FUNDAÇÃO GETULIO VARGAS
ESCOLA DE DIREITO FGV DIREITO RIO
GRADUAÇÃO EM DIREITO

AMANDA PIMENTA GIL PROTA

Proteção de dados pessoais e privacidade na Era da Internet:
Análise da legislação brasileira sob a luz da legislação europeia

Rio de Janeiro, 22 maio de 2017

FUNDAÇÃO GETULIO VARGAS
ESCOLA DE DIREITO FGV DIREITO RIO
GRADUAÇÃO EM DIREITO

AMANDA PIMENTA GIL PROTA

Proteção de dados pessoais e privacidade na Era da Internet:
Análise da legislação brasileira sob a luz da legislação europeia

Trabalho de Conclusão de Curso, sob orientação do Professor **Eduardo Magrani** apresentado à FGV DIREITO RIO como requisito parcial para obtenção de grau de bacharel em Direito.

Rio de Janeiro, 22 maio de 2017

FUNDAÇÃO GETULIO VARGAS
ESCOLA DE DIREITO FGV DIREITO RIO
GRADUAÇÃO EM DIREITO

Proteção de dados pessoais e privacidade na Era da Internet:

Análise da legislação brasileira sob a luz da legislação europeia

Elaborado por

AMANDA PIMENTA GIL PROTA

Trabalho de Conclusão de Curso apresentado à FGV DIREITO RIO como requisito parcial para obtenção de grau de bacharel em Direito.

Comissão Examinadora:

Nome do orientador: Eduardo Magrani

Nome do Examinador 1: Carlos Affonso Souza

Nome do Examinador 2: Luca Belli

Assinaturas:

_____

Eduardo Magrani

_____

Carlos Affonso Souza

_____

Luca Belli

Nota Final: _____

Rio de Janeiro, _____ de maio de 2017.

RESUMO

Este artigo é o resultado de um estudo analítico entre a legislação brasileira e europeia sobre o tema da privacidade e proteção de dados pessoais. O referido artigo surgiu devido à crescente complexidade e relevância do tema, através da criação e intensificação de novas tecnologias na Sociedade de Informação, bem como pela inexistência de lei no ordenamento jurídico brasileiro atual que regulamente a matéria de forma específica.

Dessa forma, com a presente pesquisa aqui desenvolvida e analisada objetiva-se *(i)* demonstrar como o ordenamento europeu e brasileiro tratam o direito à privacidade e proteção de dados pessoais; *(ii)* verificar o desenvolvimento da matéria no Brasil e na Europa; *(iii)* examinar as similaridades e divergências do sistema europeu e brasileiro, através da análise dos projetos de lei sobre dados pessoais ainda em tramitação e o recém criado Regulamento 679 da União Europeia e *(iv)* expor sobre a necessidade de criação de lei geral sobre a proteção de dados e os elementos básicos e essenciais a serem abordados na referida lei.

Palavras-chave: Proteção de dados. Dados pessoais. Privacidade. Internet. Legislação Brasileira. Legislação Europeia. Regulamentação. Projetos de Lei.

ABSTRACT

This article is the result of an analytical study between Brazilian and European legislation on the subject of privacy and personal data protection. This article arose due to the increasing complexity and relevance of the theme, through the creation and intensification of new technologies in "Information Society Era", as well as the current absence of law in Brazilian legal system, which regulates specifically the matter.

Therefore, the current research hereunder developed and analyzed aims to *(i)* demonstrate how the European and Brazilian law treat the right to privacy and personal protection data; *(ii)* verify the development of the matter in Brazil and in Europe; *(iii)* examine the similarities and differences between the European and Brazilian systems, by analyzing the ongoing draft legislation regarding personal data and the newly created Regulation 679 of the European Union and *(iv)* present the need for creation of a general law on data protection, as well as the basics and essential elements to be addressed in said law.

Keywords: Data protection. Personal data. Privacy. Internet. Brazilian legislation. European legislation. Regulation. Draft of Bill.

AGRADECIMENTOS

Impossível terminar mais uma etapa da minha vida sem agradecer à toda minha família, em especial ao meu pai Klinger e à minha mãe Cristiane, que me permitiram ser tudo o que sou.

Agradeço também aos meus amigos que sempre permaneceram ao meu lado durante toda essa jornada de 5 árduos anos.

Agradeço ao meu namorado, Reinhard, pelo amor e apoio incondicional e pela ajuda crucial nas aulas em alemão de "Datenschutzrecht", inspiração para o presente trabalho.

Por fim, mas não menos importante, obrigada todo o corpo docente da FGV Direito Rio, em especial, meu mestre orientador, Eduardo Magrani, pelas incontáveis horas dedicadas a este projeto, pelo apoio e suporte fundamental, e por ser para mim um exemplo de profissional e excelência acadêmica.

Sem todos vocês nada disso seria possível.

SUMÁRIO

INTRODUÇÃO

O fenômeno denominado “sociedade da informação” representa a intensificação nas trocas de informações, devido a, sobretudo, inovações tecnológicas e digitais. A Internet, como conjunto de redes de computadores interligados, que se comunicam através de protocolo comum 1, permite a seus usuários uma troca de dados ativa e instantânea, criando uma verdadeira rede de pessoas e comunidades2.

Mais do que isso, a internet se encontra nos dias atuais em uma nova fase intitulada de internet das coisas (Internet of Things ou IoT). O conceito de internet das coisas pode ser compreendido como a habilidade de objetos físicos, presentes em nosso cotidiano, de se conectar à internet e de receber e transmitir dados[3]. Os “smart watches” e elaborados fitness trackers podem ser citados como exemplo da IoT. Estima-se[4] que o número de dispositivos e aparelhos móveis tenha superado o número de pessoas na terra[5]. Destarte um dos desafios trazidos pela IoT é justamente encontrar o equilíbrio entre a tênue linha da ampliação da inovação e da preservação da privacidade.

Nesse cenário, é produzida diariamente na internet uma quantidade devastadora de dados, dentre eles os de caráter pessoal. De acordo com pesquisa revelada pela Forbes Brasil[6], o volume de dados criados nos últimos dois anos é maior que a quantidade produzida em toda a história, permitida pela IoT e pelo fato da população conectada à internet ter crescido em mais de 60%7. No Brasil, nove a cada dez pessoas utilizam um smartphone para acessar a internet, sendo o tempo médio gasto online pelos usuários de 11 horas semanais[8]. Essa densa quantidade de dados é chamada de Big Data. Entretanto, importante ressaltar que o fenômeno do Big Data não só nos chama atenção pelo volume de dados coletados, mas também pela velocidade de armazenamento, e pela variedade e complexidade dos dados. Nesse sentido, a questão central acerca da coleta de dados ultrapassa a simples preocupação sobre o volume e se transporta para

---

[1]How the internet works em: The EDRi papers. Edição 03. 2012. Pp. 3 Et. Seq.

[2] NICbrvideos. Internet das Coisas, explicada pelo NIC.br. Disponível em youtube: https://www.youtube.com/watch?v=jlkvzcG1UMk

[3]FTC Staff Report Internet of Things: privacy & security in a connected world. Pp. 5 Et. Seq. Disponível em: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[4] Idem.

[5] Disponível em: http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

6 Disponível em: http://www.forbes.com.br/fotos/2015/10/20-fatos-sobre-a-internet-que-voce-provavelmente-nao-sabe/

7Disponível em: https://www.domo.com/blog/data-never-sleeps-4-0/

8 Disponível em: http://exame.abril.com.br/tecnologia/estudo-desvenda-habitos-de-consumo-de-internet-na-america-latina/

a utilização e finalidade de tais dados. Esses dados são muitas vezes utilizados por empresas, com finalidades comerciais e estratégicas. Tal prática, conhecida como "*behavioural advertising*" ou "*behavioural targeting*" é usada através do rastreamento das atividades do usuário na web. Por meio dessas atividades, é possível identificar quais os interesses do usuário, criar e traçar seu perfil de uso na internet e direcionar publicidade de forma mais eficiente[9]. Contudo, o uso desses dados não se limita a companhias privadas, sendo o Poder Público também um (potencial) usuário[10]. Segundo relatório da McKinsey, de 2015, dados e informações geram mais valor econômico que o comércio internacional de bens[11]. Daí se compreende a expressão de que "os dados são o novo petróleo"[12].

A questão da privacidade, como um direito humano e fundamental, se encontra ainda mais fragilizada nesse contexto, pois o usuário ao conceder e gerar tais informações e dados se expõe e queda-se desprotegido, muitas vezes sem ter a real consciência disso. Nos EUA já existem, pelo menos, dois projetos de lei que visam regular, através do governo, as práticas de marketing e behavioural targeting, uma vez que são consideradas invasivas e preocupantes sob o ponto de vista da privacidade[13].

Tendo em vista as peculiaridades e a intensidade pela qual a internet e suas tecnologias se desenvolvem é de se esperar que os problemas e inseguranças também surjam ou se potencializem. O direito, apesar de tentar prever as mais diversas hipóteses possíveis no mundo real, não consegue prever todas, ou ainda que consiga, não consegue fazê-lo de maneira perfeita. Além disso, essencial acrescentar nessa equação as hipóteses que não deveriam ser previstas ou reguladas pelo direito, mas ainda assim o são. É verdade que o direito e suas interpretações se amoldam conforme a sociedade muda. Entretanto, conforme será argumentado na parte final desse trabalho, em determinadas matérias, como a privacidade e proteção de dados pessoais na internet, é necessário que haja uma legislação e agenda positiva sobre o tema, especialmente no Brasil, a fim de que a privacidade e proteção de dados do usuário sejam efetivamente garantidas.

---

[9] How the internet Works, Pp. 16

[10] http://fgvprojetos.fgv.br/noticias/uso-de-big-data-ajuda-governo-brasileiro-gastar-de-forma-mais-eficiente

[11] IoT – Uma Estratégia Para o Brasil: Consolidação de uma visão unificada para orientação e proposição de políticas públicas sobre Internet das Coisas no Brasil. Disponível em: https://www.researchgate.net/publication/305993829_IoT_-_Uma_estrategia_para_o_Brasil#pf22

[12] Expressão utilizada pelo Vice Presidente da Microsoft em conferencia em São Francisco no ano de 2016. Disponível em: http://olhardigital.uol.com.br/pro/noticia/microsoft-diz-que-dados-sao-o-novo-petroleo/56776.

[13] Disponível em http://www.forbes.com/sites/roberthof/2011/07/20/can-behavioral-targeting-survive-privacy-worries/#3468c692609c

2. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

2.1 CONCEITO

Ao se falar de privacidade é crucial perpassar pelo seu desenvolvimento conceitual, ainda que de forma breve. O direito à privacidade, surgido no liberalismo clássico, possuía uma visão negativa e de cunho individualista, no sentido da não intrusão ou interferência do Estado e de outros na esfera privada, sendo conhecido como o direito de estar só[14][15].

O direito à privacidade16 encontra guarida internacional desde 1948 com sua previsão na Declaração Universais de Direitos do Homem e posteriormente na Convenção Europeia de Direitos Humanos, Convenção Americana de Direitos Humanos, entre outros tratados e instrumentos internacionais. A proteção da privacidade, na maioria dos tratados e declarações internacionais, era dada através da determinação da não ingerência de outrem na vida privada, familiar, na correspondência e nas comunicações. Similar é o texto conferido pela Constituição Federal Brasileira de 1988, tópico que será abordado no presente trabalho posteriormente, em seção separada.

Após intensos debates e desenvolvimento da doutrina e jurisprudência, essa visão clássica de privacidade se modificou nas últimas décadas [17]. A visão do direito à privacidade ganha forma de direito de personalidade e passa a ter uma outra concepção e tutela que não apenas o direito de estar só[18]. Dado o contexto histórico pós-guerra, o princípio da dignidade humana surgiu como reação às atrocidades cometidas naquela época, com a função de tutelar a pessoa humana em sua inteireza. Conforme ensinamentos de Maria Celina Bodin de Moraes " a personalidade é não um direito, mas sim um valor, o valor fundamental do ordenamento".[19]

O direito à privacidade começou a ser tutelado sob suas diversas facetas. Como explicado por Marcel Leonardi[20] "assuntos como liberdade de pensamento, controle sobre o

---

[14]DONEDA, Danilo. Da privacidade à proteção de dados pessoais, Pp. 5

[15]O conceito de right to be alone foi formulado em 1890, por Samuel D. Warren e Louis D. Brandeis, em seu artigo intitulado "The Right to Privacy", publicado pela Harvard Law Review.

[16]Analisando a legislação tanto internacional quanto municipal, dificilmente será encontrado um dispositivo que utilize categoricamente a palavra privacidade. Conforme exposto, a legislação optou (e ainda opta) por dar diferente denominação, tendo em vista a amplitude do conceito de privacidade, que é considerado por muitos como conceito jurídico indeterminado.

[17] VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia de informação. Dissertação (Mestrado em Direito) - Universidade de Brasília, Brasília, 2007. Pp. 134

[18]DONEDA, Danilo. Ibidem. pg. 14

[19]MORAES, Maria Celina Bodin. Danos à pessoa humana: Uma leitura civil constitucional dos danos morais.

[20]LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2012, Pp. 48

próprio corpo [21] ,quietude do lar, recato, controle sobre informações pessoais (...), autodeterminação informativa [22], entre outros, são excluídos ou incluídos, de acordo com a definição adotada". Nesse sentido, é possível notar que o direito à privacidade não se restringe apenas à uma única interpretação, visto que se relaciona com uma série de interesses diversos.

A proteção de dados pessoais pode ser vista como uma destas facetas do direito à privacidade na era da sociedade da informação. Conforme já salientado, o direito à privacidade encontra proteção sob a perspectiva de direito de personalidade e humano, devendo, pois, a proteção de dados ser tratada de igual maneira. Embora comumente andem juntos, tais direitos possuem escopos e limites próprios, que não se confundem. Por essa razão, vemos que a Carta dos Direitos Fundamentais da União Europeia tutela separadamente o respeito pela vida privada e familiar (aqui o direito à privacidade sob a perspectiva de seu conceito clássico, individualista), em seu art. 7º e a proteção de dados pessoais, em seu art. 8º. [23]

Para seguirmos com a análise, é necessário delimitar o que se entende por dados pessoais. A definição de dados pessoais, na legislação brasileira, não é bem definida, como se verá em momento posterior neste estudo. Entretanto, é possível compreender dados pessoais como quaisquer informações relativas a um indivíduo identificado ou identificável[24]. De acordo com a legislação europeia [25], a pessoa natural identificável é aquela possa "ser identificada, direta ou indiretamente, em especial por referência a um identificador, como, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular".

Em consonância com o que fora exposto supra, a conceituação de privacidade é uma tarefa difícil, podendo ser desmembrada em diversas partes. A Constituição Federal brasileira de 1988 trata do direito à privacidade em seu artigo 5º, inciso X, que dispõe, respectivamente:

> *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer*

[21]Como decidido em *Rode v. Wade* pela Suprema Corte dos EUA, cuja decisão determinou a possibilidade de realização de aborto pela mulher com base em seu direito à privacidade.
[22]O direito à autodeterminação informativa (*Recht auf Informationelle Selbsbestimmung*), de acordo com o entendimento do Tribunal Constitucional Alemão (*Bundesverfassungsgericht*), na decisão **conhecida como *Volkszählung*** apesar da inexistência de previsão explícita na norma fundamental alemã *(Grundgesetzt*) constitui direito de personalidade**.**
[23]LEONARDI, Marcel. Ibidem, Pp.80
[24]EUROPA, Convenção 108
[25]EUROPA, Regulamento 2016/679

> *natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
>
> *X - **são invioláveis a intimidade, a vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*

Nota-se que em nenhum momento no texto constitucional há referência ou menção explícita de um direito à privacidade. No entanto, é pacífico na jurisprudência a existência de um direito fundamental à privacidade [26], que retira seu fundamento do próprio texto constitucional, no artigo supramencionado. A proteção à privacidade é obtida, nesse contexto, através da proteção da intimidade, vida privada, honra, imagem, correspondência e das comunicações.

Ademais, o texto constitucional prevê hipótese de proteção da privacidade e de dados pessoais[27], em seu artigo 5º, inciso LXXII, através do habeas data. O habeas data surgiu como resposta à repressão de órgãos públicos durante o período militar. O instrumento constitucional poderá ser impetrado para dar conhecimento pelo impetrante (titular) dos seus dados que se encontram à disposição do poder público ou ainda para a ratificação de seus dados. Sem embargo, ao analisar a ação constitucional, Danilo Doneda, conclui que "ela não é acompanhada de instrumentos que possam torna-la ágil e eficaz o suficiente para a garantia fundamental de proteção de dados pessoais".[28] Não obstante, muito importante frisar que o direito à privacidade e a ação do habeas data se encontram no rol dos direitos fundamentais da Constituição Federal de 1988, não podendo esses direitos serem objeto de emenda, por isso denominados de cláusulas pétreas, vide disposição do artigo 60 § 4º do texto constitucional. As cláusulas pétreas são assim classificadas porque não podem ser objeto de emenda constitucional, ou seja, a remoção de tais direitos só é permitida pelo poder constituinte

---

26Exemplo: Mandado de Segurança nº 00364172320108110000 36417/2010- Tribunal de Justiça do Mato Grosso; e Apelação Cível nº 20130810075553- Tribunal de Justiça do Distrito Federal

27A ação de habeas data visa à proteção da privacidade do indivíduo contra revelação de dados pessoais falsos ou equivocados, ou por prática abusiva. Em - APELACAO 0067696-28.2012.8.19.0002- Relatora Des. Patricia Serra Vieira - Decima Câmara Cível. – Tribunal de Justiça do Rio de Janeiro.

28DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico, V. 12, N. 2, 2011. Pp. 104

originário, quando da elaboração de nova constituição. Não é por menos que a Constituição Federal de 1988 é considerada como rígida, dado os obstáculos e requisitos para sua alteração.

Além do tratamento constitucional conferido ao direito à privacidade, a legislação infraconstitucional também regula o tema. O artigo 21 do Código Civil estabelece que a vida privada da pessoa natural é inviolável. Fora tal artigo, não há outras menções no Código Civil do direito à privacidade, havendo, todavia, outros dispositivos que tutelam os direitos da personalidade como um todo.[29]

No campo das relações consumeristas, é vital compreender que o consumidor, em muitas das vezes, é a parte mais vulnerável da equação, sendo comumente denominado como hipossuficiente. Dessa forma, no que tange à proteção de seus dados, o legislador tratou da matéria de forma prudente e cautelosa.

O Código de Defesa do Consumidor, em sua seção VI, versa sobre o direito à privacidade sob o prisma da proteção de dados pessoais em banco de dados. É possível extrair do referido artigo, caput, os princípios da transparência e livre acesso, pois é direito do consumidor ter acesso às suas informações e dados pessoais que constem em cadastros, fichas ou registros, bem como sobre as fontes de tais informações e dados. Ao consumidor é garantido ainda o direito de alteração e correção de seus dados quando incorretos ou desatualizados, convergindo com o princípio da adequação ou realidade, além de estabelecer limite temporal para o armazenamento dos dados, em consonância com o direito ao esquecimento.

1.2 PRINCÍPIOS GERAIS SOBRE A PROTEÇÃO DE DADOS

Dada a seriedade que é lidar com dados pessoais e a intensidade pela qual eles são produzidos, foram estabelecidos princípios gerais[30] com uma finalidade dupla: a de limitar o uso de tais dados por terceiros (governo, empresas privadas, etc) e a de garantir uma proteção e controle por parte do titular dos dados (*data subject*).

O princípio da finalidade determina que os dados pessoais devem ser somente coletados quando o seu uso e finalidade forem específicos, legítimos, explícitos e seu tratamento posterior não sejam incompatíveis com o seu uso.

29BRASIL, Capítulo II do Código Civil.

[30]Alguns desses princípios são encontrados no projeto de lei PL 5276/16 e também na legislação europeia, como no Data Protection Act 1998 do Reino Unido, na Diretiva 95/46/CE e Regulamento (UE) 2016/679

É necessário ainda que haja o fornecimento de informações clara e precisas aos titulares dos dados pessoais acerca do tratamento de tais dados, como preleciona o princípio da transparência ou publicidade.

O princípio da adequação prega que além do dever de a finalidade ser compatível com o tratamento de dados, é imprescindível que haja adequação e relevância no tratamento de acordo com as legítimas expectativas do titular, dado o contexto do tratamento.

Aos titulares é garantido inclusive a consulta descomplicada e gratuita de seus dados pessoais bem como as modalidades de tratamento, sob o princípio do livre acesso.

O princípio da necessidade se revela através da imposição de limitação do tratamento de dados ao mínimo necessário para a realização de suas finalidades, de maneira proporcional e não excessiva, sendo certo que caso haja a possibilidade de se atingir a mesma finalidade com dados anônimos, o tratamento de dados pessoais não seria mais cabível.

Ademais é direito do titular que seus dados sejam mantidos sempre atualizados, com exatidão, clareza e devido a sua relevância para com a finalidade de seu tratamento, sob o escopo do princípio da qualidade dos dados.

Mister salientar a existência de outros princípios, que variam de acordo com a legislação adotada. Conforme será argumentado adiante, é possível identificar e distinguir alguns princípios elencados no projeto de lei 5276/16 dos princípios elencados na legislação europeia. Todavia, ressalta-se que apesar de diferente denominação ou classificação, esses princípios possuem a premissa basilar e central de garantir um maior controle ao titular dos dados pessoais e de limitar o uso e tratamento de tais dados por terceiros.

1.3 O PAPEL DO CONSENTIMENTO: A PROTEÇÃO DOS DADOS PESSOAIS SENSÍVEIS

Como se pode imaginar, não são todos os dados pessoais que demandam tutela tão intensa e especial. Os que exigem são chamados de dados pessoais sensíveis. Isso não significa dizer, entretanto, que os dados não sensíveis (dados que para serem coletados não necessitam de prévio e expresso consentimento do titular[31]) podem ser usados livremente. Conforme supracitado existem princípios que devem ser seguidos, independentemente do caráter dos dados pessoais (sensíveis ou não). Oportuno salientar que os dados pessoais não sensíveis,

[31]VIEIRA, Tatiana Malta. Ibidem. Pp. 256

quando coletados e agrupados, podem representar um risco à privacidade do seu titular, posto que através deles é possível traçar um perfil desse titular (profiling)[32].

Os dados pessoais sensíveis, por sua vez, são aqueles cujo tratamento representam um risco significativo à direitos fundamentais, por pertencer a aspectos da vida íntima do titular (origem racial ou étnica, posicionamento religioso ou político, por exemplo). Por essa razão, os dados pessoais sensíveis requerem prévio e expresso consentimento do titular, sendo ele considerado o único apto a autorizar o uso e processamento de seus dados. O consentimento deve ser livre, informado e específico.

Um dos modelos comumente utilizados quando se trata de consentimento, é o modelo denominado de autogerenciamento da privacidade (*privacy self-management*). Tal modelo pressupõe que o titular, através de sua autonomia, tem o poder de decisão em suas mãos acerca do uso e tratamento de seus dados. Apesar de parecer eficiente, o referido modelo enfrenta críticas que merecem nossa atenção[33]. Dentre tais críticas são comumente citadas por estudiosos da área de *Economics of Information Secutiry* (disciplina voltada para análise econômica relacionada a questões de segurança) a incompletude informacional, racionalidade limitada e desvios psicológicos sistemáticos de racionalidade[34].

De acordo com Hebert A. Simon, em sua análise sobre a estrutura de escolha racional humana, a racionalidade limitada pode ser entendida na medida em que *"os agentes racionalmente limitados experimentam limites na formulação e resolução de problemas complexos e no processamento (recebimento, armazenamento, recuperação, transmissão) de informações"*[35]. É dizer que a racionalidade limitada, na verdade, exprime a incapacidade do usuário em tomar a sua decisão de forma mais racional, por não compreender as complexidades envolvidas, e/ou tampouco entender todas as informações a ele fornecidas, de modo que esta incompletude e/ou imperfeição das informações leva o usuário à hipótese de tomar uma decisão minimamente aceitável, o que não significa que esta será a decisão mais consciente ou socialmente desejável.

Nesse sentido, as críticas acima mencionadas podem ser traduzidas em possibilidades nas quais parte dos titulares dos dados não tenha conhecimento da política de uso de seus dados quando baixam aplicativos, utilizam as redes sociais, entre outros. Os termos de uso raramente

---

[32] Disponível em: http://economia.estadao.com.br/noticias/geral,voce-e-o-produto,1701371

[33]Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, Harvard L. Rev. 1880 (2013). Pp. 126

[34]Alessandro Acquisti & Jens Grossklags. Privacy and Rationality: A Survey. IEEE Security & Privacy (2005), pp. 24/25

[35] Tradução livre. SIMON, Herbert A. (1957) *Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting*, New York: John Wiley and Sons.

são lidos, talvez por falta de interesse do usuário ou talvez por serem incrivelmente longos e técnicos, quase similares à um contrato de adesão. De acordo com survey realizado em 2004, pela Carnegie Mellon University[36], 41% das pessoas integrantes do grupo denominado "com grande preocupação sobre privacidade" admitiram que raramente leem políticas de privacidade[37]. Por consequência, existe uma assimetria de informações entre as partes envolvidas, tendo em vista que o titular não sabe, de fato, como e para quais finalidades seus dados serão extraídos[38].

É possível também que os usuários não consigam dimensionar o valor de tais dados e, por conseguinte, não conseguem mensurar os riscos inerentes à coleta destes, sendo este um exemplo claro de racionalidade limitada[39]. É possível, também, que ainda sejam impossibilitados de acessar o conteúdo de um site ou plataforma digital por não terem consentido em sua totalidade com os termos de uso. Essa última hipótese, ao estabelecer o consentimento como condição *sine-qua-non* para o uso de tais "serviços" e plataformas é perigoso, pois pode representar um verdadeiro obstáculo a muitos usuários, que por sua vez ou irão ceder de seu direito à privacidade ou se encontrarão isolados do mundo virtual. Nesse sentido, explica Bruno Bioni que o modelo de "tudo ou nada", isto é, concordar ou negar o consentimento, mistifica ainda mais o conceito de autodeterminação informacional[40]. Tal mistificação reside no fato de que, em muitos casos, esse modelo de tudo ou nada impõe ao usuário uma única alternativa: a de aceitação dos termos em sua integralidade (tudo) ou ficar "de fora" de tal serviço (nada).

No que tange ao consentimento e ao autogerenciamento da privacidade é difícil encontrar um nível ótimo de proteção, unicamente por esse modelo, que ao mesmo tempo não estabeleça o consentimento, em sua inteireza, como requisito prévio (podendo representar grande barreira e desestímulo ao uso benéfico e positivo de tais plataformas) e que não mine o titular ao se sentir preso em uma "armadilha sem saída", no qual sua única opção seja aceitar a política de uso e tratamento de seus dados. Portanto, conclui-se que é indispensável pensar em outros mecanismos que complementem o modelo de autogerenciamento da privacidade. Uma

---

[36]T. Vila, R. Greenstadt, and D. Molnar, "Why We Can't be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market," The Economics of Information Security, L.J. Camp and S. Lewis, eds., Kluwer, 2004, pp. 143–154.

[37] ibid

38BIONI, Bruno Ricardo. Prize norms and functional perspective of law: a new normative production to foster a holistic privacy regulation. PP. 93 Et. Seq.

39Acquisti, Alessandro. Economics of Information Security: Privacy and Rationality in Individual Decision Making. PP. 26 Et. Seq.

40"*The "agree" or "decline" of privacy polices take a straightforward "all or nothing" approach, mystifying even more the concept of informational self-determination.*

estratégia regulatória a ser considerada é a de sanções monetárias, como ocorre nos Estados Unidos com o sistema de "*enforcing privacy promises*", ou seja, "cumprir com as promessas de privacidade", onde empresas são penalizadas caso não cumpram com as suas regras e políticas de privacidade estabelecidas[41]. À empresa Google foi demandado o pagamento de multa no montante de $ 22.5 milhões de dólares, por ter rastreado usuários com *Iphone, Ipad* e computadores Mac da marca Apple, contornando as configurações de proteção de privacidade do web browser Safari[42.] É verdade que a referida estratégia também não é perfeita e possui como desvantagem, dentre outras, o seu caráter repressivo. Dessa forma, para que a sanção seja aplicada, é necessário que primeiro haja violação do direito da privacidade para que a medida seja tomada.

Em um cenário ideal, a estratégia mais eficiente deveria garantir seus resultados antes mesmo de uma possível violação da esfera da privacidade, agindo de forma preventiva. Isso seria possível através de estratégias que promovam incentivos, sejam eles de natureza fiscal ou não. Regimes de incentivos permitem que empresas ou demais atores envolvidos sejam não só penalizados quando não obedecerem determinadas regras, mas também possuam benefícios, como a redução de impostos se determinadas políticas regulatórias sejam adotadas no âmbito interno da companhia[43]. Podemos concluir, portanto, que existe uma vasta possibilidade de regulação sobre o papel do consentimento na área da privacidade e proteção de dados pessoais, que possuem simultaneamente vantagens e desvantagens, devendo então ser averiguadas e analisadas em um contexto concreto para que se possa atingir de forma mais eficiente o objetivo a que se destina/propõe.

2. DA REGULAÇÃO INFRACONSTITUCIONAL DA PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL

Tendo em vista a grande inovação tecnológica e digital abordada no tópico I anteriormente, o legislador brasileiro iniciou, ainda que timidamente, a discutir o tema da internet, informação e tratamento de dados em alguns diplomas normativos. Com efeito, foi neste cenário que a Lei 12.527 de 2011 foi criada. A referida lei, também chamada de Lei de

41BIONI, Ibidem, Pp. 5
42 Disponível em: https://www.theguardian.com/technology/2012/aug/09/google-record-fine-ftc-safari
43BALDWIN, Robert; CAVE, Martin and LODGE, Martin; Understanding Regulation: : theory, strategy and practice. Second Edition. Oxford. PP. 3 Et. Seq.

Acesso à informação, foi implementada para regulamentar o art. 5º, XXXIII da Constituição Federal, que dispõe:

> *"todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado".*

Dentre suas disposições, destaca-se para efeitos do presente estudo, o art. 31 que disciplina sobre o tratamento de informações pessoais, que deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. Além disso, o mesmo dispositivo determina o consentimento como regra a autorização de acesso ou divulgação. No entanto, existem hipóteses que dispensam a necessidade de obtenção de consentimento, como: cumprimento de ordem judicial, defesa de direitos humanos, pesquisas científicas, entre outros (art. 31, § 3º, I ao V).

Ainda nesta mesma linha, foi aprovada em 2012 a lei 12.373 que versa sobre crimes ocorridos no meio da internet, como o crime de invasão de dispositivo informático, tipificado no art. 154-A do Código Penal[44]. Este novo dispositivo no Código Penal inserido pela lei de crimes informáticos evidencia de forma inequívoca a preocupação do legislador no que tange a proteção de informações e dados pessoais, especialmente no âmbito digital.

A despeito de tudo isso, persistia a necessidade de criação de lei que dispusesse da matéria de forma mais específica e atualizada. Dessa forma, após amplos debates entre governo e sociedade, a lei 12.965 de 2014, também conhecida como Marco Civil da Internet, foi promulgada, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no país.

Nas palavras de Vinícius Borges Fortes[45] "o Marco Civil representa o maior avanço normativo diretamente vinculado ao uso da internet na vida civil brasileira", uma vez que "trouxe ao meio jurídico o debate sobre a necessidade de uma norma jurídica que recepcionasse e reconhecesse direitos dentro do contexto da internet no Brasil"[46]. Dessa forma, essencial a sua análise para o tema objeto deste trabalho.

---

[44] BRASIL, Lei 12.737
[45] FORTES, Vinícius Borges. Os direitos de privacidade e a proteção de dados pessoais na internet. Rio de Janeiro. Lumen Juris. 2016. Pp. 120
[46] Ibidem. Pp. 120

Os pilares do diploma legal supracitado são a neutralidade da rede, a privacidade e liberdade de expressão. No que concerne o presente artigo, forcar-se-á na análise do diploma legal sob o prisma da privacidade.

A proteção da privacidade é elencada como princípio a ser resguardado no uso da internet no Brasil, estabelecido já no início do Marco Civil da Internet, em seu art. 3º, inciso II, bem como a proteção de dados pessoais, em seu inciso III.

Em seu artigo 7º a lei 12.965 versa sobre os direitos do usuário da internet e, após a leitura atenta de seus incisos, pode-se inferir que a privacidade é tutelada sob suas mais diversas facetas e perspectivas, seja pela inviolabilidade da intimidade e vida privada, conforme art. 7º, I, seja pela inviolabilidade e sigilo do fluxo de comunicações do usuário via internet ou comunicações privadas armazenadas (incisos II e III respectivamente). Ademais, é assegurado ao usuário o fornecimento de informações claras e completas sobre coleta, uso, armazenamento e tratamento de dados pessoais (art. 7º, inciso VIII), bem como o consentimento expresso sobre tal coleta, uso, armazenamento e tratamento (inciso IX do artigo supramencionado).

Imprescindível ressaltar que além da tutela sob a perspectiva principiológica, a privacidade e a liberdade de expressão nas comunicações são condições necessárias para o pleno exercício do direito de acesso à internet (art. 8º). Isso significa dizer que uma proteção mais objetiva é possível, ao contrário da análise de ponderação de princípios no caso concreto, conferindo um caráter de maior concretude ao instituto da privacidade.

Além disso, o Marco Civil da Internet tutela de forma específica a proteção aos dados pessoais, ao lado da proteção aos registros e às comunicações privadas. O art. 10 da lei estabelece que a guarda e disponibilização de dados pessoais e do conteúdo das comunicações privadas devem atender à preservação da privacidade (através da intimidade, da vida privada, da honra e da imagem, em consonância com o disposto no art. 5º incisos X e XII da Constituição Federal). Em leitura conjunta do mencionado artigo nos §§1º e 3º tem-se que somente em determinados casos (quando de qualificação pessoal, filiação e endereço) é possível o fornecimento de dados sem ordem judicial. Isto significa dizer que, via de regra, apenas mediante ordem judicial é possível a disponibilização de dados e comunicações privadas, vide art. 10 §§1º e 2º.

Apesar da contribuição relevante do Marco Civil da Internet, ao se delimitar definições técnicas sobre o tema, como o que seria entendido por internet, terminal e aplicações de internet, por não ser uma legislação direcionada à proteção de dados pessoais, a referida lei peca por não demarcar outros conceitos básicos e primordiais sobre o tema. No entanto, importante frisar

que o Decreto 8.771/16 regulamenta diversos pontos do Marco Civil, dentre eles a neutralidade da rede e a proteção de dados pessoais. Não obstante, tal decreto é igualmente silente quanto ao que seriam os chamados "dados pessoais". Nesse sentido, indaga-se: como é possível almejar a proteção de dados pessoais quando sequer há definição legal do que seriam estes ou o que caracterizaria o tratamento de dados? Tais questionamentos nos levam a crer que embora sua importância no Brasil, o Marco Civil da Internet também se mostra insuficiente e datado, até certo ponto, haja vista o exponencial desenvolvimento das tecnologias e o fenômeno do Big Data[47].

3. DA REGULAÇÃO DA PRIVACIDADE E PROTEÇÃO DE DADOS NA EUROPA

Neste capítulo, serão abordadas as legislações europeias que disciplinam e regulam a proteção de dados no continente europeu. Não obstante, imperiosa se faz uma breve análise do tema na história europeia, considerada a verdadeira pioneira na regulamentação da matéria.

Em 1970, no estado de Hesse, localizado em Wiesbaden – Alemanha, foi criada a primeira lei sobre proteção de dados na Europa, a então chamada: *Datenschutzgesetz*. A criação da referida ainda impulsionou a constituição de uma lei a nível nacional sobre a temática, inicialmente intitulada de *Bundesdatenschutzgesetz*, passando a vigorar em todo o território alemão em 1979 [48].

Em um momento não muito posterior, o Tribunal Constitucional Alemão reconheceu, no caso conhecido comumente por "Lei do Censo" ou "*Volkszählungsurteil*", o direito da autodeterminação informativa (*Recht auf informationelle Selbsbestimmung*), direito esse intrinsicamente relacionado à personalidade do indivíduo[49]. Como bem apontado por Vinícius Borges Fortes:

"Ressalta-se a fundamental importância do conceito de autodeterminação informacional, instituído na vanguarda normativa alemã, e que constitui a gênese normativa da proteção de dados pessoais no continente europeu, que pode ser evidenciado na Constituição Europeia, nas Diretivas e Regulamentos".

---

[47] GOMES, Rodrigo Dias de pinho. Breves considerações sobre desafios à privacidade diante do Big Data na Sociedade da Informação. V Encontro Internacional do CONPEDI Montevidéu-Uruguai. pg. 290
[48] Borges, Vinícius Fortes. Ibidem. Pp. 154
[49] Ibidem. Pp.154

A título exemplificativo do supramencionado, tem-se o artigo 8º, 1, da Carta dos Direitos Fundamentais da União Europeia, na qual determina que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".

Oportuno ressaltar, neste momento, o sistema peculiar existente no continente europeu. A União Europeia possui natureza jurídica "sui generis". No entanto, pode-se afirmar de que se trata de um bloco econômico, político e social e tem como seus integrantes os Estados-Membros signatários de seus tratados, estes que detêm de personalidade jurídica própria. Como forma de garantir harmonia no bloco e com finco nos seus ideais de verdadeira integração entre os países-membros, a União Europeia possui como instrumentos legais para o exercício de suas competências as decisões, recomendações, diretivas e regulamentos[50].

Conforme disposição do artigo 288 do Tratado de Funcionamento da União Europeia (TFEU), recomendações e pareceres não possuem efeito vinculante, isto é, os Estados-Membros não são obrigados a segui-los. Por sua vez, as decisões, diretiva e regulamentos vinculam os Estados-Membros. No entanto, nas decisões que especificarem seus destinatários, os efeitos decorrentes desta somente serão obrigatórios para tais partes.

As diretivas possuem efeito vinculante na medida em que os Estados-Membros estão obrigados a alcançar o objetivo traçado por esta. Conclui-se, pois, que os Estados-Membros possuem autonomia e discricionariedade para optar pela melhor forma e meio de atingir o objetivo da diretiva. Isto significa dizer que os efeitos vinculantes na diretiva são limitados ao seu objetivo. É importante ressaltar que a diretiva precisa ser transposta tempestivamente pelo Estado-Membro, ou seja, deve ser internalizada no ordenamento jurídico nacional dentro do prazo determinado em seu texto. A internalização de uma diretiva deverá ser feita por um ato do governo, seja através de lei, decreto lei ou decreto legislativo regional.[51] Caso o prazo determinado para a transposição da diretiva não seja cumprido, é possível levar a questão ao Tribunal de Justiça da União Europeia, nos termos dos art. 259 a 260 do TFEU.

Os regulamentos, por outro lado, possuem caráter geral e são vinculantes em todos os seus elementos. Sendo assim, os regulamentos vinculam os Estados-Membros não só quanto aos objetivos a serem alcançados (como acontece com as diretivas), mas também quanto à forma e meios para lograr com suas finalidades. Ademais, por força de determinação do TFEU,

[50] EUROPA, Art. 288 Tratado de Funcionamento da União Europeia.
[51]Disponível em: https://infoeuropa.eurocid.pt/files/database/000061001-000062000/000061756.pdf

os regulamentos possuem aplicabilidade direta. Como consequência disso, é dispensado – e vedado! - qualquer ato de internalização do regulamento ao ordenamento jurídico nacional.

A sucinta explicação acima é crucial para a compreensão do desenvolvimento da legislação europeia sobre proteção de dados pessoais, na medida em que inicialmente a matéria era especialmente tratada pela Diretiva 95/46/CE e atualmente o assunto é disciplinado a nível do Regulamento 679/2016.

A Diretiva 95/46/CE, de 24 de Outubro de 1995, foi criada levando em consideração as diferenças entre os Estados-Membros quanto ao nível de proteção dos direitos e liberdades das pessoas, especialmente no que se refere ao direito à vida privada e do tratamento de dados pessoais[52], com o objetivo de se obter um tratamento equivalente e homogêneo dentre os Estados-Membros sobre proteção de dados pessoais.[53] A referida diretiva será tratada de forma breve abaixo, uma vez que é considerada como a legislação basilar da União Europeia, pois é ela quem centraliza os principais conceitos sobre a temática, determinando princípios gerais acerca da tutela dos dados pessoais[54].

Frisa-se que para fins do presente estudo, a análise comparada entre legislação brasileira e europeia será feita com o enfoque no Regulamento 679/2016, por este ser mais recente e detalhado sobre o tema.

A diretiva 95/46/CE delimitou, em seu artigo 2º, conceitos essenciais para a interpretação normativa, como o que seriam dados pessoais, tratamento de dados, consentimento, entre outros. O conceito de dados pessoais na diretiva 95/46/CE é tido como "qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa). É 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, da sua identidade física, fisiológica, psíquica, econômica, cultural ou social". Como se verá adiante, o referido conceito se manteve, praticamente intacto, no atual Regulamento 679/2016.

O artigo 6º da diretiva estabelece os princípios sobre a proteção de dados pessoais, quais sejam:

- ✓ Princípio da lealdade, licitude e transparência;

[52] EUROPA, Preâmbulo (7) Diretiva 95/46/CE.
[53] EUROPA, Preambulo (8) Diretiva 95/46/CE
[54] GUIDI, Guilherme Berti de Campos. Modelos Regulatórios para Proteção de Dados Pessoais. ITS/RIO. Pp. 4

- ✓ Princípio da limitação à finalidade;
- ✓ Princípio da adequação e minimização dos dados;
- ✓ Princípio da exatidão;
- ✓ Princípio da necessidade e da duração da retenção de dados;
- ✓ Princípio da segurança;

A diretiva também disciplina sobre o consentimento: o art. 7º determina que o tratamento de dados somente poderá ser efetuado se a pessoa der o seu consentimento inequívoco. Ademais, o consentimento deve ser também informado e específico[55].

Outro ponto importante é o que se refere à vedação de dados pessoais sensíveis, chamados na diretiva como "categorias específicas de dados". Dados pessoais sensíveis são aqueles que revelam a origem racial ou étnica, as opiniões políticas, convicções religiosas ou filosóficas, bem como a filiação sindical, dados relativos à saúde e a vida sexual. A vedação ao tratamento de tais dados é a regra geral, no entanto, o art. 8º, 2 apresenta as possíveis exceções à tal regra:

- Quando houver o consentimento explícito para o tratamento;
- Quando o tratamento for necessário para cumprimento de obrigações e direitos do responsável pelo tratamento, desde que autorizado por lei;
- Quando o tratamento for necessário para proteger interesses vitais da pessoa ou de terceiros, nos quais estiverem físicas ou legalmente incapazes de dar o seu consentimento;
- Quando o tratamento for efetuado no âmbito das suas atividades legítimas e com garantias adequadas;
- Quando o tratamento disser respeito a dados manifestamente públicos ou necessário ao exercício ou defesa de um direito em um processo judicial.

No capítulo 5, reservado sobre a disciplina dos direitos do titular dos dados, é possível encontrar direitos como: direito ao acesso aos dados, direito de oposição, direito a informação básica, direito de retificação e direito de eliminação de dados.

No que se refere a transferência internacional de dados, a diretiva estabelece como a regra a sua proibição, salvo nos casos previstos na diretiva e somente quando suas condições

[55] EUROPA, Regulamento 679/16. Art. 2(h).

necessárias forem satisfeitas[56]. Igualmente, há a previsão de recursos e sanções em caso de descumprimento das disposições da diretiva, de acordo com o capítulo III.

Como exposto acima, diretivas são criadas para harmonizar a legislação dos países membros acerca de um determinado tema e propor diretrizes a serem seguidas nacionalmente pelos Estados-Membros. Sobre o ponto, é justamente a isso o que a diretiva 95/46/CE se propôs. Se por um lado, um dos pontos positivos da diretiva analisada é a implementação de legislação a nível europeu no que tange a proteção de dados, por outro, vê-se que esta somente vincula os Estados-Membros quanto aos seus objetivos.

Importante destacar a existência de outras normas que complementam a regulamentação da proteção de dados pessoais na Europa, como o Regulamento nº 45/2001 (relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados) e a diretiva 2002/58/EC (sobre o tratamento de dados pessoais e proteção da privacidade no setor de comunicações eletrônicas).

O regulamento 679/2016, aprovado em abril de 2016 na cidade de Bruxelas, entrará em vigor no dia 25 de maio de 2018. O referido regulamento representa uma reforma na legislação de proteção de dados no continente europeu, de forma a revogar, nesta data, a diretiva 95/46/CE.

De acordo com a Comissão Europeia57, a reforma da proteção de dados foi proposta devido as diferenças no modo como cada Estado-Membro aplicava a diretiva 95/46. Tais diferenças criaram um cenário de complexidade, incerteza jurídica e de elevados custos administrativos. Além disso, a diretiva foi elaborada em 1995, com uma conjuntura completamente diferente dos dias atuais, onde se vive a Era da Informação e do Big Data. Nesse sentido, houve uma intensa necessidade de modernização da legislação sobre proteção de dados pessoais, para que a lei alcance diversas hipóteses e questões anteriormente não existentes ou previstas.

Ao se analisar o Regulamento, pode-se perceber de antemão que a sua base não se difere da diretiva de 1995 e que muitos dispositivos se mantiveram praticamente intactos ou sem alterações substanciais. Todavia, o Regulamento traz consigo outras disposições não elencadas na diretiva: o regulamento conta com o total de 99 detalhados e específicos artigos, ao passo

[56] EUROPA, Regulamento 679/16 Art. 25 – 1 ao 6
[57] EUROPA. Comissão Europeia: Fact Sheet Disponível em: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

que a Diretiva 95/46/CE possui menos da metade (34 artigos). Para cumprir com os objetivos deste estudo, serão analisadas a seguir algumas inovações interessantes sobre o tema.

De acordo com a Comissão Europeia, a reforma da proteção de dados permite o desenvolvimento da proposta de "Mercado Digital Único" (Digital Single Market), através da adoção das seguintes medidas:

- Um continente, uma lei: tanto indivíduos quanto organizações e empresas lidarão com uma legislação única sobre a matéria;
- *One-stop-shop*: empresas terão que lidar com uma única autoridade supervisora, o que simplifica e reduz custos de transação nos negócios das empresas na UE.
- Mesmas regras para as empresas e organizações independentemente do local onde estas se encontram.

No que se refere aos conceitos elencados no art. 4º do regulamento 679/2016, pequenas foram suas alterações. Nesse aspecto, cumpre destacar a novidade trazida pelo Regulamento sobreo conceito de pseudominização, não existente na diretiva. A pseudominização é definida como "tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável". A inovação é tida como positiva, pois explicitamente encoraja tais organizações a utilizarem da pseudominização como medidas de segurança58.

Outra alteração que merece destaque é no que tange ao papel do consentimento. De acordo com a diretiva de 95/46, o consentimento deve ser livre, informado e específico. Todavia, foi o regulamento em seu artigo 7º, que trouxe condições aplicáveis ao consentimento, a saber:

- O responsável pelo tratamento deve poder demonstrar que obteve o consentimento do titular dos dados;
- Caso a declaração de consentimento seja na forma escrita e diga a respeito sobre mais de um assunto, é necessário que o pedido de consentimento seja apresentado de forma a distingui-lo claramente de tais outros assuntos, com uma linguagem clara, inteligível e simples.

[58] Unlockig the EU general data protection regulation: a practical handbook on the EU's new data protection law. White Case. 25 Julho 2016. pagina 20.

- O titular tem o direito de retirar a qualquer momento o sentimento que foi dado, sendo certo que a retirada de tal consentimento não compromete a licitude do tratamento efetuado com base no consentimento anteriormente dado.
- É necessário a verificação com máxima atenção se a prestação do serviço demanda o consentimento como um requisito necessário para sua utilização. Ou seja, deve-se perguntar: a prestação de tal serviço está subordinada ao consentimento para o tratamento de dados pessoais? Tal consentimento é necessário para a execução do contrato?

Nesse sentido, pode-se concluir que autorizações genéricas e aquiescência passiva não podem ser consideradas como consentimento, tampouco o silêncio ou o sistema de caixas pré-marcadas (*pre-ticked boxes*).

O Regulamento 679 também inova o tema do consentimento ao disciplinar sobre o consentimento extraído de crianças. De acordo com o art. 8o, é lícito o tratamento de dados de crianças com pelo menos 16 anos de idade, desde que o seu consentimento seja expresso. Em caso de menores de 16 anos, o tratamento somente será lícito e permitido se, e na medida em que, o consentimento for dado ou autorizado pelos titulares das responsabilidades parentais da criança. É também facultado aos Estados-Membros a mudança deste parâmetro, desde que não estipulem idade inferior a 13 anos.

Cumpre-se destacar ainda que o regulamento estabelece um direito à limitação do tratamento de dados, no qual os titulares dos dados possuem o direito de restringir o tratamento de seus dados pessoais, em determinadas situações especificadas em seu art. 18, por exemplo, quando o tratamento for ilícito e o titular solicitar a limitação de sua utilização.

Além do já exposto, o Regulamento 679 traz expressamente em seu texto a determinação de que haja a promoção da privacidade pela própria tecnologia, de acordo com o artigo 25 que disciplina sobre a proteção de dados pessoais pela "*privacy by design*" e "*privacy by default*". Veja-se o inteiro teor do dispositivo:

> ***Article 25***
>
> ***Data protection by design and by default***
>
> *1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the*

> *controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*
> *2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*
> *3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.*

Dessa forma, vê-se nitidamente a preocupação do legislador europeu de se garantir a privacidade dos titulares de dados pessoais desde a concepção dos sistemas de informação e dispositivos técnicos. Nos termos do artigo 25, os responsáveis pelo tratamento de dados devem adotar medidas técnicas e de organização adequadas tanto na determinação de como se dará o meio do tratamento, quanto no tratamento em si, de forma a salvaguardar a privacidade e a efetiva proteção de dados pessoais.

Com efeito, deve também o responsável pelo tratamento de dados assegurar como padrão ("*by deafult*") que somente os dados necessários para determinada finalidade específica sejam tratados.

Nesse diapasão, afirma a Comissão Europeia[59] que os modelos de privacidade por design e por padrão irão incentivar as empresas a inovar e desenvolver novos métodos e tecnologias para garantir a proteção de dados pessoais, bem como permitirá a criação de novas ferramentas e soluções tecnológicas e organizacionais.

Outro grande feito do regulamento europeu reside na criação de autoridades independentes para a proteção de dados, nos termos do capítulo VI do Regulamento. As

[59] Cf. Nota 57

autoridades de controle serão responsáveis pelo “enforcement” das regras e princípios estabelecidos no regulamento. Dessa forma, existirá um sistema de proteção de dados mais uniforme e consistente, no qual as normas serão aplicadas de forma isonômica. Tal sistema proporcionará benefícios estimados em 2.3 bilhões de euros por ano[60].

De fato, ao se analisar o regulamento, é possível observar variadas diferenças entre as disposições estabelecidas na diretiva 95/46/CE. Todavia, não se deve concluir que tais diferenças representam uma verdadeira transmutação no cerne da proteção de dados pessoais, tampouco que a referida reforma seja entendida como uma perspectiva diametralmente oposta ao já existente. Em verdade, o Regulamento 679 deve ser entendido como uma modernização, adaptação e aprimoramento das normas anteriormente vigentes.

Após a breve análise de algumas inovações trazidas pelo Regulamento 679 da União Europeia, serão estudados no tópico seguinte os projetos de lei em andamento no Brasil, no qual serão exploradas suas semelhanças e divergências para com as normas europeias.

4. DOS PROJETOS DE LEI SOBRE PROTEÇÃO DE DADOS NO BRASIL

Atualmente são encontrados diversos projetos de lei no Congresso Nacional que versam sobre proteção de dados, tais quais o PLS 181/14, do senador Vital do Rêgo, PL 131/2014, apresentado pela Comissão Parlamentar de Inquérito da Espionagem, o projeto 330/2013 apresentado pelo Senados Antônio Carlos Valadares, o projeto de lei 4.060 de 2012 foi apresentado pelo Deputado Milton Monti, o projeto de lei 5276/2016, apresentado pelo Poder Executivo, entre outros. No entanto, considerando o objetivo do presente estudo, serão analisados os três últimos projetos de lei mencionados, haja vista o diálogo direto e profundo destes para com o escopo desta análise.

O projeto de lei nº 330/2013 foi apresentado pelo Senador Antônio Carlos Valadares, do PSB de Sergipe, com a finalidade de se estabelecer no ordenamento jurídico do país, legislação que versasse sobre o tema da proteção de dados. Na exposição de seus motivos e justificativas, o senador afirma que “hoje, mais do que nunca, a informação acerca da vida e dos hábitos das pessoas constitui instrumento poderoso nas mãos de quem deseja lhes influenciar as convicções e os comportamentos”. Como consequência direta disso, continua o legislador, há uma invasão contínua das esferas da vida privada e intimidade, sendo essencial a

[60]Cf. Nota 57

reunião de preceitos pertinentes ao tema em um único diploma legal, a fim de que seja proporcionado tutela jurídica efetiva e satisfatória a tais direitos de personalidade.

O Projeto de Lei do Senado nº 330/2013 conta com 19 artigos, dentre os quais são estabelecidos conceitos e definições, princípios gerais sobre o tema, bem como os direitos básicos dos titulares de dados.

A despeito de sua tentativa de conferir uma tutela mais adequada e efetiva aos dados pessoais, o mencionado projeto de lei peca por ser um tanto quanto sucinto e deixar de abordar questões tão relevantes como a liberdade de expressão, livre iniciativa, a criação de um órgão nacional sobre o tema, entre outros.

O projeto de lei 4.060 de 2012 foi apresentado pelo Deputado Milton Monti e dispõe sobre o tratamento de dados pessoais e dá outras providências. Tal projeto representa uma das primeiras tentativas de abordar a questão de dados pessoais de forma específica e detalhada. Vê-se que dos artigos 1 ao 7o do projeto há a exposição de seus objetivos, bem como a delimitação de sua aplicabilidade e determinação de conceitos básicos essenciais, como a definição de dados pessoais e tratamento de dados. Não desmerecendo sua valia, é o projeto de lei 5.276 de 2016, apresentado pelo Poder Executivo, o grande responsável pelo aprofundamento do debate e das questões referentes ao tema. Dessa forma, oportuno notar que o PL 5.276/16 encontra-se atualmente apenso ao PL 4.060/12.

O PL 5.726/16 dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Semelhantemente ao que faz o PL anterior, o PL 5.276 também disciplina sobre os seus objetivos e conceitos norteadores para a aplicação da futura lei, como se verá adiante. Fundamental notar, desde logo, que o PL 5.276 não se limita a isso e vai além: estabelece princípios, determina de forma robusta e detalhada os requisitos para o tratamento de dados, define direitos do titular, delimita a forma de tratamento de dados pessoais pelo poder público, dispõe da transferência internacional de dados, dentre outros.

Como será possível se concluir adiante, o PL 5.276/16 sofreu forte influência da legislação europeia, guardando evidentes semelhanças especificamente para com o Regulamento 2016/679 EU.

Importante ressaltar que logo de início o PL 5.276/16 estabelece como a proteção de dados pessoais e privacidade deverá ser analisada, levando sempre em consideração a autodeterminação informativa, a liberdade de expressão, a inviolabilidade da intimidade, vida

privada, honra e imagem, o desenvolvimento econômico e tecnológico e a livre iniciativa e concorrência e defesa do consumidor (art. 2º, I ao V, PL 5.276/16).

O PL 5.276/2016, em seu artigo 5o, define dado pessoal como aquele relacionado à pessoa natural identificada ou identificável, sendo os números identificativos, dados locacionais ou identificadores também abrangidos, quando estes estiverem relacionados a uma pessoa. Essencial apontar que o PL 5.276 aborda em seu artigo 5º a definição de dados pessoais sensíveis, idêntico à definição trazida pelo regulamento europeu.

Dentre as definições trazidas pelo projeto de lei brasileiro, vale salientar o inciso XII do art. 5º, que define como processo de anonimização qualquer procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Nesse sentido, encontra-se no Regulamento 679 da EU o conceito de pseudominização que, embora não seja tratado de maneira exatamente idêntica no projeto de lei 5.276/16, guarda certa semelhança com a definição de anonimização. A pseudominização é tida como o tratamento de dados pessoais de forma que estes deixem de poder ser atribuídos a um titular específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Outra definição importante trazida na legislação europeia e até então não prevista explicitamente no PL 5.276/16 é o "*profiling*" (definição de perfis), qual seja: qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações. Em consonância com o já abordado no item 2.3, o *profiling* é uma técnica amplamente utilizada por empresas com a mais diversa finalidade. Nesse sentido, como bem apontado no estudo realizado pela Coalizão Direitos na Rede61, é essencial que a legislação que venha a ser adotada no Brasil igualmente contemple tal definição, uma vez que o uso descontrolado do profiling pode categorizar pessoas em determinados segmentos e assim reforçar e acentuar a desigualdade social e discriminação contra minorias.

O PL 5.276 também dispõe sobre princípios gerais com as finalidades de limitar o uso de tais dados por terceiros e de garantir proteção e controle por parte do titular dos dados. Dessa

[61] Coalizão Direitos na Rede: Contribuições ao Congresso Nacional acerca dos PLs sobre a proteção de dados pessoais, página 2, item C.

forma, são estabelecidos em seu artigo 6o os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção e não discriminação. Por sua vez, o Regulamento europeu, no artigo 5o, consagra os seguintes princípios:

(a) Licitude, lealdade e transparência: os dados são objetos de tratamento lícito, leal e transparente.

(b) Limitação da finalidade: dados são coletados para finalidades legítimas, explícitas, determinadas e compatíveis.

(c) Minimização dos dados: dados são adequados, pertinentes e limitados ao que é necessário relativamente às suas finalidades.

(d) Exatidão: dados são exatos e atualizados, sendo permitida a retificação dos dados inexatos e desatualizados.

(e) Limitação de conservação: dados são conservados, via de regra, apenas durante o período necessário para as finalidades para as quais são tratados.

(f) Integridade e confidencialidade: dados são tratados de forma a garantir sua segurança e confidencialidade, incluindo a proteção contra seu tratamento não autorizado, ilícito ou contra sua perda.

(g) Responsabilidade: o responsável pelo tratamento de dados é responsável pelo cumprimento das disposições acima e deve poder comprová-lo.

Apesar da distinta denominação, é possível identificar a correspondência entre princípios estabelecidos no PL com aqueles estabelecidos no Regulamento, senão vejamos:

PROJETO DE LEI 5.276/16	**REGULAMENTO 679 UE**
Princípio da transparência	Princípio da licitude, lealdade e transparência
Princípio da finalidade e princípio da adequação Princípio da necessidade	Princípio da limitação da finalidade Princípio da minimização
Princípio da qualidade dos dados	Princípio da exatidão e princípio da limitação da conservação

Princípio da segurança	Princípio da integridade e confidencialidade

No contexto brasileiro, a ideia de privacidade *by default* pode ser exprimida, de forma implícita, dos princípios da finalidade, adequação, necessidade e segurança[62].

Aos titulares também são assegurados os direitos de confirmação da existência de tratamento, acesso aos dados e correção dos dados incompletos, inexatos ou desatualizados. É garantido, outrossim, o direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com as finalidades dispostas na lei, bem como aqueles dados que tiverem sido fornecidos sem consentimento. Por fim, são previstos os direitos de portabilidade dos dados pessoais a outro fornecedor de serviço ou produto e de aplicação das normas de defesa do consumidor quando estas couberem para a proteção de dados pessoais.

O consentimento, questão crucial no que se refere à proteção de dados pessoais, salientado na subseção 2.3, é um dos requisitos estabelecidos no art. 7 do PL para o tratamento de dados. De acordo com o art. 7º, inciso I, o consentimento do titular deve ser livre, informado e inequívoco, bem como deve ser fornecido por escrito ou por qualquer outro meio que o certifique, conforme se extrai do art. 9, caput. No que se refere ao tratamento de dados pessoais, este somente será possível nas hipóteses previstas pelo art. 7 do projeto de lei.

Adicionalmente, quando o consentimento se der por escrito, a cláusula deve ser destacada das demais cláusulas contratuais, cabendo ao responsável o ônus da prova de que o consentimento foi obtido em conformidade com a lei. O tratamento de dados será vedado quando oriundo de erro, dolo coação, estado de perigo ou simulação, vide art. 9, parágrafo 2º.

Quaisquer autorizações genéricas serão consideradas nulas, sendo possível também a revogação do consentimento, a qualquer momento, mediante manifestação expressa do titular. Entretanto, como anteriormente mencionado e conforme se extrai da tabela abaixo, o projeto de lei brasileiro não traz disposição expressa no que se refere ao consentimento extraído de crianças e adolescentes, ao passo que há tal previsão no Regulamento. No entanto, como se verifica na tabela abaixo, o PL 5.276/16 disciplina genericamente, em seu artigo 14, que “o

[62] Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais, pág. 50

tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, nos termos da legislação pertinente".

O art. 8º do projeto de lei brasileiro versa sobre o acesso facilitado às informações sobre o tratamento de seus dados, que devem ser disponibilizados de forma clara, adequada e ostensiva sobre a finalidade específica do tratamento, a forma e duração do tratamento, identificação do responsável, entre outros. No regulamento europeu, vê-se a equivalência destas disposições em seus artigos 12 e 13, que versam, respectivamente, sobre transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados, e informação e acesso aos dados pessoais.

Um dos pontos mais importantes tanto pelo PL quanto pelo regulamento europeu diz respeito ao tratamento de dados pessoais sensíveis. Nunca é demais relembrar que os dados sensíveis são aqueles cujo revelam a origem racial ou étnica, as opiniões políticas, convicções religiosas ou filosóficas e dados referentes à saúde ou a vida sexual e dados genéticos ou biométricos de uma pessoa. Nessa linha, como não poderia deixar de ser, a vedação ao tratamento de dados pessoais sensíveis é a regra, tanto no projeto de lei brasileiro quanto no regulamento 649 UE. Entretanto, existem exceções previstas no art. 11 do Projeto de Lei 5.276/16 e no art. 9º do Regulamento 679 UE.

No Capítulo V do PL 5.276/16 há a previsão acerca da possibilidade de transferência internacional de dados. Contudo, a possibilidade é restringida apenas aos casos previstos nos incisos de I ao VII do art. 33. Igualmente existe disposição sobre transferência internacional de dados no Regulamento 679. As semelhanças e equivalências sobre esta matéria entre o PL e o Regulamento europeu podem ser encontradas na tabela abaixo.

Um dos pontos mais importantes do PL 5.276/16 é o que se refere à criação de um órgão único competente para lidar com assuntos sobre dados pessoais, bem como o Conselho Nacional de Proteção de Dados e da Privacidade.

O art. 53 determina a criação de um órgão competente que seja designado para zelar pela implementação e pela fiscalização da lei sobre matéria de dados pessoais, seja através da elaboração de diretrizes para uma política nacional de proteção de dados pessoais e privacidade ou seja pela edição de normas sobre a proteção de dados pessoais e privacidade, dentre outras atribuições.

No que tange ao cenário europeu, já existia em cada território nacional dos Estados Membros da EU, autoridades específicas para lidar com o tema de dados pessoais. Não obstante, foi o Regulamento 679 que trouxe a determinação de um órgão único para toda a União Europeia.

Na tabela abaixo (**Tabela II**), é possível verificar algumas outras correspondências importantes das disposições entre o Projeto de Lei brasileiro 5.276/16 e o Regulamento 679 da UE.

PROJETO DE LEI 5.276/16	**REGULAMENTO 679 UE**
Art. 5º Definição de dado pessoal	**Art. 4º** Definição de dado pessoal
Art. 5º Dados pessoais sensíveis	**Art. 9º, 1** Categorias especiais de dados
Art. 7º c/c art. 9º Consentimento	**Art. 7º** Consentimento
Art. 14 Tratamento de dados pessoais de crianças e adolescentes	**Art. 8** Consentimento de crianças
Art. 8º Acesso às informações	**Art. 12 e 13** Acesso aos dados
Art. 11 Vedação ao tratamento de dados pessoais sensíveis	**Art. 9º, 2** Vedação ao tratamento de categorias especiais de dados
Art. 18, II c/c art. 19 Acesso aos dados	**Art. 15** Acesso aos dados
Art. 18, III Direito à correção de dados	**Art. 16** Direito de retificação de dados

Art. 18, V Portabilidade de dados **Art. 18, VI** Eliminação de dados	**Art. 20** Portabilidade de dados **Art. 17 c/c art. 19** Direito ao esquecimento (direito de apagar os dados)
Art. 18, § 1º Titular pode se opor ao tratamento	**Art. 21** Direito de oposição
Art. 20 Revisão de decisões em tratamento automatizado, incluindo o tema de perfis **Art. 31 e 32** Responsabilidade por descumprimento do PL **Capítulo V** Transferência internacional de dados **Art. 33, I** Nível de proteção equiparável ao da lei c/c **Art. 34, caput** “garantias suficientes”	**Art. 22** Decisões individuais automatizadas, incluindo definições de perfis **Art. 24** Responsabilidade pelo descumprimento do regulamento **Capítulo V** transferência internacional de dados **Art. 45** Critério da adequação
Art. 33, III Quando a transferência é necessária para a proteção da vida ou incolumidade física do titular ou terceiro	**Art. 49, f** Proteção de interesses vitais do titular ou de outrem, se esse titular estiver física ou legalmente incapaz de dar seu consentimento
Art. 33, V Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional	**Art. 50** Disciplina sobre cooperação internacional da proteção dos dados pessoais e que a comissão e autoridades de controle tomarão as medidas necessárias destinadas a tal cooperação.
Art. 33 VI Transferência de dados é necessária para executar política pública ou atribuição legal de serviço público	**Art. 49, d** Quando a transferência for necessária por importantes razões de interesse público

Art. 33 VII Transferência quando o titular tiver fornecido seu consentimento e alerta de possíveis riscos	**Art. 49, a** Titular der explicitamente o seu consentimento para a transferência e alerta aos possíveis riscos
Art. 41 Encarregado pelo tratamento de dados pessoais	**Art. 37** Designação do encarregado da proteção de dados
Art. 42 Responsabilidade e ressarcimento de danos	**Art. 82** Direito de indenização e responsabilidade
Art. 45 ao 49 Segurança e sigilo de dados	**Art. 90** Segurança e sigilo de dados
Art. 52 Sanções administrativas	**Art. 84** Sanções administrativas
Capítulo VIII, Seção II Órgão competente e Conselho Nacional de proteção de dados e da privacidade	**Art. 68** Comitê Europeu para a proteção de dados

Feita a análise da tabela, é possível concluir que o PL 5.276 foi fortemente inspirado no modelo europeu de proteção de dados. No que pese os questionamentos e críticas se o PL 5.276 trata-se de uma “inspiração” ou “importação de um modelo jurídico”, mister se faz salientar que independentemente da denominação que queira se adotar, fato é que o continente europeu é tido como referência sobre o assunto. Sobre esse ponto, ressalta-se que a diretiva 95/46/CE tratou por quase 20 anos, suficiente- e satisfatoriamente do tema de proteção de dados pessoais no continente europeu. Portanto, é perfeitamente compreensível e legítimo que outros sistemas jurídicos, inclusive o brasileiro, utilizem tal modelo como inspiração na criação de legislação própria.

5. DA NECESSIDADE DE CRIAÇÃO DE LEI GERAL SOBRE A PROTEÇÃO DE DADOS E DE SEUS ELEMENTOS BÁSICOS ESSENCIAIS

Após todo o exposto, resta-se inequívoco a necessidade de criação de lei geral sobre a proteção de dados pessoais. Isto porque o grande vácuo normativo nesta área prejudica não só

os titulares de dados pessoais, que se encontram vulneráveis, como também o Estado e o setor privado, que correm o risco de serem punidos pelo uso de tais dados, uma vez que não há clareza ou definição nos limites para sua utilização. Nesse aspecto, a regulação sobre o tema se faz essencial para garantir a segurança jurídica, princípio basilar do ordenamento jurídico brasileiro, e para o avanço da Internet das Coisas e novas tecnologias de forma controlada na sociedade.

Além disso, a necessidade de uma lei geral sobre o tema se intensifica com o avanço da Internet das Coisas (IoT), na qual se desdobra para os demais setores de mercado[63]. Dessa forma, se faz imperiosa uma lei de âmbito nacional, com aplicabilidade irrestrita e multisetorial, permitindo que seu âmbito de incidência alcance diversos segmentos, tanto do setor público quanto do privado.

Afim de garantir o supra exposto, cumpre-se frisar que alguns elementos mínimos essenciais devem ser previstos na lei geral de proteção de dados a ser adotada no país, seja através dos projetos de lei já existente ou seja através, até mesmo, da elaboração de uma nova lei. Dentre esses aspectos destacam-se:

- definição de conceitos como: dados pessoais, dados pessoais sensíveis, tratamento de dados, consentimento, anonimização e profiling;
- princípios garantidores e limitadores sobre o tratamento e uso de dados pessoais, como: princípios da finalidade, necessidade, adequação, transparência e segurança;
- delimitação do papel do consentimento;
- determinação de padrões que minimizem os riscos à privacidade como os modelos de *"privacy by design"* ou "*privacy by default*"[64];
- criação de uma autoridade nacional especializada e técnica para conferir efetividade às questões relacionadas à proteção de dados pessoais no país.

No entanto, nada impede – muito pelo contrário, é até desejável! – que outros pontos sejam abordados em tal regulamentação, como se vê no PL 5.276/16. Tal projeto de lei é o que versa sobre a matéria de forma mais específica, dispondo de forma satisfatória (quase) todos os pontos anteriormente elencados. Tal projeto de lei contempla vários aspectos não trazidos pelos

[63] BIONI, R. Bruno. Privacidade e Proteção de Dados Pessoais em 2017. JOTA. Disponível em: https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/privacidade-e-protecao-de-dados-pessoais-em-2017-10012017.

[64] BIONE, R. Bruno. Como o Brasil pode ter um plano Nacional de IoT Inovador? JOTA. Disponível em: https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/como-o-brasil-pode-ter-um-plano-nacional-de-iot-inovador-12052017

demais projetos, como já apontado supra. Nessa linha, a Carta Aberta de Apoio[65] ao PL 5.276/16, subscrita por mais de 40 entidades engajadas sobre o assunto, expõe:

> *Trata-se, portanto, [o PL 5.276] de uma proposta legislativa capaz de suprir eficazmente grave lacuna no ordenamento jurídico brasileiro, a ponto de trazer segurança jurídica para o cidadão, para a atividade empresarial e para a administração pública no tratamento dos dados pessoais [...]*

Conclui-se, pois, que caso venha a ser aprovado, o PL 5.276/16 servirá, *a priori*, para regulamentar a nível nacional de forma satisfatória matéria tão delicada e de suma importância, acalmando os anseios dos personagens envolvidos nesta área e promovendo a segurança jurídica desejada, para garantir efetividade aos direitos de privacidade e proteção de dados já encontrados no sistema jurídico brasileiro de forma esparsa.

6. CONSIDERAÇÕES FINAIS

As questões relacionadas ao direito à privacidade e proteção de dados pessoais se tornam ainda mais complexas nos dias atuais, cujo ambiente está constante e intensamente em contato com o mundo digital e novas tecnologias.

Dessa forma, o presente buscou analisar a evolução histórico-jurídica, no Brasil e no mundo, do conceito de privacidade e proteção de dados pessoais. Resumidamente, vê-se que o direito de privacidade não é mais compreendido como direito de ser deixado só (de não interferência estatal), mas sim como um direito de personalidade e direito humano. Viu-se, outrossim, que o conceito de privacidade também repercute em outras esferas e tocam outros direitos a ela relacionados, como o direito à proteção de dados pessoais. O direito à proteção de dados pessoais está intimamente ligado ao direito à privacidade. Estes, no entanto, como explicado supra, possuem escopo e limites próprios e, portanto, não se confundem.

Adicionalmente, o presente trabalho buscou delimitar conceitos vitais e princípios gerais sobre o tema, quais sejam: o que seriam dados pessoais e dados pessoais sensíveis, o que se entende como consentimento e qual seu escopo, bem como os princípios da necessidade, adequação, licitude, transparência, entre outros. Também foi abordada a problemática que envolve o papel do consentimento na proteção de dados pessoais, no qual se concluiu que o

[65] Carta Aberta de Apoio ao PL 5.276. Brasília, 02 de Junho de 2016. Disponível em: http://intervozes.org.br/wp-content/uploads/2016/06/Carta-Aberta.-PL-Dados-Pessoais.02.06.2016.pdf

modelo de *privacy self-management* deve ser repensado, por atribuir um ônus muito pesado ao usuário do serviço/titular dos dados pessoais.

No que se refere ao âmbito nacional, viu-se que a disciplina sobre privacidade se encontra esparçada e segmentada na legislação brasileira, possuindo, no entanto, proteção à nível constitucional no art. 5º, X da Constituição Federal de 1988. Nesse mesmo sentido, verifica-se que existem outros diplomas legais que versam sobre a matéria da privacidade, como o Código Civil e Marco Civil da Internet.

O Marco Civil da Internet representa um grande avanço no que tange a regulamentação de matérias relacionadas diretamente à internet. Como ressaltado anteriormente, um dos pilares do Marco Civil se refere à privacidade. Com efeito, a referida lei estabelece princípios, deveres e garantias aos usuários da internet. Ao lado do princípio da privacidade, tem-se o princípio da proteção de dados pessoais. Tal tema é ainda abordado pelo Marco Civil, no qual é determinado que a guarda e disponibilização de dados pessoais deve atender à preservação da privacidade e que somente com ordem judicial é possível a disponibilização de dados e comunicações privadas.

Sendo assim, fica claro que o referido instrumento legal trouxe importantes regras sobre a privacidade e proteção de dados em um cenário de quase completa lacuna jurídica. No entanto, como salientado, o Marco Civil não se aprofundou em outros temas importantes sobre dados pessoais – como a criação de um órgão competente que venha analisar questões referentes à matéria, tampouco delimitou conceitos essenciais sobre o tema, como o que seriam dados pessoais, tratamento de dados, entre outros.

Pelo acima exposto, constatou-se a crescente urgência da adoção de matéria específica que tutele o tema dos dados pessoais como um todo, isto porque tal necessidade é potencializada em um mundo cada vez mais globalizado e tecnológico.

Com efeito, a pesquisa estudou o ordenamento jurídico europeu, uma vez que o referido continente foi um dos pioneiros sobre o tema abordado e continua, até hoje, com sua característica vanguardista, como se extrai do Regulamento 679 da UE. O recém-aprovado regulamento nasceu como uma reforma à questão da proteção de dados, com a finalidade precípua de modernizar sua legislação e, consequentemente, garantir maior harmonia entre as ações e decisões dos estados membros do bloco.

Conforme exposto no trabalho, a base substancial da antiga diretiva 95/46/CE se manteve praticamente intacta no Regulamento 679. Não obstante, algumas inovações foram trazidas pelo regulamento, dentre as quais destaca-se o conceito de pseudominização dos dados,

condições específicas acerca do consentimento e tratamento de dados, o consentimento referente à crianças e adolescentes, a transferência internacional de dados e a criação de um órgão único competente para lidar com a matéria (o Comitê Europeu para a proteção de Dados).

Após análise da legislação europeia, o presente artigo se preocupou em versar sobre os Projetos de Lei ainda em tramitação no país. Dentre os Projetos de Lei, a análise foi concentrada no Projeto de Lei 5.276/16 pelos motivos anteriormente elencados. Com o exame anterior da regulamentação europeia sobre o tema, foi possível identificar algumas semelhanças e diferenças entre o regulamento 679 e o PL 5.276/16, principalmente no que tange aos princípios a serem observados, os direitos dos titulares dos dados pessoais, o papel do consentimento e a ideia de criação de um único órgão competente para tratar da matéria de dados pessoais. Dessa forma, verificou-se que existe uma forte inspiração no regime jurídico europeu acerca da proteção de dados pessoais.

Por fim, o presente trabalho buscou analisar, sucintamente, a necessidade de criação de uma lei geral sobre o tema, estabelecendo alguns aspectos essenciais a serem trazidos pelo instrumento normativo a ser adotado no país. Destacou-se, pois, a necessidade de delimitação de conceitos básicos como dados pessoais, dados pessoais sensíveis e tratamento de dados; a abordagem do papel do consentimento na tutela da privacidade e proteção de dados pessoais; mecanismos de proteção da privacidade através do "*privacy by design*" e "*privacy by default*" e a criação de um órgão nacional dirigido por profissionais técnicos e com expertise sobre o tema para atuar na formulação de normas e diretrizes sobre a proteção de dados, bem como na fiscalização da lei.

BIBLIOGRAFIA:

Livros e Artigos:

ACQUISTI, Alessandro. Economics of Information Security: Privacy and Rationality in Individual Decision Making; IEEE Security & Privacy, 2005. Pp. 26

ACQUISTI, Alessandro & GROSSKLAGS Jens. Privacy and Rationality: A Survey. IEEE Security & Privacy (2005), Pp. 24/25

BALDWIN, Robert; CAVE, Martin and LODGE, Martin; Understanding Regulation: : theory, strategy and practice. Second Edition. Oxford. Pp. 3 Et. Seq.

BIONI, Bruno Ricardo. Prize norms and functional perspective of law: a new normative production to foster a holistic privacy regulation. PP. 93 Et. Seq. Disponível em: <http://www.ifip-summerschool.org/wp-content/uploads/2015/08/Summer-School-2015-PreProceedings.pdf > Acesso em 20.05.2017

BIONI, R. Bruno. Privacidade e Proteção de Dados Pessoais em 2017. JOTA. Disponível em: https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/privacidade-e-protecao-de-dados-pessoais-em-2017-10012017 Acesso em 20.05.2017

BIONI, R. Bruno. Como o Brasil pode ter um plano Nacional de IoT Inovador? JOTA. Disponível em: https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/como-o-brasil-pode-ter-um-plano-nacional-de-iot-inovador-12052017. Acesso em 21.05.17

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico, V. 12, N. 2, 2011. Pp. 104

DONEDA, Danilo. Da privacidade à proteção de dados pessoais.

FORTES, Vinícius Borges. Os direitos de privacidade e a proteção de dados pessoais na internet. Rio de Janeiro. Lumen Juris. 2016. Pp. 120

GOMES, Rodrigo Dias de pinho. Breves considerações sobre desafios à privacidade diante do Big Data na Sociedade da Informação. V Encontro Internacional do CONPEDI Montevidéu-Uruguai. pg. 290.

GUIDI, Guilherme Berti de Campos. Modelos Regulatórios para Proteção de Dados Pessoais. ITS/RIO. Pp. 4

LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2012

MORAES, Maria Celina Bodin. Danos à pessoa humana: Uma leitura civil constitucional dos danos morais.

SIMON, Herbert A. (1957) Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting, New York: John Wiley and Sons, *apud* BARROS, GUSTAVO. Herbert A. Simon and the concept of rationality: Boundaries and procedures. Revista de Economia Política, 2010. Pp. 457 Et. Seq.

SOLOVE, Daniel J., Privacy Self-Management and the Consent Dilemma, Pp. 126 Harv. L. Rev. 1880 (2013)

T. VILA, R. Greenstadt, and D. Molnar, "Why We Can't be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market," The Economics of Information Security, L.J. Camp and S. Lewis, eds., Kluwer, 2004, Pp. 143–154.

VIEIRA, Tatiana Malta. O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO: efetividade desse direito fundamental diante dos avanços da tecnologia de informação

WHITE CASE, Unlockig the EU general data protection regulation: a practical handbook on the EU's new data protection law. 25 Julho 2016. Pp. na 20

Legislação e textos oficiais:

BRASIL, Constituição Federal da República do Brasil de 1988

BRASIL, Decreto 8.771 de 2016

BRASIL, Decreto Lei 2.848 de 1940. Código Penal.

BRASIL, Lei 9.507 de 1997. "Lei do *Habeas Data*".

BRASIL, Lei 12.965 de 2014. Marco Civil da Internet.

BRASIL, Lei 12.527 de 2011. Lei de Acesso à Informação.

BRASIL, Lei 8.078 de 1990. Código de Defesa do Consumidor.

BRASIL. Lei 10.406 de 2002. Código Civil.

BRASIL, Lei 12.373 de 2012. Lei de Crimes Cibernéticos.

BRASIL, Projeto de Lei 330 de 2013

BRASIL Projeto de Lei 4.060 de 2012

BRASIL Projeto de Lei 5276 de 2016

EUROPA, Conselho da Europa: Convenção 108 de 1981

EUROPA, Regulamento 2016/679/UE

EUROPA, Tratado de Funcionamento da União Europeia de 2012

EUROPA, Diretiva 95/46/CE

EUROPA. Comissão Europeia: Fact Sheet Disponível em: <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm.> Acesso em 21.05.2017

EUROPA, Disponível em: https://infoeuropa.eurocid.pt/files/database/000061001-000062000/000061756.pdf

Relatórios, Notícias & Vídeos:

Carta Aberta de Apoio ao PL 5.276. Brasília, 02 de Junho de 2016. Disponível em: <http://intervozes.org.br/wp-content/uploads/2016/06/Carta-Aberta.-PL-Dados-Pessoais.02.06.2016.pdf> Acesso em 18.05.2017

Coalizão Direitos na Rede: Contribuições ao Congresso Nacional acerca dos PLs sobre a proteção de dados pessoais, página 2, item C.

Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais, pág. 50

How the internet Works, The EDRi papers. 3ª Edição, 2012. PP. 3 e Pp. 16 Et Seq. Disponível em https://edri.org/files/2012EDRiPapers/how_the_internet_works.pdf

NICbrvideos. "A internet das coisas, explicada pelo NIC.br" Youtube: Disponível em youtube: <https://www.youtube.com/watch?v=jlkvzcG1UMk>. Acesso em 21.05.2017

FTC Staff Report Internet of Things: privacy & security in a connected world. Pp. 5 Et. Seq. Disponível em: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> Acesso em 21.05.2017

INDEPENDENT UK, There are officialy more mobile devices than people in the world. Disponível em: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html> Acesso em 21.05.207

FORBES, 20 fatos sobre a internet que você provavelmente não sabe. Disponível em: <http://www.forbes.com.br/fotos/2015/10/20-fatos-sobre-a-internet-que-voce-provavelmente-nao-sabe/> Acesso em 21.05.2017

THE GUARDIAN, Google to pay record $22.5m fine to FTC over Safari tracking. Disponível em: <https://www.theguardian.com/technology/2012/aug/09/google-record-fine-ftc-safari> Acesso em 21.05.2017

FORBES, Can behavioural targeting survive privacy worries. Disponível em: <http://www.forbes.com/sites/roberthof/2011/07/20/can-behavioral-targeting-survive-privacy-worries/#3468c692609c> Acesso em 21.05.2017

UOL, OLHAR DIGITAL, Microsoft diz que dados são o novo petróleo. Disponível em: <http://olhardigital.uol.com.br/pro/noticia/microsoft-diz-que-dados-sao-o-novo-petroleo/56776> Acesso em 21.05.2017

DOMO, Data never sleeps. 4.0 Disponível em: <https://www.domo.com/blog/data-never-sleeps-4-0/> Acesso em 21.05.2017

EXAME, Estudo desvenda hábitos de consumo de internet na América Latina. Disponível em: <http://exame.abril.com.br/tecnologia/estudo-desvenda-habitos-de-consumo-de-internet-na-america-latina/ > Acesso em 21.05.2017

FGV PROJETOS, Uso de Big Data ajuda governo brasileiro gastar de forma mais eficiente. Disponível em: <http://fgvprojetos.fgv.br/noticias/uso-de-big-data-ajuda-governo-brasileiro-gastar-de-forma-mais-eficiente> Acesso em 21.05.2017