UNIVERSIDADE FEDERAL DO RIO DE JANEIRO CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS FACULDADE DE DIREITO

ANÁLISE REGULATÓRIA DA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

AMANDA BALBÃO DA SILVA

Rio de Janeiro

2017 / 1

AMANDA BALBÃO DA SILVA

ANÁLISE REGULATÓRIA DA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Flávio Alves Martins**.

Rio de Janeiro
2017 / 1

CIP - Catalogação na Publicação

Silva, Amanda Balbão da
S586a Análise regulatória da proteção de dados pessoais na Internet / Amanda Balbão da Silva. -- Rio de Janeiro, 2017.
80 f.

Orientador: Flávio Alves Martins.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2017.

1. Dados Pessoais. 2. Internet. 3. Privacidade. 4. Proteção de Dados. 5. Análise Regulatória. I. Martins, Flávio Alves, orient. II. Título.

CDD 340.0285

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

AMANDA BALBÃO DA SILVA

ANÁLISE REGULATÓRIA DA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Flávio Alves Martins**.

Data da Aprovação: ____ / ____ / _____.

Banca Examinadora:

_____

Professor Dr. Flávio Alves Martins

_____

Membro da Banca

_____

Membro da Banca

Rio de Janeiro
2017 / 1

RESUMO

Este trabalho tem por objetivo analisar as medidas regulatórias adotadas no Brasil e ao redor do mundo no que tange à proteção de dados pessoais e da privacidade na Internet. Além dos marcos regulatórios do setor, a temática da tecnologia relacionada à segurança das informações é abordada através do estudo de conceitos como *Internet of Things* (*IoT*), *Big Data* e criptografia, cada vez mais presentes no cotidiano de grande parte da população global, em decorrência da rápida popularização da Internet. Atualmente, é possível dizer que estamos vivendo em uma era digital, e o Direito precisa estar minimamente preparado para lidar com a realidade virtual. Neste cenário de hiperconexão, exposição e compartilhamento de dados, observamos o surgimento de modalidades de violação de direitos fundamentais específicas ao meio virtual, e que, portanto, necessitam de amparo legal igualmente específico para que a privacidade dos usuários de Internet não seja banalizada ou violada em prol de interesses corporativos.

Palavras-chave: Internet; dados pessoais; privacidade; tratamento; proteção de dados.

ABSTRACT

This paper aims to analyze the regulatory measures adopted in Brazil and around the world in reference to the protection of personal data and privacy on the Internet. Besides the sector's regulatory landmarks, the topic of technology related to the information's security is approached through the studies of concepts such as Internet of Things (IoT), Big Data and cryptography, each time more present in the routine of most of the global population, due to Internet's fast popularization. Nowadays, it is possible to say that we are living in a digital era, and Law must be minimally prepared to deal with the virtual reality. In this scenery of hiperconnection, exposure and sharing of data, we observe the rise of modalities of violation of fundamental rights specific of the virtual environment, and that, therefore, need an equally specific legal support, so that the privacy of Internet users will not be trivialized or violated in favor of corporative interests.

Keywords: Internet; personal data; privacy; treatment; data protection.

SUMÁRIO

1 INTRODUÇÃO

Nos dias atuais, na chamada Era Digital, observamos um cenário de hiperconectividade, compartilhamento demasiado de informações e hiperexposição dos que se aventuram a criar perfis em redes sociais ou interagir em plataformas virtuais. A ferramenta que mais contribui com a diminuição de barreiras entre os seres humanos, a nível global, é a Internet, que se propaga através dos mais diversos meios: computadores, notebooks, tablets, smartphones e assim por diante.

Como é de conhecimento geral, a Internet e os aparatos a ela relacionados vêm se desenvolvendo aceleradamente nos últimos anos. Hoje em dia temos dispositivos, aplicativos e tecnologias que sequer cogitávamos ter ainda ontem. Se o acesso à rede mundial de computadores era antes um privilégio de poucos, a realidade atual é significativamente mais conectada e acelerada.

Não é surpreendente, portanto, que tenha havido um aumento igualmente admirável – ou assustador, para os saudosos da era anterior – no número de usuários conectados à rede. Segundo dados do E-Commerce Brasil[1], em 2015, o Brasil era o terceiro país no mundo que mais gasta seu tempo na Internet, perdendo apenas para Tailândia e Filipinas, com a marca de 5,4 horas diárias frente à tela. E se estes números já impressionam por si só, pensemos ainda que, de acordo com a mesma pesquisa, somos apenas o 19º país do mundo quanto à penetração de Internet sobre o total da população. Isso significa que grande parte dos brasileiros ainda não tem acesso à rede, o que abre espaço para o crescimento no número de usuários nos próximos anos.

O preocupante, porém, é que junto à taxa de usuários, se expandem em idêntica proporção as taxas de ilícitos relacionados a dados: perdas, roubos, fraudes, dentre outros incidentes. De acordo com o consultor técnico sênior de Email Fraud Protection da Return Path, Pablo Dewes[2], anualmente, em média, 4,5 bilhões de dólares são perdidos apenas em decorrência de fraudes via e-mail.

---

1 Pesquisa mostra dados da Internet no Brasil em 2015. Mercado. E-Commerce Brasil. 20 fev. 2015. Disponível em: <https://www.ecommercebrasil.com.br/noticias/pesquisa-mostra-dados-da-internet-no-brasil-em-2015/>. Acesso em: 05 jun. 2017.

2 DEWES, Pablo. A gestão de risco e os desafios da segurança no varejo online. Segurança. E-Commerce Brasil. 28 set. 2015. Disponível em: <https://www.ecommercebrasil.com.br/artigos/a-gestao-de-risco-e-os-desafios-da-seguranca-no-varejo-online/>. Acesso em: 28 maio. 2017.

Ainda, neste contexto de disseminação de informações, é comum que nos esqueçamos de que alguns desses dados podem ser excessivamente íntimos ou particulares para que sejam acessados por um número indeterminado de pessoas, muitas vezes desconhecidas, ou em determinados contextos não previstos pelo titular das informações no momento em que decidiu torná-las acessíveis. Em razão desta ignorância, corremos o risco de nos expormos demasiadamente em plataformas virtuais, aplicativos e redes sociais.

Todavia, ainda que se possa atingir um alto nível de conscientização dos usuários, que são os titulares de dados pessoais no ambiente virtual, há que se falar em medidas positivas de proteção aos dados pessoais e à privacidade no meio cibernético. Nesta toada, observamos que juristas e legisladores ainda buscam se adaptar a um mundo conectado, procurando uma forma de criar leis ou atuar nos tribunais de maneira eficiente e que supere as limitações tradicionais de regulação e tutela jurisdicional. Isto nos faz compreender o quanto a persecução da positivação de direitos no ambiente digital se faz necessária à proteção dos usuários que lá trafegam. Além disso, é também útil aos provedores, que se encontram no polo oposto dessa relação jurídica, para que possam ter um referencial sobre como atuar de forma a evitar futuros litígios, que poderiam cominar em condenações.

Embora tenhamos no Brasil, atualmente, a Lei nº 12.965 de 2014, conhecida como Marco Civil da Internet, a mesma carece de regulamentação em alguns pontos, no que concerne à proteção de dados e da privacidade. Nessa linha, urge o debate atinente à regulação das atividades de gerência de dados pessoais dos usuários da rede mundial de computadores. É necessário garantir a privacidade e intimidade dos usuários, ao mesmo tempo em que seja permitida uma certa flexibilidade, para que possa haver avanço no setor tecnológico. É também de extrema importância que os usuários sejam informados sobre os procedimentos aos quais seus dados pessoais são submetidos, e que possam optar por autorizar ou não as diferentes formas de tratamento de dados.

A proteção de dados pessoais é um tema recente, cujos desdobramentos se complexificam a cada dia. Introduziremos, no decorrer deste trabalho, termos como *Big Data* e *IoT*, que são indicativos do que está no horizonte do uso de dados. Observaremos a atuação de outros países e blocos econômicos, que estão tratando ou pretendem tratar do tema via legislação interna ou tratados internacionais, e veremos, como já mencionado, que a proteção às informações que trafegam na rede mundial de computadores carece de regulação específica a nível nacional.

Veremos que, buscando providenciar garantias e segurança aos usuários, a nova Lei de Proteção de Dados, quando inserida no plano interno, deverá almejar um equilíbrio entre direitos fundamentais, de modo que nenhuma das partes envolvidas no tratamento de dados se sinta lesada. Notaremos que o direito à informação e o direito à privacidade constantemente entram em conflito, o que faz com que seja árduo o debate tanto entre especialistas da área quanto no âmbito legislativo.

Assim, a partir da análise dos sujeitos e termos envolvidos neste tema, das experiências regulatórias estrangeiras, bem como dos precedentes judiciais a nível nacional e das propostas legislativas atualmente em tramitação no Congresso Nacional, este trabalho pretende construir um panorama geral da proteção da privacidade e dos dados pessoais na Internet.

Tentou-se demonstrar a atualidade, a relevância e a função social do tema a ser pesquisado neste trabalho. Realizar um levantamento das discussões que vêm ocorrendo em território nacional e em outros países é de suma importância para compreender como serão tratadas as problemáticas envolvendo esta imensa gama de usuários e dados. Como estabelecer uma legislação nacional que ampare o usuário, parte hipossuficiente na relação com os provedores de Internet, para que não tenha lesados os seus direitos fundamentais no ambiente virtual, é o que nos questionamos quando observamos o cenário regulatório atual.

Novamente, cabe ressaltar que a conscientização do usuário da rede mundial de computadores é outro aspecto que a presente monografia se propõe a analisar, extremamente necessário à proteção da privacidade no ambiente virtual, complementarmente à criação de lei interna. Em sua passagem pelo Brasil em junho de 2016, Indra Spiecker, diretora do Centro de Pesquisas sobre Proteção de Dados da Universidade de Frankfurt e estudiosa no tema, alertou quanto a essa necessidade.

Assim sendo, justificando em linhas gerais a escolha do tema, concedamos destaque à relevância social do debate acerca da possibilidade de elaboração de uma lei específica sobre proteção de dados pessoais no ambiente virtual, que supra as necessidades do Marco Civil da Internet. Além disso, abordar as ações do usuário frente às novas tecnologias, que se somarão à legislação na defesa de seus direitos, mostra-se de extrema utilidade a todos os cidadãos conectados no Brasil, que carecem, em muitos casos, de uma educação digital.

Por fim, a tendência à expansão da utilização da Internet e do desenvolvimento de novos aplicativos e dispositivos conectados à rede demonstra a atualidade do presente tema.

Somados todos estes fatores, resta justificada uma pesquisa mais aprofundada, a ser desenvolvida ao longo deste trabalho.

O estudo terá início, inevitavelmente, com a conceituação dos elementos principais concernentes ao tema e às regulações que visam trata-lo. Como veremos, são conceitos indispensáveis ao estudo da proteção e do tratamento de dados pessoais, que auxiliarão na compreensão dos demais tópicos.

2 TRATAMENTO DE DADOS PESSOAIS NO AMBIENTE VIRTUAL

2.1 Conceitos

Uma das maiores contradições referentes à proteção de dados pessoais no ambiente virtual é a conceituação dos elementos e atividades relacionados aos dados. Isso porque, ao mesmo tempo em que as definições são necessárias para que se saiba o que é o objeto de estudo ou da lei de proteção de dados, elas são também um grande risco ao engessamento e consequente inutilidade do dispositivo legal. Definir, afinal, é limitar. E é de conhecimento geral que a Internet e a tecnologia estão em constante evolução e são, portanto, avessas a circunscrições e termos fechados.

O ato de criar uma definição, portanto, deve ser cauteloso. O legislador deve cuidar para que o conceito constante da lei seja claro e preciso o suficiente para haver certeza do que se trata tal elemento, porém com certo grau de generalização ou elasticidade, para que possa abarcar as tecnologias que surgem ao longo do tempo ou que não estavam previstas para serem acolhidas por aquele dispositivo legal no momento de sua elaboração.

Neste sentido, Danilo Doneda[3] relatou, durante o 30º Seminário Internacional da ABDTIC[4], que:

> "Quando se trata da proteção de dados pessoais como tema a ser regulado, deixa-se para trás considerações subjetivas, relativas à privacidade ou não, e parte-se para uma regulação objetiva: existem dados pessoais, que são informações referentes a uma pessoa, e essas informações poderão ser usadas ou não, dependendo do que a lei estabelecer. Isso é algo concreto, que deve ser simples, para que possa ser transformado em um código de boas práticas ou em um programa ou algoritmo que possa ser lido e introduzido a um modelo de negócios."

3 Bacharel em Direito pela Universidade Federal do Paraná (UFPR), com mestrado e doutorado em Direito Civil pela UERJ. Atualmente é consultor da Secretaria Nacional do Consumidor do Ministério da Justiça (Senacon) e do Comitê Gestor da Internet no Brasil (CGI.br). É membro do conselho consultivo sobre privacidade do Projeto Global Pulse, da Organização das Nações Unidas. É membro do conselho consultivo do Projeto Criança e Consumo, do Instituto Alana. Foi Coordenador-Geral de Estudos e Monitoramento de Mercado da Senacon/MJ. Foi professor na Faculdade de Direito do Estado do Rio de Janeiro (UERJ), Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) e Fundação Getulio Vargas (FGV). Foi pesquisador visitante na Autoridade Garante para a Proteção de Dados em Roma, Itália, Na Università deli Studi di Camerino (Camerino, Itália) e no Instituto Max Planck para Direito Privado Comparado e Internacional (Hamburgo, Alemanha). Autor de livros e diversos artigos sobre direito civil, direito à privacidade e proteção de dados pessoais. Disponível em: <http://www.internetlab.org.br/pt/equipe/cv/#danilo-doneda> Acesso em: 15 jan. 2017.

4 30º SEMINÁRIO INTERNACIONAL DA ASSOCIAÇÃO BRASILEIRA DE DIREITO DA TECNOLOGIA DA INFORMAÇÃO E DAS COMUNICAÇÕES. Painel: Temas atuais em proteção de dados pessoais e privacidade. 2016. São Paulo. SP.

Desta afirmação, extraímos a compreensão de que a objetividade é aliada do operador do direito quando este se debruça à atividade de conceituar elementos. A abrangência legal acima mencionada, ou seja, a flexibilidade da definição, não deve ser entendida como uma abstração absoluta. Para haver real proteção aos dados pessoais, é necessário tornar nítidos seus objetos e seu alcance, englobando, assim, a segurança no próprio corpo da legislação.

Deste modo, é relevante que se tenha em mente a existência de polêmicas relacionadas à conceituação dos objetos do tratamento de dados pessoais, bem como a complexidade e a importância da tarefa de estabelecer definições. Por afetar diversos setores econômicos e sociais, já foram realizadas, no Brasil, duas consultas públicas sobre uma provável legislação específica. A primeira ocorreu em 2011[5]; a segunda, em 2015.[6] Atualmente, temos algumas propostas concretas tramitando no Congresso Nacional, sobre as quais falaremos adiante. O que nos interessa, neste ponto, é que todas trazem uma série de definições, sobre as quais falaremos a seguir.

2.1.1 Dado Pessoal

Iniciamos a análise com o conceito mais simples e menos controverso. Embora haja diferenciações quanto à definição de dado pessoal no cenário internacional, bem como nas proposições legislativas tramitando no Congresso, o ponto central se mantém: trata-se de informação relativa a uma pessoa identificada ou identificável. Esta informação, que pode ser de qualquer natureza, é passível de ser armazenada, processada e transferida a terceiros conforme o que determina a legislação que lhe é aplicada.

Como exemplos de dados pessoais, podemos citar dados locacionais, como o endereço residencial, e números identificativos, como os de documentos de identidade (RG, CPF).

---

[5] SANTOS, Ludmila. Governo quer mais proteção para dados na internet. Consultor Jurídico. 25 jan. 2011. Disponível em: <http://www.conjur.com.br/2011-jan-25/consulta-publica-traca-diretrizes-lei-protecao-dados-pessoais>. Acesso em 27 maio.2017

6 SALOMÃO, Lucas. Governo abre consulta pública sobre proteção de dados pessoais na web. G1. Brasília. DF. 28 jan. 2015. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/01/governo-abre-consulta-publica-sobre-protecao-de-dados-pessoais-na-web.html>. Acesso em: 27 maio. 2017.

2.1.2 Dado Anônimo ou Anonimizado

Dados anônimos, por sua vez, são dados que não podem mais identificar um indivíduo, à exceção dos casos em que tais dados sofrem um processo de desanonimização, ou seja, de reversão da sua qualidade de anônimo.

Como exemplo de dados anônimos, podemos citar um evento que ocorre no sítio virtual YouTube, notório *player* gratuito de vídeos. É de conhecimento dos gestores e usuários do YouTube que determinado vídeo obteve, por exemplo, 20 milhões de acessos. A quantidade de acessos está disposta na página de exibição do próprio vídeo e pode ser vista por qualquer um que acesse o *site*. Tal informação foi fornecida por cada usuário no momento em que assistiu ao vídeo e passou por um processo de anonimização, ou seja, de retirada de informações ou características que a vinculam ao usuário que a forneceu, para que pudesse integrar um rol meramente estatístico, indicador da popularidade daquele determinado vídeo. Observando esta estatística, não é mais possível identificar quais usuários acessaram o vídeo, embora deles tenha originado essa informação. O dado é, portanto, anônimo. Ou diz-se que foi anonimizado.

É importante ressaltar que, embora não sejam dados pessoais, os dados anônimos não podem ser tratados de qualquer maneira, pois são dados que em algum momento pertenceram a um indivíduo. Em outras palavras, a informação jamais deixará de se referir a uma pessoa – apenas não seremos capazes de saber quem é. Bem, ao menos enquanto não for realizada a desanonimização do dado, que é um processo de reversão do anonimato cada vez mais barato, acessível e utilizado no mercado, devido aos avanços constantes no setor tecnológico.

O progresso da tecnologia, portanto, traz consigo a necessidade de reforçar a proteção dos dados anônimos. De acordo com Danilo Doneda[7], em palestra concedida à ABDTIC em

7 Bacharel em Direito pela Universidade Federal do Paraná (UFPR), com mestrado e doutorado em Direito Civil pela UERJ. Atualmente é consultor da Secretaria Nacional do Consumidor do Ministério da Justiça (Senacon) e do Comitê Gestor da Internet no Brasil (CGI.br). É membro do conselho consultivo sobre privacidade do Projeto Global Pulse, da Organização das Nações Unidas. É membro do conselho consultivo do Projeto Criança e Consumo, do Instituto Alana. Foi Coordenador-Geral de Estudos e Monitoramento de Mercado da Senacon/MJ. Foi professor na Faculdade de Direito do Estado do Rio de Janeiro (UERJ), Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) e Fundação Getulio Vargas (FGV). Foi pesquisador visitante na Autoridade Garante para a Proteção de Dados em Roma, Itália, Na Università deli Studi di Camerino (Camerino, Itália) e no Instituto Max Planck para Direito Privado Comparado e Internacional (Hamburgo, Alemanha). Autor de livros e diversos artigos sobre direito civil, direito à privacidade e proteção de dados pessoais. Disponível em: <http://www.internetlab.org.br/pt/equipe/cv/#danilo-doneda> Acesso em: 15 jan. 2017.

2016[8], a técnica historicamente utilizada no tratamento dos dados anônimos é de utilização de normas permissivas. Em outras palavras, se o dado for anônimo, as leis de proteção não incidirão sobre ele. Essa ótica vem sendo mitigada, na medida em que não é possível considerar qualquer dado, hoje em dia, como absolutamente anônimo. Como já mencionado, o progresso tecnológico facilitou imensamente a atividade de reidentificação. Atualmente, a questão não é "se" o dado poderá perder sua qualidade de anônimo, quando, como e por quais razões se busca o acesso à tecnologia necessária para desanonimizá-lo. Quanto a isto, ressaltem-se algumas considerações do diretor da Agência Espanhola de Proteção de Dados, José Luis Rodríguez, em reportagem realizada pelo Jornal El País[9]:

> "Os metadados podem ser dados pessoais e muitas vezes o são", recorda o diretor da Agência Espanhola de Proteção de Dados, José Luis Rodríguez. "Para que não sejam dados pessoais têm de ser anônimos, com uma dissociação irreversível", acrescenta. Se, como nessa pesquisa, é possível fazer o caminho inverso dos metadados à identidade da pessoa, então seria aplicada a legislação sobre privacidade. Para Rodríguez, o problema de fundo é que "na medida que existe cada vez mais informação disponível, debilita-se a anonimização porque há mais possibilidades de combinar e, portanto, de identificar ou individualizar a pessoa".

É preciso reconhecer que o próprio conceito de dados anônimos já não é, tecnicamente, tão fixo, imutável a ponto de se presumir que as leis de proteção de dados não possam ser aplicadas a tal categoria de dados. Ainda que tais dados não sejam desanonimizados, é possível que gerem efeitos sobre o indivíduo a quem a informação um dia pertenceu.

Um exemplo desta situação problemática seria a construção de perfis comportamentais. Isto porque, através de dados anônimos ou anonimizados, como dados de compras, por exemplo, é possível reidentificar um indivíduo – ou seja, alcançar um dado pessoal desta pessoa, ou mesmo um dado sensível, que será melhor explicado adiante. Tal possibilidade já foi testada mais profundamente por um grupo de pesquisadores do Media Lab do Instituto Tecnológico de Massachusetts (MIT), segundo reportagem do Jornal El País (2015)[10]. Neste ponto, é pertinente uma breve reflexão de Yves-Alexandre de Montjoye, pesquisador do MIT e coautor da referida pesquisa.

---

8 30º SEMINÁRIO INTERNACIONAL DA ASSOCIAÇÃO BRASILEIRA DE DIREITO DA TECNOLOGIA DA INFORMAÇÃO E DAS COMUNICAÇÕES. Painel: Temas atuais em proteção de dados pessoais e privacidade. 2016. São Paulo. SP.

9 CRIADO, Miguel Ángel. Quatro compras com o cartão bastam para identificar qualquer pessoa. Privacidade na Internet. El País. 30 jan. 2015. Disponível em: <http://brasil.elpais.com/brasil/2015/01/29/ciencia/1422520042_066660.html>. Acesso em: 27 maio. 2017.

10 CRIADO, Miguel Ángel. Quatro compras com o cartão bastam para identificar qualquer pessoa. Privacidade na Internet. El País. 30 jan. 2015. Disponível em: <http://brasil.elpais.com/brasil/2015/01/29/ciencia/1422520042_066660.html>. Acesso em: 27 maio. 2017.

> "É o paradoxo dos dias de hoje. As bases com imensas quantidades de dados anonimizados servem para mostrar a unicidade do ser humano. (...), não se trata tanto do aspecto previsível dos humanos, mas de como nossa conduta (e nossos padrões de compra) nos fazem únicos em comparação com outros".

Faz-se mister ressaltar, todavia, que, do ponto de vista regulatório, não deve haver confusão entre dados anônimos e dados pessoais. As diferentes categorias não devem ser reguladas da mesma maneira. Fazê-lo traria problemas, pois o processo de reidentificação (desanonimização) nem sempre ocorre. Além disso, é possível que dados anônimos sejam utilizados de forma responsável e positiva. Seria o caso de dados anônimos utilizados pelo Poder Público na elaboração de políticas públicas. O legislador não pode, portanto, assumir que haverá mau uso destes dados.

Sendo assim, na inadequação de providências regulatórias que visem uma aproximação demasiada das formas de tratamento de dados anônimos e pessoais, cresce a responsabilidade dos provedores e gestores de bancos de dados, no sentido de dar um tratamento legítimo e lícito aos dados que estão em seu poder, não realizando a reidentificação e respeitando o titular dos dados, ainda que possuam tecnologia suficiente para realizar a desanonimização.

Aumenta, também, a consideração do "risco" nas atividades ligadas aos dados anônimos. Conforme a tecnologia avança, se populariza e o custo dos aparatos tecnológicos diminui, torna-se cada vez mais constante o risco de que o dado anônimo possa ser desanonimizado. Este risco leva a outros, como a discriminação de indivíduos, comunidades, dentre outros.

Assim sendo, é importante levar em consideração a noção de risco quando da elaboração de uma futura lei de proteção de dados, especialmente no tocante aos dados anônimos. Afinal, com o passar do tempo e a crescente confusão entre as categorias de dados, o risco vem se tornando um elemento central. Todo cuidado é necessário para que o tratamento indevido de um dado anônimo não leve a consequências danosas ao seu titular, imprevistas em sua própria categoria.

2.1.3 Dado Sensível

É correto dizer que os dados sensíveis são a categoria de dados que merece maior proteção legal. Podemos considerar dados sensíveis como informações importantes sobre um indivíduo, ligadas a etnia, religião, orientação sexual, opiniões políticas, dentre outras.

A razão pela qual tais dados devem possuir um alto grau de proteção regulatória é que, considerada sua sensibilidade, a divulgação ou compartilhamento destes dados pode desencadear ações discriminatórias em relação ao titular. Ou, ainda, é possível que haja tentativa, por parte do detentor das informações, de obter vantagens ou cometer abusos perante o titular dos dados.

Um exemplo de atividade danosa contra o titular dos dados é a situação em que uma companhia de seguros tem acesso indireto a dados relativos à saúde do assegurado. Ao tomar conhecimento das mazelas que aquele indivíduo possui ou dos riscos de desenvolver determinadas doenças, a companhia pode decidir elevar o preço de sua oferta de seguro.

A situação acima deixa nítida a necessidade de proteção acentuada dos dados sensíveis pela regulação, para que não haja prejuízo ao titular. Aqui, novamente, o avanço tecnológico é um fator preocupante, posto que dados sensíveis podem ser alcançados de maneira diversa da convencional e impossível de ser prevista e abarcada previamente pelo legislador.

Nos dias atuais, os dados sensíveis citados no exemplo acima, referentes à saúde de seu titular, poderiam ser obtidos através da análise de uma fotografia em alta definição, por exemplo, havendo tecnologia e tratamento adequados para tanto.

2.1.4 Dado Cadastral

Dados cadastrais são frequentemente confundidos com dados pessoais. O Marco Civil Civil da Internet (Lei nº 12.965 de 2014), em seu art. 10, §3º[11], faz distinção entre dados pessoais e dados cadastrais, sendo estes últimos aqueles que podem ser utilizados para a finalidade específica de acesso mediante requisição de autoridades investigativas. Ou seja, em

11 Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 3o O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

caso de investigação de crime ou outra necessidade de obtenção de dados, a autoridade administrativa competente poderá, sem necessidade de expedição de mandado judicial, ter acesso aos dados cadastrais.

Podemos citar como exemplos de dados cadastrais a filiação e o endereço de uma pessoa. Embora devam ser diferenciados dos dados pessoais, não é verdadeira a afirmação de que dados cadastrais não necessitam de proteção do arcabouço jurídico. Afinal, muitas vezes o mesmo dado pode ser enquadrado tanto como pessoal quanto como cadastral. O diferencial é que, sendo dado cadastral, está enquadrado na exceção disposta pelo Marco Civil, eliminando a necessidade de ordem judicial para obtenção de acesso.

Neste diapasão, podemos concluir que, para todos os demais dados além dos dados cadastrais, é necessária, no Brasil, a apresentação de ordem judicial para sua obtenção. Esta necessidade de mandado judicial gera grandes debates relacionados à obrigatoriedade de armazenamento de dados, criptografia e competência das autoridades investigativas para requererem tais dados.

2.1.5 Banco de Dados

Banco de dados (em inglês, *database*) é uma coleção de dados inter-relacionados organizada de forma estruturada por meio de uma rede. Entendemos como "rede" um sistema de informação que permita a reunião e compartilhamento destes dados armazenados. As informações disponíveis no banco de dados podem ser acessadas diretamente, mediante acesso ao próprio dispositivo no qual estão armazenadas, ou por meio da rede, quando se encontram em dispositivos remotos.

Os bancos de dados são úteis ao armazenamento e utilização (tratamento) de dados de diversas categorias: pessoais, sensíveis ou cadastrais. As informações ali armazenadas podem ser consultadas a qualquer momento pelos responsáveis pelo tratamento de dados, além de serem passíveis de atualizações e correções.

É importante frisar que as leis de proteção de dados são aplicáveis a estes bancos, portanto todos os direitos e garantias dos usuários devem ser respeitados durante o gerenciamento.

A vantagem dos bancos de dados é que estes permitem que mais de um indivíduo tenha acesso, simultaneamente, ao seu conteúdo. Além disso, é possível armazenar um rol considerável de informações.

2.1.6 Tratamento de Dados Pessoais

É correto utilizar o termo "tratamento de dados pessoais" quando nos referimos às atividades ou operações relacionadas a dados ou bancos de dados. Tais atividades incluem o compartilhamento de dados, classificação, armazenamento, comparação, contagem, retificação, exclusão, dentre outras.

Geralmente, o tratamento é autorizado pelo titular, que é o indivíduo a quem pertencem os dados. Esta autorização é denominada consentimento e tem gerado grandes polêmicas no Brasil e no mundo. Uma das discussões se refere à necessidade, ou não, de consentimento explícito para determinadas atividades de tratamento de dados.

O Projeto de Lei nº 5.276 de 2016, principal proposta de criação de lei específica de proteção de dados pessoais que tramita na Câmara dos Deputados no momento, traz em seu art. 7º[12] as possiblidades em que o tratamento de dados pode ocorrer. E justamente neste artigo são detalhadas as hipóteses de necessidade ou não de consentimento do titular dos dados.

O PL estipula que, em geral, deve ser fornecido consentimento livre e inequívoco por parte do titular, que poderá ser revogado sem ônus e a qualquer momento. As exceções

12 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento pelo titular de consentimento livre e inequívoco;
II – para o cumprimento de uma obrigação legal pelo responsável;
III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;
IV – para a realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais;
V – quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular dos dados;
VI – para o exercício regular de direitos em processo judicial ou administrativo; VII
– para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII – para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
IX – quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.

envolvem: (i) dados de acesso público irrestrito; (ii) cumprimento de uma obrigação legal; (iii) realização de pesquisa histórica, científica ou estatística, priorizando a anonimização; (iv) exercício de direitos em processo judicial ou administrativo; (v) proteção da vida, saúde ou incolumidade física; (vi) execução de procedimentos contratuais ou pré-contratuais; (vii) proteção do crédito.

2.1.7 Responsável pelo Tratamento de Dados

Uma última definição que se faz necessária diz respeito ao responsável pelo tratamento de dados. A nomenclatura desta figura ainda não está totalmente definida mesmo no âmbito das proposições legislativas. Além disso, verificamos nos principais projetos de lei em tramitação – PLS nº 330 de 2013 e PL nº 5.276 de 2016 – três categorias de indivíduos que estão relacionados às atividades de tratamento de dados: responsável, operador e encarregado. As definições destes elementos constam nos incisos VI e VII do art. 3º[13] do PLS nº 330 de 2016, e nos incisos VIII, IX e X do art. 5º[14] do PL nº 5.276 de 2016.

De maneira generalizada, podemos considerar que estas figuras têm em comum o fato de serem interlocutores do titular de dados na relação de tratamento. As distinções ocorrem na esfera da responsabilidade frente a violações de direitos do titular e mau uso dos dados, bem como das atividades específicas exercidas por cada um.

Chamamos de "responsável" pelo tratamento de dados o indivíduo a quem competem as decisões referentes ao tratamento. O responsável determinará como deverão ser conduzidas as atividades, e é ele que irá determinar quem será o "operador", que é o indivíduo que realizará, na prática, o tratamento de dados. O PL nº 5.276 de 2016 introduz uma figura extra, que não

13 Art. 3º Para os efeitos desta Lei, considera-se: (...)
VI – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII – operador: a pessoa jurídica contratada pelo responsável pelo banco de dados, encarregada do tratamento de dados pessoais;

14 Art. 5º Para os fins desta Lei, considera-se:
(...)
VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
IX – operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável;
X – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente;

se encontra nas previsões do PLS nº 330 de 2013: o encarregado. O encarregado pelo tratamento de dados seria, de acordo com a proposta, o indivíduo que atuaria como canal de comunicação entre o responsável pelo tratamento e os titulares e órgãos públicos. Cabe ressaltar que o encarregado deve ser, necessariamente, pessoal natural, enquanto tanto o responsável quanto o operador poderão ser pessoas naturais ou jurídicas, de acordo com o que está disposto em ambos os projetos de lei.

2.2 Criptografia

No dicionário, a definição é concisa: criptografia é a "arte ou processo de escrever em caracteres secretos ou em cifras"[15]. A criptografia é, nos dias de hoje, de fácil acesso e, por isso, empregada por diversos aplicativos e sistemas operacionais. No ambiente virtual, é largamente utilizada como uma forma de proteger informações pessoais, dados sensíveis, números de cartões de crédito, conteúdos de conversas em redes sociais, dentre outros dados cujo sigilo é desejado pelos titulares. Trata-se, portanto, de um mecanismo de segurança.

A técnica consiste em proteger mensagens escritas, convertendo-as em códigos ou cifras que só serão acessíveis por meio de uma chave temporária e exclusiva do receptor destas mensagens. Os que desconhecem tais convenções, ou seja, quaisquer outros indivíduos conectados à rede aos quais a mensagem não foi direcionada, não são capazes de visualizar seu conteúdo.

Existe grande discussão em âmbito interno e internacional relacionada à criptografia enquanto obstáculo a investigações criminais. No Brasil, são preocupantes os diversos precedentes judiciários de ordenar o bloqueio em território nacional do WhatsApp, aplicativo de mensagens instantâneas mais utilizado no país atualmente[16].

15 MICHAELIS. Dicionário Brasileiro da Língua Portuguesa. Português Brasileiro. Criptografia. Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=criptografia>. Acesso em: 27 maio. 2017.
16 MANZONI JÚNIOR, Ralphe. WhatsApp é o aplicativo mais usado pelos brasileiros. IstoÉ. Dinheiro. Bastidores das empresas. 18 jan. 2017. Disponível em: <http://www.istoedinheiro.com.br/blogs-e-colunas/post/20170118/whatsapp-aplicativo-mais-usado-pelos-brasileiros/10223>. Acesso em: 27 maio. 2017.

A primeira ordem de bloqueio data de fevereiro de 2015, expedida pelo juiz Luis Moura Correia, da Central de Inquéritos da Comarca de Teresina, Piauí[17]. Pouco tempo depois, em dezembro de 2015, a 1ª Vara Criminal de São Bernardo do Campo (SP) ordenou novo bloqueio[18], alegando que o WhatsApp não havia atendido a uma determinação judicial de julho de 2015, em um processo criminal que corria em segredo de justiça. Em maio e julho de 2016, novas decisões de bloqueio foram proferidas, com a justificativa de que a direção do WhatsApp havia se negado a compartilhar informações essenciais a uma investigação criminal[19].

Todas as decisões de bloqueio de aplicativos em razão de negativa de cooperação com as autoridades por parte de seus administradores sofreram duras críticas. Em todos os casos, o principal argumento do WhatsApp para justificar sua negativa em fornecer as informações solicitadas é o de que nem mesmo eles teriam acesso a tais dados, tendo em vista o sistema criptográfico utilizado pelo aplicativo.

Conforme reportagem do jornal O Estado de S. Paulo (Estadão), o WhatsApp aderiu à criptografia em 2012, protegendo o conteúdo das mensagens trocadas por seus usuários. A criptografia de ponta a ponta, contudo, que fornece proteção do início ao fim da transmissão da mensagem, só foi implementada em 2014. Tal criptografia que abrange todo o trajeto do conteúdo é a mais eficiente em termos de segurança, por permitir que apenas emissor e receptor tenham acesso ao conteúdo, excluindo do acesso inclusive os próprios administradores do aplicativo. Porém, por este mesmo motivo, causa frisson aos operadores do direito que entendem pela legalidade – e obrigatoriedade – de disponibilização do conteúdo de conversas em meio virtual, por parte dos provedores de aplicação, em caso de decisão judicial que assim determine. Ora, se não é tecnicamente possível o acesso ao conteúdo, resta definitivamente prejudicada a obrigação de disponibilizá-lo.

Para conciliar a proteção à privacidade dos usuários destes aplicativos, frequentemente é sugerida a criação de um *backdoor*, ou seja, de uma "porta" de acesso ao conteúdo, caso seja

17 Decisão de juiz do Piauí manda tirar WhatsApp do ar em todo o Brasil. G1. Piauí. 25 fev. 2015. Disponível em:<http://g1.globo.com/pi/piaui/noticia/2015/02/decisao-de-juiz-do-piaui-manda-tirar-whatsapp-do-ar-em-todo-o-brasil.html>. Acesso em: 27 maio. 2017.

18 WhatsApp bloqueado: operadoras são intimadas a barrar app no país por 48h. G1. São Paulo. 16 dez. 2015. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/12/operadoras-sao-intimadas-bloquear-whatsapp-no-brasil-por-48-horas.html>. Acesso em: 27 maio. 2017.

19 SOPRANA, Paula. Justiça determina bloqueio do WhatsApp pela terceira vez em sete meses. Época. 19 jul. 2016. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/07/justica-determina-bloqueio-do-whatsapp-pela-terceira-vez-em-sete-meses.html>. Acesso em: 27 maio. 2017.

necessário. Ora, não seria incorreto dizer que se trata de uma falha proposital na segurança – criticável, portanto, do ponto de vista dos que prezam pela proteção de dados. Nesse sentido, o especialista em segurança e desenvolvimento e diretor de pesquisas do Instituto Igarapé, Robert Muggah, rejeita a obrigatoriedade de criação de backdoors em entrevista concedida à Revista Época em 2016[20]:

> Muitos governos – incluindo os democráticos – estão profundamente preocupados com a criptografia de mensagens em plataformas como WhatsApp Telegram, Wickr, Gliph, Signal Private Messenger e tantas outras. Eles estão preocupados porque essas plataformas são usadas por células terroristas, pelo crime organizado, por pedófilos e, também, por manifestantes e opositores políticos legítimos. Certo ou errado, eles temem que esse tipo de informação transmitida não seja monitorada, muito menos apresentada como prova julgamentos. Na verdade, WhatsApp e Telegram não podem cumprir com uma ordem judicial que demande o acesso ao conteúdo trocado por seus serviços. Eles argumentam que simplesmente não têm a informação a dar, já que é criptografada. Assim, algumas autoridades públicas têm pressionado empresas de tecnologia a criar acessos backdoor. No entanto, é bem improvável que as empresas de tecnologia façam isso. Gigantes como Apple, Google e Facebook simplesmente têm muito a perder [como clientes, lucros e mercado]. Nos últimos anos, essas companhias se tornaram extremamente proativas em proteger a privacidade de seus clientes. Uma companhia sabe muito bem que, se o fato de eles criarem um backdoor para o governo se tornar público, isso pode acabar com seus negócios. Nos Estados Unidos, muitos políticos estão criando leis para forçar as companhias a criar backdor em plataformas criptografadas. Esse debate foi inflamado depois dos ataques em Paris, em novembro de 2015, mas começou em 2011, quando a Apple lançou o iOS7 e passou a criptografar seus smartphones – junto ao iMessages e às ligações do FaceTime. O argumento de que o uso de criptografia deixa terroristas na sombra é ilusório porque há uma grande oferta de novas tecnologias [televisões com câmeras e microfones, tecnologia que acompanha carros com GPS conectados à internet, aplicações caseiras e gadgets vestíveis] que as autoridades poderiam usar para monitorar os suspeitos. Talvez hoje existam mais ferramentas disponíveis ao governo do que jamais existiu.

A quebra da criptografia seria, portanto, uma forma facilitada e sem altos custos para se obter uma imensa leva de informações pessoais. Por isso o anseio da justiça em legaliza-la. Por outro lado, fica claro o prejuízo à privacidade de todos os usuários, e não apenas àqueles investigados pela justiça, com a criação de mecanismos que violem a criptografia. Todavia, a questão é complexa por exigir, na resolução do caso concreto, o afastamento de um direito constitucionalmente assegurado em prol de outro direito de igual relevância: ou se preserva o direito à privacidade dos usuários, ou se preza pelo direito à informação e pela segurança, permitindo o acesso a dispositivos, dados e conteúdos de mensagens transmitidas pela rede mundial de computadores.

---

[20] SOPRANA, Paula. Como a polícia pode dar a volta na criptografia do WhatsApp. Época. 23 jul. 2016. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/07/como-policia-pode-dar-volta-na-criptografia-do-whatsapp.html>. Acesso em: 27 maio. 2017.

A criptografia, enfim, não é um assunto polêmico apenas em terras brasileiras. Amber Rudd, Secretária de Defesa do Reino Unido, fez duras críticas ao sistema de criptografia de aplicativos como o WhatsApp após o ataque ocorrido próximo ao Parlamento britânico, em março de 2017, que levou à morte de quatro pessoas e deixou dezenas de feridos[21]. Em entrevista à Rede BBC, Rudd demonstrou ser favorável à quebra da criptografia e fez renascer no cenário europeu a discussão quanto à criação de *backdoors*[22].

Seguindo a mesmo linha de raciocínio da Secretária de Defesa britânica, os Ministros do Interior Thomas de Maizière, da Alemanha, e Matthias Fekl, da França, requereram ao Parlamento Europeu, no dia 27 de março de 2017, que criassem instrumentos jurídicos que possibilitassem a exigência de colaboração de provedores OTTs – como o WhatsApp, por exemplo – com as autoridades investigativas.

2.3 Big Data

Se antes era um termo desconhecido, atualmente o *Big Data* é familiar mesmo a indivíduos que não lidam diretamente com tecnologia e tratamento de dados. Trata-se de um imenso aglomerado de dados, estruturados ou não, que quando tratados e analisados geram resultados que não poderiam ser alcançados observando-se cada informação separadamente. Dados estruturados são aqueles que possuem uma organização lógica, enquanto os dados não estruturados são informações avulsas, que ainda precisarão se organizadas e associadas. Estas grandes bases de dados podem ser de natureza comercial, educacional, científica, governamental, administrativa, dentre outras.

Tais dados necessitam de ferramentas computacionais que permitam sua análise e associação, tornando possível seu aproveitamento. Possuindo a tecnologia adequada, é possível utilizar o *Big Data* por meio de diversas maneiras, obtendo vantagens com as novas informações descobertas através do cruzamento de dois ou mais dados pré-existentes.

---

21 Ataque perto do Parlamento britânico em Londres deixa 4 mortos, incluindo suspeito. Mundo. G1. Brasil. 22 mar. 2017. Disponível em: <http://g1.globo.com/mundo/noticia/tiroteio-fora-do-parlamento-britanico-deixa-feridos.ghtml>. Acesso em: 27 maio. 2017.

22 AMARAL, Bruno do. Europa pressiona WhatsApp pelo fim da criptografia em investigações de terrorismo. Mobile Time. 27 mar. 2017. Disponível em: <http://www.mobiletime.com.br/27/03/2017/europa-pressiona-whatsapp-pelo-fim-da-criptografia-em-investigacoes-de-terrorismo/468662/news.aspx?__akacao=4011184&__akcnt=012c3547&__akvkey=a6b3&utm_source=akna&utm_medium=email&utm_campaign=MOBILE+TIME+News+-+27%2F03%2F2017+20%3A01>. Acesso em: 27 maio. 2017.

Neste diapasão, Ronaldo Goldschmidt e Eduardo Bezerra, autores do livro "*Data Mining*: conceitos, técnicas, algoritmos, orientações e aplicações", elucidam algumas técnicas de Data Mining, um subgrupo do universo *Big Data* pautado no desenvolvimento e aplicação de técnicas de utilização e aproveitamento do *Big Data*, em artigo elaborado em novembro de 2016[23].

Temos a técnica denominada Descoberta de Associações, que consiste basicamente em descobrir padrões e repetições dentro de um conjunto de dados. Esta modalidade de *Data Mining* é frequentemente utilizada no setor de Marketing, pois por meio dela é possível estabelecer padrões de comportamento e consumo. Outra técnica comum é a Classificação, que é de grande utilidade, por exemplo, ao setor financeiro. Tomando como exemplo uma empresa de seguros, a atividade analítica consiste em desvendar uma função que mapeie um conjunto de registros, de modo a classifica-los e, assim, permitir que sejam identificados clientes adimplentes e inadimplentes através da classificação de seus dados. Esse sistema ajudaria na filtragem para concessão de empréstimos.

Goldschmidt e Bezerra revelam também, em seu estudo, que o *Big Data* vem sendo utilizado em diversos setores no território nacional, a saber: Educação, Telecomunicações, Ações Sociais, Finanças, Comércio, Saúde e mesmo no setor Tributário, em uma tentativa de otimizar a arrecadação de impostos, por meio de análise de dados dos contribuintes que revelassem padrões e permitissem a antecipação de fraudes ao Fisco.

O objetivo neste ponto não é esgotar as possibilidades em torno do *Big Data*, mas tão somente esclarecer o conceito e a existência de inúmeros métodos de tratamento destas informações. Fica claro o quão lucrativas as descobertas decorrentes do cruzamento de dados podem ser aos envolvidos com o setor privado, bem como os inúmeros benefícios organizacionais e econômicos ao setor público.

Todavia, a existência de tantas formas de tratamento e de megabancos de dados amplia a apreensão quanto à segurança destas informações. Ora, se novas informações estão sendo "criadas", melhor dizendo, descobertas através de atividades de tratamento, é possível que tais dados se enquadrem em categorias não previstas anteriormente pelo usuário que concedeu as informações primeiras que o originaram. É o que ocorreria se, durante o cruzamento de dois

[23] GOLDSCHMIDT, Ronaldo; BEZERRA, Eduardo. Exemplos de aplicações de data mining no mercado brasileiro. ComputerWorld. 27 jun. 2016. Disponível em: <http://computerworld.com.br/exemplos-de-aplicacoes-de-data-mining-no-mercado-brasileiro>. Acesso em: 27 maio. 2017.

dados pessoais, se revelasse um dado sensível. Deste modo, é imprescindível que, ainda que não faça menção ao *Big Data*, especificamente, uma futura Lei de Proteção de Dados atente à hipótese de situações inesperadas de surgimento de novos dados que necessitem de maior proteção. Por se tratar de uma imensa quantidade de dados, requerer o consentimento do usuário estaria fora de cogitação. Uma alternativa viável, neste caso, poderia ser a anonimização dos dados gerados pelos processos de exploração do *Big Data*.

Essa preocupação não é uma exclusividade brasileira. A questão foi recentemente abordada no Japão, em reunião do chamado Industrial Structure Council, na qual o governo discutiu formas de criar uma legislação que pudesse, simultaneamente, proteger os dados pessoais e incentivar o investimento em seu tratamento e uso criativo, sem gerar temor nas empresas de incorrer em ilícitos enquanto buscam inovação.[24]

A incerteza permanece, contudo. Em março de 2017, a comissária da União Europeia Margrethe Vestager relatou que ainda não há investigações quanto ao impacto do armazenamento de um grande volume de dados, mas que tal análise será necessária enquanto assistimos ao avanço da exploração do *Big Data*.[25]

2.4 Internet of Things (IoT)

Traduzida literalmente como Internet das Coisas, a *Internet of Things* (*IoT*) é o futuro da conexão via rede mundial de computadores. É possível conceber *IoT* como um cenário de hiperconexão entre objetos e seres humanos ou entre objetos e objetos, por meio da Internet. Os *smartphones* são os exemplos mais comumente conhecidos desta geração de dispositivos conectados, porém outros estão se popularizando, como é o caso das televisões, geladeiras, relógios e carros 'inteligentes'.

As vantagens trazidas pelos dispositivos da era *IoT* são muitas, todas girando em torno da otimização: de tempo, de gastos, de atividades, etc. Os detentores de um relógio conectado, por exemplo, podem obter dados ligados a sua saúde ou mesmo visualizar e-mails profissionais e receber avisos de redes sociais. *IoT*, contudo, não são apenas facilidades. a

24SEKIGUCHI, Toko. Japan debate on Big Data IP protection hits classic issue of regulation v. innovation. MLEX Market Insight. Jurisdiction: Asia, Japan, North East Asia. 17 mar. 2017.

25 CROFTS, Lewis. Big Data case in Europe 'still to come', Vestager says. MLEX Market Insight. Jurisdiction: EU, Europe. 31 mar. 2017.

privacidade de usuários de dispositivos inteligentes é uma grande preocupação, e a realidade de conexão entre tudo e todos que se mostra próxima é um desafio aos reguladores em todo o mundo. Há a necessidade de lidar com o *IoT* da mesma maneira que se lida com o *Big Data*, buscando proteger o usuário sem frear a inventividade e os avanços na área tecnológica.

O Brasil ainda está alguns passos atrás neste âmbito. Durante debate da Futurecom em outubro de 2016, algumas figuras relevantes no setor deram seus pareceres. José Gontijo, diretor de Indústria, Ciência e Tecnologia do Ministério da Ciência, Tecnologia, Inovações e Comunicações, entende que o ponto central a ser discutido no caso dos dispositivos conectados não é o monitoramento dos usuários, mas que informações serão geradas e como serão tratadas pelo setor privado e pelo governo. Por sua vez, Leonardo Capdeville, CTO da TIM, se mostrou preocupado com a infraestrutura de rede, sugerindo que o primeiro desafio a ser superado é garantir acesso à Internet com eficiência e qualidade no país. O diretor de tecnologia de rede e sistemas da Oi, Pedro Falcão, está sintonizado com este pensamento.[26]

Em fevereiro de 2017 foi encerrada uma consulta pública pela Secretaria de Política de Informática do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), cujos resultados serão analisados para elaboração de diretrizes do Plano Nacional de Internet das Coisas (*IoT*). Além da supracitada Secretaria do MCTIC, foi criada a Câmara de Internet das Coisas, que é composta por representantes do MCTIC e outros 42 órgãos do governo, centros de pesquisa e entidades representativas.

O objetivo do Plano é desenvolver uma política nacional de desenvolvimento do setor de *IoT* no Brasil, com ações públicas e políticas que se estenderão até 2022. A Agência Nacional de Telecomunicações (Anatel) estima que o país possui, atualmente, em torno de 20 milhões de conexões entre dispositivos.[27]

Assim como no caso do Big Data, a segurança do imenso rol de dados coletados é uma preocupação para o legislador. A futura Lei de Proteção de Dados nacional deve ser preparada de modo a abarcar este quadro de ultraconexão que em breve se concretizará no Brasil. De acordo com Caio Mário da Silva Pereira Neto, diretor da FGV Direito de São Paulo, não há como cogitar a obrigação de requerer o consentimento expresso do usuário a cada operação de

---

[26] AMARAL, Bruno do. IoT ainda traz incertezas ao setor. Internet das Coisas. TeleTime. 18 out. 2016. Disponível em: <http://convergecom.com.br/teletime/18/10/2016/iot-ainda-traz-incertezas-ao-setor/>. Acesso em: 27 maio. 2017.

27 Consulta sobre o Plano Nacional de IoT recebeu 2,28 mil contribuições. CIO. 16 fev. 2017. Disponível em: <http://cio.com.br/tecnologia/2017/02/16/consulta-sobre-o-plano-nacional-de-iot-recebeu-2-28-mil-contribuicoes/>. Acesso em: 27 maio. 2017.

coleta de dados, em um cenário altamente conectado. Como solução, sugere a coleta de dados dissociados e anônimos.[28]

Como visto, a conexão e, consequentemente, a coleta de dados estão em constante aprimoramento e cada vez mais frequentes em nosso cotidiano. Em razão do caráter internacional da Internet, que não possui fronteiras físicas, o cuidado com a privacidade dos titulares dos dados que trafegam na rede é um dever universal. Assim sendo, é conveniente que abordemos no próximo capítulo como é regulada a proteção de dados pessoais internacionalmente, analisando legislações nacionais e de blocos econômicos.

28 AMARAL, Bruno do. IoT ainda enfrenta barreiras regulatórias para decolar no Brasil. TeleTime. 7 fev. 2017. Disponível em: <http://convergecom.com.br/teletime/07/02/2017/iot-ainda-enfrenta-barreiras-regulatorias-para-decolar-no-brasil/?noticiario=TT&__akacao=3934077&__akcnt=012c3547&__akvkey=19e6&utm_source=akna&utm_medium=email&utm_campaign=TELETIME+News+-+07%2F02%2F2017+22%3A46>. Acesso em: 27 maio. 2017.

3 PANORAMA INTERNACIONAL

Como dito anteriormente, uma das características mais notáveis da Internet é sua aversão a limitações espaciais. Ainda que o caráter transfronteiriço não seja desculpa para que não se elabore uma legislação a nível nacional, pois é extremamente relevante que haja um arcabouço regulatório específico para fundamentar a aplicação do direito interno, acaba inspirando países a trabalharem conjuntamente, como podemos observar nas tentativas de uniformização da proteção da privacidade no ambiente virtual por parte de determinados blocos econômicos ou parceiros comerciais.

União Europeia e Asia-Pacific Economic Cooperation (APEC)[29] vêm buscando a uniformização do nível de proteção entre seus países-membros, trabalhando em direção a acordos – no caso do APEC – ou regulações – como ocorre na União Europeia – relativos à proteção de dados, buscando, se não uma identidade, ao menos um patamar mínimo de tutela em todos os países pertencentes àquele bloco ou fórum econômico regional.

Individualmente, alguns países também se encontram em um nível regulatório mais avançado, possuindo legislações exemplares de proteção de dados pessoais. Outros países, como o Brasil, caminham a passos lentos e ainda estão em processo de elaboração de uma lei interna específica sobre o tema.

Neste sentido, é fundamental observar as previsões legais já estabelecidas nos países e blocos econômicos mais avançados na matéria, observando suas experiências para aproveitá-las, no que couberem, no preparo de nosso próprio diploma legal. Iniciaremos o estudo do cenário internacional pela União Europeia, expoente na regulação da proteção de dados pessoais no ambiente virtual.

3.1 União Europeia

Em abril de 2016, foi promulgado o Regulamento nº 2016/679, conhecido como General Data Protection Regulation (GDPR)[30], em substituição à Diretiva Europeia de

[29] About APEC. What is Asia-Pacific Economic Cooperation?. Asia-Pacific Economic Cooperation. APEC Secretariat. 2017. Disponível em: <http://www.apec.org/About-Us/About-APEC>. Acesso em: 27 maio. 2017.

30 EUROPE UNION. Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

Proteção de Dados de 1995, ultrapassada e inapta para lidar com as lides decorrentes da utilização de novas tecnologias. O GDPR entrará em vigor em maio de 2018, concedendo maiores garantias aos usuários em relação ao tratamento de seus dados pessoais e simplificando o ambiente regulatório para as empresas que realizam tais operações.

O arcabouço regulatório da proteção de dados pessoais na União Europeia é constituído pelo GDPR somado à ePrivacy Directive, também conhecida como Directive on Privacy and Electronic Communications[31], diretiva que o complementa e que foi adotada em janeiro de 2017.

As recentes introduções destes dois diplomas legais fazem parte de um plano de ação da Comissão Europeia para estabelecer e garantir a segurança do chamado Digital Single Market. Trata-se de uma estratégia que visa a livre circulação de pessoas, serviços e capital no ambiente cibernético, objetivando o crescimento da economia digital na região. A estratégia foi adotada em maio de 2015 e inclui diversas iniciativas para tornar este cenário possível.[32]

No que tange aos padrões de proteção de dados pessoais, dentre outras previsões, a ePrivacy Directive determina que: (i) os novos players de comunicação por meio eletrônico, como o WhatsApp, por exemplo, estejam sujeitos às regras de privacidade da União Europeia, fornecendo o mesmo nível de segurança dos provedores tradicionais de telecomunicações; (ii) a privacidade é garantida ao conteúdo e aos metadados, que são dados sobre outros dados, das comunicações online; (iii) os navegadores forneçam um modo facilitado para que os usuários consintam ou não com a coleta de cookies. Em caso de cookies que coletem informações não invasivas, como aqueles que guardam informações do "carrinho de compras" em um site de vendas, ou utilizados para contabilizar o número de visitantes do site, não é necessário requerer o consentimento do usuário; (iv) devem ser banidos os chamados *spams*, que são as comunicações não solicitadas, como e-mails de marketing não solicitados.[33]

---

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. Brussels. Disponível em: <http://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 27 maio. 2017.

[31] Proposal for an ePrivacy Regulation. Digital Single Market. Strategy. European Commission. 2017. Disponível em: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>. Acesso em: 27 maio. 2017.

32Digital Single Market. Strategy. European Commission. 2017. Disponível em: <https://ec.europa.eu/digital-single-market/en/digital-single-market>. Acesso em: 27 maio. 2017.

33 Proposal for an ePrivacy Regulation. Digital Single Market. Strategy. European Commission. 2017. Disponível em: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>. Acesso em: 27 maio. 2017.

Por sua vez, o General Data Protection Regulation impõe limitações e obrigações relativas à proteção da privacidade no ambiente digital, estabelecendo rígidas previsões para o tratamento de dados de cidadãos europeus, mesmo quando for realizado fora deste continente. Embora o regulamento sirva para simplificar o ambiente regulatório, como dito anteriormente, empresas situadas fora do continente europeu podem ter maiores preocupações após sua implementação, por se tratar de uma legislação bastante rigorosa quanto às restrições e obrigação de transparência no tratamento de dados pessoais e que implicará em adequações nos sistemas e políticas de privacidade de diversos *players* do setor. Outra grande preocupação será o alto valor da multa por infringência ao GDPR, que pode alcançar o patamar de 20 milhões de euros ou 4% da receita global anual da companhia.[34]

Além da previsão de multas severas, o General Data Protection Regulation trouxe inovações importantes ao cenário europeu[35]. Dentre elas, podemos citar a portabilidade de dados. Trata-se de um direito do titular de transferir livremente suas informações pessoais de um serviço conectado à rede a outro serviço. Atualmente, a portabilidade é prática comum para números de celulares e contas bancárias, inclusive no Brasil.

Outras medidas são a coleta de permissão para uso de dados pessoais, ou seja, de consentimento do titular de dados para que seja realizado o tratamento; o aviso obrigatório aos titulares em caso de dados comprometidos ou expostos por ataques de hackers ou outros tipos de violações; elaboração de relatórios de risco e documentação e monitoramento das atividades de tratamento de dados, por parte dos responsáveis; e a necessidade de elaborar as políticas de privacidade com uma linguagem clara e compreensível ao descrever as atividades que serão realizadas com os dados obtidos pelo serviço oferecido.

A novidade mais interessante, todavia, é a previsão do direito ao esquecimento. Em maio de 2014, o Tribunal de Justiça da União Europeia proferiu a decisão de apagar dados pessoais da internet, em um caso envolvendo ferramentas de busca *online*, como Google e Bing[36]. Este caso emblemático fez com que empresas que prestam tais serviços passassem a

---

34AMARAL, Bruno do. Nova regulação europeia de privacidade de dados trará impacto para outras regiões. MWC 2017. TeleTime. 28 fev. 2017. Disponível em: <http://convergecom.com.br/teletime/28/02/2017/nova-regulacao-europeia-de-privacidade-de-dados-trara-impacto-para-outras-regioes/>. Acesso em: 27 maio. 2017.

35 UE expande 'direito ao esquecimento' a todo serviço na internet. G1. São Paulo. 15 abr. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/ue-expande-direito-ao-esquecimento-todo-servico-na-internet.html>. Acesso em: 27 maio. 2017.

36 RODRIGUES JÚNIOR, Otavio Luiz. Direito de apagar dados e a decisão do tribunal europeu no caso Google (Parte 2). Direito Comparado. Consultor Jurídico. 28 maio. 2014. Disponível em:

analisar pedidos de cidadãos europeus de exclusão de informações pessoais, prática que agora é exigida pelo GDPR. Além dos buscadores virtuais, redes sociais e outros serviços que lidam com o tratamento de dados pessoais também estarão obrigados a assegurar o direito ao esquecimento nos casos em que seja averiguada real necessidade.

Durante a implementação do GDPR, os entes privados não serão os únicos a realizarem esforços para adaptarem-se às novas exigências. De acordo com o regulamento, cada Estado-membro da União Europeia deverá estabelecer uma autoridade específica para fiscalizar a aplicação do regulamento e atuar em caso de infrações. A União Europeia já possui sua própria Autoridade Europeia para a Proteção de Dados (AEPD), com sede em Bruxelas, Bélgica, com o intuito de garantir que todas as instituições do bloco resguardem o direito à privacidade de seus cidadãos durante o processamento de dados pessoais.[37]

Por fim, cabe comentar brevemente como será situação do Reino Unido neste cenário após sua saída da União Europeia, popularmente conhecida como Brexit. Em março de 2017, a International Association of Privacy Professionals (IAPP)[38], associação que treina e certifica profissionais especializados em privacidade, publicou relatório que revela que 94% dos profissionais ligados à privacidade, em mais de duzentas organizações do Reino Unidos, estão se preparando para adotar a GDPR.[39] Todavia, persiste a incerteza quanto ao futuro pós-Brexit, pois ainda não foi descartada pelo Reino Unido a hipótese de criação de uma lei nacional de proteção de dados.

3.2 Estados Unidos

Em razão do modelo federalista norte-americano, que concede grande autonomia aos Estados inclusive no plano regulatório, verificamos a existência de uma multiplicidade de leis e diretivas esparsas sobre privacidade, bem como guias específicos sobre a proteção da privacidade – seja dentro ou fora do ambiente *online* – em determinados setores, como o

---

<http://www.conjur.com.br/2014-mai-28/direito-comparado-direito-apagar-dados-decisao-tribunal-europeu-google-espanha>. Acesso em: 27 maio. 2017.

[37] EUROPEAN DATA PROTECTION SUPERVISOR. The EU's independent data protection authority. Disponível em: <https://edps.europa.eu/edps-homepage_en?lang=pt>. Acesso em: 27 maio. 2017.

38 The International Association of Privacy Professionals. Disponível em: <https://iapp.org/>. Acesso em: 27 maio. 2017.

39 UK privacy professionals preparing for new EU rules despite Brexit, IAPP says. MLEX Market Insight. Jurisdiction: EU, Europe. 15 mar. 2017.

bancário, consumerista e o de saúde, por exemplo. Não há uma lei federal específica sobre o tema, que determine como se dará o tratamento e proteção de dados pessoais a nível nacional.

Além da ausência de regulação federal, os Estados Unidos carecem de uma autoridade específica para a proteção de dados. O que se observa no país é a atuação dos órgãos reguladores com base em leis que não são sobre privacidade, exclusivamente, mas que acabam sendo utilizadas para coibir práticas abusivas relacionadas ao tratamento de informações pessoais. As leis consumeristas, por exemplo, são frequentemente aplicadas com esta finalidade.

Em um primeiro momento, o principal órgão guardião da privacidade em terras norte-americanas era a Federal Trade Commission (FTC)[40], agência federal especializada na proteção de consumidores. Todavia, esse panorama sofreu alterações em 2015, quando a Federal Communications Commission (FCC) adquiriu competência para estipular regras de privacidade aos provedores de serviços de Internet (ISPs), enquanto a FTC ficaria responsável pela fiscalização dos demais agentes.

Tal competência foi delegada à FCC quando os ISPs passaram a integrar o rol de agentes sob a jurisdição do conjunto de regras de neutralidade da FCC, denominado Open Internet Order. Naquela época, durante a gestão do presidente Tom Wheeler, estipulou-se que os provedores teriam a obrigação de alertar os usuários quanto às informações que seriam coletadas e como seriam tratadas, bem como de garantir que este tratamento seria realizado com um rigoroso padrão de segurança. Além disso, tornaram-se regras a coleta de consentimento opt-in dos usuários, bem como a opção de utilização dos serviços sem o fornecimento de dados.[41]

Contudo, a eleição de Donald Trump à presidência dos Estados Unidos levou a um retrocesso neste cenário regulatório, com a nomeação do republicano Ajit Pai a *chairman* da FCC em janeiro de 2017.[42] Pai, conservador, alinhado à política de Trump e avesso às medidas democráticas adotadas por Wheeler na gestão anterior, confia em uma política que,

---

40 FEDERAL TRADE COMISSION. Washington, DC. Estados Unidos. Disponível em: <https://www.ftc.gov>. Acesso em: 27 maio. 2017.

41 AGÊNCIAS. EUA avançam em proposta de privacidade na internet. Link. Estadão. 31 mar. 2016. Disponível em:<http://link.estadao.com.br/noticias/empresas,eua-avancam-em-proposta-de-privacidade-na-internet,10000047929>. Acesso em: 27 maio. 2017.

42 AMARAL, Bruno do. Trump confirma Ajit Pai como novo chairman da FCC. TeleTime. 23 jan. 2017. Disponível em: <http://convergecom.com.br/teletime/23/01/2017/trump-confirma-akit-pai-como-novo-chairman-da-fcc/>. Acesso em: 27 maio. 2017.

ao invés de regulamentar os provedores de Internet, aposta na desregulação do setor de telecomunicações e na liberdade dos modelos de negócios – o que significa, por exemplo, a autorização de práticas como o *zero rating* (tarifa-zero para determinados serviços) e o afastamento de medidas pró neutralidade de rede.

Como consequência, no início de abril de 2017 foi sancionada pelo presidente Trump a lei que reverteu a regulamentação da FCC de proteção à privacidade para provedores de Internet adotada em 2015.[43] Este movimento gerou apreensão quanto à manutenção das práticas protetivas de dados pessoais das operadoras, após o relaxamento do arcabouço regulatório.

3.3 América Latina

A América Latina é um continente que possui um caminho considerável a ser trilhado em busca da proteção de dados no ambiente cibernético. Atualmente, as jurisdições que possuem leis específicas de proteção de dados pessoais são: Argentina, Uruguai, Chile, Colômbia, Costa Rica, Curaçao, Peru e Trindade e Tobago.[44] O próprio Brasil, expoente da região, ainda está em vias de elaboração de uma lei específica para estes fins.

Das nações citadas no parágrafo anterior, Argentina e Uruguai são as únicas cujas leis de proteção de dados foram reconhecidas pela Comissão Europeia como suficientemente adequadas. As decisões nº 2003/490/EC e nº 2012/484/EU foram, respectivamente, as que atestaram os níveis de qualidade das legislações argentina e uruguaia.[45]

Enquanto países como Equador e Brasil estão em fase de discussão de projetos de lei sobre proteção de dados, a legislação Chilena, já consolidada e que pode ser considerada

---

[43] AMARAL, Bruno do. Trump sanciona lei que revoga regra de privacidade de usuários. Internacional. TeleTime. 4 abr. 2017. Disponível em: <http://convergecom.com.br/teletime/04/04/2017/trump-sanciona-lei-que-revoga-regra-de-privacidade-de-usuarios/?noticiario=TT>. Acesso em: 27 maio. 2017.

[44] RICH, Cynthia. Privacy Laws Around the World. ABA Journal. 29 ago. 2016. Disponível em; <http://www.abajournal.com/advertising/article/privacy_laws_around_the_world/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email>. Acesso em: 27 maio. 2017.

[45] European Commission decisions on the adequacy of the protection of personal data in third countries. Justice. European Commission. 2017. Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>. Acesso em: 27 maio. 2017.

rigorosa em suas disposições, carece ainda de previsões relativas ao registro e transferência internacional de dados, além de não estabelecer um órgão regulador específico para a área.[46]

Em relação à Argentina, a Lei de Proteção de Dados Pessoais, em vigor desde 2000, impõe altos padrões de segurança ao tratamento de informações pessoais de pessoas físicas ou jurídicas, registros e bancos de dados. Estabelece também uma autoridade específica para a proteção de dados a nível nacional. Um ponto falho, porém, é ausência de imposição de notificação aos usuários em caso de fraude ou vazamento de dados.

Dentre as características mais marcantes da legislação argentina, podemos citar a divisão das medidas de segurança em três níveis: (i) básico, que se refere às bases de dados que contém dados pessoais; (ii) médio, no caso de empresas privadas que atuem como agentes públicos, entidades públicas e proprietários de bases de dados que devem atuar em sigilo; (iii) alto ou crítico, referente às bases de dados que contenham dados sensíveis.

Por fim, a lei argentina proíbe a transferência internacional de dados a países que não proporcionem medidas adequadas de proteção, embora ainda não tenha divulgado quais países considera ou não aptos a cumprir tal exigência. Há exceções, porém, como nos casos em que há consentimento específico do titular dos dados ou a realização de um contrato. Atualmente, os contratos são analisados caso a caso pela autoridade argentina, que disponibiliza textos de cláusulas que são utilizados como parâmetro durante a avaliação destes acordos de transferência internacional.

O Uruguai, por sua vez, conta com a Lei nº 18.331 de 2008 para regular a proteção de dados pessoais. O país possui uma autoridade independente específica para fiscalizar a proteção à privacidade de dados. A legislação, que foi emendada em 2010, se opõe à lei Argentina por requisitar a notificação e registro em caso de fraude ou vazamento de dados. [47]

Por outro lado, a lei uruguaia se assemelha à argentina por também restringir a transferência internacional de dados a países que forneçam proteção adequada conforme legislação interna e padrões internacionais. As exceções, porém, são muitas, e se dão: (i) em

---

[46] RICH, Cynthia. Privacy Laws Around the World. ABA Journal. 29 ago. 2016. Disponível em; <http://www.abajournal.com/advertising/article/privacy_laws_around_the_world/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email>. Acesso em: 27 maio. 2017.

[47] RICH, Cynthia. Privacy Laws Around the World. ABA Journal. 29 ago. 2016. Disponível em; <http://www.abajournal.com/advertising/article/privacy_laws_around_the_world/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email>. Acesso em: 27 maio. 2017.

casos de cooperação judiciária internacional, estabelecida em tratado ou convenção; (ii) na troca de informações médicas, por motivos particulares ou por razões de ordem pública; (iii) para transferências de bancos ou estoques; (iv) no caso de cooperação internacional contra o crime organizado, terrorismo e tráfico de drogas; (v) com o consentimento da parte interessada; (vi) para a execução de contratos ou medidas pré-contratuais, ou de acordos que envolvam terceiros; (vii) para salvaguardar interesse público, ou reconhecer direitos e salvaguardar interesses em um processo judicial; (viii) nos casos em que os dados fornecidos sejam públicos ou abertos ao público em geral ou aos que comprovem legítimo interesse no acesso.

Além destas diversas exceções, a autoridade de proteção de dados pode, ainda, autorizar uma transferência internacional quando o responsável pelo tratamento fornecer – via cláusula contratual, por exemplo – garantias suficientes à proteção dos dados transferidos, dos direitos fundamentais e liberdades individuais de seu titular.

3.4 Japão

O Regulamento de Proteção de Dados japonês, em vigor desde 2005, regula o tratamento de dados pessoais no setor privado. Em setembro de 2015, foram aprovadas emendas ao regulamento, com o objetivo de fortalecer a proteção de dados e, simultaneamente, encorajar a utilização dos mesmos. Uma prática incentivada é anonimização para fins comerciais, que pode ser útil à rotina empresarial de tratamento de dados, além de impedir a obstrução do fluxo internacional de dados. Isto porque dados anonimizados costumam não requerer proteção muito rigorosa, em comparação aos dados pessoais e sensíveis. As emendas, todavia, só entrarão em vigor em maio de 2017.

Em janeiro de 2016, entrou em vigor a previsão legal de criação de uma Comissão para Proteção de Dados Pessoais (Personal Information Protection Commission – PIPC), uma autoridade independente responsável por fiscalizar o cumprimento das medidas protetivas.

Em razão do atual período de vacância das emendas, o Japão ainda deve criar restrições às transferências internacionais de dado. Atualmente, existe apenas a obrigação de notificação

em caso de eventos danosos ou de compartilhamento de dados com terceiros.[48] Há, ainda, a obrigação os entes privados que realizam tratamento de dados a coletar o consentimento dos titulares caso queiram repassar as informações a terceiros.

Embora a lei tenha sido emendada e diversas diretrizes tenham sido postas à consulta pública em novembro de 2016, a lei japonesa ainda apresenta muitas "áreas cinzentas", que trazem insegurança jurídica ao setor privado. Tais incertezas acabam sendo um empecilho a um dos objetivos do governo, que é incentivar o uso de dados. Shinichi Ogata, advogado especializado em proteção de dados e compliance no Escritório Eichi Law, em Osaka, relata ao noticiário MLex que a lei não esclarece devidamente, por exemplo, se as operações de armazenamento de dados em nuvens seriam consideradas como transferência de dados a terceiros. A classificação depende de especificidades contratuais e de como ocorre o tratamento dos dados, o que gera incertezas e receio por parte dos entes privados.[49]

De acordo com Naoko Ogawa, gerente da organização Keidanren (Federação Japonesa de Negócios)[50], as companhias japonesas possuem grandes quantidades de informações, porém não as exploram tanto, em comparação a outros países.[51] O governo estaria, então, tentando promover uma "quarta revolução industrial" envolvendo a *Internet of Things*, inteligência artificial e o *Big Data*.

Os consumidores japoneses, em geral, tendem a ser indiferentes quanto ao fornecimento de seus dados no ambiente virtual. Entretanto, têm reações exageradas em casos de vazamento de dados ou outros ilícitos, o que traz receio às empresas de explorar amplamente o grande volume de dados disponível, ou mesmo lançar novos serviços baseados na coleta e tratamento de dados.

3.5 Acordos Internacionais

---

48 RICH, Cynthia. Privacy Laws Around the World. ABA Journal. 29 ago. 2016. Disponível em; <http://www.abajournal.com/advertising/article/privacy_laws_around_the_world/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email>. Acesso em: 27 maio. 2017.

49 SAKAMAKI, Sachiko. Japan Inc. cautious about innovative data businesses, as amended privacy law looms. Jurisdiction: Asia, Japan, North East Asia. MLEX Market Insight. 31 mar. 2017.

50 KEIDANREN. Japan Business Federation. Disponível em: <http://www.keidanren.or.jp/en/profile/pro001.html>. Acesso em: 28 maio. 2017

51 SAKAMAKI, Sachiko. Japan Inc. cautious about innovative data businesses, as amended privacy law looms. Jurisdiction: Asia, Japan, North East Asia. MLEX Market Insight. 31 mar. 2017.

Embora as legislações internas tenham importância inquestionável na proteção da privacidade *online* e dos dados pessoais, estamos nos referindo à rede mundial de computadores. Como o nome já diz, é uma ferramenta global, que desconhece limitações físicas. Esta característica revela a utilidade de acordos internacionais, que forneçam maiores garantias aos países envolvidos por estabelecerem, para todos, um padrão de tratamento de dados e de medidas de proteção.

Nesta toada, passemos a uma breve análise de alguns dos principais acordos internacionais relacionados à proteção de dados na Internet.

3.5.1 Privacy Shield

Como observamos neste capítulo, a União Europeia possui restrições quanto à transferência de dados de cidadãos europeus a países que não proporcionem adequada proteção. Por tal motivo, foi realizado, em 2000, um acordo entre este bloco econômico e os Estados Unidos. O acordo Safe Harbour trazia garantias à U.E. de que os dados de seus cidadãos teriam a devida proteção das companhias norte-americanas durante o armazenamento e tratamento.[52]

Em 2015, a Corte de Justiça europeia declarou a invalidade do acordo Safe Harbour, após as polêmicas declarações de Edward Snowden. Snowden, ex-analista da Agência Nacional de Segurança norte-americana (NSA), havia vazado documentos secretos dos Estados Unidos em 2013, que revelavam detalhes de um plano de espionagem das comunicações via telefone e internet.[53]

Houve, então, um período em que empresas que mantinham negócios com a União Europeia tiveram que recorrer a cláusulas contratuais padronizadas, que forneceriam garantias quanto à proteção de dados. Até que, em julho de 2016, foi aprovado pela Comissão Europeia

52 GIBBS, Samuel. What is 'safe harbour' and why did the EUCJ just declare it invalid?. Internet. The Guardian.
6 out. 2015. Disponível em: <https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection>. Acesso em: 28 maio. 2017.

53 REUTERS. Rússia estende residência de Snowden após perdão dos EUA a Manning. G1. 18 jan. 2017. Disponível em: <http://g1.globo.com/mundo/noticia/russia-estende-residencia-de-snowden-apos-perdao-dos-eua-a-manning.ghtml>. Acesso em: 28 maio. 2017.

o acordo Privacy Shield, que impõe medidas de proteção e transparência mais rígidas do que as de seu antecessor, protegendo os direitos fundamentais destes cidadãos.[54]

O Privacy Shield é composto por: (i) rígidas obrigações às empresas norte-americanas que tratam dados de cidadãos europeus, com constantes revisões e atualizações para que o nível de proteção se mantenha; (ii) obrigação de segurança e transparência por parte do governo norte-americano, incluindo limitações de acesso governamental a dados, como consequência das delações de Edward Snowden. Estados Unidos se comprometeram, inclusive, a cessar as práticas de espionagem denunciadas; (iii) efetiva proteção dos direitos individuais, com a implementação de mecanismos para recepcionar reclamações de indivíduos que considerem que seus dados tenham sido utilizados indevidamente, buscando solucionar o problema; (iv) realização de uma revisão anual pela Comissão Europeia, em parceria com o Departamento de Comércio dos Estados Unidos.

As empresas norte-americanas que tenham interesse na aderência ao Privacy Shield devem certificar ao Departamento de Comércio dos Estados Unidos que cumprem os princípios deste acordo, ficando passíveis de fiscalização para atestar a veracidade dessa alegação.

Cabe ressaltar que este acordo sofreu abalos com a alteração da cena política norte-americana e suas consequências. A revogação das novas regras de privacidade da FCC para os provedores de Internet, sancionada pelo presidente Trump e arquitetada por Ajit Pai, atual *chairman* da FCC, incomodaram o Parlamento Europeu.

A reação se deu em abril de 2017, com a aprovação de uma resolução que estabelece um processo de revisão anual, a ser realizado pela Comissão Europeia, para garantir que, dentro do conturbado cenário político norte-americano, os dados de cidadãos europeus ainda estejam sendo tutelados de maneira devida, conforme a GDPR e os direitos humanos. A primeira revisão está prevista para setembro de 2017.[55]

---

54 The EU-U.S. Privacy Shield. Justice. European Commission. Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm>. Acesso em: 28 maio. 2017.

55 AMARAL, Bruno do. Parlamento Europeu critica política de privacidade de Trump e pede revisão de acordos. Internacional. TeleTime. 6 abr. 2017. Disponível em: <http://convergecom.com.br/teletime/06/04/2017/parlamento-europeu-critica-politica-de-privacidade-governo-trump-e-pede-revisao-de-acordos/?noticiario=TT&__akacao=4078097&__akcnt=012c3547&__akvkey=b105&utm_source=akna&utm_medium=email&utm_campaign=TELETIME+News+-+06%2F04%2F2017+22%3A51>. Acesso em: 28 maio. 2017.

Além das alterações nas regras da FCC, outros fatores motivaram a União Europeia a tomar esta medida. As novas regras da Agência Nacional de Segurança (NSA), que autorizam o compartilhamento de dados entre agências governamentais norte-americanas sem ordem judicial; a ausência de previsão de reparação judicial efetiva de direitos para os cidadãos europeus, tanto no acordo quanto na legislação estadunidense; e os desfalques nos corpos de supervisão de privacidade no governo dos Estados Unidos foram outros fatores que levaram à recente decisão do Parlamento Europeu.

3.5.2 Asia Pacific Economic Cooperation (APEC)

Chamamos de Asia-Pacific Economic Cooperation (APEC) o fórum regional econômico criado em 1989 para alavancar e integrar economicamente a região Ásia-Pacífico. O APEC possui 21 Estados-membros: Estados Unidos, Canadá, México, Peru, Chile, Nova Zelândia, Austrália, China, Hong Kong, Rússia, Coréia do Sul, Japão, Singapura, Vietnã, Malásia, Filipinas, Tailândia, Papua-Nova Guiné, Indonésia, Taipé Chinês e Brunei Darussalam.[56]

Em dezembro de 2005, foi publicado o APEC Privacy Framework, com o objetivo de promover a proteção da privacidade no comércio eletrônico entre os países membros e, ao mesmo tempo, evitar a criação de barreiras desnecessárias ao fluxo de dados.[57] O documento traz definições do que são "dados pessoais", "controlador de dados pessoais" e "informações disponíveis ao público"; princípios que regem a utilização de dados e um guia de implementação para os Estados-membros.

Para impulsionar a implementação do Privacy Framework, lideranças do APEC desenvolveram, em 2011, após contribuições das sociedades civil e industrial, o sistema Cross Border Privacy Rules (CBPR). O CBPR cria mecanismos de proteção à privacidade em casos

[56] About APEC. What is Asia-Pacific Economic Cooperation?. Asia-Pacific Economic Cooperation. APEC Secretariat. 2017. Disponível em: <http://www.apec.org/About-Us/About-APEC>. Acesso em: 27 maio. 2017.

57 APEC Privacy Framework. APEC#205-SO-01.2. Dez. 2005. Reports. Electronic Commerce Steering Group. p. 36. Disponível em: <http://publications.apec.org/publication-detail.php?pub_id=390>. Acesso em: 28 maio. 2017

de transferência internacional de dados dentro da região Ásia-Pacífico, mas com pretensões de expandir-se para outras áreas.[58]

É exigido dos membros da APEC que possuam uma Autoridade competente no plano interno para assuntos relacionado à privacidade, para que possam garantir a devida execução da CBPR. Além disso, devem participar do Cross-border Privacy Enforcement Arrangement (CPEA). Os principais propósitos da CBPR são: (i) possibilitar a transferência internacional de dados na região Ásia-Pacífico, ainda que leis nacionais a impeçam; (ii) harmonizar a proteção de dados na região; (iii) aumentar o nível geral de proteção da privacidade na região.

Atualmente, quatro economias da região aderiram à CBPR: Estados Unidos, México, Japão e Canadá. Contudo, outras economias demonstram interesse em participar. É o caso da Nova Zelândia, Coréia do Sul, Filipinas, Tailândia, Vietnã, Singapura, Hong Kong e Austrália.[59]

Em recente declaração ao noticiário MLex, em abril de 2017, um membro do Departamento de Comércio dos Estados Unidos se mostrou confiante quanto ao potencial da CBPR de se tornar um passo significante em direção à uma certificação global de proteção à privacidade, vindo a substituir acordos de alcance mais restrito, como é o caso do Privacy Shield.[60]

3.5.3 Trans-Pacific Partnership (TPP)

Trans-Pacific Partnership Agreement (TPP), estabelecido em 2015, é um grande acordo de comércio multinacional, do qual participam onze países em ambos os lados do Pacífico, que juntos representam grande percentual do PIB mundial. São eles: Austrália, Brunei Darussalam, Canadá, Chile, Japão, Malásia, México, Nova Zelândia, Peru, Singapura e

58 FORTIN-COUSENS, Anick; HEYDER, Markus. A Model for Global Privacy Protections. Bloomberg BNA. Privacy and Security Law Report by The Bureau of National Affairs, INC. 2015. APEC Privacy Rules for Cross-Border Data Flows.

59 Greater Protection for Consumers as Canada Joins Asia-Pacific Privacy Regime. Asia-Pacific Economic Cooperation. Ottawa, Canada. 15 abr. 2015. Disponível em: <http://www.apec.org/Press/News-Releases/2015/0415_CBPR.aspx>. Acesso em: 28 maio. 2017.

60 SWIFT, Mike. Commerce Department bullish on growth of trans-Pacific data transfer framework. Jurisdiction: Asia, Canada, Japan, Latin America, Mexico, North America, North East Asia, South Korea, Taiwan, USA. MLEX Market Insight. 20 abr. 2017.

Vietnã.[61] Os Estados Unidos eram membros do TPP até 2017, quando o presidente Donald Trump assinou uma ordem executiva ordenando sua retirada do acordo.[62]

O foco do TPP é a ampliação do livre comércio e integração da região do Pacífico. Além das disposições clássicas, o TPP possui provisões especiais para o comércio eletrônico, que asseguram a liberdade do tráfego internacional de dados e informações. Esta abertura econômica multinacional justifica a saída dos Estados Unidos durante o novo regime presidencial, posto que a atual política de governo é protecionista e voltada ao fomento da indústria nacional.

Nos trechos do acordo em que constam disposições relativas à privacidade, mas especificamente, no Capítulo 14, observamos a existência de uma definição de dados pessoais similar à da GDPR, abrangendo informações pessoais sobre uma pessoa identificada ou identificável.

Há a obrigação de que os Estados-membros adotem ou mantenham um arcabouço legal que garanta a proteção dos dados pessoais dos usuários no comércio eletrônico. Além disso, devem conceder esforços para desenvolver mecanismos que promovam a compatibilidade entre diferentes regimes de proteção de dados. Vale lembrar que todos os Estados-membros, com exceção do Vietnã e de Brunei Darussalam, já possuem leis que tratam da proteção à privacidade e da transferência internacional de dados.

Ainda que reconheça que cada país-membro possui suas próprias leis, o TPP os obriga a permitir a transferência internacional de dados por vias eletrônicas, inclusive dados pessoais, quando essa atividade é essencial à condução de quaisquer espécies de negócios, sejam para fins comerciais ou não.

Outras previsões incluem a garantia de que nenhum Estado-membro possa requerer dos entes privados, como condição para que ocorra a negociação, a localização dos dispositivos de armazenamento e processamento de dados para fins comerciais em seu território. Além disso, resta reconhecida a importância de haver uma resposta interna a um problema de segurança computacional, além da identificação e mitigação de instruções ou códigos maliciosos que afetem as redes dos países membros.

---

61 OW, Jack. The Trans-Pacific Partnership's take on personal data. TaylorWessing. Dez. 2015. Disponível em: <https://united-kingdom.taylorwessing.com/globaldatahub/article-the-tpp-take-on-personal-data.html>. Acesso em: 28 maio. 2017.

62 O que é o TPP, o acordo econômico entre 11 países do qual Trump retirou EUA. BBC Brasil. 24 jan. 2017. Disponível em: <http://www.bbc.com/portuguese/internacional-38729570>. Acesso em: 28 maio. 2017.

3.5.4 Transatlantic Trade and Investment Partnership (TTIP)

Transatlantic Trade and Investment Partnership (TTIP)[63] é uma série de acordos comerciais e de investimentos entre Estados Unidos e União Europeia, que tratam de diversos temas, como legislação ambiental, alimentos, barreiras regulatórias, dentre outros. Sua ratificação está prevista para 2018.[64]

Houve uma tentativa de incluir a proteção de dados no âmbito do TTIP em 2013, porém tal movimento foi rejeitado pelo Parlamento Europeu. Foi decidido que incluir a privacidade como uma temática abordada pelo TTIP seria prejudicial aos cidadãos europeus, pois enfraqueceria seu direito à privacidade. Vivan Reding, vice-presidente da Comissão Europeia, enfatizou que a proteção de dados está fora do escopo do TTIP.[65]

Levantou-se a questão de que tratar da privacidade em um acordo comercial e de investimentos, como é o caso do TTIP, poderia gerar um afrouxamento da proteção, como ocorreu quando o tema foi abordado pelo Anti-Counterfeiting Trade Agreement (ACTA), acordo de 2012 entre diversos países, incluindo Estados Unidos e a União Europeia. O TTIP poderia carregar consigo os elementos centrais do ACTA, tornando-se um ataque à privacidade individual, por permitir práticas como o monitoramento das atividades *online* de pessoas físicas.[66]

Ainda é grande a pressão política para que a privacidade seja trazida ao âmbito do TTIP, o que seria uma forma de diminuir o impacto das rígidas imposições trazidas pela GDPR. Em artigo crítico do jornal The Guardian[67], o escritor e pesquisador Evgeny Morozov alega que acordos como o TTIP são realizados sob a ótica corporativa e, portanto, preveem medidas que

---

63 About TTIP. Trade. European Commission. Disponível em: <http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/>. Acesso em: 28 maio. 2017.

64 LEONARD, John. TTIP vs GDPR - who will win the data protection wars?. Legislation and Regulation. Computing. 25 jan. 2016. Disponível em: <http://www.computing.co.uk/ctg/analysis/2443135/ttip-vs-gdpr-who-will-win-the-data-protection-wars>. Acesso em: 28 maio. 2017.

65 Data protection ruled out of EU-US trade talks. Financial Times. 2013. Disponível em: <https://www.ft.com/content/92a14dd2-44b9-11e3-a751-00144feabdc0>. Acesso em 28 maio. 2017.

66 WILLIAMS, Lee. What is TTIP? And six reasons why the answer should scare you. Comment. Independent. 6 out. 2015. Disponível em: <http://www.independent.co.uk/voices/comment/what-is-ttip-and-six-reasons-why-the-answer-should-scare-you-9779688.html>. Acesso em: 28 maio. 2017.

67 MOROZOV, Evgeny. What happens when policy is made by corporations? Your privacy is seen as a barrier to economic growth. Data Protection. Opinion. The Guardian. 12 jul. 2015. Disponível em: <https://www.theguardian.com/commentisfree/2015/jul/12/ttip-your-data-privacy-is-a-barrier-to-economic-growth>. Acesso em: 28 maio. 2017.

beneficiariam as grandes empresas. O setor governamental poderia encontrar brechas que lhes trouxessem vantagens, como exceções à privacidade por razões de segurança nacional, o que nos leva à conclusão de que acordos comerciam que promovam o relaxamento de medidas rígidas de proteção de dados possam ser custosos justamente à sociedade civil, o setor social mais vulnerável.

3.5.5 Organização de Cooperação e Desenvolvimento Econômico (OCDE)

A Organização para a Cooperação e Desenvolvimento Econômicos (OCDE) é composta pelos países mais industrializados do mundo e alguns países emergentes, que se organizar para trocar informações, alinhar políticas e promover seu desenvolvimento e crescimento econômico. Embora não seja um dos 34 países-membros da OCDE, o Brasil tem permissão para atuar em Comitês que lhe são de interesse. Em 2015, o Brasil assinou um Acordo Marco de Cooperação com a OCDE, fortalecendo sua relação com a organização.[68]

As primeiras medidas de proteção da privacidade foram tomadas pela OCDE em 1980, com a publicação das Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Tratam-se de recomendações do Conselho da OCDE em apoio aos três princípios comuns aos seus países membros: democracia pluralista, respeito aos direitos humanas e economias de mercado aberto.[69]

Tais diretrizes representam um consenso internacional a respeito da coleta e do gerenciamento de dados pessoais. Seus princípios são claros, flexíveis e suficientemente amplos para possibilitar a adaptação às mudanças tecnológicas. Abrangem todos os métodos utilizados no tratamento de dados pessoais, todos os tipos de processamento de dados pessoais e todas as categorias de dados, aplicando-se em âmbito nacional e internacional.

São princípios básicos das diretrizes: (i) princípio de limitação da coleta, que prevê que a coleta de dados seja relizada por meios legais, justos e com o consentimento do titular; (ii)

---

[68] Organização para a Cooperação e Desenvolvimento Econômico, OCDE. Secretaria de Assuntos Internacionais. Ministério da Fazenda. Disponível em: <http://www.sain.fazenda.gov.br/assuntos/politicas-institucionais-economico-financeiras-e-cooperacao-internacional/ocde>. Acesso em: 28 maio. 2017.

[69] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Rights and Translation unit, Public Affairs and Communications Directorate. Organization For Economic Co-operation And Development. 2003. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 28 maio. 2017.

princípio de qualidade dos dados, que devem ser exatos, completos, atualizados e ter relação com a finalidade de seu uso; (iii) princípio de definição da finalidade, que prevê que a finalidade deve ser indicada no momento da coleta; (iv) princípio de limitação de utilização, que proíbe a divulgação e compartilhamento de dados na ausência de consentimento ou previsão legal; (v) princípio do back-up de segurança; (vi) princípio de abertura, que prevê transparência quanto às políticas de privacidade e tratamento de dados pessoais; (vii) princípio de participação do indivíduo, que garante ao titular o direito de acessar, modificar, corrigir ou deletar seus dados pessoais; (viii) princípio de responsabilização, que prevê que o controlador de dados terá de prestar contas da observância das medidas previstas.

Em 2013, as Diretrizes da OCDE passaram pela primeira atualização desde sua implementação em 1980.[70] As atualizações de 2013 não alteraram os princípios básicos acima expostos, porém trouxeram inovações que modernizaram a abordagem da OCDE em relação ao fluxo internacional de dados, detalharam elementos-chave do significado de "organização responsável" e fortaleceram a execução das leis de privacidade. Em última instância, o objetivo é incentivar a execução de medidas práticas de proteção da privacidade, através de uma abordagem baseada na gestão de risco.

A obrigação de notificação ao titular dos dados e à autoridade competente em caso de fraude ou vazamento de dados foi trazida pela revisão de 2013. Além disso, alguns novos conceitos foram introduzidos, como, por exemplo, o de "estratégias de privacidade nacionais" e "programas de gestão de privacidade".

Esta breve análise do panorama internacional nos traz a certeza da relevância do GDPR, regulamento europeu de proteção de dados, que influencia a construção de leis internas mesmo em países externos a este bloco econômico. Nota-se também um movimento incipiente de elaboração de acordos geograficamente mais abrangentes. Porém, embora surjam comentários ocasionais, não há neste momento qualquer plano concreto de criação de um regulamento global.

A implementação de uma regulação mundial, contudo, não afastaria a necessidade de criação de uma legislação brasileira de proteção de dados. Como veremos no próximo Capítulo, a ausência de regulamento específico para o tratamento de dados pessoais no plano

[70] The OECD Privacy Framework. 2013 OECD Privacy Guidelines. Internet Economy. Organization For Economic Co-operation And Development. 2013. Disponível em: <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>. Acesso em: 28 maio. 2017.

interno vem gerando grandes problemas no Brasil. Decisões judiciais desproporcionais, como as que determinam o bloqueio de aplicativos de mensagem em todo o território nacional, são um exemplo do risco trazido pela ausência de uma Lei de Proteção de Dados no plano interno. Analisaremos a seguir, portanto, a atual movimentação do Poder Legislativo neste sentido.

4 CENÁRIO BRASILEIRO

Adentrando a esfera regulatória nacional, o destaque é, definitivamente, a ausência de lei específica de proteção de dados. Servimo-nos de uma proteção disposta dispersamente na legislação interna, ou seja, em múltiplos diplomas legais. Embora a dispersão seja problemática por si só, por dificultar a assimilação e aplicação do direito, o fato de não haver legislação específica impede a abordagem completa do tema. Isto porque não há espaço em outras leis para versar sobre assuntos tão específicos, como, por exemplo, como se dará a transferência internacional de dados, havendo clara necessidade de que isto seja feito de maneira apartada, em uma lei própria.

Como veremos, a tarefa de preencher estes vazios vem cabendo ao Poder Judiciário, considerando que não se pode deixar um conflito jurídico sem solução. Contudo, como veremos, ainda não foi consolidada jurisprudência sobre o tema. As decisões judiciais são recentes e frequentemente discrepantes entre si.

Fica claro, portanto, o quão relevante é a análise realizada no último item deste trabalho, acerca dos projetos de lei que atualmente tramitam no Congresso Nacional. Considerando que a tradição jurídica brasileira se atém ao sistema de Civil Law, não surpreende que o caminho a ser seguido para sanar esta insegurança seja através da positivação. Se algum destes projetos for aprovado, e há grande expectativa de que isto ocorra em breve, provocará grandes alterações no cenário nacional, não somente no campo do Direito, mas também levará a mudanças na atuação de agentes privados em relação à proteção e tratamento de dados.

Assim sendo, vejamos, primeiramente, as garantias à privacidade e à proteção de dados atualmente dispostas na legislação brasileira.

4.1 Legislação nacional

A primeira fonte dos direitos correlatos à privacidade e proteção de dados no ambiente virtual a ser citada é a Constituição Federal de 1988, no que tange às suas previsões gerais de tutela à privacidade, bem como às previsões no âmbito das comunicações. Da Carta Magna,

extraímos o princípio da privacidade e intimidade no inciso X[71] do artigo 5º, e princípio do sigilo das comunicações no inciso XII[72] do mesmo artigo. Tais princípios permearão a relação entre o titular de dados e quaisquer indivíduos que realizarem funções ligadas ao tratamento. São, ainda, de extrema importância na atuação do Poder Judiciário, que deve sempre realizar uma ponderação entre os princípios envolvidos para identificar a melhor solução.

O direito ao sigilo e à privacidade frequentemente colide com o direito à informação, todos direitos fundamentais. As restrições ao direito à informação são geralmente associadas à censura e a atos restritivos de direitos humanos, por obstruírem o exercício da cidadania e da soberania popular. Assim sendo, é importante que o Judiciário realize a ponderação com razoabilidade, de acordo com as circunstâncias do caso concreto, concluindo qual direito deve prevalecer em cada situação fática.

O plano infraconstitucional também possui dispositivos pertinentes. No Código Civil (Lei nº 10.406 de 2002), o artigo 21 se dispõe a tratar da vida privada da pessoa natural[73], concedendo ao Poder Judiciário competência para atuar, a pedido do interessado, em casos de violação desta norma.

Todavia, a proteção de dados no ambiente virtual encontra morada mais adequada no Marco Civil da Internet (Lei nº 12.965 de 2014) e em seu Decreto Regulamentador (Decreto nº 8.771 de 2016). A privacidade e a proteção de dados pessoais são estabelecidas como princípios que regerão as relações no ambiente virtual logo artigo 3º, nos incisos II e III[74]. O inciso III tem especial importância por trazer em seu texto que a proteção de dados pessoais se dará "na forma da lei", fomentando a discussão quanto à necessidade de criação de lei específica de proteção de dados no Brasil, a nível federal.

Algumas outras disposições relativas ao tratamento ou proteção de dados pessoais e da privacidade estão dispostas ao longo do Marco Civil. As mais notáveis estão no Capítulo II, que versa sobre os direitos e garantias dos usuários na Internet, e no Capítulo III, mais

---

71 "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;"

72 "XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;"

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

74 "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
(...)
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;".

especificamente na Seção II deste capítulo, que é inteiramente dedicada à proteção dos registros, dados pessoais e da comunicação privada. Nesta toada, o papel do Decreto Regulamentador 8.771 de 2016 é garantir maior robustez às previsões gerais sobre o tratamento e a proteção de dados contidas no Marco Civil.

Seguindo a análise do plano infraconstitucional, temos o Código de Defesa do Consumidor (Lei nº 8.078 de 1990), que é amparado pelo Decreto Regulamentador nº 7.962 de 2013 para melhor tutelar as relações do comércio eletrônico[75] e promover proteção tão eficaz ao consumidor no ambiente virtual quanto aquela concedida às relações de consumo convencionais. O próprio Marco Civil da Internet permite, no inciso XIII do artigo 7º, a aplicação subsidiária do CDC nas relações de consumo virtuais.[76]

Por sua vez, a esfera penal conta com a Lei nº 12.737 de 2012, popularmente conhecida como Lei Carolina Dieckmann ou Lei dos Crimes Cibernéticos, para lidar com outro viés da proteção de dados. Seu propósito é tipificar tipifica delitos informáticos, com previsão multa e detenção por ao menos três meses em caso de alteração ou destruição de dados ou invasão de dispositivos informáticos, estejam eles conectados ou não à rede mundial de computadores. Apesar das poucas disposições, esta lei sofreu severas críticas quando surgiu no cenário regulatório brasileiro. Isto porque sua aprovação se deu antes mesmo da promulgação do Marco Civil da Internet, tendo sido concedido pouco tempo para discussão e planejamento das disposições na seara legislativa.

Em 2014, a Lei dos Crimes Cibernéticos ganhou destaque com a Ação Civil Pública nº 0028553-98.2014.8.08.0024[77], iniciada na 5ª Vara Cível de Vitória (Espírito Santo), que determinou a remoção dos aplicativos Secret e Cryptic, sendo que o segundo apenas oferecia suporte ao primeiro, das lojas online que o comercializavam, bem como dos dispositivos dos usuários que haviam realizado o download, em razão da descoberta de uma ilicitude. Embora o aplicativo Secret prometesse o anonimato aos seus usuários, que postavam mensagens publicamente pela plataforma, este anonimato não era real, pois o autor das mensagens poderia ser identificado mediante o acesso ao IP (*Internet Protocol*) de seu dispositivo. Além

---

75 BRASIL. Decreto nº 7.962, de 15 de março de 2013. Poder Executivo. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm>. Acesso em: 28 maio. 2017.

76 "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet."

77 DECISÃO. Ação Civil Pública. Processo nº 0028553-98.2014.8.08.0024. Natureza Cível. 5ª Vara Cível. Vitória, Espírito Santo. Distribuído em: 18 ago. 2014. Disponível em: <http://s.conjur.com.br/dl/juiz-proibe-aplicativo-secret-celulares.pdf>. Acesso em: 28 maio. 2017.

disso, o anonimato é vedado pela Carta Magna brasileira, o que gerou discussões e cominou na referida Ação Civil Pública.

Após recurso da Google contra a decisão de remoção dos aplicativos, o desembargador convocado Jorge Henrique Valle dos Santos destacou, na ocasião, a Lei dos Crimes Cibernéticos para confrontar a decisão de remoção dos aplicativos dos dispositivos dos usuários, alegando que a referida lei veda a invasão de dispositivos informáticos. De acordo com seu entendimento, o Judiciário não deveria incorrer em práticas criminalmente tipificadas para solucionar conflitos, violando o direito a privacidade de todos os usuários do aplicativo.[78]

Como pudemos observar, poucas são as previsões atualmente em vigor no que tange à proteção de dados no ambiente virtual. Por esta razão, o caso mencionado no parágrafo anterior não foi o único a gerar controvérsia. A seguir veremos algumas decisões judiciais paradigmáticas relacionadas ao tema, que permitirão compreender o trajeto percorrido pelo Poder Judiciário até o momento, na busca por garantir a justiça e a devida proteção aos direitos das partes mesmo na ausência de regulamentação específica.

4.2 Decisões judiciais e entendimentos doutrinários

Em sua fala durante o 30º Seminário Internacional da ABDTIC[79], que ocorreu no segundo semestre de 2016, Carlos Affonso Souza[80], cofundador e diretor do ITS Rio, apresentou três modelos de medidas que vêm sendo adotados no Brasil nos últimos três anos. Mesmo que não estejamos falando em jurisprudência, que de fato não existe no país em relação a esta matéria, é útil analisar as formas através das quais o Poder Judiciário tem reagido às situações de violação ou negativa de acesso a dados inseridos no ambiente virtual.

---

[78] Suspensa liminar que determinou remoção do aplicativo Secret. Justificando. Carta Capital. 15 set. 2014. Disponível em: <http://justificando.cartacapital.com.br/2014/09/15/suspensa-liminar-que-determinou-remocao-de-aplicativos/>. Acesso em: 28 maio. 2017.

79 30º SEMINÁRIO INTERNACIONAL DA ABDTIC. Painel: Temas atuais em proteção de dados pessoais e privacidade. Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações. 2016. São Paulo. SP.

80 Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (Uerj). Professor da Faculdade de Direito da UERJ e da PUC-Rio, lecionando disciplinas como Direito e Tecnologia, Direito dos Contratos e História do Direito. Pesquisador Visitante do Information Society Project, da Faculdade de Direito da Universidade de Yale. Membro da Comissão de Direito Autoral da OAB/RJ (desde 2007). Policy Fellow da ONG Access. Consultor do Observatório da Internet no Brasil, uma iniciativa do Comitê Gestor da Internet no Brasil (CGI.br). Cofundador e diretor do ITS Rio. Disponível em: <https://itsrio.org/pt/institucional/#equipe>. Acesso em: 28 maio. 2017.

As primeiras decisões objetivavam a remoção do aplicativo de lojas virtuais brasileiras, ou que atuantes no território nacional, que o disponibilizassem. Podemos citar como exemplo o caso do já mencionado do aplicativo Secret, desenvolvido por uma companhia norte-americana e que ganhou popularidade no Brasil à época de seu lançamento. Uma vez que a empresa detentora do aplicativo Secret não possuía estabelecimento no Brasil, a decisão judicial se voltou às lojas online que disponibilizavam o aplicativo, proibindo a comercialização do mesmo. Esta foi a primeira maneira encontrada pelo Judiciário para evitar que um aplicativo que estivesse violando a lei nacional permanecesse disponibilizado no país.

Decisões como esta trazem reflexões quanto à lentidão do Direito frente à velocidade das inovações tecnológicas. É perfeitamente possível imaginar que, nos dias atuais, um aplicativo lançado há apenas uma ou duas semanas possa figurar entre os mais utilizados no Brasil. Aplicações e redes sociais ganham popularidade com rapidez impressionante no ambiente virtual. Por outro lado, não se pode esperar que a empresa provedora da aplicação possua filiais em todos os países no qual o aplicativo é disponibilizado em tão pouco tempo. Fica a indagação, portanto, sobre como a futura lei de dados disporá, e como atuará o Poder Judiciário em caso de violação de leis nacionais por empresas estrangeiras sem escritório no Brasil.

O segundo método a ser comentado ocorreu também com o aplicativo Secret neste mesmo episódio. Trata-se da ordem de remoção do aplicativo não apenas das lojas virtuais, como também dos dispositivos móveis que o baixaram. Como vimos, a medida foi severamente criticada e acabou sendo revertida em instância superior. A utilização da Lei dos Crimes Cibernéticos para justificar a reversão pode parecer extrema, por considerar que a remoção do aplicativo seria uma invasão aos dispositivos dos usuários, porém traz à tona o quanto os conteúdos armazenados em celulares, computadores e outros aparelhos informáticos fazem parte da intimidade de seu detentor, e o quanto a proteção de informações no ambiente virtual é necessária e desejada.

O terceiro modelo decisório, de grande notoriedade, é o bloqueio do aplicativo em todo o território nacional. Tais recentes e polêmicas decisões, especialmente no caso do aplicativo WhatsApp, geraram grande discussão quanto a determinados artigos do Marco Civil,

colocando-o como núcleo da discussão. Isso porque o artigo 12 deste diploma legal[81] traz algumas formas de sanção a infrações previstas no próprio Marco Civil. Dentre estas sanções está a possibilidade de suspensão ou proibição das atividades previstas no artigo 11, quais sejam, a "coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet".[82]

É justamente esta a origem da controvérsia. Enquanto alguns entendem que é possível o bloqueio do aplicativo como um todo, fundamentando a decisão no artigo 12 do MCI, outros juristas, o Ministro do Supremo Tribunal Federal Ricardo Lewandowski, entendem que tão somente as atividades previstas no artigo 11 devem ser suspensas. O artigo 12 é utilizado para fundamentar este entendimento, sendo interpretado de maneira mais literal e menos abrangente. Essa multiplicidade de interpretações gera insegurança jurídica e coloca em risco a credibilidade do Marco Civil, que passou a ser demonizado, principalmente pela população leiga, que o relaciona diretamente aos bloqueios de aplicativos, muito embora as decisões de reversão do bloqueio também se pautem no MCI.

Todavia, é evidente a desproporcionalidade da medida de bloqueio de um aplicativo m todo o território nacional, especialmente quando se trata de um dos aplicativos de mensagem mais utilizados pelos brasileiros, de acordo com pesquisa realizada em 2016[83]. Este caso nos leva a refletir quanto à importância de haver proporcionalidade na aplicação de sanções pelo Poder Judiciário, bem como dá destaque à necessidade de promulgação de lei específica que regule a matéria eficientemente, porém possuindo um viés principiológico. Afinal, especificidades podem engessar a legislação, considerando a frequência e a velocidade dos avanços tecnológicos.

---

[81] "Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.".

[82] "Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros."

[83] PAIVA, Fernando. WhatsApp: um em cada três usuários no Brasil liga pelo app diariamente. MobileTime. 3 mar. 2016. Disponível em: <http://www.mobiletime.com.br/03/03/2016/whatsapp-um-em-cada-tres-usuarios-no-brasil-liga-pelo-app-diariamente/433922/news.aspx>. Acesso em: 28 maio. 2017.

Esta medida ainda nos faz questionar a inadequação de um remédio jurídico que ataque uma aplicação por inteiro, enquanto poderia e deveria, na verdade, atingir somente a conduta ilícita em si. Ora, se o tratamento de dados é realizado de maneira inadequada, que se coíba a atividade de tratamento, apenas. Ainda que o aplicativo não seja capaz de manter sua funcionalidade, evitaria uma extensão indevida da punição. A própria decisão de bloqueio não gera efeitos didáticos; o enfoque se dá no castigo à empresa objeto da ação, e não na repreensão e prevenção da conduta ilícita.

Uma quarta medida, ainda carente de esforços do poder público, é o aprimoramento dos acordos de cooperação judiciária entre países e blocos econômicos. Isto é válido não apenas para aqueles casos, já discutidos, de ausência de filial da empresa infratora em território nacional, mas também para garantir o *law enforcement* e impulsionar a troca de informações e a cooperação judiciária internacional.

Repetindo a máxima: a Internet frequentemente desconhece fronteiras geográficas. Deste modo, incrementar a cooperação internacional e a realização de acordos internacionais seria o caminho mais promissor. Possuir um canal de diálogo aberto com outros países seria de grande utilidade, inclusive, na aplicação da lei no plano interno, diminuindo a ocorrência de medidas radicais e ofensivas, como a suspensão de aplicativos no território nacional. Além disso, observar experiências regulatórias estrangeiras é sempre útil ao trabalho do legislador interno, que poderá descartar ideias ou inseri-las em seus próprios projetos conforme observa as consequências práticas trazidas pelos dispositivos de outros ordenamentos.

Não é intenção deste trabalho eximir operadores do Direito de procurarem aperfeiçoar a tutela de direitos na era cibernética, porém a dificuldade em lidar com questões relacionadas à Internet transcende o Poder Judiciário. É uma dificuldade humana, de uma geração que, em um curto período de tempo, passou a lidar intensa e diariamente com a tecnologia e o acesso a uma quantidade imensurável de informações. Ainda estamos aprendendo a lidar com nossa própria privacidade dentro do meio virtual. Muitos indivíduos sequer enxergam seus dados pessoais como a nova moeda de troca, podendo incorrer no erro de não dar a devida importância à proteção destes dados. Como bem frisa o advogado Victor Drummond, em sua obra "Internet, Privacidade e Dados Pessoais"[84]:

84 DRUMMOND, Victor. Internet, Privacidade e Dados Pessoais. Editora Lumen Juris. 2003. Rio de Janeiro. P. 142.

> "Os dados pessoais devem ser protegidos em face da fragilidade que o cidadão apresenta pelo simples fato de ser titular. No momento que os cidadãos tomarem ciência da importância de sua própria intimidade revelada pelos dados que a si pertencem, haverá um maior equilíbrio entre as grandes corporações, o Estado e o cidadão comum.
> O direito à privacidade, enquanto espécie do gênero direitos da personalidade, parece estar sendo romantizado tanto no âmbito da Internet e da sociedade tecno-comunicacional quanto fora dela. Ele deve ser preservado, ainda que não deva ser sacralizado."

4.3 Projetos de Lei

A análise dos marcos regulatórios atuais e das mais relevantes decisões judiciais revela a escassez de amparo legislativo à proteção de direitos fundamentais no ambiente virtual, que traz à tona a necessidade de criação de uma lei federal específica de proteção de dados pessoais neste setor. Tal legislação seria capaz de lidar com questões que não poderiam ser endereçadas nos diplomas legais pré-existentes, dada sua especificidade, além de trazer unificação às regras de proteção de dados e, assim, facilitar o *law enforcement*, melhor dizendo, a aplicação e manutenção do direito.

Deste modo, falaremos agora de três iniciativas do Congresso Nacional de inserir esta necessária lei no ordenamento jurídico brasileiro, quais sejam: o Projeto de Lei do Senado nº 330 de 2013; e os Projetos de Lei nº 4.060 de 2012 e nº 5.276 de 2016, que tramitam na Câmara dos Deputados. O objetivo é melhor discutir o que propõem, analisando especificamente os dispositivos que possam gerar problemas futuros, em caso de aprovação do projeto de lei.

4.3.1 Projeto de Lei do Senado nº 330 de 2013

Destacando-se como a mais principiológica das propostas de lei sobre proteção de dados no ambiente virtual, o Projeto de Lei do Senado nº 330 de 2013, de autoria do Senador Antonio Carlos Valadares, está em posição intermediária entre os três projetos de lei a serem analisados neste trabalho no quesito detalhamento. Pode-se dizer que, embora sua abrangência signifique que exigirá regulamentação posterior, é exatamente esta a característica mais atraente deste projeto às entidades que realizam o tratamento de dados.

Em outubro de 2015, o texto original foi substituído pelo Substitutivo do Senador Aloysio Nunes Ferreira, que apresentou relatório favorável ao projeto e aprovou, total ou parcialmente, onze emendas ao texto original. Consideraremos, portanto, o substitutivo durante esta análise.

Logo no início, mais especificamente no Art. 2º[85], um ponto salta aos olhos: estipula-se que a lei será aplicada ao uso e tratamento de dados pessoais, indiferentemente de qual o mecanismo empregado para tanto. A redação deste artigo pode levar a um sério problema relacionado aos critérios de aplicação da norma, posto que não menciona expressamente que a lei será aplicada no ambiente digital.

Esta omissão permite ao aplicador do direito fazer uso de dois critérios de aplicação da norma, à sua escolha, em caso de antinomia – ou seja, de conflito aparente de normas – envolvendo a futura lei de proteção de dados e o Marco Civil da Internet. Estamos falando dos critérios da cronologia e da especialidade. Em caso de fraude ou violação de dados pessoais no ambiente virtual, ou qualquer outra espécie de lesão ocorrida durante o tratamento, teremos duas hipóteses: (i) utilizar o critério da cronologia, elegendo a Lei de Proteção de Dados por ser mais recente; (ii) utilizar o critério da especialidade, que nos leva a outra bifurcação problemática: este critério determinaria que deve ser utilizado o Marco Civil, por sei lei específica ao ambiente virtual, ou o correto seria a utilização da Lei de Proteção de Dados, considerando que é específica ao tratamento de dados pessoais?

A problemática poderia ser facilmente evitada com a inserção, neste art. 2º, de referência explícita ao "ambiente digital" no qual a lei se aplicará, evitando a multiplicidade de alternativas de lei utilizável gerada pela aplicação do critério da especialidade.

Ainda no art. 2º, uma sutil questão deve ser levantada quanto ao §4º[86]. A redação deste parágrafo indica que o legislador entende como dados desanonimizados os "dados inicialmente anônimos que, por qualquer técnica, mecanismo ou procedimento, permitam, a qualquer momento, a identificação do titular". Há que se pensar se a expressão "a qualquer momento" não estaria, hoje mesmo, ultrapassada. Isto porque o conceito de anonimato e de dados anônimos no ambiente virtual já foi mitigado por estudiosos e pesquisadores que se

[85] "Art. 2º Esta Lei aplica-se ao uso e ao tratamento de dados pessoais realizados no todo ou em parte no território nacional ou que nele produza ou possa produzir efeito, qualquer que seja o mecanismo empregado."
[86] "§ 4º Os dados desanonimizados, assim compreendidos aqueles dados inicialmente anônimos que, por qualquer técnica, mecanismo ou procedimento, permitam, a qualquer momento, a identificação do titular, terão a mesma proteção dos dados pessoais, aplicando-se aos responsáveis por sua coleta, armazenamento e tratamento o disposto nesta Lei."

debruçam sobre o tema, dados os constantes avanços tecnológicos. Neste sentido, cabe refletir se não seria equivocado definir dado desanonimizado como um dado que pode identificar a qualquer momento seu titular, pois mesmo os dados considerados anônimos possuem hoje tal potencial. Melhor seria dizer que dados desanonimizados são aqueles que reidentificam o titular, tratando-se de uma característica inata a espécie de dado, de modo a evitar a caducidade da expressão antes mesmo que a lei entre em vigor.

O art. 3º, por sua vez, traz definições de termos relevantes ao tema. O inciso II deste artigo traz a definição de dado pessoal sensível[87]. Ainda que não seja criticável, a redação nos remete a um problema similar ao que ocorre com os dados anonimizados e seu pontencial de reidentificação. Neste caso, há que se considerar que, com a tecnologia atual, é possível alcançar um dado sensível através de análises de dados que, separadamente, são considerados apenas dados pessoais. Uma prática comum – porém não a única – de se chegar a um dado sensível a partir da análise conjunta de múltiplos dados pessoais é a chamada clusterização (*clustering*). Vinícius Veloso de Melo, doutor em Ciências da Computação e Matemática Computacional pela Universidade de São Paulo (USP), define o objetivo deste procedimento da seguinte forma[88]:

> "O objetivo da tarefa de clustering é agrupar objetos (ou exemplos) baseado nas características que que esses objetos possuem, de tal maneira que seja maximizada a similaridade entre objetos pertencentes a um mesmo agrupamento e minimizada a similaridade entre agrupamentos distintos. Ou seja, procura-se a homogeneidade dos objetos dentro de um mesmo agrupamento enquanto maximiza-se a diferença entre os agrupamentos."

Simplificadamente, a atividade de clusterização consiste em inserir objetos em grupos com base em suas características. Este método de tratamento de dados pode propiciar maior compreensão dos do conjunto de dados original, além de desvendar correlações inicialmente imperceptíveis. Trata-se também de uma etapa inicial, que facilita outras atividades de tratamento de dados, como a classificação, dentre outras. De modo geral, atividades que

---

87 "II – dado pessoal sensível: qualquer dado pessoal que revelem a orientação religiosa, política ou sexual, a convicção filosófica, a procedência nacional, a origem racial ou étnica, a participação em movimentos políticos ou sociais, informações de saúde, genéticas ou biométricas do titular dos dados;"

88 MELO, Vinicius Veloso de. 2005. Clustering de artigos científicos em uma Ferramenta Inteligente de apoio à Pesquisa. Dissertação. Universidade de São Paulo. Maio. 2005. p. 11. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiNkrGVh-bTAhUFjJAKHZkpDFUQFggkMAA&url=http%3A%2F%2Fwww.teses.usp.br%2Fteses%2Fdisponiveis%2F55 %2F55134%2Ftde-11122014-104427%2Fpublico%2FViniciusVelosodeMelo_ME.pdf&usg=AFQjCNGiCAq_wUTI2mRf30YAxoKgOcaqUw >. Acesso em: 28 maio. 2017.

implicam a análise de informações aleatórias com o objetivo de associá-las são um desafio às leis de proteção de dados.

Os algoritmos de buscadores na Internet, como é o caso do Google, podem se valer da clusterização para criar um perfil do usuário que realiza a busca. Neste exemplo, através do histórico de navegação, que atualmente não é classificado pela legislação como dado sensível, é possível enquadrar o usuário em grupos como "simpatizante de religião afro-brasileira" e "interessado em penteados para cabelos crespos". Ainda que este indivíduo seja inserido em outros grupos, estas duas classificações por si só já permitiram uma assunção bastante assertiva de sua origem racial – que é dado sensível. Destarte, observamos que um dado sensível pode ser aferido a partir de dados pessoais. Resta dúvidas sobre qual seria a melhor tática legislativa para tutelar estes dados obtidos pela análise cruzada. Parece inviável, porém, classificar clusters (agrupamentos) ou históricos de navegação como dados sensíveis, especialmente dada a relevância destes em certas atividades econômicas, como a publicitária, por exemplo.

Há uma última observação quanto ao art. 3º, referente ao inciso XIV, que traz a definição de dado anonimizado ou anônimo[89]. Como já discutimos no item 2.1.2 deste trabalho, existe a preocupação quanto à proteção de dados que sofrem o processo de desanonimização, ou seja, de reversão da qualidade de anônimo. No momento, o substitutivo não traz previsão quanto a como serão tratados os dados desanonimizados. O ideal é que sejam tratados como dados pessoais, porém este entendimento carece de positivação.

A próxima questão relevante a ser discutida se refere ao §1º do art. 5º.[90] Este dispositivo é de grande importância por estabelecer que haverá um órgão competente para a proteção de dados pessoais. Entretanto, não o define, de modo que isso deverá ser feito em regulamentação futura. As preocupações do setor privado são quanto à eleição de órgãos de proteção ao consumidor para exercer este papel, que seriam mais restritivos em relação às empresas. Este, porém, não é o único motivo pelo qual a criação de uma autoridade específica, e não a delegação de competência a um órgão pré-existente, seria o melhor

89 "XIV – dado anonimizado ou anônimo: dado relativo a um titular que não possa ser identificado, considerando a utilização dos meios técnicos razoáveis e disponíveis na ocasião de sua coleta ou tratamento."

90 "Art. 5º O Poder Público atuará para assegurar, quanto ao tratamento de dados pessoais, a liberdade, a igualdade, a inviolabilidade da intimidade, da vida privada, da honra e da dignidade da pessoa humana.
§ 1º Os órgãos públicos federais, estaduais, do Distrito Federal e municipais elaborarão e darão ampla publicidade a suas políticas de privacidade, que tratarão das operações de coleta, tratamento e uso compartilhado de dados realizadas no âmbito de todas as suas atividades, respeitando o disposto nesta lei e as normas aprovadas pelo órgão competente."

caminho. Para que uma autoridade específica possa realizar a fiscalização do cumprimento da norma de maneira adequada, é necessário que possua um corpo técnico multidisciplinar, ou seja, que abarque diversas áreas do conhecimento, como Segurança da Informação, Direito, Análise de Sistemas, dentre outras. Dada essa necessidade de especialização do órgão público, fica evidente que a capacitação de órgãos já existentes, que acumulariam às suas funções originais a tutela da proteção de dados pessoais, é inviável.

Outro ponto extremamente relevante diz respeito ao consentimento do titular de dados quanto às atividades relacionadas ao tratamento. Pode-se dizer que, quanto às adjetivações do consentimento, o PLS 330 de 2013 se mostra satisfatório. O inciso IV do artigo 6º qualifica o consentimento como "livre, específico, inequívoco e informado"[91]. O adjetivo "livre" indica que o titular não pode ser coagido a consentir. "Específico", por sua vez, é um termo que pode gerar reclamações dos entes regulados, por dar margem à interpretação de que o consentimento deve ser fornecido para cada atividade de tratamento realizada, ou renovado a cada alteração nas atividades de tratamento – algo que seria custoso aos responsáveis pelo tratamento, ou mesmo tormentoso aos titulares, caso o consentimento seja requerido constantemente, terminando, por exemplo, por engessar a navegação em *websites*. O termo "Inequívoco" e "informado" servem à garantia de que o titular está devidamente informado e compreende verdadeiramente suas obrigações, seus direitos e a que espécie de tratamento seus dados estarão submetidos.

O artigo 12 traz algumas hipóteses em que não é necessário consentimento[92] para a realização do tratamento de dados pessoais: (i) na execução de contrato ou na fase précontratual; (ii) no cumprimento de obrigação legal pelo responsável; (iii) para pesquisa jornalística, histórica ou científica sem fins lucrativos; (iv) pelo poder público, havendo

---

91 "IV – consentimento livre, específico, inequívoco e informado sobre coleta, armazenamento e tratamento de dados pessoais, que deverá sempre ocorrer de forma destacada;"

92 "Art. 12. O tratamento de dados pessoais somente pode ser realizado nas seguintes hipóteses:
I – mediante consentimento livre, específico, inequívoco e informado concedido pelo titular dos dados;
II – na execução de um contrato ou na fase précontratual de uma relação em que o titular seja parte; III – quando necessário para o cumprimento de obrigação legal pelo responsável;
IV – quando realizado exclusivamente no âmbito da pesquisa jornalística, histórica ou científica sem fins lucrativos e desde que sejam tomadas medidas adicionais de proteção;
V – quando necessário para a realização de atividades específicas de pessoas jurídicas de direito público, mediante decisão motivada, e desde que a obtenção do consentimento represente obstáculo à consecução do interesse público;
VI – quando necessário para tutela da saúde ou proteção da incolumidade física do titular ou de terceiro; VII – quando necessário para garantir a segurança da rede e da informação;
VIII – quando necessário para atender aos interesses legítimos do responsável pelo tratamento ou do terceiro a quem os dados sejam comunicados, desde que não prevaleçam sobre os interesses ou os direitos e liberdades fundamentais do titular dos dados."

interesse público; (v) para tutela da saúde ou incolumidade física do titular ou de terceiro; (vi) para garantir a segurança da rede e da informação; (vii) para atender aos interesses legítimos do responsável pelo tratamento, desde que não confrontem interesses e direitos do titular.

Entretanto, a redação do inciso relativo aos interesses legítimos do responsável não é suficientemente precisa quanto aos limites, alcance e aplicação do legítimo interesse das empresas com relação à utilização não consentida de dados pessoais, de modo que este tópico demandará regulamentação posterior e/ou interpretação dos Tribunais.

Seguindo a análise, deparamo-nos com outro item relevante: a responsabilidade dos responsáveis pelo tratamento em caso de dano. Tal previsão se encontra nos parágrafos 1º e 2º do artigo 20[93], que determinam que a responsabilidade em caso de dano decorrente ou associado à comunicação ou à interconexão será solidária entre todos os entes que tiveram acesso aos dados, bem como no art. 34[94], nos casos de empresas ou entidades integrantes de grupo econômico que infringirem a lei de proteção de dados. Definitivamente, não é a previsão desejada por empresas que realizam atividades de tratamento de dados, porém traz proteção mais efetiva ao titular.

A comunicação aos titulares em caso de tais incidentes danosos está prevista no artigo 24 do projeto, que contém inconsistências em sua redação. Isto porque o §4º deste artigo[95] ordena a "pronta comunicação aos titulares afetados pelo incidente de segurança a que se refere o caput, independente de determinação do órgão competente" quando for possível identificar que o incidente coloque em risco a segurança ou possa causar danos aos titulares. Contudo, o caput[96] não menciona a obrigação de comunicar aos titulares a ocorrência de incidentes, dispondo apenas que o órgão competente deve ser comunicado. Ou seja, o §4º faz referência a fato que não está previsto no caput. Embora seja possível supor que o intuito do legislador é dispor que a comunicação aos titulares só é obrigatória e independente da determinação do órgão competente quando o incidente colocar em risco a segurança ou causar

93 "§ 1º A comunicação e a interconexão de dados pessoais sujeitam todos aqueles que tiverem acesso aos dados às mesmas obrigações legais e regulamentares do responsável.
§ 2º Em caso de dano decorrente ou associado à comunicação ou à interconexão, respondem solidariamente todos aqueles que tiverem acesso aos dados."

94 "Art. 34. Serão solidariamente responsáveis as empresas ou entidades integrantes de grupo econômico, de fato ou de direito, quando pelo menos uma delas praticar infração a esta Lei."

95 "§ 4º A pronta comunicação aos titulares afetados pelo incidente de segurança a que se refere o caput será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos."

96 "Art. 24. O responsável deverá comunicar imediatamente ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares."

danos ao titular, há que se reconhecer que a redação deve ser aperfeiçoada para evitar equívocos.

Por fim, falemos sobre a transferência internacional de dados. A matéria começa a ser tratada na Seção IV do projeto de lei. Observamos que o artigo 26 restringe a transferência internacional a algumas hipóteses[97]: (i) quando se tratar de país que proporcione o mesmo grau de proteção concedido pela lei brasileira; (ii) com o consentimento informado, específico e próprio do titular; (iii) para o cumprimento de obrigação legal; (iv) para tutela da saúde ou proteção da incolumidade física do titular ou de terceiro; ou (v) em caso de cooperação internacional de inteligência e investigação.

Este artigo, porém, possui uma questão problemática referente ao parágrafo único[98], que determina que "a autoridade competente gerenciará o regime de autorizações para transferência de dados pessoais ao exterior". O parágrafo não menciona em quais circunstâncias será demandada a autorização para que ocorra a transferência internacional, gerando incerteza. Caso se aplique a todas as hipóteses de transferência previstas no mesmo artigo, tal disposição legal seria questionável, uma vez que o tratamento de dados pessoais não é serviço público que implica necessidade de autorização de órgãos governamentais. Tal ingerência na livre atividade econômica dos responsáveis pelo tratamento de dados poderia ser considerada uma violação ao princípio fundamental da livre iniciativa, previsto no inciso IV do artigo 1º da CRFB[99].

4.3.2 Projeto de Lei nº 4.060 de 2012

97 "Art. 26. A transferência internacional de dados pessoais somente pode ser realizada nas seguintes hipóteses: I – para países que proporcionem o mesmo grau de proteção de dados previsto nesta Lei;
II – quando o titular, após ser devidamente informado do caráter internacional do tratamento e dos riscos existentes no tratamento de dados no país de destino, consentir de forma específica e própria;
III – quando necessário para o cumprimento de obrigação prevista na legislação brasileira;
IV – quando necessário para tutela da saúde ou proteção da incolumidade física do titular ou de terceiro;
V – na cooperação internacional entre Estados relativa às atividades de inteligência e investigação, conforme previsto nos instrumentos de direito internacional dos quais o Brasil seja signatário."

98 "Parágrafo único. Autoridade competente gerenciará o regime de autorizações para transferência de dados pessoais ao exterior."

99 "Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
(...)
IV - os valores sociais do trabalho e da livre iniciativa;"

A primeira proposta de criação, no âmbito da Câmara dos Deputados, de uma lei de proteção de dados pessoais, o fez de maneira deveras principiológica e vaga. O Projeto de Lei nº 4.060 de 2012, de autoria do deputado Milton Monti, traz disposições gerais relativas ao tratamento de dados pessoais, porém sem se aprofundar na questão da segurança e proteção destas informações. Mesmo após a apresentação de emendas ao texto inicial, em maio de 2016, pelo deputado relator Sóstenes Cavalcante, a superficialidade permanece.

Pela leitura do artigo 3º[100], identificamos que o projeto concede importância especial ao Código de Defesa do Consumidor, estendendo a aplicação dos princípios deste diploma legal aos sujeitos submetidos à lei de proteção de dados pessoais. Outros dispositivos, como os artigos 21 e 22, também mencionam a aplicação do CDC, o que indica que a atividade de tratamento de dados é abordada por um viés mais econômico por essa proposta legislativa, diferentemente do que ocorre com as outras que estão em tramitação no Congresso Nacional, cuja ótica é mais voltada aos direitos fundamentais.

Em relação às definições, trazidas pelo artigo 7º, não houve a preocupação em delimitar mais detalhadamente os sujeitos que atuam no tratamento de dados. O único sujeito definido é o "responsável" pelo tratamento[101], a quem compete possuir e tomar decisões quanto à base de dados. Fica evidente a carência de inserir outras figuras que participam da cadeia econômica, o que facilitaria a regulação e a aferição de responsabilidade de cada sujeito em caso de violação de dados.

Algumas carências da proposta são bastante significativas. A primeira delas diz respeito ao estabelecimento de uma autoridade específica para a proteção de dados. O projeto não estipula a criação de órgão competente, tampouco designa a função de tutela a outro órgão público já existente. Pelo contrário, o artigo 23[102] estimula a autorregulamentação, exercida por Conselhos de Autorregulamentação criados por entidades representativas de responsáveis pelo tratamento de dados. Tais Conselhos teriam competência para estabelecer padrões éticos

---

100 "Art. 3º. A proteção aos direitos e garantias mencionados no artigo primeiro desta lei deverá ser promovida com observância dos princípios constitucionais da Defesa do Consumidor, Livre iniciativa, Liberdade de Comunicação e Ordem Econômica, nos termos dos artigos 1º, IV, 5º, inc. IX, XXXII, 170 e 220 da Constituição Federal."

101 "Art. 7º. Para os fins da presente lei, entende-se como:
V - responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem compita, na qualidade de possuidora de arquivo, registro, base ou banco de dados, a tomada de decisões referentes à realização de tratamento de dados pessoais;"

102 "Art. 23. As entidades representativas de responsáveis pelo tratamento de dados pessoais poderão instituir Conselhos de Autorregulamentação, que formularão códigos que definirão parâmetros éticos para tratamento de dados, comunicação comercial, bem como condições para sua organização, funcionamento, controle e sanções."

e operacionais aplicáveis à atividade de tratamento, embora não excluíssem a obrigação dos responsáveis de se adequar às diretrizes do CDC.

É preocupante, ainda, a ausência de menção à liberdade de expressão. A liberdade de comunicação está prevista nos artigos 3º[103] e 10[104], porém trata-se de valor similar, não idêntico. Não pode haver lei de proteção de dados no ambiente virtual que se esquive da discussão envolvendo os direitos à expressão e à privacidade, frequentemente colidentes e que são, inclusive, um dos principais pontos motivadores da criação da regulação. A garantia da liberdade de expressão é essencial ao estado democrático de direito, sendo inviável sua omissão à preservação de atividades jornalísticas ou que explorem e façam uso de informações no meio virtual.

A proteção aos dados sensíveis é também pouco explorada. Apenas dois dispositivos, quais sejam, o parágrafo único do artigo 11[105] e o artigo 12[106] tratam da proteção especial concedida a essa espécie de dado. O artigo 11 se refere de forma pouco aprofundada à adoção de medidas tecnológicas em auxílio à proteção e manutenção dos dados durante o tratamento, que devem ser proporcionais ao tipo de dado. Por sua vez, o artigo 12 permite o tratamento de dados pessoais sensíveis mediante autorização do titular, por qualquer meio que permita sua manifestação de vontade ou por imposição legal. Este último artigo não é adequado à proteção do titular, visto que legitima práticas como a obtenção de consentimento via contratos complexos e prolixos, que dificultam a real compreensão das implicações pelo titular dos dados e limitam a capacidade de negociação dos mesmos.

---

103 "Art. 3º. A proteção aos direitos e garantias mencionados no artigo primeiro desta lei deverá ser promovida com observância dos princípios constitucionais da Defesa do Consumidor, Livre iniciativa, Liberdade de Comunicação e Ordem Econômica, nos termos dos artigos 1º, IV, 5º, inc. IX, XXXII, 170 e 220 da Constituição Federal."

104 "Art. 10. A disciplina jurídica do tratamento de dados pessoais tem como objetivos fundamentais a proteção dos direitos básicos do consumidor, a garantia da ordem econômica e a manutenção da livre iniciativa e da liberdade de comunicação, de modo que em seu âmbito deverão ser observados os princípios estabelecidos nesta lei."

105 "Art. 11. O responsável pelo tratamento de dados, bem como eventuais subcontratados, deverão adotar medidas tecnológicas aptas a reduzir ao máximo o risco da destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular.
Parágrafo Único. As medidas a serem adotadas devem ser proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis."

106 "Art. 12. O início do tratamento de dados pessoais sensíveis, quando não solicitado pelo titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal."

Frise-se, ainda, que o artigo 11 supramencionado é o único que versa sobre segurança dos dados. Não há, no texto, quaisquer outras medidas específicas de proteção e segurança, o que torna este projeto bastante inferior, neste ponto, aos outros dois abordados neste trabalho.

Outro ponto relevante está presente no artigo 13[107]. A emenda aprovada pelo relator em 2016 modificou um direito do titular de dados: se antes lhe era concedido o direito de requerer o "bloqueio do registro", atualmente a redação do artigo lhe confere o direito de bloquear o tratamento de dados pessoais e a interconexão. A redação é polêmica por dar margem à interpretação de que este artigo assegura o direito ao esquecimento sem quaisquer condicionamentos ao pedido. O texto não é suficientemente claro, portanto, se aprovado, a execução do direito ao esquecimento dependerá de interpretação judiciária favorável.

A questão do consentimento é igualmente abandonada pelo PL em questão, que não disponibiliza sequer a definição ou classificação do consentimento – por exemplo, como explícito, informado ou específico, a exemplo do que ocorre nos demais projetos de lei. Apenas o artigo 12, já mencionado, fala em autorização do titular para tratamento de dados sensíveis. O artigo 17[108], por sua vez, obriga a obtenção de consentimento dos responsáveis legais para o tratamento de dados pessoais de crianças. Desse modo, foi insuficientemente explorada a forma como deve ser obtida a permissão do titular.

Neste sentido, se mostra deveras problemático o artigo 14[109], por permitir o compartilhamento de dados com terceiros sem o consentimento do titular. Ora, não é preciso muita reflexão para concluir que o efeito extremo de tal disposição seria a livre circulação de dados entre entes dos setores privado e público, sob a mera justificativa de que contribuem indiretamente para a realização do tratamento. Em resumo, trata-se de relaxamento à proteção de dados e menosprezo ao dever de informar ao titular sobre quais pessoas jurídicas têm acesso a suas informações. Ressalte-se, enfim, que não existe qualquer disposição no PL quanto à transferência internacional de dados, contribuindo com a insegurança jurídica reinante.

---

107 "Art. 13 O tratamento de dados pessoais ou a sua interconexão respeitará a lealdade e boa fé, de modo a atender aos legítimos interesses dos seus titulares, lhes devendo ser garantido sempre o direito ao bloqueio do tratamento de dados pessoais e da interconexão, salvo se necessário para cumprimento de obrigação legal ou contratual."

108 "Art. 17. O tratamento de dados pessoais de crianças somente será possível mediante o consentimento dos seus pais, responsáveis legais ou por imposição legal."

109 "Art. 14. Respeitado o disposto no art. 13, os responsáveis pelo tratamento de dados poderão compartilhá-los, inclusive para fins de comunicação comercial, com empresas integrantes de um mesmo grupo econômico, parceiros comerciais ou terceiros que direta ou indiretamente contribuam para a realização do tratamento de dados pessoais."

4.3.3 Projeto de Lei nº 5.276 de 2016

Falemos, finalmente, do Projeto de Lei nº 5.276 de 2016, de autoria do Poder Executivo, o mais apto dentre todas as proposições a se tornar a futura Lei de Proteção de Dados Pessoais, em razão de sua similaridade com o regulamento europeu de proteção de dados (GDPR) e da ampla participação social em sua construção.

A fase inicial de elaboração, quando se tratava ainda de Anteprojeto de Lei de Proteção de Dados Pessoais, foi aberta a comentários de pessoas jurídicas e físicas, por meio de plataforma digital[110] no sítio do Ministério da Justiça e Cidadania. Posteriormente, em junho de 2016, o deputado Alessandro Molon, relator do agora Projeto de Lei de Proteção de Dados Pessoais, disponibilizou o texto novamente à consulta pública, desta vez em plataforma digital[111] pertencente à Câmara dos Deputados. Vale ressaltar que o texto original sofreu alterações em maio de 2016, quando foram propostas onze emendas parlamentares ao projeto.

O PL 5.276 de 2016 garante proteção aos direitos fundamentais dos titulares e suas disposições condizem com os padrões internacionais de proteção de dados. Logo no inciso II[112] do artigo 2º, encontramos menção à liberdade de expressão, de comunicação e de opinião. Por sua vez, o inciso III do mesmo artigo[113] garante a inviolabilidade da intimidade da vida privada, da honra e da imagem. Ainda que à primeira vista os dois princípios pareçam opostos, pelos direitos que resguardam, é extremamente relevante que ambos estejam positivados, posto que não cabe à regulação eleger um ou outro como o mais relevante na orientação do tratamento de dados pessoais. Apenas a análise judiciária do caso concreto, por meio da ponderação, pode definir qual prevalecerá em eventual litígio. Também em reforço à proteção da liberdade de expressão, o inciso II do artigo 4º[114] dispõe que as atividades jornalísticas, artísticas, literárias e acadêmicas estarão fora do escopo dessa lei.

---

110 Proteção de Dados Pessoais. Debate Público. Pensando o Direito. Ministério da Justiça. Disponível em: <http://pensando.mj.gov.br/dadospessoais/>. Acesso em: 28 maio. 2017.

111 Proteção de Dados Pessoais. Consulta Pública. PL 5.276/2016. E-Democracia. Wikilegis. Câmara dos Deputados. Disponível em: <https://edemocracia.camara.leg.br/wikilegis/bill/46/>. Acesso em: 28 maio. 2017.

112 "Art. 2º A disciplina da proteção de dados pessoais tem como fundamento o respeito à privacidade e:
(...)
II – a liberdade de expressão, de comunicação e de opinião;"

113 "III – a inviolabilidade da intimidade, da vida privada, da honra e da imagem;"

114 "Art. 4º Esta Lei não se aplica ao tratamento de dados:
(...)

A qualificação do consentimento do titular ao tratamento de dados pessoais se encontra no inciso I do artigo 7º[115] e no artigo 9º[116] do projeto. Determinou-se que tal consentimento deve ser livre, informado e inequívoco. Embora tenham sido oferecidas emendas em 2016 a este artigo, permaneceram tais exigências relativas ao consentimento para o tratamento desta espécie de dado. Todavia, a qualificação do consentimento para realização do tratamento de dados sensíveis sofreu alterações com a Emenda nº 4, também proposta em 2016. Anteriormente, o consentimento para tratamento de dados sensíveis era qualificado no inciso I do artigo 11[117] como "livre, inequívoco, informado, expresso e específico". Porém, a nova redação impõe que tal consentimento seja qualificado apenas como "livre e inequívoco", diminuindo consideravelmente o nível de proteção dos titulares em relação aos seus dados sensíveis. Se antes havia graus diferenciados de consentimento para cada espécie de dado, que garantiam a transparência no processo de tratamento e que o nível de proteção estivesse de acordo com o tipo de informação, se o texto emendado permanecer desta forma, estas garantias se perderão parcialmente.

Seguindo a análise, verificamos que caso a atividade de tratamento importe em coleta continuada de dados, estipula-se que o titular deve ser periodicamente informado acerca das principais características do tratamento (§3º do artigo 8º)[118]. Por fim, o artigo 40[119] traz a obrigação de coleta de consentimento do titular para que se efetue a transferência de dados entre responsáveis ou operadores de direito privado.

Impossível não conceder grande destaque à designação de um órgão competente para regular o tratamento de dados pessoais. Embora o PL não fale em autoridade específica e independente, a Seção II do Capítulo VIII prevê a criação de um Conselho Nacional de Proteção de Dados e da Privacidade, como uma tentativa de criar um mecanismo de participação social. Embora o órgão competente seja reiteradamente mencionado no decorrer do texto, este se abstém de especificar como será a composição e o funcionamento do ente

---

II – realizado para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos; ou"

115 "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento pelo titular de consentimento livre, informado e inequívoco;"

116 "Art. 9º O consentimento previsto no art. 7º, I deverá ser livre, informado e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique."

117 "Art. 11. É vedado o tratamento de dados pessoais sensíveis, exceto salvo:
I – com fornecimento de consentimento livre, inequívoco, informado, expresso e específico pelo titular:"

118 "§3º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado periodicamente sobre as principais características do tratamento, nos termos definidos pelo órgão competente, sendo respeitados os segredos comercial e industrial."

119 "Art. 40. A comunicação de dados pessoais entre responsáveis ou operadores de direito privado dependerá do consentimento do titular, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei."

competente, tornando necessária a edição de regulamento posterior. De qualquer forma, a figura da autoridade competente é bem explorada ao longo de todo o projeto, não restando dúvidas de que este é um tópico que ainda deve ser debatido mais detalhadamente.

É importante ressaltar, ainda, que o PL 5.276 de 2016 faz menção explícita à Lei de Acesso à Informação[120] (Lei nº 12.527 de 2011) no artigo 23[121], no parágrafo único do artigo 26[122] e no parágrafo único do artigo 44[123]. Tais menções proporcionam as seguintes garantias: (i) o tratamento de dados pessoais realizado por pessoas jurídicas de direito público deve atender a uma finalidade pública; (ii) a transferência de dados do poder público a entes privados só ocorrerá em casos de execução descentralizada de atividade pública, sendo estipulado um fim específico e determinado; (iii) não há responsabilidade solidária para o agente que atua no exercício dos deveres da Lei de Acesso à Informação.

Por sua vez, a transferência internacional de dados pessoais é regulada pelos artigos 33, 34 e 35. O artigo 33 elenca as hipóteses em que é permitida a transferência internacional[124]. É exigido, para as transferências em geral, que o país receptor possua nível de proteção de dados ao menos compatível com o proporcionado pela lei brasileira, e os critérios utilizados para aferição do nível de proteção do país estrangeiro estão dispostos no parágrafo único[125] do

---

120 BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Poder Legislativo. Brasília. DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 28 maio. 2017.

121 "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1º da Lei 12.527, de 18 de novembro de 2011, deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou o cumprimento de atribuição legal pelo serviço público."

122 "Parágrafo único. É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que o exija exclusivamente para este fim específico e determinado, observado o disposto na Lei 12.527, de 2011, bem como nos casos em que houver previsão legal ou respaldo em convênio celebrado com entidades privadas, com finalidade específica."

123 "Parágrafo único. A responsabilidade solidária não se aplica aos casos de tratamento realizado no exercício dos deveres de que trata a Lei nº 12.527, de 18 de novembro de 2011, relativos à garantia do acesso a informações públicas."

124 "Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
I – para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;
II – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;
III – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
IV – quando o órgão competente autorizar a transferência;
V – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
VI – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24.; ou
VII – quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos."

125 "Parágrafo único. O nível de proteção de dados do país será avaliado pelo órgão competente, que levará em conta:

artigo 33. Considerando que este artigo também permite, dentre outras hipóteses, que haja transferência mediante autorização do órgão competente, o artigo 34 traz mais detalhes quanto a esta autorização. Por fim, o artigo 35 determina a responsabilidade objetiva e solidária entre cedente e cessionário, o que traz maior segurança, indiretamente, ao titular de dados.

Quanto à segurança de dados, o projeto em questão traz diversas previsões. A segurança de dados é inserida no inciso VII do artigo 6º[126], inclusive, como um dos princípios que regerão toda a atividade de tratamento. É imperativo que sejam utilizadas medidas técnicas e administrativas atualizadas durante todo o tratamento, e que sejam adequadas à espécie de dado que visam tutelar. O PL ainda prevê a eliminação dos dados ao término do tratamento (artigo 16, caput)[127] e a publicação de relatórios de impacto de privacidade (artigo 32)[128], além de dedicar o Capítulo VII inteiramente à segurança e às boas práticas. Neste ponto, portanto, o projeto se mostra bastante sólido.

Por último, cabe ressaltar o artigo 18, que, no inciso VI[129], permite a exclusão de dados pessoais a qualquer momento quando o titular houver consentido com o tratamento. Há que se ter cautela com a interpretação deste dispositivo, de modo a evitar abusos em nome do já mencionado direito ao esquecimento. O risco é de que dados cuja retirada seja requerida por seus titulares sejam, na verdade, informações de interesse público e que devem permanecer disponíveis e acessíveis, em prol deste interesse. Seria útil incorporar ao texto uma ressalva nesse sentido, de modo a não vedar o direito ao esquecimento, porém condicioná-lo à não configuração de interesse público.

I – as normas gerais e setoriais da legislação em vigor no país de destino;
II – a natureza dos dados;
III – a observância dos princípios gerais de proteção de dados pessoais previstos nesta
Lei; IV – a adoção de medidas de segurança previstas em regulamento; e
V – as outras circunstâncias específicas relativas à transferência."

[126] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...)
VII – segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;"

[127] "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:"

[128] "Art. 32. O órgão competente poderá solicitar a agentes do poder público a publicação de relatórios de impacto de privacidade e sugerir a adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público."

[129] "Art. 18. O titular dos dados pessoais tem direito a obter, em relação aos seus dados:
(...)
VI – eliminação, a qualquer momento, de dados pessoais com cujo tratamento o titular tenha consentido; e"

Percebemos, deste modo, que a maior complexidade do PL 5.276 o torna o mais apto a lidar com as dificuldades do mundo cibernético. Suas disposições, em comparação aos demais projetos de lei, são mais ricas em detalhes e orientações à atuação dos entes públicos e privados. Além disso, está em consonância com padrões internacionais de proteção de dados, visto que seu texto reflete, em grande parte, o que está contido no General Data Protection Regulation, exemplo de legislação neste âmbito.

5 CONCLUSÃO

A análise das propostas que tramitam hoje no Congresso Nacional revela, não de maneira surpreendente, o quanto é custoso ao Direito acompanhar o avanço tecnológico e propiciar um ambiente simultaneamente seguro e aberto à inovação, que pareça atraente tanto aos usuários da rede mundial de computadores quanto às empresas provedoras de rede ou desenvolvedoras de aparatos tecnológicos.

Nota-se que o tema aqui tratado apresenta relevância (i) jurídica, tendo em vista que a problemática da questão regulatória se faz necessária para proporcionar segurança jurídica aos atores envolvidos e sanar quaisquer temores dos que disponibilizam suas informações pessoais diariamente nas redes, voluntária ou involuntariamente – o segundo caso se dá, como vimos, por exemplo, com o histórico de navegação na rede, que muitos usuários sequer têm consciência de que pode ser visualizado e utilizado comercialmente por provedores; (ii) política, em razão de estar circunscrito na atuação do Poder Público, na política de regulação e no controle estatal por meio de suas agências reguladoras; e (iv) social, devido à ampla utilização dos meios virtuais a nível global e da altíssima frequência com que os diversos tipos de dados trafegam nestes meios. A função social do tema é latente, considerando que quase todos os cidadãos, no momento histórico em que nos encontramos, possuem dados pessoais conectados à rede cibernética, melhor dizendo, em posse de provedores ou servidores.

Compreendemos que mesmo a tarefa mais simples e primordial como a definição dos termos utilizados e dos agentes envolvidos no tratamento de dados pessoais pode se mostrar complexa e repleta de desdobramentos. Prova disso é a dificuldade nas legislações de todo o mundo em lidar com as diferentes espécies de dados e suas inconstâncias e necessidades específicas, como é o caso dos dados anônimos ou anonimizados, cuja forma de tratamento é ainda objeto de debate, em razão do barateamento e da popularização de técnicas de reidentificação.

Vimos que tentativas de tentar proteger informações no meio virtual possuem seus ônus, tendo em vista que, dentre os bilhões de dados que trafegam diariamente pela rede mundial de computadores, pode haver informações úteis à segurança pública que passam despercebidas ou que não podem ser alcançadas devido ao sigilo. Como se fosse um lado diverso da mesma moeda, diariamente a privacidade de diversos titulares de dados é colocada em risco também

em nome da segurança, bem como são tomadas medidas proporcionais por magistrados carentes de legislação e jurisprudência. O Poder Judiciário e os que nele atuam não poderiam, decerto, ser algo além de um reflexo da sociedade em que se inserem. E quando se fala em privacidade no ambiente cibernético, o despreparo é generalizado.

Analisamos as discussões em torno de uma legislação nacional específica sobre a proteção de dados pessoais e da privacidade na rede mundial de computadores. Tendo em vista que outros Estados soberanos já possuem tal marco regulatório e que mesmo blocos econômicos se encontram adiantados na referida regulação, como é o caso da União Europeia, faz-se necessário um estudo comparado do tema para que, analisando os posicionamentos legislativos já adotados, visualizem-se as possíveis medidas que podem ser tomadas na elaboração de uma lei eficaz e que atenda às necessidades brasileiras.

De igual maneira, as divergências teóricas sobre o tema foram consideradas neste trabalho, bem como as diferentes posições tomadas pelos estudiosos e especialistas frente às colisões entre princípios constitucionais, que por excelência não se eliminam no embate, mas devem ser ponderados para que prevaleça o preferível à situação que se apresenta.

Todavia, ainda que as dificuldades sejam perceptíveis, a expansão da utilização de dados trazida pela *Internet of Things* deixa claro que é necessário persistir na regulação da atividade de tratamento, para evitar abusos e violações de direitos fundamentais. Em um cenário de hiperconexão, é premente que exista um arcabouço regulatório sólido, no sentido de não deixar brechas à utilização indevida de dados e à lesão de direitos de seus titulares, porém flexível a ponto de não engessar a navegação na rede ou frear o desenvolvimento tecnológico, bem como para abarcar dispositivos e técnicas que ainda estão por vir.

Há muito que se explorar e descobrir mesmo em relação ao que já estamos familiarizados, como é o caso, por exemplo, o *Big Data* e da utilização de algoritmos. Ainda que diversos segmentos do mercado sejam assíduos exploradores das facilidades e benefícios trazidos por estes elementos, como é o caso da publicidade, com o marketing personalizado, ainda há muito que evoluir em outros setores da sociedade que ainda não estão intimamente ligados à Internet e desconhecem, ou não podem ainda arcar com os custos de uma operacionalização mais moderna e conectada.

Ficou evidente que é necessário conhecer melhor a realidade virtual em âmbito nacional, o comportamento dos usuários brasileiros e dos provedores que aqui têm sede ou

realizam suas operações de tratamento de dados. Ainda, é igualmente essencial explorar a legislação brasileira já existente sobre o ambiente virtual, especialmente quando se refere ao uso de dados ou aos princípios ligados ao tema, para que se verifica a melhor maneira de implementar uma lei específica de proteção de dados pessoais.

Como vimos, nos países ou blocos econômicos que já têm como uma realidade a ampla utilização da tecnologia, em um cenário de barateamento de aparatos tecnológicos, também encontram percalços ao abordar o tema da proteção à privacidade e às informações. Atualmente, o tema vem sendo tratado de forma mais consistente pela União Europeia, por meio do General Data Protection Regulation, que traz previsões detalhadas e protetivas dos direitos humanos válidas para todos os Estados-membros do bloco. Por outro lado, países como Japão e Estados Unidos, embora desenvolvidos, possuem ainda muitas fragilidades no trato interno.

É útil, portanto, que o Brasil se inspire em experiências estrangeiras bem sucedidas durante o processo de elaboração de sua própria lei específica de proteção de dados pessoais. Assim, é possível aferir qual a melhor forma de lidar com tópicos como a determinação de uma autoridade competente, regras para a transferência internacional de dados e em relação ao consentimento do titular de dados para a realização do tratamento. Ainda que passíveis de críticas, os marcos regulatórios internacionais se mostram um bom ponto de partida para o legislador nacional.

Por último, pudemos verificar que, para que seja possível controlar a atuação dos responsáveis pelas operações de tratamento, compartilhamento e guarda de dados, bem como para garantir os direitos fundamentais de seus titulares, se faz necessária a criação de uma Autoridade Competente. Tal autoridade regulatória deverá ser dotada de independência e autonomia, e deve ser assegurada a participação da sociedade em sua atuação. Ainda, sua estrutura deve ser altamente setorial, englobando as mais diversas áreas – engenharia, sociologia, dentre outras – para garantir o *enforcement*. Esse corpo técnico deve possuir conhecimentos ou ser capaz de providenciar assistência técnica sobre linha de montagem, agronomia, informática e quaisquer outros ramos econômicos que possam vir a fazer uso de dados, garantindo que haja equilíbrio e propriedade nas tomadas de decisão.

Mesmo a observação de experiências não muito bem sucedidas no plano internacional, bem como dos precedentes judiciais falhos no plano interno, devem ser analisados de modo a evitar disposições e decisões judiciais desastrosas no futuro, que lesionem direitos e falhem na

proteção das partes envolvidas no tratamento de dados pessoais. Decisões judiciais desproporcionais, como a determinação de bloqueio e exclusão de aplicativos não se mostraram aptas a conceder a tutela que pretendiam.

Notamos, assim, por todo exposto, que ainda há um longo caminho a ser trilhado em direção a um consistente diploma legal nacional de proteção de dados e da privacidade na Internet. O presente trabalho mostrou as dificuldades existentes no cenário atual, porém outros imprevistos podem surgir, conforme a sociedade se adapta e as tecnologias evoluem. O Direito, pelo menos no que tange ao aspecto legislativo, não pode, por sua própria essência, acompanhar tais desdobramentos com a mesma velocidade. Permanece, contudo, a esperança de que o Congresso Nacional, com a colaboração de todos os setores da sociedade, não poupe esforços na elaboração de uma Lei interna de Proteção de Dados Pessoais pautada nas melhores práticas internacionais e com foco na proteção dos direitos humanas e garantias individuais.

REFERÊNCIAS BIBLIOGRÁFICAS

30º SEMINÁRIO INTERNACIONAL DA ABDTIC. **Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações**. 2016. São Paulo. SP.

About APEC. What is Asia-Pacific Economic Cooperation?. Asia-Pacific Economic Cooperation. **APEC Secretariat**. 2017. Disponível em: <http://www.apec.org/About-Us/About-APEC>. Acesso em: 27 maio. 2017.

About TTIP. Trade. **European Commission**. Disponível em: <http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/>. Acesso em: 28 maio. 2017.

AGÊNCIAS. EUA avançam em proposta de privacidade na internet. Link. **Estadão**. 31 mar. 2016. Disponível em: <http://link.estadao.com.br/noticias/empresas,eua-avancam-em-proposta-de-privacidade-na-internet,10000047929>. Acesso em: 27 maio. 2017.

AMARAL, Bruno do. Europa pressiona WhatsApp pelo fim da criptografia em investigações de terrorismo. **MobileTime**. 27 mar. 2017. Disponível em: <http://www.mobiletime.com.br/27/03/2017/europa-pressiona-whatsapp-pelo-fim-da-criptografia-em-investigacoes-de-terrorismo/468662/news.aspx?__akacao=4011184&__akcnt=012c3547&__akvkey=a6b3&utm_source=akna&utm_medium=email&utm_campaign=MOBILE+TIME+News+-+27%2F03%2F2017+20%3A01>. Acesso em: 27 maio. 2017.

AMARAL, Bruno do. IoT ainda enfrenta barreiras regulatórias para decolar no Brasil. **TeleTime**. 7 fev. 2017. Disponível em: <http://convergecom.com.br/teletime/07/02/2017/iot-ainda-enfrenta-barreiras-regulatorias-para-decolar-no-brasil/?noticiario=TT&__akacao=3934077&__akcnt=012c3547&__akvkey=19e6&utm_source=akna&utm_medium=email&utm_campaign=TELETIME+News+-+07%2F02%2F2017+22%3A46>. Acesso em: 27 maio. 2017.

AMARAL, Bruno do. IoT ainda traz incertezas ao setor. Internet das Coisas. **TeleTime**. 18 out. 2016. Disponível em: <http://convergecom.com.br/teletime/18/10/2016/iot-ainda-traz-incertezas-ao-setor/>. Acesso em: 27 maio. 2017.

AMARAL, Bruno do. Nova regulação europeia de privacidade de dados trará impacto para outras regiões. MWC 2017. **TeleTime**. 28 fev. 2017. Disponível em:

<http://convergecom.com.br/teletime/28/02/2017/nova-regulacao-europeia-de-privacidade-de-dados-trara-impacto-para-outras-regioes/>. Acesso em: 27 maio. 2017.

AMARAL, Bruno do. Parlamento Europeu critica política de privacidade de Trump e pede revisão de acordos. Internacional. **TeleTime**. 6 abr. 2017. Disponível em: <http://convergecom.com.br/teletime/06/04/2017/parlamento-europeu-critica-politica-de-privacidade-governo-trump-e-pede-revisao-de-acordos/?noticiario=TT&__akacao=4078097&__akcnt=012c3547&__akvkey=b105&utm_source=akna&utm_medium=email&utm_campaign=TELETIME+News+-+06%2F04%2F2017+22%3A51>. Acesso em: 28 maio. 2017.

AMARAL, Bruno do. Trump confirma Ajit Pai como novo chairman da FCC. **TeleTime**. 23 jan. 2017. Disponível em: <http://convergecom.com.br/teletime/23/01/2017/trump-confirma-akit-pai-como-novo-chairman-da-fcc/>. Acesso em: 27 maio. 2017.

AMARAL, Bruno do. Trump sanciona lei que revoga regra de privacidade de usuários. Internacional. **TeleTime**. 4 abr. 2017. Disponível em: <http://convergecom.com.br/teletime/04/04/2017/trump-sanciona-lei-que-revoga-regra-de-privacidade-de-usuarios/?noticiario=TT>. Acesso em: 27 maio. 2017.

APEC Privacy Framework. APEC#205-SO-01.2. Dez. 2005. Reports. **Electronic Commerce Steering Group**. p. 36. Disponível em: <http://publications.apec.org/publication-detail.php?pub_id=390>. Acesso em: 28 maio. 2017

ARTICLE 19. Proteção de dados pessoais no Brasil. Análise dos Projetos de Lei em tramitação no Congresso Nacional. Licença: Creative Commons 3.0. Nov. 2016.

Ataque perto do Parlamento britânico em Londres deixa 4 mortos, incluindo suspeito. Mundo. **G1**. Brasil. 22 mar. 2017. Disponível em: <http://g1.globo.com/mundo/noticia/tiroteio-fora-do-parlamento-britanico-deixa-feridos.ghtml>. Acesso em: 27 maio. 2017.

Banco de Dados. Glossário. High-Tech. **CCM**. Maio. 2017. Disponível em: <http://br.ccm.net/contents/65-introducao-aos-bancos-de-dados>. Acesso em: 28 maio. 2017.

BERBERT, Lúcia. Consentimento é ponto-chave da proposta de lei de proteção a dados pessoais. **TI Inside Online**. 28 jan. 2015. Disponível em: <http://convergecom.com.br/tiinside/home/internet/28/01/2015/consentimento-e-ponto-chave-da-proposta-de-lei-de-protecao-dados-pessoais/>. Acesso em: 28 maio. 2017.

BRASIL. Constituição da República Federativa do Brasil de 1988. Publicação em: 5 out. 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em 28 maio. 2017.

BRASIL. Decreto nº 7.962, de 15 de março de 2013. Poder Executivo. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm>. Acesso em: 28 maio. 2017.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em 28 maio. 2017.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em 28 maio. 2017.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Poder Legislativo. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 28 maio. 2017.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Poder Legislativo. Brasília. DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 28 maio. 2017.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em 28 maio. 2017.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União. Atos do Poder Legislativo. Brasília. DF. 24 abril. 2014. Seção 1. p. 1.

BRASIL. Projeto de Lei nº 5.276, de 2016. Câmara dos Deputados. Autoria: Poder Executivo. Apresentado: 15 maio. 2016. Brasília. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 27 maio. 2017.

BRASIL. Projeto de Lei nº 4.060, de 2012. Câmara dos Deputados. Autoria: Deputado Milton Monti. Apresentado: 13 jun. 2012. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 28 maio. 2017.

BRASIL. Projeto de Lei do Senado nª 330, de 2013. Senado Federal. Autoria: Senador Antonio Carlos Valadares. Apresentado: 13 ago. 2013. Brasília. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/113947>. Acesso em: 27 maio. 2017.

CARVALHO FILHO, José dos Santos. Manual de Direito Administrativo. 10ª Edição. Editora Lumen Juris. Rio de Janeiro, 2003.

Cartilha de Segurança para Internet. Cert.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <https://cartilha.cert.br/criptografia/>. Acesso em: 28 maio. 2017.

Commission decisions on the adequacy of the protection of personal data in third countries. Justice. **European Commission**. 2017. Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm>. Acesso em: 27 maio. 2017.

Consulta sobre o Plano Nacional de IoT recebeu 2,28 mil contribuições. **CIO**. 16 fev. 2017. Disponível em: <http://cio.com.br/tecnologia/2017/02/16/consulta-sobre-o-plano-nacional-de-iot-recebeu-2-28-mil-contribuicoes/>. Acesso em: 27 maio. 2017.

CRIADO, Miguel Ángel. Quatro compras com o cartão bastam para identificar qualquer pessoa. Privacidade na Internet. **El País**. 30 jan. 2015. Disponível em: <http://brasil.elpais.com/brasil/2015/01/29/ciencia/1422520042_066660.html>. Acesso em: 27 maio. 2017.

CROFTS, Lewis. Big Data case in Europe 'still to come', Vestager says. **MLEX Market Insight**. Jurisdiction: EU, Europe. 31 mar. 2017.

Data protection ruled out of EU-US trade talks. **Financial Times**. 2013. Disponível em: <https://www.ft.com/content/92a14dd2-44b9-11e3-a751-00144feabdc0>. Acesso em 28 maio. 2017.

DECISÃO. **Ação Civil Pública**. Processo nº 0028553-98.2014.8.08.0024. Natureza Cível. 5ª Vara Cível. Vitória, Espírito Santo. Distribuído em: 18 ago. 2014. Disponível em: <http://s.conjur.com.br/dl/juiz-proibe-aplicativo-secret-celulares.pdf>. Acesso em: 28 maio. 2017.

Decisão de juiz do Piauí manda tirar WhatsApp do ar em todo o Brasil. **G1**. Piauí. 25 fev. 2015. Disponível em: <http://g1.globo.com/pi/piaui/noticia/2015/02/decisao-de-juiz-do-piaui-manda-tirar-whatsapp-do-ar-em-todo-o-brasil.html>. Acesso em: 27 maio. 2017.

DEWES, Pablo. A gestão de risco e os desafios da segurança no varejo online. Segurança. **E-Commerce Brasil**. 28 set. 2015. Disponível em: <https://www.ecommercebrasil.com.br/artigos/a-gestao-de-risco-e-os-desafios-da-seguranca-no-varejo-online/>. Acesso em: 28 maio. 2017.

DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 25ª edição. Editora Atlas. São Paulo, SP. 2012.

Digital Single Market. Strategy. **European Commission**. 2017. Disponível em: <https://ec.europa.eu/digital-single-market/en/digital-single-market>. Acesso em: 27 maio. 2017.

DRUMMOND, Victor. Internet, Privacidade e Dados Pessoais. **Editora Lumen Juris**. 2003. Rio de Janeiro. P. 142.

EUROPE UNION. Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). **Official Journal of the European Union**. Brussels. Disponível em: <http://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 27 maio. 2017.

EUROPEAN DATA PROTECTION SUPERVISOR. The EU's independent data protection authority. Disponível em: <https://edps.europa.eu/edps-homepage_en?lang=pt>. Acesso em: 27 maio. 2017.

FEDERAL TRADE COMISSION. Washington, DC. Estados Unidos. Disponível em: <https://www.ftc.gov>. Acesso em: 27 maio. 2017.

FORTIN-COUSENS, Anick; HEYDER, Markus. A Model for Global Privacy Protections. **Bloomberg BNA**. Privacy and Security Law Report by The Bureau of National Affairs, INC. 2015. APEC Privacy Rules for Cross-Border Data Flows.

GIBBS, Samuel. What is 'safe harbour' and why did the EUCJ just declare it invalid?. Internet. **The Guardian**. 6 out. 2015. Disponível em: <https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection>. Acesso em: 28 maio. 2017.

GOLDSCHMIDT, Ronaldo; BEZERRA, Eduardo. Exemplos de aplicações de data mining no mercado brasileiro. **ComputerWorld**. 27 jun. 2016. Disponível em: <http://computerworld.com.br/exemplos-de-aplicacoes-de-data-mining-no-mercado-brasileiro>. Acesso em: 27 maio. 2017.

Greater Protection for Consumers as Canada Joins Asia-Pacific Privacy Regime. **Asia-Pacific Economic Cooperation**. Ottawa, Canada. 15 abr. 2015. Disponível em:

<http://www.apec.org/Press/News-Releases/2015/0415_CBPR.aspx>. Acesso em: 28 maio. 2017.

HEKIMA. O dicionário de Big Data. Big Data Business. 14 maio. 2016. Disponível em: <http://www.bigdatabusiness.com.br/o-dicionario-do-big-data-3/>. Acesso em: 28 maio. 2017.

KEIDANREN. Japan Business Federation. Disponível em: <http://www.keidanren.or.jp/en/profile/pro001.html>. Acesso em: 28 maio. 2017.

LEONARD, John. TTIP vs GDPR - who will win the data protection wars?. Legislation and Regulation. **Computing**. 25 jan. 2016. Disponível em: <http://www.computing.co.uk/ctg/analysis/2443135/ttip-vs-gdpr-who-will-win-the-data-protection-wars>. Acesso em: 28 maio. 2017.

LEONARDI, Marcel. Internet e regulação: o bom exemplo do Marco Civil da Internet. **Revista do Advogado**, número 115, ano XXXII. Associação dos Advogados de São Paulo. 2012. Disponível em: <http://leonardi.adv.br/2012/04/internet-e-regulacao-o-bom-exemplo-do-marco-civil-da-internet/>. Acesso em: 27 maio. 2017.

MACHADO, André. Dados dos usuários não são mercadoria, diz Alessandro Molon: Relator do Marco Civil da Internet diz que lei protegerá liberdade de expressão e privacidade. **O Globo**. 01 jul. 2012. Disponível em: < http://oglobo.globo.com/economia/dados-dos-usuarios-nao-sao-mercadoria-diz-alessandro-molon-5367541>. Acesso em: 27 maio. 2017.

MANZONI JÚNIOR, Ralphe. WhatsApp é o aplicativo mais usado pelos brasileiros. **IstoÉ**. Dinheiro. Bastidores das empresas. 18 jan. 2017. Disponível em: <http://www.istoedinheiro.com.br/blogs-e-colunas/post/20170118/whatsapp-aplicativo-mais-usado-pelos-brasileiros/10223>. Acesso em: 27 maio. 2017.

MASSO, Fabiano Del, et al. Marco Civil da Internet: Lei 12.965/2014. Editora Revista dos Tribunais. São Paulo, SP. 2014.

MENDES, Gilmar Ferreira, et al. Direito, Inovação e Tecnologia. Volume 1. Editora Saraiva. São Paulo, SP. 2014.

MELO, Vinicius Veloso de. 2005. Clustering de artigos científicos em uma Ferramenta Inteligente de apoio à Pesquisa. Dissertação. **Universidade de São Paulo**. Maio. 2005. p. 11. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiNkrGVh-bTAhUFjJAKHZkpDFUQFggkMAA&url=http%3A%2F%2Fwww.teses.usp.br%2Fteses%2Fdisponiveis%2F55%2F55134%2Ftde-11122014-

104427%2Fpublico%2FViniciusVelosodeMelo_ME.pdf&usg=AFQjCNGiCAq_wUTI2mRf30YAxoKgOcaqUw>. Acesso em: 28 maio. 2017.

MICHAELIS. Dicionário Brasileiro da Língua Portuguesa. Português Brasileiro. Criptografia. Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=criptografia>. Acesso em: 27 maio. 2017.

MORGAN, Jacob. A Simple Explanation Of 'The Internet Of Things'. Leadership. **Forbes**. 13 maio. 2014. Disponível em: <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#45efd4ba6828>. Acesso em: 28 maio. 2017.

MOROZOV, Evgeny. What happens when policy is made by corporations? Your privacy is seen as a barrier to economic growth. Data Protection. Opinion. **The Guardian**. 12 jul. 2015. Disponível em: <https://www.theguardian.com/commentisfree/2015/jul/12/ttip-your-data-privacy-is-a-barrier-to-economic-growth>. Acesso em: 28 maio. 2017.

O que é o TPP, o acordo econômico entre 11 países do qual Trump retirou EUA. **BBC Brasil**. 24 jan. 2017. Disponível em: <http://www.bbc.com/portuguese/internacional-38729570>. Acesso em: 28 maio. 2017.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Rights and Translation unit, Public Affairs and Communications Directorate. **Organization For Economic Co-operation And Development**. 2003. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 28 maio. 2017.

Organização para a Cooperação e Desenvolvimento Econômico, OCDE. Secretaria de Assuntos Internacionais. **Ministério da Fazenda**. Disponível em: <http://www.sain.fazenda.gov.br/assuntos/politicas-institucionais-economico-financeiras-e-cooperacao-internacional/ocde>. Acesso em: 28 maio. 2017.

OW, Jack. The Trans-Pacific Partnership's take on personal data. **TaylorWessing**. Dez. 2015. Disponível em: <https://united-kingdom.taylorwessing.com/globaldatahub/article-the-tpp-take-on-personal-data.html>. Acesso em: 28 maio. 2017.

PAIVA, Fernando. WhatsApp: um em cada três usuários no Brasil liga pelo app diariamente. **MobileTime**. 3 mar. 2016. Disponível em: <http://www.mobiletime.com.br/03/03/2016/whatsapp-um-em-cada-tres-usuarios-no-brasil-liga-pelo-app-diariamente/433922/news.aspx>. Acesso em: 28 maio. 2017.

Pesquisa mostra dados da Internet no Brasil em 2015. Redação. Mercado. **E-Commerce Brasil**. 20 fev. 2015. Disponível em: <https://www.ecommercebrasil.com.br/noticias/pesquisa-mostra-dados-da-internet-no-brasil-em-2015/>. Acesso em 28 maio. 2017.

PRESCOTT, Roberta. Proteção de dados: o mais importante é conscientizar as pessoas. Notícias Abranet. **Associação Brasileira de Internet**. 12 ago. 2016. Disponível em: <http://www.abranet.org.br/Noticias/Protecao-de-dados%3A-o-mais-importante-e-conscientizar-as-pessoas-1151.html#.WBfR8i0rLIV>. Acesso em: 28 maio. 2017.

Proposal for an ePrivacy Regulation. Digital Single Market. Strategy. **European Commission**. 2017. Disponível em: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>. Acesso em: 27 maio. 2017.

Proteção de Dados Pessoais. Consulta Pública. PL 5.276/2016. E-Democracia. Wikilegis. **Câmara dos Deputados**. Disponível em: <https://edemocracia.camara.leg.br/wikilegis/bill/46/>. Acesso em: 28 maio. 2017.

Proteção de Dados Pessoais. Debate Público. Pensando o Direito. **Ministério da Justiça**. Disponível em: <http://pensando.mj.gov.br/dadospessoais/>. Acesso em: 28 maio. 2017.

REUTERS. Rússia estende residência de Snowden após perdão dos EUA a Manning. **G1**. 18 jan. 2017. Disponível em: <http://g1.globo.com/mundo/noticia/russia-estende-residencia-de-snowden-apos-perdao-dos-eua-a-manning.ghtml>. Acesso em: 28 maio. 2017.

RICH, Cynthia. Privacy Laws Around the World. **ABA Journal**. 29 ago. 2016. Disponível em; <http://www.abajournal.com/advertising/article/privacy_laws_around_the_world/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email>. Acesso em: 27 maio. 2017.

RODRIGUES JÚNIOR, Otavio Luiz. Direito de apagar dados e a decisão do tribunal europeu no caso Google (Parte 2). Direito Comparado. **Consultor Jurídico**. 28 maio. 2014. Disponível em: <http://www.conjur.com.br/2014-mai-28/direito-comparado-direito-apagar-dados-decisao-tribunal-europeu-google-espanha>. Acesso em: 27 maio. 2017.

ROSA, Fernanda. Como usar o Big Data na prática?. Analytics. Gestão. Artigos. **E-Commerce Brasil**. 3 nov. 2015. Disponível em:

<https://www.ecommercebrasil.com.br/artigos/como-usar-o-big-data-na-pratica/>. Acesso em: 28 maio. 2017.

SAKAMAKI, Sachiko. Japan Inc. cautious about innovative data businesses, as amended privacy law looms. Jurisdiction: Asia, Japan, North East Asia. **MLEX Market Insight**. 31 mar. 2017.

SALOMÃO, Lucas. Governo abre consulta pública sobre proteção de dados pessoais na web. **G1**. Brasília. DF. 28 jan. 2015. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/01/governo-abre-consulta-publica-sobre-protecao-de-dados-pessoais-na-web.html>. Acesso em: 27 maio. 2017.

SANTOS, Ludmila. Governo quer mais proteção para dados na internet. **Consultor Jurídico**. 25 jan. 2011. Disponível em: <http://www.conjur.com.br/2011-jan-25/consulta-publica-traca-diretrizes-lei-protecao-dados-pessoais>. Acesso em 27 maio.2017

SEKIGUCHI, Toko. Japan debate on Big Data IP protection hits classic issue of regulation v. innovation. **MLEX Market Insight**. Jurisdiction: Asia, Japan, North East Asia. 17 mar. 2017.

SOPRANA, Paula. Como a polícia pode dar a volta na criptografia do WhatsApp. **Época**. 23 jul. 2016. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/07/como-policia-pode-dar-volta-na-criptografia-do-whatsapp.html>. Acesso em: 27 maio. 2017.

SOPRANA, Paula. Justiça determina bloqueio do WhatsApp pela terceira vez em sete meses. **Época**. 19 jul. 2016. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/07/justica-determina-bloqueio-do-whatsapp-pela-terceira-vez-em-sete-meses.html>. Acesso em: 27 maio. 2017.

Suspensa liminar que determinou remoção do aplicativo Secret. Justificando. **Carta Capital**. 15 set. 2014. Disponível em: <http://justificando.cartacapital.com.br/2014/09/15/suspensa-liminar-que-determinou-remocao-de-aplicativos/>. Acesso em: 28 maio. 2017.

SWIFT, Mike. Commerce Department bullish on growth of trans-Pacific data transfer framework. Jurisdiction: Asia, Canada, Japan, Latin America, Mexico, North America, North East Asia, South Korea, Taiwan, USA. **MLEX Market Insight**. 20 abr. 2017.

The EU-U.S. Privacy Shield. Justice. **European Commission**. Disponível em: <http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm>. Acesso em: 28 maio. 2017.

The International Association of Privacy Professionals. Disponível em: <https://iapp.org/>. Acesso em: 27 maio. 2017.

The OECD Privacy Framework. 2013 OECD Privacy Guidelines. Internet Economy. **Organization For Economic Co-operation And Development**. 2013. Disponível em: <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>. Acesso em: 28 maio. 2017.

TOZETTO, Cláudia. Criptografia impede 'grampo' em conversa no WhatsApp. **O Estado de S.Paulo**. 19 jul. 2016. Disponível em: <http://brasil.estadao.com.br/noticias/geral,criptografia-impede-grampo-em-conversa-no-whatsapp,10000063854>. Acesso em: 28 maio. 2017.

UE expande 'direito ao esquecimento' a todo serviço na internet. **G1**. São Paulo. 15 abr. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/ue-expande-direito-ao-esquecimento-todo-servico-na-internet.html>. Acesso em: 27 maio. 2017.

UK privacy professionals preparing for new EU rules despite Brexit, IAPP says. **MLEX Market Insight**. Jurisdiction: EU, Europe. 15 mar. 2017.

VENOSA, Sílvio de Salvo. Direito Civil (Parte Geral). Volume 1. 3ª Edição. Editora Atlas. São Paulo, SP. 2003.

WhatsApp bloqueado: operadoras são intimadas a barrar app no país por 48h. **G1**. São Paulo. 16 dez. 2015. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/12/operadoras-sao-intimadas-bloquear-whatsapp-no-brasil-por-48-horas.html>. Acesso em: 27 maio. 2017.

WILLIAMS, Lee. What is TTIP? And six reasons why the answer should scare you. Comment. **Independent**. 6 out. 2015. Disponível em: <http://www.independent.co.uk/voices/comment/what-is-ttip-and-six-reasons-why-the-answer-should-scare-you-9779688.html>. Acesso em: 28 maio. 2017.