridade supervisora, esta, essencial para a efetivação fiscalização e aplicação do direito fundamental à privacidade.

Também, o Marco Civil da Internet deixa de elencar a totalidade dos já citados "Fair Information Principles", que formam um rol de questões que devem ser objeto de análise por um ordenamento jurídico no que tange à proteção dos dados pessoais. O citado diploma legal foi omisso em relação ao princípio da publicidade, pois não regulou a criação de bancos que tratem de dados pessoais na internet. Da mesma

forma, embora contenha previsão a respeito da exclusão dos dados pessoais de bancos de dados, com o término da relação negocial (artigo 7º, inciso X), o Marco Civil da Internet foi lacunoso no que toca ao princípio da exatidão e do livre acesso dos usuários aos ditos bancos de dados. Ainda, conquanto o artigo 10, parágrafo 4º, do Marco Civil faça menção a procedimentos de segurança na guarda e disponibilização de dados pessoais, o fato de o artigo condicionar tal proteção à observância de um regulamento, implica em não atendimento do princípio da segurança. Enfim, pode-se afirmar que o único "Fair Information Principle" suficientemente observado pela Lei n. 12.965/14 foi o princípio da finalidade, disposto no seu artigo 7º, inciso VIII, da mencionada lei.

Como se nota, a despeito do avanço decorrente da elaboração do Marco Civil da Internet, é possível afirmar que a lei é falha e obscura em diversos aspectos relativos à proteção de dados pessoais, não sendo suficiente à ampla proteção do direito fundamental à vida privada, no que se inclui o direito à proteção dos dados pessoais.

Em verdade, contraditoriamente, o quadro legislativo atual não permite ao Brasil sequer dar cumprimento ao estabelecido no artigo 4º da Resolução n. 68/167, proposta pelo próprio País à ONU.

Assim sendo, o simples conceito alargado de privacidade somado a uma legislação esparsa e lacunosa sobre o assunto não se mostra suficiente para evitar abusos e nem supre a expectativa dos brasileiros em relação à proteção de seus dados pessoais.

Com efeito, as recentes violações de dados pessoais noticiadas pela imprensa brasileira despertaram na sociedade a consciência a respeito da importância da proteção de dados pessoais e o cidadão brasileiro tem-se mostrado preocupado com a insegurança gerada pela ausência de regulação do assunto, demonstrando possuir alto grau de consideração por sua privacidade diante de eventual ameaça.

Nesse aspecto, em 2015, foi divulgada pesquisa envolvendo doze países, apontando que o brasileiro, ao lado dos alemães e holandeses, possui grande preocupação com a segurança conferida a seus dados pessoais.[92]

De acordo com o estudo, 53% dos consumidores brasileiros afirmaram ter receio de eventual violação de seus dados pessoais,

[92] Disponível em: <http://assets.unisys.com/Documents/Microsites/UnisysSecurityInsights/USI_150227i_Globalreport.pdf.>. Acesso em: 9 jan. 2016.

demonstrando a sensação de vulnerabilidade do cidadão e, bem assim, a necessidade de regulamentação do assunto.

A ausência de regulamentação específica e compreensiva sobre o tema gera insegurança jurídica – tanto para os usuários quanto para as pessoas jurídicas que, de algum modo, utilizam dados pessoais em suas atividades – inconsistente com o atual estágio da tecnologia e com o volume de coleta e tratamento de dados dos indivíduos.

Vale ressaltar que, ainda, houve tentativa de autorregulamentação do uso de dados pessoais no Brasil. Como exemplo, a Associação Brasileira de Marketing Direito e associações signatárias desenvolveram o texto do Código Brasileiro de Autorregulamentação para Proteção de Dados Pessoais; mas, não há notícias a respeito da efetiva aplicação das normas criadas.[93]

De qualquer modo, como visto, nos Estados Unidos, a experiência da autorregulamentação não se mostrou exitosa, já que naquele país, os cidadãos, o Estado e muitas empresas concordaram que tal modelo não seria suficiente para a efetiva proteção dos dados pessoais de seus usuários, o que gera desconfiança na segurança conferida aos dados pessoais, principalmente, quando há coleta de dados de usuários residentes em outros países, em especial daqueles pertencentes à União Europeia.

Como já aventado, enquanto os Estados Unidos (modelo híbrido) relega a proteção de dados pessoais, primordialmente, à autorregulação, a União Europeia (modelo compreensivo) confere à proteção de dados pessoais o caráter de direito fundamental, com alargada proteção legislativa.

Destarte, a despeito da já abordada vantagem da autorregulação, pois possibilita melhor adequação à realidade social, a reconhecida insuficiência do sistema norte-americano de regulação do uso de dados pessoais, que prioritariamente faz uso de tal modelo, somada às similitudes no tratamento do direito à privacidade no Brasil e na União Europeia, implica na necessidade de se legislar de forma específica e abrangente a respeito do tema, garantindo aos cidadãos brasileiros o mesmo nível de proteção de que gozam os cidadãos europeus, principalmente, quando se têm em conta os avanços tecnológicos das últimas décadas, que maximizam as possibilidades de violação de direitos individuais garantidos pela Constituição.

[93] Disponível em: <http://www.abemd.org.br/pagina.php?id=54>. Acesso em: 9 jan. 2016.

Cumpre destacar que, como na Europa, o Brasil atribui expressamente o caráter de "fundamental" ao direito à vida privada (que, numa interpretação ampla, abarca também a proteção dos dados pessoais), conferindo-lhe, ainda, hierarquia constitucional, diferentemente dos Estados Unidos, que abordam tal direito de forma fragmentada.

De outro lado, o brasileiro tem demonstrado mais apreço à privacidade e mais preocupação com o grau de ameaça a este direito, na era informacional, em especial após o incidente de vigilância em massa envolvendo o governo norte-americano.

Além disso, no Brasil, assim como na Europa, o direto à privacidade possui um caráter positivo, ou seja, além do dever de se abster de intervir na privacidade (aspecto negativo), o Estado também tem o dever de assegurar tal direito.

Em verdade, a semelhança de tratamento conferido à privacidade, no Brasil e na Europa, permite a constatação de que tal direito fundamental, no que se inclui a proteção de dados pessoais, estaria mais bem protegido por meio de legislação e fiscalização abrangentes.

Em síntese, pode-se dizer que a proteção alargada dos dados pessoais, no Brasil, permitirá o resgate da segurança do cidadão quanto ao uso de seus dados pessoais, promovendo, ainda, o comércio eletrônico, por meio de criação de regras uniformes. Ademais, considerando a possibilidade de afetação do comércio transnacional gerada pela adoção da Diretiva Europeia de 1995, atualizada recentemente, necessário, também, que esta lei seja consistente com os padrões europeus, que se mostraram de vanguarda.

Nesse sentido, observa-se que, no geral, os projetos de lei em trâmite se basearam nos nortes ditados pela atual diretiva europeia.

O projeto em trâmite pela Câmara dos Deputados parece ser uma versão resumida da diretiva, sendo omisso em relação à transferência internacional de dados, à autoridade competente e a diversos direitos que estão dispostos nos outros dois projetos.

Já os projetos de lei apresentados pelo Senado Federal e pelo Ministério da Justiça mostram-se mais completos e mais fiéis ao conceito de legislação compreensiva. Em verdade, ao que parece, tais projetos de lei são os mais aptos a sanar as lacunas legislativas existentes no Brasil, trazendo previsões muito semelhantes àquelas contidas na atual diretiva europeia.

Contudo, nenhum dos projetos mencionados cria efetivamente uma autoridade competente para fiscalização do uso de dados

pessoais, o que seria essencial para efetiva fiscalização e aplicação do direito fundamental à privacidade, nos termos do compromisso assumido pelo Brasil junto à ONU (artigo 4º, "d", da Resolução n. 68/167). Segundo o parecer da Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática do Senado Federal, a criação da autoridade nacional supervisora seria de competência da Presidência da República, nos termos do art. 61, parágrafo 1º inciso II, "e", da Constituição Federal.[94]

Enfim, cumpre citar que o projeto do Ministério da Justiça, em seu artigo 50, deixa margem para a autorregulação, quando prevê a possibilidade de criação de regras de boas práticas pelos responsáveis pelo tratamento de dados, demonstrando a possibilidade de convivência do modelo compreensivo e do modelo de autorregulação, com vistas ao aprimoramento da proteção da privacidade do cidadão.

5. Conclusão

O surgimento de novas tecnologias para coleta e tratamento de dados pessoais provocou, paralela e paulatinamente, uma tentativa de resgate à privacidade, o que gerou a necessidade de estabelecimento de um marco regulatório sobre o assunto.

Em muitos países, como no Brasil, por exemplo, as leis não acompanharam a tecnologia, deixando lacunas significativas em termos de proteção de dados pessoais. Assim, com atraso vintenário em relação aos países europeus, o País ainda não possui lei específica que trate do assunto, não atingindo o grau de adequação necessário, como aquele garantido, por exemplo, pela União Europeia e pela Argentina.

Ainda, embora se reconheça a importância do Marco Civil da Internet, por certo, tal lei não confere nível de proteção suficientemente abrangente aos dados pessoais, máxime quando considerada a importância do tema para a sociedade atual.

Vale destacar que o Brasil não dispõe de uma autoridade específica para a proteção de dados pessoais, o que dificulta a fiscalização e aplicação das provisões legais, em especial em caráter preventivo, relegando tal tarefa ao Poder Judiciário, que atua de forma repressiva.

---

[94] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 9 jan. 2016.

Por essa razão, somada ao fato de a legislação sobre o assunto ser esparsa e não específica, o Brasil ganhou nota mínima em termos de proteção aos dados pessoais e fez jus à classificação "limitada", numa escala que parte da proteção "pesada", para a "robusta", seguindo para a "moderada" e, enfim, para a "limitada", de acordo com o grupo DLA Piper´s Global Data Protection and Privacy"[95], o que demonstra que o tema merece ser tratado com seriedade.

Assim, com foco no desenvolvimento tecnológico e regulatório da proteção de dados, este trabalho tentou demonstrar que os quadros legislativos de proteção de dados no Brasil, nos Estados Unidos e na União Europeia são deveras distintos e representam, respectivamente, uma esfera de proteção fraca, média e abrangente.

Ainda, este estudo, distinguindo os sistemas regulatórios opostos utilizados pela União Europeia e pelos Estados Unidos, tentou apontar as vantagens de uma regulamentação compreensiva, que confere, por meio da harmonização, proteção para o cidadão e estímulo às atividades empresariais ou governamentais que fazem uso de dados pessoais.

Vale mencionar que o sistema estadunidense de proteção de dados pessoais é apontado pelos próprios estudiosos norte-americanos como insuficiente para os fins propostos, em especial, quando comparado com o sistema europeu, que proporciona níveis de proteção mais fortes.[96]

Portanto, uma lei específica e abrangente sobre proteção de dados afigura-se necessária para a proteção da privacidade do cidadão brasileiro e para o estabelecimento de segurança jurídica não apenas para os indivíduos, mas também para aquelas pessoas jurídicas que utilizam o tratamento de dados em suas atividades.

Em suma, a elaboração de uma legislação específica para a proteção dos dados pessoais, bem como a criação de uma autoridade autônoma para tratar do assunto, é essencial e inevitável na era informacional, pois, sem a regulamentação e respectiva fiscalização, o titular dos dados estaria vulnerável e não disporia de remédios legais para sanar eventuais danos.

---

[95] DATA Protection Laws of the World. Disponível em: <http://dlapiperdataprotection.com/#handbook/world-map-section>. Acesso em: 10 dez. 2015.

[96] BYGRAVE, Lee A. *Privacy and data protection in an international perspective*. 2010. p. 196-199. Disponível em HeinOnline.

Enfim, analisando-se os projetos de lei em trâmite no País sobre o tema, em geral, foi possível notar que as normas e princípios adotados pela União Europeia são o norte da legislação que está por vir, confirmando o papel vanguardista do velho mundo, e demonstrando a opção do legislador nacional pela regulamentação abrangente e uma tendência à harmonização global do assunto, com base na diretiva europeia, suprindo as lacunas atualmente existentes, conferindo um nível de proteção mais elevado aos dados pessoais e resguardando o comércio transnacional.

Como reconhecido pelo próprio Senado Federal no parecer recentemente aprovado pela Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, relativo ao projeto de lei sobre o assunto,

> [n]ote-se, nesse ponto, o quão defasado está o Estado brasileiro na temática de proteção de dados pessoais. A Europa discute, de forma propositiva, a questão há mais de duas décadas, pelo menos. O Brasil, portanto, não pode mais tardar em editar uma lei que disponha sobre o tratamento dos dados pessoais, assegurando proteção aos cidadãos e oferecendo segurança jurídica às corporações públicas e privadas.[97]

Nesse sentido, espera-se que o legislativo brasileiro compreendendo a importância e relevância do tema para o cidadão, priorize e acelere a tramitação dos projetos de lei que tratam sobre o assunto, em especial, atualizando-os e incorporando, inclusive, os avanços recentes da legislação europeia, na qual se espelham.

Somente uma legislação abrangente protegeria suficientemente o direito fundamental à privacidade, no que se inclui a proteção aos dados pessoais.

Quem ganha é o cidadão, mas não só, pois o estabelecimento de um marco legal compreensivo gera segurança jurídica, alinhando o ordenamento jurídico brasileiro a uma tendência internacional, e os reflexos financeiros são inegáveis.

---

[97] Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 9 jan. 2016.