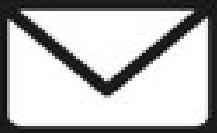
BIG DATA

INTERNET DAS COISAS



TECNOLOGIA E INOVAÇÃO NO DIREITO DIGITAL

DESAFIOS DA PRIVACIDADE E DA PROTEÇÃO DE DADOS

LARISSA KAKIZAKI DE ALCANTARA

Big Data e Internet das Coisas: Desafios da Privacidade e da Proteção de Dados no Direito Digital

Larissa Kakizaki de Alcantara

São Paulo - SP

2017

Aos meus pais, por confiar e apoiar.

Ao Diego, por nunca desistir de mim.
A minha família, por ser única.

Sumário

INTRODUÇÃO

A internet se faz cada vez mais presente no dia a dia de seus usuários, seja como entretenimento, como fonte de trabalho, para estudos. Qualquer que seja sua função é praticamente impossível se ver livre dela. Tornou-se algo deveras importante e ao mesmo tempo perigoso.

Assim, do mesmo modo que ela cresceu pelo mundo a fora, ela adentrou áreas inimagináveis. O Direito Digital surgiu e, diferente do que muitos pensam, não se trata de um ramo autônomo do direito, mas sim uma comunicação com os demais ramos do direito.

A internet, então, avançou em variados níveis desde o seu surgimento. A tecnologia por si só trouxe novos desafios para quem a utilizasse, bem como questionamentos significativos para o Direito.

Questiona-se sobre a privacidade dos usuários, pois é um direito previsto e que deve ser protegido. Não se trata apenas de um princípio, pois se encontra presente na Constituição Federal. Violá-lo, como muito se tem feito por parte de usuários no mundo digital, é algo que acaba por causar danos irreparáveis.

Além disso, é imprescindível frisar a relevância da proteção de dados pessoais. Muitas empresas esquecem o quanto se faz necessário deixar transparente aos usuários o que se fará com esses dados. Desde a coleta dos mesmos – e quais serão os dados coletados –, até o seu uso e armazenamento – bem como o período deste –, são importantes.

Contudo, esses dois questionamentos valem para diversas ramificações do Direito Digital. Tudo que está englobado dentro desta área

deve tomar extrema cautela no que tange à privacidade e à proteção de dados.

Por isso, visando analisar assuntos que estão em alta perante a tecnologia e que é tendência no mundo atual, com a possibilidade de crescer cada vez mais.

O primeiro capítulo tem a intenção de trazer o conceito básico de Big Data e Internet das Coisas. Seus significados, para que servem, o que elas fazem e o que nos trazem hoje em dia, desde suas vantagens até suas desvantagens.

Ambas estão interligadas e se fazem cada vez mais presentes no dia a dia digital. A tendência é cada vez mais termos um volume maior de dados, bem como possuir tudo conectado com a internet. Contudo, por mais benéfico que isso possa soar, nem todos os usuários estão cientes dos desafios e riscos que elas trazem, bem como resolvê-los.

Assim, diante desses dois importantes assuntos, far-se-á necessário uma abordagem quanto à privacidade e à proteção dos dados, sendo este o segundo capítulo, pois como mencionado anteriormente, precisamos de uma análise geral e jurídica destes temas a fim de explicar aos usuários o seu comportamento na rede.

E não só os usuários que fornecem seus dados ou que navegam na internet, mas também as empresas; companhias que coletam dados e se utilizam deste material para impulsionar os próprios negócios e inovar as tecnologias que nós já possuímos.

Os direitos dos cidadãos devem ser preservados, bem como as empresas tem a função de manter transparência e sinceridade a fim de que haja benefício mútuo.

Ademais, para trazer um esclarecimento mais palpável sobre o tema, o terceiro capítulo trará a indispensável comparação com o sistema jurídico dos Estados Unidos, da União Europeia e outros países. Os dois primeiros, de conhecimento de muitos, são mais avançados na parte tecnológica do que o Brasil e, por tal motivo, estão mais bem preparados juridicamente. Já os demais, também trazem a sua preocupação perante a proteção de dados.

Portanto, toda e qualquer informação sobre o assunto torna-se pertinente para o sistema judiciário brasileiro, uma vez que ele pode seguir os mesmos moldes ou adaptá-lo.

Outrossim, é imprescindível se questionar: eles estão seguros ou não? É possível confiar nessa nova tecnologia? O que as empresas tem feito para proteger os dados que nós compartilhamos com eles? Como o judiciário brasileiro pretende lidar com essas questões? Como os outros países estão lidando com esses assuntos de modo jurídico? Como o ordenamento alheio pode ajudar o Brasil a trazer melhorias para o próprio judiciário?

As dúvidas pertinentes ao Direito Digital são inúmeras e, por isso, o presente trabalho visa dirimir tais questionamentos e até mesmo trazer soluções plausíveis para o futuro desta área.

A Internet das Coisas, a Big Data e a Privacidade são a tríade[1] do nosso futuro tecnológico.

CAPÍTULO 1 – BIG DATA E INTERNET DAS COISAS

1. Conceitos e Efeitos

A internet, por mais que já exista há muitos anos, tornou-se a realidade do dia a dia das pessoas em um intervalo de tempo consideravelmente curto. Incorporou-se no nosso meio como algo que, para muitos, beira ao essencial. No entanto, está longe de se assemelhar a falta que faria se estivéssemos sem água, comida ou qualquer outro serviço básico que utilizamos todos os dias.

Porém, quando falamos sobre comunicação, a internet torna-se um serviço essencial e que ainda traz muita discussão juridicamente falando. Isso tudo se dá devido ao crescimento acelerado da internet ao redor do mundo.

A tecnologia avançou e, com ela, veio o crescimento alarmante de informações dos mais diversos tipos.

Patrícia Peck Pinheiro menciona, inclusive, que a informação possui um ciclo de vida, na qual pode ser impactado se não soubermos diferenciar que se faz necessário, ou seja, exige-se a concordância expressa para o uso dos dados, com apenas ser suficiente a ciência; noutras palavras, apenas o mero consentimento.

> “O ciclo de vida da informação envolve, basicamente:
>
> - Coleta – captura da informação e sua inclusão em uma base de dados.
> - Acesso – o mero contato com o dado pessoal individualizado ou banco de dados pessoais, sem necessidade de ter um resultado.
> - Consulta – pesquisa sobre determinada pessoa em banco de dados já formado.
> - Enriquecimento – inclusão de outros dados a respeito de pessoa da qual já se tem algumas informações registradas; inclui a atualização da informação.

- Armazenamento em terceiro – terceirização da atividade de armazenamento e proteção de dados pessoais por ente autorizado. Ex.: fornecedor de *storage*.
- Transferência – compartilhamento de informação entre banco de dados, completo ou parcial da base.
- Remoção – é a exclusão da informação de forma definitiva da base de dados[2]".

Os dados estão em todos os lugares, sejam divulgados por nós através das redes sociais e cadastros que fazemos, sejam dados básicos e públicos, que qualquer um pode ter acesso. E, junto com eles, vem a necessidade de protegê-los, motivo pela qual sua proteção é de suma importância, bem como a privacidade de seus usuários.

Portanto, o avanço tecnológico e o aumento de dados foi algo alarmante e que tende a apenas aumentar ao longo dos anos. Ou seja, há uma espécie de avalanche de dados criada diariamente e, com isso, unidades de medida como o *gigabyte* não são mais suficientes para comportar esses dados. Assim, diante dessa explosão de números e de tudo o que foi exposto, nós temos a *Big Data*.

Cada página acessada, pelo celular, tablet ou computador, envia uma quantidade de informações para quem a requisitou; as coisas mais simples feitas no dia a dia de alguém geram dados. Não se trata apenas de informações produzidas pelas grandes companhias, pois cada usuário tem um perfil e, para melhor complementá-lo, são utilizadas suas ligações, mensagens, cartões de crédito, viagens. E, com isso, tais dados ficam armazenados para serem utilizados, seja como forma de publicidade, para saber os gostos e desejos de seus usuários, seja como forma de melhorar produtos, mapear o trânsito, a medicina, ou qualquer outro serviço existente que possa se utilizar disso.

> "A quantidade de informações digitais é inesgotável: toda interação eletrônica, toda operação bancária e de crédito e cada simples

> assinatura de uma revista ficarão digitalmente gravados e ligados a indivíduos específicos, havendo notável risco de violação do sigilo desses dados para finalidades várias, inclusive ilícitas, ainda que inúmeros usuários da rede não tenham ciência do perigoso rastro que deixam a cada acesso. Tal registro de dados fica armazenado através de cookies, que servem para guardar diversas informações sobre preferências do utente, quando foi realizado o último acesso à página que instalou o respectivo cookie, senha de acesso ao site, entre outras[3]".

O estudo sobre a *Big Data* não é algo de agora. Na verdade, existem inúmeros artigos publicados nos Estados Unidos que mostram o quanto as pessoas estavam preocupadas com o grande crescimento de dados ao passo que a tecnologia tornava-se mais desenvolvida.

Big Data, em tradução literal, significa "grandes dados" e, um de seus grandes desafios, é interpretar esses dados corretamente. Tudo o que nós fazemos deixa um "traço digital" ou "dados", na qual existe a possibilidade de utilizar e analisar.

Além disso, trata-se de um termo que passou por vários significados, sendo o primeiro deles de Doug Laney, os três V's[4]: Volume, velocidade e variedade. São três palavras chaves que trazem a diferença.

Volume, em palavras simples, significa o tanto de dados que é criado todos os dias, sendo que o número tem dobrado a cada 40 (quarenta) meses, mais ou menos[5].

A quantidade de dados que a internet possui por segundo, hoje em dia, é um montante absurdo. E é por isso que várias empresas veem coletando uma quantidade grande de informações, fazendo com que as unidades de medidas, como *gigabyte*, não comportem mais os dados, soando como algo extremamente pequeno – algo que, até ontem, parecia

impossível –, e tornando-se cada vez mais comum ouvir sobre *petabyte*, *exabyte* e outras unidades ainda maiores.

O Presidente Executivo do Google, Eric Schmidt, mencionou o tanto de dados que nós produzíamos antigamente e o quanto nós produzimos hoje:

> "Do início da civilização até 2003, a humanidade gerou cinco *exabytes* de dados. Agora, nós produzimos cinco *exabytes* de dados a cada dois dias e o ritmo está acelerando"[6].

Além do volume, existe a velocidade, o segundo V mencionado. Esta, por sua vez, tem seu significado literal. Trata-se de velocidade em seu tempo real, tornando possível para uma empresa ser mais ágil do que a sua competidora. Portanto, conhecimentos mais rápidos de determinados dados, podem gerar uma vantagem para empresas rivais. Por isso, muitos acreditam que a velocidade é ainda mais importante do que o volume.

Por fim, o terceiro V, conhecido como variedade, na qual nada mais é do que uma possibilidade de locais de onde os dados podem ser recolhidos. Isto é, mensagens, redes sociais, celulares e qualquer outro tipo de fonte que disponibilize informações.

Noutras palavras, de modo resumido, trata-se de tecnologia de armazenamento e, também, de análise de volumes e variedade de dados com uma maior velocidade. Serão coletadas variados tipos de informações com a finalidade de serem analisadas para, posteriormente, serem usufruídas.

Boa parte dessas informações é produzida pelos usuários (consumidores), pois a maior parte, mais da metade inclusive, é gerada pelas empresas. Dados fornecidos pelo *Facebook*, por exemplo, vão desde

pessoas, atividades e localizações, estas, todas ligadas entre si. Elas podem servir inclusive para publicidade, ou seja, é através dele que as empresas descobrem seus gostos e interesses, utilizando-se disso para divulgar o melhor anúncio, cuja atenção do consumidor será captada, fazendo-o clicar na loja e acessar a página.

E esses dados não servem apenas para esse tipo de publicidade, que às vezes soa invasivo demais, como se as empresas conhecessem mais sobre os usuários do que deveriam, a ponto de fornecer o que eles acreditam que seja o requerido, aumentando as vendas em suas empresas. Eles também servem para melhorar o conteúdo de uma empresa, gerando, consequentemente, um aumento na produtividade. Pode ser para planos de saúde, GPS etc.

Como mencionado anteriormente, algumas empresas, inclusive, tem levado esses dados para outro nível, qual seja, em alguns casos, tem as ajudado a tomar decisões em tempo real, aumentando sua vantagem contra os competidores e gerando mais uma utilidade para as informações coletadas.

É o caso, por exemplo, de companhias como Amazon.com, eBay e Google, que vem testando fatores que podem determinar o modo de aumentar as vendas e os envolvimentos dos usuários[7].

Ou seja, a *Big Data* vem sendo utilizada há muito tempo, principalmente por grandes empresas, com o intuito de experimentar novas oportunidades de negócios. Hoje em dia, no entanto, seu conceito já está mais expandido e, consequentemente, a sua função, o seu uso, e o que cada um pode fazer com essa grande quantidade de informações.

Existem, inclusive, mais dois V's[8] que devemos levar em consideração, quais sejam a veracidade, pois muitos dos dados formados pelas redes sociais, por exemplo, com o *Twitter*, vem de informações com erros ortográficos, *hash tags*, abreviações, linguagem coloquial e muitos outros. Portanto, a *Big Data* também nos permite trabalhar com esse tipo de dado, que é cada vez mais comum no dia a dia.

O outro V que também se mostra bastante importante, é o que chamamos de valor. Nem todos os dados coletados são úteis, sendo uma porcentagem muito baixa de dados que tem algum valor e que foram, de fato, analisados quanto a isso.

Ainda, devido a essa grande gama de dados produzida, os aparelhos eletrônicos que possuímos acabam se tornando obsoletos, motivo pela qual estão sempre em constante atualização. Ou seja, quanto mais dados são armazenados, mais a tecnologia tem que acompanhar esse crescimento e nos faz entrar em uma nova era, onde informação digital existe em qualquer tópico relacionado a negócios.

Esta era, inclusive, mostra que o modo como utilizamos a tecnologia, como *Cloud Computing* (Computação em Nuvem)[9], por exemplo, acabam por redistribuir os custos, ou seja, trazem novas formas para os usuários consumirem não só produtos, mas serviços também de um modo mais barato. Tornando-se, então, possível que empresas pensem em novos modelos de negócios.

Ademais, cada um de nós, usuários, estamos produzindo mais e mais dados ao longo dos anos e, ainda por cima, dados poderosos. E esse crescente número de volume de dados, vem trazendo tecnologias de captura e análise de informações com preços mais baixos.

Em resumo, a cada minuto do nosso dia, informações sobre a nossa vida são previstas através da *Big Data*, independente de estarmos cientes disso ou não.

Peter Norvig, diretor de pesquisa do Google, inclusive disse: “Nós não temos melhores algoritmos. Nós temos apenas mais dados[10]”.

E um dos grandes “culpados” pelo aumento absurdo de volumes de dados é devido ao surgimento da tecnologia sem fio e produtos inteligentes. Trata-se do famoso crescimento da Internet das Coisas (IoT) e o mundo digital tende apenas a aumentar durante os anos.

Kevin Ashton, que escreve para RFID *Journal*, é conhecido por ter sido o primeiro a mencionar o “Internet of Things”, noutras palavras, o primeiro a descrever o termo utilizado.

Em um artigo para RFID *Journal*, ele deixou claro, no entanto, que não tinha qualquer controle sobre o termo em questão. Contudo, Kevin Ashton enfatiza algo de suma importância e que muitas pessoas esquecem: “Os computadores de hoje – e, consequentemente, a internet – são quase totalmente dependentes dos humanos para informações[11]”.

Ou seja, para Kevin, a grande questão aqui é não se esquecer de que o nosso meio ambiente é físico e não somos baseados em ideias, mas sim em coisas. Por mais que as ideias e informações sejam importantes, as coisas são ainda mais. Entretanto, a tecnologia de hoje em dia é extremamente dependente dos dados originados pelas pessoas, consequentemente fazendo os computadores saberem mais sobre ideias do que coisas.

Em complemento ao mencionado anteriormente, Ashton diz:

> “Se tivéssemos computadores que sabem tudo sobre o que precisam saber sobre coisas – usando dados que eles reuniram sem qualquer ajuda nossa –, seríamos capazes de rastrear e contar tudo, e reduzir muito o desperdício, perdas e custo. Saberíamos quando as coisas precisariam ser substituídas, reparadas ou revistas, e se estão boas ou já passaram do tempo[12]”.

Noutras palavras, para Kevin Ashton, necessário se faz que os computadores coletem informações eles mesmos, de modo que eles consigam ver o mundo eles próprios, sem a limitação do ser humano de colocar os dados coletados.

O artigo mencionado é de 2009 e, desde então as descobertas frente à Internet das Coisas vem crescendo muito. No entanto, é algo que necessita ser observado sempre, pois o IoT tem o potencial para mudar o mundo se manuseada da maneira correta, do mesmo modo que a internet mudou e ainda traz inúmeras outras mudanças consigo.

A ideia que a Internet das Coisas passa é a de possibilitar, a qualquer tempo e lugar, a comunicação com qualquer coisa. É uma nova tendência e mais um passo muito importante do crescimento da tecnologia.

Segundo a revista Abinee, em uma recente matéria sobre IoT, ela traz uma simples e direta definição sobre o que é internet das coisas: “rede de objetos identificados com endereço IP[13] que se comunicam sem interação humana”.

Ou seja, são objetos conectados que se utilizam da inteligência, da internet, gerando inúmeras possibilidades e oportunidades de negócios nos mais variados setores. O termo utilizado, inclusive, é *machine to machine* ou “M2M”[14], que significa interação entre as máquinas. Elas trocam informações e comandos entre si para que determinada ação seja executada.

A sua evolução é tamanha que estima-se cerca de 30 (trinta) bilhões de dispositivos no universo da Internet das Coisas até 2020[15]". A tendência, porém, é aumentar mais e mais ao longo dos anos. Isso vale tanto para as interações entre as máquinas (M2M), quanto para a grande quantidade de informações que tem sido geradas (Big Data).

Ainda, a revista Abinee reuniu algumas empresas associadas para passar sua visão sobre a Internet das Coisas, bem como o que ela representa ao mercado brasileiro. Assim, a Nokia Solutions apresentou, de maneira resumida, o que é o IoT em sua concepção e quais os seus benefícios:

> "A IoT interconecta e permite a troca de dados de forma autônoma entre as coisas, que podem ser máquinas, mediadores inteligentes, sensores ou objetos de uso diário como produtos consumidos no mercado de varejo ou os *wearables*[16]. As certificações devem ser simplificadas para permitir o baixo custo dos dispositivos[17]".

Uma definição, também de uma das empresas associadas da revista Abinee, na qual integram a Comissão de IoT desta entidade, é a da Intel:

> "Antes de mais nada, a Internet das Coisas é a indústria do conhecimento. Nesse sentido, a tendência natural de seu desenvolvimento passa pela identificação de setores com massa crítica, quer pela existência de conhecimento específico, quer pela magnitude dos impactos esperados com seu emprego. O Brasil apresenta oportunidades únicas em agricultura, educação, telecomunicações, energia, esportes e entretenimento[18]".

Outra definição para a Internet das Coisas, dessa vez da McKinsey&Company é: "Conectar objetos físicos é criar novos modelos de negócios, melhorar processos, e poder reduzir custos e riscos[19]".

Noutras palavras, a Internet das Coisas é muito mais do que aparenta. Está além de cidades, carros, relógios, objetos inteligentes como é

mencionado. O IoT está no centro, tendo como interligações softwares, *wearables*, infraestrutura, tecnologia, “coisas” e segurança[20]. Trata-se de um mercado valiosíssimo, com um crescimento acelerado e que tem previsão de valer trilhões de dólares até 2020.

Ela dá início a um novo padrão entre pessoas e objetos. E, conforme mencionado, não se trata apenas de carros inteligentes, que tem ganhado destaque na mídia pelos mais variados testes atualmente. O IoT traz um novo leque de setores, como a saúde, moradia, transporte, energia, construções, entre outros. E, sim, todos eles levarão a palavra “inteligente” com eles.

Cumpre ressaltar, ainda, que a Internet das Coisas inexiste sem a Big Data, pois elas estão claramente conectadas. Sem a análise dos dados não é possível ter a inteligência, ou seja, não há como ter a conexão dos objetos. Além disso, não há como conectar esses objetos sem usar corretamente as informações coletadas. Portanto, Big Data e IoT andam lado a lado nesse crescimento e, inclusive, trazem os mesmos tipos de desafios para a sociedade.

Com o crescimento da Internet das Coisas, foi criada uma espécie de “revista em quadrinhos” na Comunidade Europeia. O intuito era uma melhor didática, uma linguagem mais fácil para explicar o que é do que se trata o IoT, bem como motivar um público muito maior para questões que possuem um grande impacto social.

Em virtude disso, o Fórum de Competitividade de IoT – Brasil, em 2012, conseguiu permissão para trazer a versão brasileira desses quadrinhos com o apoio do Instituto de Tecnologia de Software e Serviços (ITS), também participante do fórum. O “gibi” conta com textos, imagens e vídeos através de uma leitura dinâmica e prática.

> “Quando os objetos podem sentir o ambiente e se comunicar, eles se tornam **ferramentas poderosas para entender coisas complexas e responder a elas com eficiência.** Embora tais objetos inteligentes possam interagir com humanos, é mais provável que interajam ainda mais entre si automaticamente, sem intervenção humana atualizando-se com as tarefas do dia[21]”. (grifo nosso)

Para Ovidiu Vermesan, o IoT tem um objetivo muito óbvio e bem direto: “O propósito da Internet das Coisas é melhorar a vida[22]”.

Ou seja, seu intuito é, de fato, trazer melhorias para todos os indivíduos e usuários da tecnologia, que cada vez mais cresce e se mostra deveras importante em nosso dia a dia.

Ovidiu ainda complementa:

> “Em nossa pesquisa, estamos focando nestas questões ao instituir que os dispositivos devem dar suporte a padrões comuns de **privacidade, segurança e confiabilidade** desde o design. Além disso, com os dispositivos sendo independentes de interação humana, também temos que lidar com a questão da responsabilidade. Alguns dispositivos serão de propriedade pública, outros, privada. Se um mau comportamento é detectado, precisamos saber quem é o responsável[23]”. (grifo nosso).

E é exatamente aí que entram os problemas, pois, por mais benéfico que possa ser ter a Big Data e a Internet das Coisas, há os desafios e as problemáticas, anteriormente citados, que precisam ser enfrentados pela sociedade a fim de se manter conectado.

2. Desafios e Problemáticas

É estimado que a Internet das Coisas trará um *boom* muito grande, onde a quantidade de dispositivos conectados a internet irá crescer cerca de 13 (treze) bilhões hoje em dia para 50 (cinquenta) bilhões até 2020. Além disso, a indústria do Big Data possui uma expectativa de crescimento de aproximadamente dez bilhões de dólares em 2013 para cerca de cinquenta e quatro bilhões de dólares em 2017[24].

Ela nada mais é do que a próxima revolução tecnológica, gerando cada vez mais dados e o impacto que ela trará será sentido por todo o universo da Big Data, fazendo com que empresas precisem melhorar suas ferramentas atuais e tecnologia a fim de que todo o volume de dados gerado seja acomodado.

A proteção de Dados e a Privacidade do usuário são duas questões de suma importância que devem ser abordadas com muito cuidado. Trata-se de dois dos principais desafios que a Big Data e a Internet das Coisas enfrentam no cenário atual.

E é por esse motivo que o ordenamento jurídico brasileiro precisa usar suas Leis e tudo que está ao seu alcance para, do modo mais correto e permissível, proteger seus usuários na internet, visto que a Big Data e a Internet das Coisas trazem grandes vulnerabilidades que precisam ser sanadas.

O professor Marcel Leonardi cita, em sua obra Tutela e Privacidade na Internet, o seguinte trecho: “O Poder Judiciário sente-se questionado pela evolução tecnológica[25]”. Aqui, é possível notar a dificuldade que o nosso ordenamento tem para com a tecnologia e o direito.

Portanto, a dificuldade encontra-se em oferecer a solução para um problema que, embora tenhamos a privacidade e a intimidade como direitos fundamentais presentes na Declaração Universal dos Direitos Humanos, na Constituição Federal e, também, no Marco Civil da Internet, bem como referência a Proteção de Dados, ainda encontra-se muito em aberto.

Na edição de junho de 2016 da Revista Abinee nº 86, ela traz uma matéria especial sobre IoT.

> "Um mercado de dezenas de bilhões de dólares. Atento ao enorme potencial da Internet das Coisas no Brasil, o governo elabora o Plano Nacional de IoT e propõe um amplo debate com diversos setores da economia. À frente da Secretaria de Inclusão e Internet do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC)[26]".

Maximiliano Martinhão fala sobre as políticas públicas voltadas às novas tecnologias no Brasil e, com isso, responde a duas perguntas importantes sobre privacidade e proteção. A primeira delas é:

> "Diante da complexidade e abrangência deste tema, quais os desafios para a modernização da legislação atual, inclusive a relacionada à P&D, para atender às necessidades futuras de IoT? Um dos desafios será permitir e estimular, de forma organizada, a ampla qualidade de serviços que surgirão com a Internet das Coisas, sem deixar de proporcionar qualidade, confiabilidade e segurança à sua utilização. Temas como Segurança e Privacidade de Dados, uso de base de dados coletadas para tomadas de decisões, *analitics*, entre outros, surgirão com essa nova realidade. O Estado sempre deverá estar atento para que a legislação continue possibilitando o surgimento de novos mercados, com responsabilidade, mas ao mesmo tempo sem inviabilizá-los. Ademais, há o desafio de estimular cada vez mais P&D compartilhado entre empresas e em parcerias público-privado (PPPs), além de ampliar a utilização de instrumentos de fomento, como, por exemplo, chamadas públicas conjuntas internacionais[27]".

Diante do exposto, é notado o quanto a legislação que nós possuímos precisa se adaptar a nova tecnologia. Com o surgimento do Marco Civil da Internet e outras Leis, bem como da própria Constituição Federal, necessário será ficar atento ao que eles trazem a fim de não violá-las. As empresas precisam estar cientes do que elas podem e devem fazer, bem como os usuários tem direito de transparência com tudo aquilo que firmarem.

A privacidade e a proteção de dados pessoais são tópicos sensíveis e que afetam não só os usuários, mas todos os que estão envolvidos com essa nova tecnologia. Ou seja, o impacto é em absolutamente tudo que tem relação com a internet.

Ao redor do mundo existem mais de 100 países com legislação voltada a tutela da privacidade no país. Foram inspiradas no modelo de regulamentação que se iniciou na Europa, o mesmo modelo que inspira o Brasil.

E, embora o Brasil esteja atrasado face a essa regulamentação, já há caminhos a serem seguidos, como o Marco Civil da Internet, a própria Constituição Federal, o Código de Defesa do Consumidor e, principalmente, o Anteprojeto de Lei de Proteção de Dados Pessoais.

O InternetLab[28], inclusive, acompanhou o processo de consulta pública, publicando um relatório com tudo que estava sendo discutido. Ainda, eles afirmam que se trata de um tema complexo, na qual diversos grupos interessados ainda discutem sobre os pontos sensíveis deste Anteprojeto.

Ainda, a fim de reforçar a importância da discussão do Projeto de Lei de Proteção de Dados, o InternetLab lançou uma semana especial[29]

para o assunto em questão, abordando 5 (cinco) temas centrais da Lei mencionada.

Em um dos temas, o especial sobre “Big Data: quais proteções os titulares de dados têm a sua disposição?”, foi levantado um questionamento relevante referente a Lei, um dos principais pontos de discussão atualmente.

Ademais, a outra pergunta refere-se ao posicionamento do governo frente a um dos maiores desafios que precisamos enfrentar, relacionado à como atuar para garantir segurança da informação, tratamento e privacidade de dados.

> “Queremos abrir um debate amplo com os diversos setores para dar o tratamento adequado a essas questões. Isso é relevante para preservar o equilíbrio entre a segurança, a privacidade de dados e o surgimento de novas soluções e ampliação do mercado[30]”.

Noutras palavras, trata-se de um desafio que não envolve apenas uma área, mas todas as que se envolvem com a tecnologia, que estão lidando com o crescimento constante da Big Data e da Internet das Coisas. E, por isso, o Direito Digital e suas Leis precisam se mostrar presentes, de modo a trazer regras perante um tema tão importante.

CAPÍTULO 2 – PRIVACIDADE E PROTEÇÃO DE DADOS

2.1. O que é e a sua importância

Com o advento da tecnologia, qualquer mínima informação fornecida pode ser utilizada e, consequentemente, sua privacidade violada. Os usuários da internet esquecem que, não só existe lei no mundo digital, mas que os direitos previstos aos seres humanos também se aplicam ao navegarmos na internet.

Tornou-se difícil proteger a privacidade do cidadão com as mudanças tecnológicas. Contudo, é de suma importância lembrar que o direito à privacidade está presente na Declaração Universal de Direitos Humanos de 1948 e na Constituição Federal de 1988, sendo extremamente importante dentro e fora das redes. Ou seja, o amparo legal existe e precisa ser respeitado.

O conceito de privacidade de acordo com o artigo 12 da Declaração Universal de Direitos Humanos é: “Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques”.

Além disso, como já mencionado, é um direito protegido pela Magna Carta, portanto, um direito de todo cidadão e encontra-se no artigo 5º, inciso X.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
>
> 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;

Vejamos que a preocupação frente ao direito à privacidade não é algo que vem de hoje. Ainda, é possível perceber que a Constituição Federal dividiu o direito à privacidade em: imagem, dados, informações; domicílio; comunicações.

De maneira geral, trata-se do quanto sua vida privada é, de fato, pessoal e ninguém tem o direito de invadi-la ou denegri-la. E seria relativamente simples, considerando que correspondências não podem ser violadas, informações sem o seu consentimento não podem ser divulgadas e, exceto os dados públicos, nada poderia ser exposto sem a sua vontade.

Entretanto, com os sites de compras na internet, cadastros, redes sociais, a coleta de dados tornou-se comum. Os usuários inseriam tudo que lhes era pedido, sequer se importavam em ler os termos de uso antes de cada aceite; e com o crescimento da Big Data, a coleta de dados ficou ainda maior.

Portanto, cada mínima informação que o usuário já se prestou a colocar na internet está ali, disponível para que as empresas e qualquer um possam acessar. Uma invasão de privacidade que todos que navegam

permitem que sejam coletados; cada clique, cada procura, tudo isso deixa algum rastro.

Para melhor elucidar essa questão, há um caso famoso que demonstra como um simples acesso pode gerar uma grande confusão.

A Target, uma empresa especializada em vendas *on-line* e *off-line*, descobriu através de registros eletrônicos e pelo hábito de navegação da pessoa, junto com outras informações coletadas que permitiu formar um tipo de perfil específico. Este perfil possibilitou que a loja descobrisse a gravidez da usuária através dos dados fornecidos.

Com isso, na época, a empresa Target enviou cupons de desconto em produtos para gravidez para a usuária e quem acabou por recebê-los foi o pai da cliente. Inconformado com aquela atitude um tanto invasiva por parte de uma loja que, na sua concepção, não teria como saber uma informação tão íntima, o progenitor foi até uma das lojas questionar o motivo de estarem enviando aquele tipo de cupom a sua filha, menor de idade, que não estava grávida.

No entanto, ao confrontar sua filha, o pai acabou por descobrir que a loja estava correta em sua afirmação, pois de fato ela estava grávida.

O que a empresa Target fez foi aprofundar sua pesquisa, ou seja, ela investiu no famoso *marketing* digital. Especialistas dessa área tinham o desafio de, não só acessar os registros eletrônicos da própria empresa, mas também os que eram coletados por parceiros de propaganda e informações pessoais, tais como localização geográfica, hábitos pessoais e históricos de empregos, toda e qualquer informação que soasse pertinente, mesmo que sozinho não aparentasse relevante, mas que combinado com os dados corretos podem levar a conclusões valiosas.

Assim, foi possível que a empresa identificasse diversos produtos que, combinado com os dados disponíveis, permitiu atribuir aos seus clientes a “possibilidade de gravidez” e, ainda, lhes permitia estimar a data em que a criança viria a nascer. Ou seja, não era algo certo, mas sim uma probabilidade muito grande de que as clientes na qual eles enviassem os cupons estivessem, de fato, grávidas.

O caso dessa cliente cujo pai descobriu a gravidez através dos cupons enviados pela empresa tornou-se famoso. A esse tipo de metodologia dá-se o nome de *profiling*[31] através do universo de dados chamado Big Data. Portanto, temos aqui, mais uma vez, o quão grande é esse universo e o quanto ele desafia a privacidade e proteção dos usuários na internet.

A explosão de tecnologia acabou por fazer as empresas captarem grandes quantidades de informações sobre seus usuários, tanto *on-line* quanto *off-line*. O que a empresa Target fez é utilizado por várias outras empresas, sempre no intuito de melhorar algo em seu próprio mercado.

Contudo, é válido lembrar que nem toda empresa é transparente quanto aos dados coletados ou a sua permissão. Por isso, é de suma importância à leitura minuciosa dos termos de uso de cada rede social, aplicativo, site de compra e venda, entre outros, que o usuário possa vir a querer utilizar. Apenas colocar que aceita, sem ler, pode significar que você está dando completa liberdade para que aquela empresa faça o que bem entender com os seus dados pessoais.

A privacidade é algo que deve ser preservada, não só por quem fornece os serviços, mas também por quem oferece os dados. Divulgar toda e qualquer informação na internet é algo que, futuramente, podem trazer problemas, sejam eles de cunho pessoal, como em emprego promissor, ou

algum crime previsto no nosso ordenamento jurídico. O que nós postamos na internet nos molda como cidadãos frequentando esse mundo virtual; trata-se do que somos.

Dados sensíveis são coletados e a grande maioria das empresas utiliza-se do modelo de negócio que requer a monetização de dados dos seus usuários.

E é aqui que, além da privacidade, entra também a proteção de dados. A coleta desses dados que, em sua grande maioria, são pessoais, acontece em demasia, principalmente por ser um modelo de negócio necessário pelas empresas.

Renato Leite Monteiro menciona:

> "Uma vez que a receita das empresas se origina principalmente da publicidade oferecida através de seus usuários, caso estas empresas não coletassem dados, elas simplesmente não existiriam. Podemos, portanto, partir de uma premissa: com regulamentação estatal ou não, dados continuarão a ser coletados e armazenados, pois o atual modelo de negócio das empresas de Internet depende dessa prática[32]".

Com isso, é possível perceber o quão importante torna-se a proteção de dados pessoais, pois, em sua grande maioria, são estes os coletados pelas empresas e, ainda, mostra o quão importante essa coleta é para elas, pois do contrário sequer existiriam.

A publicidade é algo que está presente no nosso dia a dia. Inúmeras são as propagandas que aparecerem ao redor de uma página que estamos navegando, ou nas redes sociais que utilizamos. Anúncios esses que indicam exatamente os nossos interesses, uma vez que qualquer que seja o clique que nós fazemos em uma página, acaba gerando a informação de ser algo de nossa procura.

Empresas aumentam sua produtividade, seu lucro e suas pesquisas através dos cliques que os usuários dão em seus anúncios. Eles são de suma importância, pois chamam a atenção de clientes em potencial e de clientes antigos; permitem, inclusive, que a empresa esteja sempre atualizando aquele cadastro, com informações sobre gostos antigos ou novos.

Ainda, ele complementa:

> "Outra premissa deve também ser posta: não é o fato da coleta de dados ser necessária para manter o modelo de negócios que fomenta a Internet que devemos deixar o método de coleta, tratamento e armazenamento para a autorregulação. Isso se dá por dois motivos: uma vez que dados pessoais e sensíveis podem ser coletados, a colheita demasiada e o tratamento indevido pode violar ferozmente a privacidade e a intimidade dos usuários[33]".

Assim, o nosso comportamento não é analisado apenas pelas empresas, mas por todo mundo que tem acesso aos nossos dados. Isso apenas reforça a ideia mencionada anteriormente, na qual, além de crimes por meios eletrônicos que podem e são cometidos contra os usuários, há também a sua reputação nesse mundo digital. A dependência que criamos da internet deveria nos fazer pensar no quanto é importante resguardarmos nossa identidade; e, por esse motivo, os dados devem ser protegidos e as normas para isso precisam ser claras e transparentes.

Por se tratar de tema de importante relevância, a privacidade e proteção de dados pessoais ganhou forte destaque no Marco Civil da Internet. A Lei foi objeto de consulta pública e sofreu várias alterações a fim de corrigir imprecisões e adequar-se aos interesses necessários.

Para Patrícia Peck Pinheiro, advogada especialista em Direito Digital, o Marco Civil é: "uma *lei* que veio para proteger mais a *privacidade* e a *liberdade do internauta*[34]".

Assim, no texto final da Lei 12.965/14, o artigo 3º traz:

> “Art. 3.º A disciplina do uso da Internet no Brasil tem os seguintes princípios:
>
> (...)
>
> II – proteção da privacidade;
>
> III – proteção de dados pessoais, na forma da lei;
>
> (...)”.

Com esse artigo, podemos notar que, conforme Danilo Doneda defende, a privacidade e a proteção de dados possuem conceitos diversos. Ou seja, o fato de ambas serem elencadas separadamente, demonstra que cada uma possui seu próprio conceito, mesmo que possuam ligação.

Ademais, Renato Monteiro Leite enfatiza “o inciso III acrescenta, ainda, que a proteção de dados pessoais se dará na forma da lei, abrindo espaço para futura elaboração e promulgação de lei específica, nos moldes do que já vem sendo discutido[35]”.

Houve, inclusive, debate público referente aos dados pessoais entre 2010 e 2011, com intuito de acender comentários acerca do tema e da proposta do Projeto de Lei. Cumpre ressaltar, então, que hoje tramita o Projeto de Lei 4060/2012[36], que dispõe sobre o tratamento de dados pessoais.

A importância da participação do público acerca desses temas é muito grande, visto que todos nós estamos suscetíveis a ter nossa privacidade violada. Em 2013, o assunto tornou-se uma pauta ainda maior quando esta violação atingiu a Presidência da República, mostrando que ninguém estava, de fato, seguro.

Como mencionado anteriormente, o InternetLab fez uma semana especial sobre Proteção de Dados e um dos temas de importância foi sobre Big Data e quais proteções os titulares de dados têm a sua disposição[37]. Com isso, ela buscou entender as diferentes perspectivas de cada setor a respeito da proteção de dados pessoais no nosso país.

A principal pergunta foi:

> "O PL 5.276 garante uma série de direitos ao titular dos dados pessoais, como portabilidade e eliminação, a qualquer momento, dos dados pessoais coletados. Considerando que, muitas vezes, o tratamento de dados pessoais envolve terceiros, em uma complexa cadeia de atores, garantir a eficácia desses direitos na prática pode ser uma tarefa desafiadora. Além disso, a lei confere ao titular a possibilidade de solicitar revisão de decisões tomadas com base no tratamento automatizado de seus dados pessoais. Como se sabe, muitas dessas decisões são tomadas por algoritmos. Como avalia o rol de direitos elencados pela lei? Acredita que será possível exercitá-los na prática?[38]"

De acordo com Veridiana Alimonti, da Intervozes, os direitos elencados pelo Projeto de Lei trarão mais informações e controle sobre como os dados pessoais estão sendo coletados e tratados, conferindo a possibilidade maior sobre onde manter esses dados e por qual período de tempo.

Ainda, ela enfatiza a importância que a nova legislação traga modos de consentimentos alternativos e simples, mas que sejam completos, transparentes e efetivos. Além, é claro, do incentivo ao desenvolvimento de ferramentas que visem a proteção à privacidade como padrão, de modo que a coleta de dados seja feita de acordo com o que interessa no produto ou serviço, e colocando de lado a prática dos "8 ou 80", ou seja, de que ou se aceita tudo ou não se aceita nada.

Frisou, também, o quão importante é a fiscalização do cumprimento de princípios e direitos.

Já Marcel Leonardi, Diretor de Políticas Públicas do Google do Brasil, também deu sua vertente, dizendo que: “os direitos assegurados ao titular são bastante amplos, refletindo em boa parte o modelo europeu de proteção de dados”.

Menciona, então, a essencialidade de uma autoridade de proteção de dados independente e que seja capaz de aplicar e interpretar a lei de maneira equilibrada. Além de as empresas precisarem considerar as diversificadas preocupações que seus clientes possuem quanto à privacidade, sempre mantendo transparência a clareza no que elas têm a oferecer. Ainda, elas devem seguir práticas claras para que o titular possa fazer suas próprias escolhas.

O InternetLab também conversou com Vanessa Butalla, do Serasa Experian, que acredita ser necessário buscar harmonia entre os direitos e obrigações que decorram da atividade empresarial que é exercida pelos responsáveis ao tratamento de dados pessoais.

E, por último, tratou do assunto com a Doutora Laura Schrtel Mendes, do Instituto Brasiliense de Direito Público (IDP), que menciona:

> “O direito de não se ficar sujeito a uma decisão individual automatizada consiste no direito do cidadão de não ficar submetido a decisões que influenciem significativamente a sua posição jurídica, tomadas exclusivamente com base no tratamento automatizado de dados”.

Menciona, também, a semelhança com a Diretiva Europeia 95/46/CE de proteção de dados, mostrando, novamente, que o Projeto de Lei se baseou em algo que a Europa vem estudado há mais tempo.

Assim, demonstrando a importância do Projeto de Lei de Proteção de dados, bem como do Marco Civil da Internet, fazemos a análise de mais um artigo, que tem como objetivo assegurar os direitos de seus usuários da internet:

> "Art. 7.º O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II – inviolabilidade e sigilo do fluxo de suas comunicações pela Internet, salvo por ordem judicial, na forma da lei;
>
> III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
>
> (...)".

O primeiro inciso mostra, novamente, a importância da privacidade em relação à sua vida privada e à proteção de dados, bem como uma sanção para caso haja essa violação. O referido artigo, ainda, faz menção da proteção de dados armazenados, ou seja, daqueles que ficam guardados e não somente dos que estão em trânsito.

> "Art. 7.º (...)
>
> VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicação de Internet, bem como sobre práticas de gerenciamento da rede que possa afetar sua qualidade;
>
> (...)
>
> XIII – aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na Internet".

Ainda, o inciso IV, traz a regulamentação referente à privacidade dos serviços prestados na internet, ou seja, necessário se faz informações

claras quanto à proteção de dados dos usuários, bem como o seu gerenciamento. Trata-se de uma precaução quanto aos contratos de prestação de serviços que, conforme podemos ver no inciso XIII, estão em consonância com a proteção e defesa do consumidor face às relações de consumo realizadas na internet.

Inclusive, o Código de Defesa do Consumidor já trazia em um de seus artigos o fato de que o consumidor deve ser informado toda vez que seus dados forem inseridos em uma base de dados consumerista. Porém, não faz menção quanto a sua distribuição para terceiros. Contudo, o Marco Civil da Internet traz novamente, eu seu artigo 7º, uma mudança:

> "Art. 7.º (...)
>
> VII – **não fornecimento de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet**, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) Justifiquem sua coleta;
> b) Não sejam vedadas pela legislação; e
> c) Estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais". (grifo nosso)

Pode-se interpretar, portanto, que de acordo com a Lei mencionada, o fornecimento de dados pessoais de usuários a terceiros é possível, contudo, deve-se ter consentimento livre, expresso e informado da pessoa em questão. Ele traz o consentimento prévio.

Inicialmente mencionado no artigo 3º da Lei supracitada, é possível notar que sequer há uma definição para a expressão. No entanto, o artigo 7º, inciso VII, traz uma separação entre “dados pessoais” e “dados de conexão”, trazendo mais dificuldade para o que, de fato, venha a significar dados pessoais.

O artigo 10 da presente Lei, inclusive reforça essa ideia de diferentes tipos de dados, senão vejamos:

> “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”. (grifo nosso)

Mas, afinal, o que são “dados pessoais”?

De acordo com o professor Renato Monteiro Leite[39], ao fazer a separação entre “registros de conexão” e “acesso a aplicações de internet”, acabou por determinar que: “endereços IP, mesmo sendo informação relacionada à pessoa natural identificável, não seria um dado pessoal”.

E tal informação se dá pelo simples fato de que essa distinção diverge do que está presente a Lei de Acesso a Informação, Lei 12.527/2011, em seu artigo 4º, IV, na qual conta com o conceito de informação pessoal: “aquela relacionada à pessoa natural identificada ou identificável”.

Ainda de acordo com o professor, essa interpretação está de acordo com o Anteprojeto de Lei Brasileiro de Proteção de Dados pessoais, na qual traz o conceito de dados pessoais em um de seus artigos.

> “Art. 4.º Para os fins da presente lei, entende-se como:

> I – dado pessoal: qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores;”

Portanto, com essa separação, acabou por gerar uma limitação no que tange à proteção aos direitos e garantias dos usuários.

Ademais, referente ao artigo 10 anteriormente mencionado, vemos que seu texto reafirma os princípios existentes no artigo 3º e, também, do que está disposto na Constituição Federal e no Código Civil. E, ainda, em seu § 1º, traz:

> “Art. 10. (...)
>
> § 1.º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7.º”.

Ao analisar tal parágrafo, dá-se a entender que nos casos especificados no *caput*, é quando o provedor responsável poderia fornecer os registros, bem como os dados pessoais e, se por acaso se negasse, somente então seria obrigado a fornecê-los mediante ordem judicial. Noutras palavras, em uma leitura apenas do referido parágrafo, tal interpretação é completamente possível e pode gerar problemas futuramente, principalmente no que tange à privacidade.

Com isso, o professor Renato Monteiro Leite acredita que tal redação poderia ter sido melhor elaborada.

> “**Sua interpretação isolada pode resultar em consequências desfavoráveis, como o fornecimento de registros sem ordem judicial**. Além disso, o Marco Civil não conceitua “provedor”,

> interpretação que pode ser diferente do rol elencado no art. 5.º. Seria, *e.g.*, um café que fornece Internet sem fio de graça para seus cliente um provedor de acesso, um mero proxy ou um servidor de aplicações?[40]" (grifo nosso)

É possível perceber que o Marco Civil, apesar de abordar assuntos de suma importância, comete erros em sua redação, o que pode gerar interpretações desfavoráveis e, consequentemente, atrapalhar não só as empresas que guardam esses dados, mas também os seus usuários.

Todavia, a presente Lei também trata de reforçar a ideia passada nos artigos 3.º e 7.º referente ao conteúdo de mensagens, sejam elas em fluxo ou não, especificando sua proteção:

> "§ 2.º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7.º."

O Marco Civil da Internet, então, assegura a privacidade do usuário, mesmo que ainda haja algumas falhas, em relação ao tratamento de dados pessoais e quanto à inviolabilidade e sigilo das comunicações. E, por isso, ela não traz apenas direitos como mencionado anteriormente, mas também traz deveres.

> "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 01 (um) ano, nos termos do regulamento."
>
> "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 06 (seis) meses, nos termos do regulamento."

Mais uma vez a Lei nº 12.965/14 mostra a importância da privacidade quando impõe que os registros de conexão – cuja definição encontra-se no artigo 5º, VI[41] da mesma Lei – devem se manter sigilosos, sob controle e com segurança, pelo prazo de 01 (um) ano. Ainda, impõe aos provedores de aplicação[42] o dever de guardar por 06 (seis) meses os registros de acesso a aplicações de Internet[43].

Contudo, ainda traz implicações negativas em relação à privacidade, como dito pelo professor Marcel Leonardi:

> "Lamentavelmente, o Marco Civil da Internet impôs um modelo de guarda obrigatória de dados para os provedores de aplicações, e não *facultativa*, como originalmente previsto. Adotou, assim, um modelo único de ***retenção de dados*** de forma indiscriminada, em oposição a um modelo de preservação dos dados efetivamente ligados a um ato ilícito praticado, o que implica tratar todos os usuários de Internet como suspeitos da prática de atos ilícitos, com sérias implicações para a sua privacidade.
>
> Como mencionado, em sua versão original o Marco Civil da Internet privilegiava o modelo de *preservação de dados*, impondo a provedores de conexão e de aplicações que recebem uma ordem judicial o dever de preservar, *a partir daquele momento*, dados específicos de usuários determinados, suspeitos de terem praticado crimes ou ato ilícitos por meio da Internet. Todos os demais usuários do provedor não seriam afetados.
>
> Insista-se, portanto, que para a proteção da privacidade do usuário **o modelo de preservação de dados é mais adequado**. Isso porque, nesse modelo, a guarda de registros apenas é realizada a partir do momento em que há uma denúncia ou se constata uma suspeita da ocorrência de crime ou de prática de ato ilícito, iniciando-se então o processo para os direitos dos demais usuários de um determinado serviço. Com isso, torna-se possível combater ilícitos e crimes online sem violar normas constitucionais nem afetar direitos fundamentais dos cidadãos, atendendo assim ao necessário sopesamento entre princípios e à regra da proporcionalidade.[44]"

E isso se dá ao fato de que a Diretiva Europeia 2006/24/CE[45] rejeitou esse modelo alegando que a retenção de dados violava a privacidade do cidadão. No entanto, tal Diretiva foi declarada inválida em

2014, referente à “conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações[46]”.

Porém, como mencionado no artigo 10 do Marco Civil da Internet, o sigilo face aos registros de conexão e de acesso de seus usuários é imposto aos provedores, excetuando casos em que um ato ilício é cometido por meio da Internet. Nessas situações, o sigilo pode ser quebrado mediante ordem judicial específica, conforme citado anteriormente.

Inclusive, o artigo 22[47] da mesma Lei, traz a intervenção obrigatória do Poder Judiciário no caso de revelações de informações dos usuários da Internet. E, seguindo o artigo 23[48], cabe ao juiz tomar as providências necessárias para garantir o sigilo das informações recebidas, bem como à preservação da intimidade, vida privada, honra e imagem deste usuário.

E em se tratando de Internet das Coisas, reguladores referentes à proteção de dados chegaram à conclusão de que a data gerada por dispositivos no IoT devem ser tratadas como dados pessoais[49]. Esse acordo foi regulado em uma Conferência Privada Internacional através de uma declaração pública.

Como mencionado anteriormente, a Big Data e a Internet das Coisas andam juntas. Isso se dá ao fato de que as empresas enfrentam grandes desafios para extrair dados do IoT, na qual requer uma infraestrutura própria para poder analisar essas informações. Ressaltando, ainda, há um grande volume de dados gerados por esses dispositivos, porém nem todos são importantes, o que torna ainda mais complicado para essas companhias.

Empresas precisam ter em mente que é necessário adaptar a tecnologia que elas possuem para alcançar os dados do IoT. A internet, os computadores, tudo terá impacto e deverá ser planejado para cuidar desse novo tipo de informação fornecido.

Conforme a Internet das Coisas cresce, os negócios com o IoT também aumentam e, consequentemente, mais desafios aparecerão. Portanto, importante se faz analisar cuidadosamente a Big Data e a Internet das Coisas, a fim de que a tecnologia que cada vez mais se expande, não fuja de controle.

E, enfatizando o quanto o IoT irá revolucionar o Direito Digital e a relevância de legislações que tratem o tema a fim de conferir segurança jurídica adequada tanto as empresas quanto aos seus usuários/cosumidores, os advogados Luis Fernando Prado Chaves e Maria Cecilia Oliveira Gomes exprimem:

> "Esse novo ramo do direito, multidisciplinar e totalmente dinâmico, sofrerá provavelmente uma de suas grandes revoluções à medida em que a IoT for, de fato, uma realidade de Norte a Sul do País. Atualmente, temos sólida regulamentação dos serviços de conexão e aplicação da Internet, mas fato é que a IoT não abrange apenas tais serviços. Trata-se, na verdade, de ecossistema tecnológico de extrema complexidade, o qual, certamente, ensejará novos desafios jurídicos na medida em que for implementado.
>
> Nesse sentido, **especial destaque deve ser feito à questão da privacidade**, considerando que muitos dispositivos eletrônicos que fazem ou farão parte do ecossistema de IoT têm como característica intrínseca a coleta e tratamento massivo de dados, o que, muitas vezes, pode envolver o armazenamento e compartilhamento de dados pessoais (até mesmo de dados sensíveis).
>
> Quanto a esse tema, cumpre ressaltar que ainda não existe no Brasil uma Lei Geral de Proteção de Dados Pessoais, mas apenas legislações infraconstitucionais, **as quais não são suficientes para conferir adequada segurança jurídica a empresas e usuários/consumidores com relação ao tratamento de dados no âmbito das novas tecnologias, como a de IoT**. Hoje, tramitam no Congresso, pelo menos, 3 (três) relevantes Projetos de Lei sobre Proteção de Dados Pessoais (PL 4.060/2012, PL 5.276/2016, PLS

> 330/2013), os quais ainda estão sendo objeto de estudo e debate[50]" (grifo nosso).

Diante de tudo exposto, uma das principais perguntas é: o que as empresas e o Governo tem feito para proteger a privacidade e os dados pessoais diante do crescimento da Big Data e da Internet das Coisas?

2.2. Casos famosos

A necessidade da Proteção de Dados e o Direito à Privacidade não se tratam apenas de informações pessoais que podem vir a vazar, ou por determinada empresa ter todos os dados referentes ao seu trabalho divulgado a concorrência, mas também por existir a má intenção de algumas pessoas; muitas vezes desejando apenas se beneficiar financeiramente com o caso.

Uma das tendências de 2016 foi o famoso ataque por *ransomware*[51]. Visam dinheiro fácil e de maneira rápida. Trata-se de um tipo de *malware* que pode ser instalado nos computadores quando o usuário recebe um e-mail e acaba por clicar em links direcionados a sites mal intencionados, anexos infectados ou até mesmo downloads e atualizações de software.

Através de uma criptografia, a pessoa que enviou o *malware* impede que o usuário acesse seus arquivos, sejam eles armazenados em seu computador ou celular, e até mesmo na própria nuvem; sequer o *backup* é poupado. Assim, o fraudador exige pagamento de uma quantia em troca da liberação dos dados capturados.

O desbloqueio dos dados se dá através de uma chave privada que é entregue após efetuação do pagamento ao fraudador. Ainda, há a informação de que os dados serão apagados em aproximadamente 72 (setenta e duas) horas, além de outros detalhes.

O pagamento, no entanto, não é feito através da moeda corrente no país e sim através da famosa *bitcoin*, uma criptomoeda, noutras palavras, uma moeda virtual.

No nosso ordenamento jurídico este tipo de ataque consta tipificado no Código Penal, no artigo 154-A, § 1º. Inclusive, por haver um pedido de "resgate" após o ataque, este se encontra vinculado ao crime de extorsão previsto no artigo 158 do mesmo diploma.

Porém, a dúvida maior é se o correto é pagar ou não a quantia solicitada. De acordo com o FBI (Federal Bureau of Investigation)[52] a melhor opção é entregar o dinheiro requerido. Ademais, em alguns casos, os usuários que possuíram seus dados bloqueados preferem pagar devido a grande demora em recuperá-los. Noutras palavras, entregar o montante solicitado acaba sendo mais rápido e satisfativo do que a espera pelo desbloqueio.

Contudo, pagar os valores nem sempre significa que os dados serão obtidos de volta. Portanto, embora pareça uma solução mais rápida devido ao desespero de querer obter novamente seus dados, é válido lembrar que esta deve ser a última opção.

E é exatamente pela possibilidade de, não só de perder dinheiro, mas ainda assim ter suas informações expostas, que todas as empresas devem se lembrar da importância da proteção de dados que estão sob sua responsabilidade. É obrigação dessas empresas privadas e da administração pública protege-los e, ainda, mantê-los sigilosos. Isso se encontra elencado no artigo 5º, XII, da Constituição Federal já mencionado.

Ademais, a Lei 12.527/2011 dispõe no artigo 6º, inciso III:

> "Art. 6.º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a: (...)
>
> III – proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso."

Ou seja, é de suma importância a obrigação de proteger os dados pessoais que estão de responsabilidade da dita empresa ou órgão público. Esses ataques são mais comuns do que as pessoas imaginam, principalmente para grandes empresas que possuem uma quantidade significativa de dados coletados.

Para melhor demonstrar a problemática referente à proteção de dados, existe um caso famoso mundialmente, o caso de Edward Snowden.

Trata-se de um analista de sistemas, ex-administrador de sistemas da CIA e ex-contratado dos EUA, na qual divulgou informações secretas da NSA[53] em 2013 sem autorização.

Os detalhes eram referentes à Vigilância Global de comunicações e tráfego de informações na qual eram executados através de determinados programas, alguns pela NSA e outros pela *Five Eyes Intelligence Alliance*[54].

Com isso, ele foi acusado de roubar propriedade do governo, pois acabou por divulgar dados que não lhe pertenciam e cuja descoberta foi feita por ser seu trabalho anteriormente.

O caso gerou várias discussões e controvérsias, uma vez que ele foi chamado de herói, patriota, espião e traidor após a divulgação dessas informações. Ainda, trouxe à tona debates sobre o excesso de vigilância por parte dos Estados Unidos, além de segredos do Governo e uma balança entre segurança nacional e informações privadas.

Em meio às divulgações que Snowden fez, uma delas em especial, feita pela rede social *Twitter*, trouxe alerta para o Brasil, pois foi dito que a NSA espionava a ex-presidente Dilma através de ligações que não eram criptografadas.

Ele também faz menção ao fato de que a ex-presidente Dilma foi alvo de espionagem direta, apontado em documentos que foram classificados como ultrassecretos, mas que foram revelados em 2013 pelo jornalista Glenn Greenwald.

A dita espionagem foi referente às comunicações de Dilma[55] com seus principais assessores, além disso, entre estes últimos e com terceiros.

A descoberta por parte do Brasil acendeu a discussão novamente sobre a grade importância da Proteção de Dados Pessoais, pois uma figura pública, mais precisamente quem representava o país, teve informações particulares obtidas de forma ilegal, na qual interfere diretamente com a segurança do mesmo.

Porém, este não é o único caso de vazamento de dados que podemos tomar como exemplo. Embora a segurança no que tange informações pessoais e dados sensíveis esteja aumentando com o passar do tempo devido a precauções, novas experiências, Leis que estão surgindo, como foi o caso do Marco Civil da Internet, Lei Carolina Dieckmann e o Anteprojeto de Proteção de Dados Pessoais no Brasil, ainda há casos que demonstram o quanto as empresas precisam estar preparadas para tudo o que a internet pode proporcionar; precisam continuar acompanhando a tecnologia.

Um caso que demonstra o quanto a segurança de uma empresa é imprescindível e, se não for levada a sério pode causar uma série de consequências irreversíveis, é o da Yahoo.

No final de 2016 foi revelado uma invasão ao Yahoo que expôs cerca de 500 milhões de usuários. Inclusive, foi divulgada uma advertência de que os invasores instalaram *cookies* para ter acesso a dados futuros

destes usuários. O ataque envolveu roubo de nomes, endereços de e-mail, respostas às perguntas de segurança, porém não incluiu dados de cartões de crédito ou senhas.

A empresa alertou os usuários após confirmar o roubo dos dados. No entanto, o grande problema para a empresa foi que, além de ter dados de seus usuários roubados e sem qualquer garantia de quais contas estavam seguras, o Yahoo ainda revelou que o ataque ocorreu em 2014, dois anos antes de sua revelação.

Em virtude disso, um americano que teve seus dados comprometidos moveu uma ação contra o Yahoo em nome de todos os demais usuários envolvidos na violação de seus dados pessoais, acusando a empresa de negligência[56].

Se não bastasse isso, o Yahoo revelou apenas em 2016, outro ataque que ocorreu em 2013, na qual foi comprovada a invasão a 01 (um) bilhão de contas da empresa. Neste caso, no entanto, foram roubadas nomes, informações pessoais e senhas.

Os ataques revelados trouxeram à tona a preocupação com a segurança de informações pessoais fornecidas a serviços que deveriam ser seguros, além de alertar ao fato de que há cada vez mais vítimas deste tipo de ataque. Tornou-se “comum” o roubo de dados, desde os mais simples até os mais perigosos, secretos, aqueles que não podem e não devem ser revelados.

Acontece que a empresa Yahoo estava com negociações em andamento desde julho de 2016 para venda à Verizon com uma venda inicial de US$ 4,8 bilhões, e com a revelação dos dois ataques de roubos de dados ocorridos em 2013 e 2014, tal venda foi atrasada[57].

Com isso, a Verizon propôs uma redução cerca de US$ 250 milhões e US$ 300 milhões do valor inicial, além de precisarem compartilhar a responsabilidade legal e os custos dos futuros processos relacionados às violações ocorridas.

No dia 21 de fevereiro de 2017 a Verizon finalmente fechou negócio com o Yahoo, adquirindo-a por cerca de US$ 4,48 bilhões. A diminuição do valor em relação à oferta inicial foi de US$ 350 milhões.

Em casos como esse, fica visível o quanto um sistema pode ser invadido com facilidade, mesmo quando possui segurança. O Yahoo está longe de ser uma empresa pequena, portanto significa que eles possuem ao menos algum tipo de segurança. No entanto, vale lembrar que, do mesmo modo que há pessoas experientes para proteger a segurança dessas companhias, há pessoas ainda mais determinadas a invadir esses sistemas e obter informações que não lhes pertencem com o único intuito de lucrar com isso ou até mesmo prejudicar algo ou alguém.

Portanto, o que fazer para melhorar a segurança e preservar a privacidade e a proteger os dados de seus usuários e até mesmo de seus funcionários?

O Google, por exemplo, já arranjou um modo de lidar com a evolução rápida da Internet das Coisas. Ele tem apostado em simulações para detectar falhas e problemas em sua própria segurança de forma repetitiva.

Inclusive, segundo Alex Cox[58], diretor de tecnologia do *FirstWatch* da RSA, um time de pesquisadores que utiliza inteligência e análise de segurança para combater ameaças, explicou o que o Google chegou a fazer e que as demais empresas devem apostar também:

> “O Google faz isso. Eles já simularam em ambiente controlado o que aconteceria se seus sistemas ficassem fora do ar por cinco minutos e o resultado foi que 40% (quarenta por cento) dos sistemas do mundo caíram”.

Ainda, ele complementou dizendo que “empresas estão agora trabalhando na criação de centros para verificar o impacto de falhas”.

E não é só os Estados Unidos e demais países que precisam focar em testar a própria segurança, em proteger os dados de seus usuários e funcionários, pois o Brasil também precisa estar alerta.

Recentemente a Alezzia[59], empresa de móveis, ficou famosa nas redes sociais por fazer anúncios com mulheres trajando roupas de banho com seus móveis em locais variados, porém, sua popularidade também se deu pela contratação de um estagiário acusado de tecer comentários machistas nas redes sociais.

Com isso, a empresa se tornou alvo de ataques do grupo *Anonymous* Brasil, na qual afirmou que a Alezzia foi “integralmente hackeada”, alegando possuir dados como: *backups*, e-mails, senhas e dados pessoais dos mais de 10 (dez) mil clientes que eles possuem.

E se não bastasse o roubo dos dados, que já é considerada uma falha gravíssima, o *Anonymous* fez questão de notificar os clientes da empresa sobre a falha de segurança e o roubo de dados, em um convite para processar a Alezzia pelo ocorrido.

O ataque demonstrou o quão frágil é o sistema de uma empresa e a importância de proteger os dados pessoais armazenados de seus clientes. É importante frisar que não se trata apenas de nomes, telefones, endereço, mas também da possibilidade de informação de cartões de crédito estarem salvos para realizar a famosa “compra com um click” que muitas empresas

oferecem, além do roubo de senhas que muitas vezes é a mesma de outros sites utilizados pelos usuários.

Por isso, como mencionado por Caroline Teófilo da Silva, é importante não se esquecer dos controles preventivos a fim de proteger os dados. Ou seja, "estabelecer programas anuais de conscientização em segurança da informação é essencial para diminuir os riscos de engenharia social[60]".

Portanto, por mais influente que a Big Data tenha sido na elaboração do Marco Civil da Internet, tal Lei ainda possui certas falhas e contradições em pontos relacionados à proteção da privacidade e proteção de dados pessoais.

Além disso, embora o Brasil ainda não exista uma lei em vigor que cuide especificamente da proteção de dados, já há o Anteprojeto de Lei de Proteção de Dados, com a intenção de proteger os direitos fundamentais de liberdade, intimidade e privacidade dos seus usuários.

Aliás, Patrícia Peck Pinheiro traz em seu livro, pontos de atenção que deveriam ser observados na criação de uma lei específica referente à proteção de dados pessoais em nosso país. Ela utiliza como base o que já foi apresentado no presente Anteprojeto de Lei de Proteção de Dados já mencionado outrora e cita alguns pontos de suma relevância para o Brasil, pois se trata do futuro do país e de seus usuários, bem como das próximas gerações.

> "Cuidado com o excesso de formalidade e rigidez nos requisitos para o titular dos dados dar consentimento para tratamento de seus dados pessoais (Anteprojeto arts. 7º, § § 3º, 6º, 7º e 8º, 11, 12, 13, § 2º).
>
> Necessidade de reafirmar o consentimento no ciclo de vida de uso dos dados pessoais (o Anteprojeto exige a primeira vez no art. 7º, a segunda vez no art. 23, a terceira vez no art. 29, I) e sua

> inviabilidade e a limitação para grupo econômico (Anteprojeto, art. 30).
>
> Cancelamento da base de dados (revogação) e o seu efeito em bases pretéritas (já existentes), bem como em bases que já receberam enriquecimento (Anteprojeto, arts. 15 e 17, IV).
>
> Fornecimento da base de dados para o titular (Anteprojeto, art. 18, § 3º).
>
> Revisão das decisões – Quem efetuará a revisão das decisões? O responsável pelo tratamento? O operador? Outro responsável da empresa? (Anteprojeto, art. 19).
>
> Responsabilidade pela comunicação e interconexão de dados e a necessidade de sua melhor limitação (Anteprojeto, arts. 22, 23, 31 e 32).
>
> Restrição de dados em *cloud computing*, transferência internacional e a imposição de autorização prévia que é inviável (Anteprojeto, arts. 28, 29, 30, 31 e 32).
>
> Necessidade ou não de ter um Órgão autorizante e fiscalizador e como isso ocorrerá sem paralisar os negócios e inviabilizar a livre-iniciativa (Anteprojeto, arts. 13, § 2º, 28, III e V, parágrafo único, 44, 45, 47 e 49).
>
> Prazo para guarda de registros de tratamento de dados pessoais e seu impacto (Anteprojeto, art. 40).
>
> Definição de um padrão técnico de segurança da base de dados (Anteprojeto, arts. 42, 43, 44, 45, 46 e 48).
>
> Sanções previstas e quais são os critérios de aplicação (Anteprojeto, art. 50).
>
> Prazo para se adaptar após entrada em vigor que deveria ser maior do que 120 dias devido aos seus impactos no mercado (Anteprojeto, art. 52) – ao menos 12 meses[61]".

Assim, vale lembrar que é impreterível a análise correta de todos esses pontos e vários outros mais, com a finalidade de trazer uma Lei que seja benéfica às empresas e seus usuários, além de preservar direitos que já estão estabelecidos na nossa Carta Magna.

Cumpre ressaltar, ainda, que embora não haja uma lei específica, o Poder Judiciário vem se manifestando frente a esse tema, utilizando-se de

todas as Leis brasileiras existentes até agora.

Por isso, se faz necessário que o Brasil continue tomando como base os ensinamentos dos ordenamentos jurídicos da Europa e dos Estados Unidos, pois ambos estão mais a frente em face da tecnologia e, consequentemente, com suas Leis.

CAPÍTULO 3 – CONTRASTES E REFERÊNCIAS

3.1. A visão do ordenamento Europeu

De maneira geral, tanto a Big Data como a Internet das Coisas, em qualquer lugar do mundo, acabam por ter desafios para com a transparência, a privacidade e a proteção de dados pessoais. Trata-se de uma tecnologia que vem crescendo cada vez mais e, consequentemente, necessita de um ordenamento jurídico.

Quando mencionamos a Big Data e o IoT, pensamos logo na quantidade de dados coletados e armazenados. Além disso, fazem-se necessários centros de dados equipados para lidar com essas informações adicionais que, como mencionado anteriormente, nem todos acabam sendo úteis.

De acordo com a *European Data Protection Supervisor* (EDPS)[62], um instituto independente da União Europeia, acredita que a responsabilidade e o desenvolvimento da sustentabilidade da Big Data deve se basear em quatro elementos essenciais: (i) organizações devem ser transparentes sobre o modo de processar os dados pessoais; (ii) providenciar usuários com maior grau de controle de como os dados são usados; (iii) design amigável de proteção de dados em seus produtos e serviços; e (iv) tornam-se mais responsáveis pelo que fazem.

A finalidade do EPDS é desenvolver debates dentro e fora da Europa a fim de melhorar o potencial da Lei em vigor. A Diretiva de Proteção de Dados é antiga, de 1995.

A Legislação Europeia é o grande exemplo referente à Proteção de Dados. A Diretiva 95/46/CE[63] (Diretiva de Proteção de Dados, também conhecida como “DPD”), tenta estabelecer um equilibro entre a proteção da vida privada dos cidadãos e a circulação de dados pessoais no interior da União Europeia (UE) de forma livre. Ou seja, foi fixado limites em relação ao recolhimento e à utilização de dados pessoais e, ainda, solicita a criação de um organismo nacional em cada Estado signatário, a fim de controlar as atividades relacionadas ao tratamento de dados. Inclusive, a diretiva traz que deve haver a supervisão à aplicação dos princípios e Leis de proteção à privacidade individual, na qual é deveras importante para todos os usuários.

A diretiva não se aplica para exercícios individuais ou domésticos, tampouco para as atividades que não são sujeitas à aplicação do direito coletivo, como é o caso da segurança pública, defesa e segurança do Estado. Noutras palavras, ela tem a intenção de proteger o direito à liberdade de seus usuários no que tange ao tratamento de dados pessoais.

Ainda, em um de seus artigos, a diretiva traz que seu âmbito de aplicação será a qualquer forma de processamento de dados, realizado de maneira automatizada (mesmo que parcial) ou não.

Embora já mencionado anteriormente o que são os dados pessoais, a DPD traz, em seu artigo 2º, uma definição:

> “Qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultura ou social.”

Além disso, ela traz princípios relativos à qualidade de dados que servem para sua aplicação em todas as atividades referentes ao tratamento

lícito de dados. Quais sejam:

> “1. Os Estados-membros devem estabelecer que os dados pessoais serão:
>
> a) Objeto de um tratamento leal e lícito;
>
> b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas;
>
> c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;
>
> d) Exatos e, se necessário, atualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou retificados;
>
> e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos.
>
> 2. Incumbe ao responsável pelo tratamento assegurar a observância do disposto no nº 1.”

No artigo 6º, inciso I, alínea “b” mencionado, vemos o princípio da finalidade, ou seja, é permitido que os dados pessoais sejam recolhidos apenas com finalidades determinadas, explícitas e legítimas, não podendo, posteriormente, ser utilizado de maneira diversa àquela prevista inicialmente. Assim, é possível ver que eles visam a transparência para com o usuário, a fim de que nada seja feito sem uma determinada razão.

Há, também, os princípios relativos à legitimidade do tratamento de dados, na qual o artigo 7º traz as situações que justifiquem esse

processamento. Noutras palavras, a fim de considerar legítimo, o tratamento precisa se enquadrar nas circunstâncias previstas na DPD.

> "Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se:
>
> a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou
>
> b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou
>
> c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou
>
> d) O tratamento for necessário para a proteção de interesses vitais da pessoa em causa; ou
>
> e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou
>
> f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º."

Estes princípios devem ser seguidos com a finalidade de estabelecer uma ordem em relação aos dados coletados, pois nem todos são úteis ou necessários.

O artigo 8º, inciso I, faz menção aos dados considerados sensíveis, quais sejam aqueles que falem sobre opiniões políticas, credos religiosos, filiações, origem racional ou étnica de uma pessoa, vida sexual, saúde, entre outros, são proibidos, salvo algumas exceções.

> "2. O nº 1 não se aplica quando:
>
> a) A pessoa em causa tiver dado o seu consentimento explícito para esse tratamento, salvo se a legislação do Estado-membro estabelecer que a proibição referida no nº 1 não pode ser retirada pelo consentimento da pessoa em causa; ou

> b) O tratamento for necessário para o cumprimento das obrigações e dos direitos do responsável pelo tratamento no domínio da legislação do trabalho, desde que o mesmo seja autorizado por legislação nacional que estabeleça garantias adequadas; ou
>
> c) O tratamento for necessário para proteger interesses vitais da pessoa em causa ou de uma outra pessoa se a pessoa em causa estiver física ou legalmente incapaz de dar o seu consentimento; ou
>
> d) O tratamento for efectuado, no âmbito das suas actividades legítimas e com as garantias adequadas, por uma fundação, uma associação ou qualquer outro organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, na condição de o tratamento dizer unicamente respeito aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem o consentimento das pessoas em causa; ou
>
> e) O tratamento disser respeito a dados manifestamente tornados públicos pela pessoa em causa ou for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial.”

Nestas ressalvas, é possível notar a preocupação para com o usuário. A proteção de dados foi desenvolvida para proteger os direitos fundamentais e valores, inclusive os direitos à privacidade de seus cidadãos.

Ainda, ao longo dos demais artigos, temos o direito de ser informado; o direito de acesso e de correção; o direito de objeção; o direito de não ser submetido a processos automatizados de decisão; exceções e limitações dos direitos do titular dos dados; segurança e confidencialidade dos dados; obrigação de notificação à autoridade supervisora; cadastro; sanções administrativas; transferência de dados pessoais a países não integrantes da União Europeia; códigos de conduta; autoridade supervisora da proteção de dados pessoais.

A Diretiva tem a intenção de trazer aos seus usuários todos os seus direitos, bem como dar foco na segurança de seus dados, seja na coleta, no tratamento ou na transferência. Ainda, traz também sanções e monitoramento desses dados.

O artigo 25[64], por exemplo, traz a preocupação quanto à transferência de dados para países que não integram a União Europeia. Entretanto, tal regra tem causado problemas diplomáticos com os países não membros. Isso se dá ao fato da norma exigir, em seu item 1, um nível de proteção adequado, de acordo com alguns fatores impostos, principalmente as regras que estão em vigor no país em questão.

O artigo 28[65] da Diretiva traz a importância de uma autoridade supervisora de proteção de dados, com a finalidade de monitorar a aplicação de suas normas dentro do território, afinal, é ciente de que não adianta haver regras se as mesmas não forem aplicadas ou respeitadas. Ainda, tem o poder de intervir em empresas e abrir investigações em caso de violação.

Cumpre ressaltar que, no âmbito do Reino Unido, há o Ato de Proteção de Dados de 1998[66], do Parlamento. Seu objetivo é, assim como os demais, requerer um processamento de dados justo, transparente, onde os dados pessoais sigam o propósito pela qual foram coletados, sempre trabalhando de forma legal e sem exceder; além de que os dados devem ser relevantes e adequados.

Possui, também, uma entidade supervisora chamada *Data Protection Commissioner*. Ela pode receber denúncias, realizar diligências e requerer a adequação legal do chamado controlador de dados, ou seja, aquele que os detém.

Importante lembrar que os usuários possuem direitos garantidos quanto ao acesso a seus dados pessoais, podendo, então, reclamá-los quando necessário.

E, ainda, na Alemanha, existe o Ato Federal de Proteção de Dados, com a finalidade de complementar a Diretiva Europeia nº 95/45/EC, pois estabelece a importância de proteger o usuário contra o desrespeito em face da sua privacidade na utilização dos dados pessoais. Ou seja, se permitido pelo Ato, poderá ser feita sua coleta, processamento e uso dessas informações.

Diante de tudo exposto, vemos os motivos de a Diretiva Europeia vir sendo a principal fonte de inspiração para elaboração de Leis referentes a essa temática, não só no Brasil, mas em toda a América Latina.

3.2. Ordenamentos jurídicos dos Estados Unidos

Em se tratando dos Estados Unidos, o ordenamento torna-se um pouco mais complicado. Primeiro, é necessário compreender que há Leis federais, mas também há Leis de acordo com cada Estado, ou seja, elas são variáveis e nem sempre o que é estabelecido em determinado Estado vai existir no outro, portanto, é importante entender que há muitas partes referentes ao ordenamento jurídico existente nos EUA.

É justamente por isso que, Mark Radcliffe[67], um advogado do Vale do Silício na Califórnia e que trabalha com questões referentes à Internet das Coisas, compara as Leis nos Estados Unidos com um cubo mágico, pois há como ter várias partes que se movem; várias combinações.

As Leis nos Estados Unidos são consideravelmente diferentes em relação ao que estamos acostumados no Brasil. Primeiramente, vale ressaltar que existem Leis Federais como o Ato Privado de 1974, na qual traz o foco na proteção da privacidade de todos os indivíduos em face da coleta de dados e informações pessoais, mas também existem as Leis de cada Estado.

> “O Departamento dos Estados se esforça para proteger a privacidade de todos os indivíduos, coletando uma quantidade mínima de informações pessoais identificáveis do público e de seus funcionários. Quando essa coleta é necessária, a Divisão de Privacidade assegura que o Departamento cumpra com todos os estatutos e diretrizes federais de privacidade. Com experiência em leis de privacidade, informamos o desenvolvimento de políticas de privacidade, tanto dentro do Departamento quanto em colaboração com o resto do governo federal. Promovemos a conscientização dos princípios da privacidade entre os funcionários do Departamento e procuramos construir a confiança do público através da implementação de melhores práticas através da coordenação com a comunidade de privacidade mais ampla.

> Como parte de seus deveres estatutários, a Divisão de Privacidade publica suas atuais Avaliações de Impacto de Privacidade e Avisos de Sistema de Registros[68].”

As Leis Federais devem estar de acordo com a Constituição dos Estados Unidos, que é a mais importante do país; é a base legal do governo norte-americano e é constituída de 07 (sete) artigos.

Assim, o Ato Privado mencionado acima traz o quanto o Departamento de Estado frisa a importância de proteger os dados pessoais de pessoas identificáveis e de seu próprio público.

Ainda, enfatiza o fato de que o Departamento deve cumprir com todos os estatutos e diretrizes relacionados à privacidade, bem como promover a conscientização de que os princípios da privacidade devem ser preservados, para que o público não perca a confiança em disponibilizar dados tão sensíveis para empresas e para o seu próprio país.

Os Estados Unidos, inclusive, criaram a estrutura *Safe Harbor*[69], cuja intenção era conseguir obter dados de consumidores europeus, visto que a Diretiva Europeia era clara em não deixar que nenhum dado pessoal fosse transferido para fora da Europa para países que não se encontrassem dentro dos padrões de adequação da proteção privada de dados.

Em 2000 foi decidido que os princípios dos Estados Unidos cumpriam com a Diretiva Europeia. No entanto, houve uma reclamação por parte de um usuário, alegando que os dados de seu *Facebook* não foram protegidos o suficiente e, por esse motivo, a Corte de Justiça Europeia declarou, em outubro de 2015, que a decisão do *Safe Harbor* era inválida[70]. Noutras palavras, não era mais possível cumprir os requisitos da União Europeia referente à proteção de dados.

Em 2016, porém, a Comissão Europeia e os Estados Unidos concordaram em estabelecer um novo quadro para fluxos de dados, conhecido como “EU-US Privacy Shield[71]”, sendo um substituto para o mencionado anteriormente.

O mesmo aconteceu com a Suíça, onde em janeiro de 2017 foi aprovado o “Swiss-US Privacy Shield[72]” como mecanismo válido que cumpre com os requisitos de transferência de dados pessoais da Suíça para os Estados Unidos. Este novo quadro substitui automaticamente o anterior, chamado de “US-Swiss Safe Harbor”, mesmo nome dado para o referente à União Europeia; ambos tem intenções similares.

A partir de abril de 2017[73], o Departamento de Comércio não irá mais aceitar nenhum certificado referente ao *Safe Harbor* da Suíça, do mesmo modo que já não é mais aceito o *Safe Harbor* referente à União Europeia desde outubro de 2016 devido a sua invalidação.

3.3. Outros países

A internet se tornou universal; algo que a grande maioria das pessoas deseja acesso e, não apenas isso, mas que precisam também para alguma atividade, como o próprio trabalho. Com isso, tornou-se essencial que todos os países que se utilizam desse recurso venham a pensar na importância da proteção e da privacidade.

Em outubro de 2010[74], a Corte Europeia formalizou a decisão de que a proteção de dados de Israel estava adequada aos padrões da Diretiva 95/46/CE. Juntando-se, então, a outros 06 (seis) países a poder receber datas da União Europeia.

Já na Rússia, por exemplo, a Lei de Proteção de Dados[75] pode ser encontrada na Convenção de Estrasburgo pela Proteção de Indivíduos em relação ao Tratamento Automatizado de Dados Pessoais ratificados em 2006 e a Constituição da Rússia, na qual estabelece o direito à privacidade de cada indivíduo em seus artigos 23 e 24.

Ainda, há a Lei de Proteção de Dados nº 152 FZ de 2006 e também a Lei de Informação, Tecnologias de Informação e Proteção de Informação nº 149 FZ, do mesmo ano. E, visando proteger também os dados de seus trabalhadores, há disposições sobre proteção de dados no Código do Trabalho.

Em 2014 a Lei de Proteção de Dados sofreu algumas alterações, na qual requer que os operadores de dados pessoais armazenem e processem qualquer dado dos cidadãos da Rússia nos bancos de dados localizados no país, exceto em algumas exceções.

Já na Ásia/Pacífico, há países na região como a China, Indonésia e Índia, que ainda estão atrasados. Charles Anderson[76] diz:

> “Os governos tendem a ficar muito para trás em qualquer coisa relacionada a assuntos de dados pessoais e isso acaba causando muitos problemas para empresas que querem mover seus dados ao redor do mundo ou coletá-los”.

No entanto, há algumas exceções como Nova Zelândia, Singapura e o Japão. No caso deste último, inclusive, trata-se de um país conhecido por estar muito a frente tecnologicamente. Sempre criando novas ferramentas e prezando o desenvolvimento de novas funcionalidades, bem como projetos que tendem a inovar o mundo atual. Com isso, para eles, torna-se de suma importância a proteção de tudo que é criado; de qualquer tipo de ideia.

Em 2005, entrou em eficácia o Ato de Proteção de Informações Pessoais[77] do Japão, cuja finalidade é proteger os direitos e interesses de cada indivíduo em face de seus dados pessoais. O governo japonês preza a cautela e respeito quanto à manipulação de informações pessoais, ou seja, é necessária transparência por parte de quem colhe e usa esses dados, a fim de que os cidadãos que tiveram seus dados coletados estejam cientes de que nenhuma finalidade aquém do que foi previsto seja cometida contra as informações.

O Ato frisa a necessidade de implementar medidas de seguranças de dados, afinal, não pode uma empresa coletar dados de diversos usuários sem a garantia de que eles serão devidamente protegidos. Não podem, também, obter dados de forma fraudulenta ou desonesta e, claro, o principal deles, coletar os dados com prévio consentimento de seu usuário, salvo algumas exceções.

Ainda, ela estabelece sanções penais em caso de desrespeito ao que está disposto neste Ato, mostrando, novamente, a necessidade do cumprimento do que está previsto em Lei.

Já no Canada, há uma Lei Federal chamada Ato de Proteção de Informação Pessoal e Documentos Eletrônicos[78], cuja finalidade é estabelecer regras de como as companhias que coletam dados pessoais devem protegê-los.

Inclusive, através desse Ato é possível salientar, mais uma vez, a importância de um programa privado que limite a coleta, o uso e a retenção dos dados, além de dar acesso aos usuários a informações que a empresa possua sobre eles e a possibilidade de reclamarem com a empresa caso algo não esteja correto. E, similar aos Estados Unidos, cada província canadense tem suas próprias Leis privadas.

Mostra, assim, que todo usuário possui seus direitos e eles devem ser respeitados acima de tudo. É de suma relevância que as companhias estabeleçam transparência e respeito para com seus clientes.

Além dos países mencionados anteriormente, o Conselho da Europa[79] na Internet mostra que inúmeros outros possuem código de proteção de dados e, ainda, uma entidade supervisora de dados.

Isso prova, mais uma vez, que o mundo inteiro está focado na importância da Proteção de Dados Pessoais. Não se trata de algo trivial, na qual pode ser espalhado pelo mundo digital sem que haja consequência de seus atos, tampouco se trata de informações sem importância, pois uma vez que revelada para alguém que possui interesse, pode desencadear uma série de outros fatores.

CONCLUSÃO

Visando criar a discussão sobre os desafios e problemas que a Big Data e a Internet das Coisas enfrentam face à privacidade e à proteção de dados pessoais, e mostrando a sua importância diante do que vemos no dia a dia é que se traz essa discussão.

Os temas citados mostram as vantagens que até então eles trouxeram ao mundo. A Internet das Coisas ou IoT, por exemplo, enfatiza o quanto ela está aqui para melhorar o modo como vivemos hoje e futuramente. Nos mostra o quanto tudo está cada vez mais conectado e que, ao mesmo tempo em que não podemos mais viver sem uma conexão com a internet, nós também devemos temê-la.

Outrossim, a Big Data nos mostra a quantidade monstruosa de dados que possuíamos agora e o quão rápido tem sido o seu crescimento diante de tudo o que é armazenado na internet. Ela mostra, também, o quanto a tendência é apenas aumentar; além de deixar claro que nem todo dado coletado tem serventia para quem os coleta, fazendo-nos questionar como eles são descartados, como eles são analisados, como é a segurança para com algo que é nosso.

Ele traz os conceitos referentes aos dois temas de extrema relevância atualmente. Além de demonstrar sua importância no dia a dia, no mundo e no futuro. Ainda, traz explicações sobre os dados pessoais, o que eles são e qual a sua relevância. Traz, também, o que o Brasil vem fazendo para tratar deste assunto, quais são as Leis existentes e de onde foram baseadas; bem como mostrar a comparação do nosso ordenamento jurídico com os demais, que estão mais avançados frente ao tema em questão.

Tais questionamentos são de suma relevância para o Direito Digital, pois ele não está sozinho; trata-se de uma comunicação com os demais ramos do direito. Necessário, então, dirimir os problemas para provar aos cidadãos de que essa inovação, ou seja, essa nova tecnologia que utilizamos, seja para lazer, seja para trabalho e que cada vez mais está presente em nossas vidas, é segura; de que estamos aptos a continuar usufruindo-a.

Assim, diante de todo o exposto, as respostas encontradas para essas preocupações não são absolutas. Todavia, é possível ter uma mínima noção do que estamos diante e do que nos aguarda no futuro.

Com isso, é sabido que, tanto a Internet das Coisas quanto a Big Data enfrentam um grande crescimento no mundo atual, pois com o advento da tecnologia, a tendência é apenas a maior produção de dados, ou seja, de informações que nós, usuários, vamos proporcionar na internet.

Com este crescimento, vem também a preocupação frente ao que os cidadãos devem enfrentar. Com as mais variadas redes sociais, compras *on-line*, sites de busca, *smartphones*, *tablets*, relógios inteligentes, entre outros, trouxe o conforto, a facilidade, é claro, mas também aumentou a vulnerabilidade de quem os utiliza.

O maior desafio quando mencionado a coleta de dados pessoais é, justamente, a dificuldade em preservá-los de modo correto; tratá-los, armazená-los e descarta-los, tudo isso sem ferir os direitos de seus cidadãos. E, um dos principais direitos, o que causa preocupação em todo internauta na hora de divulgar algo é, sem dúvidas, a privacidade.

É fato que o princípio da privacidade encontra-se preservado na Constituição Federal, bem como na Declaração Universal dos Direitos

Humanos. No entanto, o fato de isso ocorrer dentro da internet, um tema relativamente novo, traz variados questionamentos sobre o assunto e, o modo de como se agir, é um dos principais deles.

No Brasil, por exemplo, houve a criação do Marco Civil da Internet, que veio para proteger mais a privacidade e liberdade dos usuários. Porém, como mencionado outrora, ainda há deficiências. A Big Data foi bastante influente em sua criação, todavia ainda possui falhas e contradições que precisam ser resolvidas; lacunas em sua própria redação que podem levar a interpretações errôneas, que podem prejudicar os internautas.

Então, o que as empresas, públicas e privadas, têm que ter em mente, é que a proteção de dados tem que ser feita com muita cautela. Precisam estar sempre simulando ataques à própria rede com a finalidade de ter certeza quais são os pontos vulneráveis de sua segurança a fim de saná-los.

Ainda, precisam ter em mente que a privacidade de seus usuários deve ser preservada a todo custo, com base no que possuímos, pois, aos poucos, diante das problemáticas que são apresentadas ao Judiciário, é que se abrirá uma maior possibilidade de sanar tais problemas.

Os mais diversificados casos apresentados, que mostram claramente o perigo da falta de proteção de dados pessoais, de como somos vulneráveis diante da internet e das pessoas que querem apenas lucrar, destruir algo ou alguém, ou até mesmo visa fazer o bem de algum modo, mas acaba por machucar outras, são exemplos claros de que ainda não estamos totalmente seguros.

A tendência da Big Data e Internet das Coisas face à privacidade e à Proteção de Dados é apenas crescer, seja na quantidade de conteúdo produzido, seja em relação à segurança para mantê-los armazenados.

E, para continuar acompanhando o grande avanço tecnológico que não irá parar, faz-se necessário que as empresas e até mesmo o próprio Governo não pensem que estão livres de qualquer tipo de invasão. Manter sua segurança sempre atualizada por parte dos operadores da mesma é de suma importância, visto que sempre poderá surgir um vírus novo, outro modo de invadir o sistema operacional atual, ou uma determinada pessoa que está à frente tecnologicamente falando.

Tendo em mente isso, vale completar que devem manter em mente, também, que preservar os seus usuários é de suma importância para que eles continuem confiando nos serviços fornecidos. A divulgação de dados sem a permissão de quem o pertence é errado e pode prejudicá-la ou constrangê-la.

Ademais, vale ressaltar que a preservação da privacidade e da proteção de dados também pode ser feita pelos próprios cidadãos, através de uma leitura minuciosa dos contratos fornecidos e do quanto nós estamos disposto a divulgar na internet.

As redes sociais são perigosas, os celulares, e-mails, os documentos e informações que armazenamos nas nuvens, tudo é extremamente vulnerável e pode ser alvo de pessoas má intencionadas. Por isso, é de suma importância que os internautas tomem cuidado com seus pertences *on-line* e que as empresas estejam sempre atualizadas perante a sua segurança, pois é extremamente comum que, em virtude do dinheiro, um ataque por *ransomware* aconteça e uma companhia importante acabe por ter dados valiosíssimos divulgados sem seu consentimento.

Propagandas, sites, mensagens, e-mails, qualquer coisa em que clicarmos está passível de capturar nossos dados e armazená-los, portanto precisamos ficar atentos. Não podemos deixar de ler os famosos *termos de*

uso de cada empresa de vendas que procurarmos ou do novo aplicativo instalado no celular ou no computador, pois todos têm como objetivo conquistar a mesma coisa: mais e mais dados pessoais que nós estamos dispostos a dar no momento em que concordamos com o que está descrito.

Somos alvos das famosas publicidades, de empresas de varejo conhecendo nossos gostos e selecionando seus produtos para que sejam atrativos aos nossos olhos e possamos consumi-los. E, embora isso soe como algo bom, há suas desvantagens também devido a falta de privacidade que isso acarreta.

Ademais, não só a empresa acaba tornando-se vulnerável, mas também seus clientes, que tem dados pessoais espalhados por todo o ambiente virtual, bem como a perda de confiança naquela companhia que coletou seus dados, os armazenou e prometeu mantê-los em segurança.

Por isso, as empresas devem investir no *compliance*, para evitar que dados importantes para sua companhia, além de dados de seus funcionários e de seus clientes, sejam divulgados ou usados como moeda de troca.

E, ainda, diante do direito comparado apontado, ou seja, diante das legislações apresentadas dos outros países, fica mais fácil o Brasil tomar consciência do que ele pode e não pode fazer. Tanto a Europa quantos os Estados Unidos estão à frente do Brasil no que tange a Big Data e Internet das Coisas e, principalmente, em relação a sua legislação.

A Diretiva 95/46/CE traz o que é abordado na União Europeia, o que fez com que várias outras Leis ao redor do mundo fossem baseadas no que ela propôs. Inclusive, em seus artigos, ela traz foco na transparência, na proteção dos dados fora e dentro da UE, na privacidade e outros fatores

mais; aborda pontos importantíssimos que o nosso país deve se manter atento.

E isso também ocorre no Brasil. Seguindo a linha de que possuímos sim legislação para assuntos pertinentes a internet, mas que ainda carecem em alguns pontos, nós temos a criação do Anteprojeto de Lei de Proteção de Dados, que teve como base a Diretiva Europeia e que ainda tem alguns pontos a serem frisados.

Portanto, é importante frisar que o Brasil possui sim Leis e projetos para lidar com os casos mencionados, no entanto, é necessária uma análise séria e correta de todas as lacunas pendentes para que seja resolvido no futuro e possamos ter uma melhor legislação, com a finalidade de proteger não só a privacidade de seus usuários, mas também seus dados pessoais, as informações fornecidas que ajudam as empresas, o Governo, que ajudam a manter a economia girando dentro da internet.

A tecnologia não irá parar e tampouco a internet deixará de existir. Na verdade, a tendência para o futuro, como mencionado, é de aumentar cada vez mais. Portanto, precisamos estar de acordo com tudo que ela nos proporciona e ter em mente que a Big Data, a Internet das Coisas, a Privacidade e a Proteção de Dados estão todas ligadas, são um grande pacote que andam juntos e merecem ser preservados.

BIBLIOGRAFIA

ABRUSIO, Juliana et al. *Marco Civil da Internet:* Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014.

ASHTON, Kevin. *That 'Internet of Things' Thing*. RFID Journal. Publicado em: jun. 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986> Acesso em: 20 out. 2016.

BUGHIN, Jacques; CHUI, Michael; MANYIKA, James. *Clouds, big data, and smart assets:* Ten tech-enabled business trends to watch. McKinsey Quartely. Publicado em: ago. 2010. Disponível em: <http://www.mckinsey.com/industries/high-tech/our-insights/clouds-big-data-and-smart-assets-ten-tech-enabled-business-trends-to-watch> Acesso em: 22 out. 2016.

CENICEROS, Matt. *The Internet of Things Ecosystem:* The Value is Greater than the Sum of its "THINGS". Business 2 community. Publicado em: abr. 2014. Disponível em: <http://www.business2community.com/business-innovation/internet-things-ecosystem-value-greater-sum-things-0829370#Kp8RD2G8kqMFAwbV.97> Acesso em: 01 nov. 2016.

CHAVES, Luis Fernando Prado; GOMES, Maria Cecília Oliveira. *Por que a Internet das Coisas revolucionará o Direito Digital?* Carta Capital. Publicado em: fev. 2017. Disponível em: < http://justificando.cartacapital.com.br/2017/02/20/por-que-internet-das-coisas-revolucionara-o-direito-digital/> Acesso em: 21 fev. 2017.

Data protection laws of the world. The Venture Alley. Publicado em: mar. 2015. Disponível em: <http://www.lexology.com/library/detail.aspx?g=1a6e9e6c-affc-4e40-9270-7256ac9cf2a4> Acesso em: 16 fev. 2017.

Diretiva 95/46/CE do Parlamento Europeu. ANACOM. Disponível em: <https://www.anacom.pt/render.jsp?contentId=965550#.WG2I2vkrJPY> Acesso em: 15 jan. 2017.

Diretiva Europeia 2006/24/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32006L0024> Acesso em: 02 dez. 2016.

Documentos da NSA apontam Dilma Rousseff como alvo de espionagem. G1. Publicado em: set. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html> Acesso em: 27 fev. 2017.

DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental.* Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658> Acesso em: 01 out. 2016.

DULL, Tamara. *Big data and the Internet of Things:* Two sides of the same coin? SAS Best Practices. Disponível em: <http://www.sas.com/en_sg/insights/articles/big-data/big-data-and-iot-two-sides-of-the-same-coin.html> Acesso em: 02 nov. 2016.

Edward Snowden. Wikipedia. Disponível em: <https://pt.wikipedia.org/wiki/Edward_Snowden> Acesso em: 29 jan. 2017.

European Data Protection Supervisor. Disponível em: <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS> Acesso em: 25 jan. 2017.

Five Eyes. Wikipedia. Disponível em: <https://en.wikipedia.org/wiki/Five_Eyes> Acesso em: 26 fev. 2017.

FONSECA, Mariana. *Site da Alezzia sofre invasão por Anonymous* Brasil. Exame. Publicado em: fev. 2017. Disponível em: <http://exame.abril.com.br/pme/site-da-alezzia-sofre-invasao-pelo-anonymous-brasil/> Acesso em: 23 fev. 2017.

GLEESON, Mark; JOHNSON, Mark. *Data from the "Internet of Things" is personal data*. Publicado em: out. 2014. Disponível em: <http://www.lexology.com/library/detail.aspx?g=73bef0f2-3184-45db-bad6-6354dafe0889> Acesso em: 16 fev. 2017.

InfoWester. *O que é Cloud Computing?* Disponível em: <http://www.infowester.com/cloudcomputing.php> Acesso em: 18 nov. 2016.

InovaTCU. *Internet das Coisas:* de objetos a cidades inteligentes. Disponível em: <http://portal.tcu.gov.br/inovatcu/noticias/internet-das-coisas-de-objetos-a-cidades-inteligentes.htm> Acesso em: 20 set. 2016.

InternetLAB. *Big Data:* quais proteções os titulares de dados tem a sua disposição? Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-em-um-mundo-de-big-data-quais-tipos-de-controle-temos-em-relacao-a-nossos-dados/> Acesso em: 25 jan. 2017.

InternetLAB. *Reporta*: Proteção de Dados Pessoais. Disponível em: <http://www.internetlab.org.br/pt/conjuntura/reporta-anteprojeto-de-lei-de-protecao-de-dados-pessoais/> Acesso em: 25 ján. 2017.

Israel's data protection laws given EU approval. The Register. Publicado em: fev. 2011. Disponível em: <https://www.theregister.co.uk/2011/02/08/israel_data_protection_law_eu/> Acesso em: 16 fev. 2017.

LEMOS, Ronaldo et al. *Marco Civil da Internet.* São Paulo: Atlas, 2014.

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

MARR, Bernard. *Big Data:* The 5 Vs. Linkedin. Publicado em: fev. 2014. Disponível em: <http://pt.slideshare.net/BernardMarr/140228-big-data-volume-velocity-variety-varacity-value/8-
We_currently_only_see_thebeginnings> Acesso em: 10 out. 2016.

MARR, Bernard. What is Big Data? Linkedin. Publicado em: fev. 2014. Disponível em: <http://pt.slideshare.net/BernardMarr/140228-big-data-slide-share/4-From_the_dawn_of_civilization> Acesso em: 10 out. 2016.

MCAFEE, Andrew; BRYNJOLFSSON, Erik. Big Data: *The Management Revolution*. Harvard Business Review. Publicado em: out. 2012. Disponível em: <https://hbr.org/2012/10/big-data-the-management-revolution> Acesso em: 05 out. 2016.

MILLS, Chris. *The FBI thinks ransomware victims should 'just pay up'*. Gizmodo. Publicado em: out. 2015. Disponível em: <http://gizmodo.com/the-fbi-thinks-ransomware-victims-should-just-pay-up-1738846246> Acesso em: 20 dez. 2017.

MOREY, Timothy; FORBATH, Theodore; SCHOOP Allison. *Dados dos consumidores: modelos de transparência e confiança*. Harvard Business Review Brasil. Publicado em: fev. 2016. Disponível em: <http://hbrbr.com.br/dados-dos-consumidores-modelos-detransparencia-e-confianca/> Acesso em: 01 out. 2016.

MORGADO, Laerte Ferreira. *O cenário internacional de proteção de dados pessoais*. Necessitamos de um Código Brasileiro? Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336> Acesso em: 15 jan. 2017.

OLIVEIRA, Déborah. *Evolução de IoT acende alerta vermelho sobre segurança*. IT Forum 365. Publicado em: fev. 2017. Disponível em: <http://www.itforum365.com.br/conectividade/internet-das-coisas/evolucao-de-iot-acende-alerta-vermelho-sobre-seguranca> Acesso em: 23 fev. 2017.

PAL, Kaushik. *The Impacto of the Internet of Things on Big Data*. DataInformed. Publicado em: set. 2015. Disponível em: <http://data-informed.com/the-impact-of-internet-of-things-on-big-data/> Acesso em: 16 fev. 2017.

PALANZA, Sabrina. *Internet of things, big data e privacy:* la tríade del futuro. Publicado em: out. 2016. Disponível em: <http://www.iai.it/en/pubblicazioni/internet-things-big-data-e-privacy> Acesso em: 16 fev. 2017.

PINHEIRO, Patrícia Peck. *Direito Digital*. 6. ed. São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck et al. *Direito Digital Aplicado 2.0*. 2. ed. São Paulo: Revista dos Tribunais, 2016.

PRESSER, Mirko et al. *Inspirando a Internet das Coisas*. São Paulo: Agns, 2012.

Privacy at the Department of State. US Department of State. Disponível em: <https://www.state.gov/privacy/> Acesso em: 26 jan. 2017.

Projeto de Lei e Outras Proposições. Câmara dos Deputados. Publicado em: jun. 2012. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066> Acesso em: 15 nov. 2016.

PURDY, Mark; DAVARZANI, Ladan; OVANESSOFF, Armen. *Como a Internet das Coisas pode levar à próxima onda de crescimento no Brasil.* Harvard Business Review Brasil. Publicado em: nov. 2015. Disponível em: <http://hbrbr.com.br/como-a-internet-das-coisas-pode-levar-a-proxima-onda-de-crescimento-no-brasil/> Acesso em: 02 out. 2016.

Revista Abinee. São Paulo, n. 86, p. 3-46, junho/2016.

Securerr. *Internet of Things:* More Harm than Good? Disponível em: <http://www.securerr.com/internet-of-things-more-harm-than-good/> Acesso em: 02 out. 2016.

TALBOTT, Amy. *Privacy Laws:* How the US, EU and others protect IoT data (or don't). Publicado em: mar. 2016. Disponível em: <http://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/> Acesso em: 16 fev. 2017.

VAYENA, Effy; GASSER, Urs; WOOD, Alexandra; O´BRIEN, David R., ALTMAN, Micah. *Elements of a New Ethical Framework for Big Data Research*. 72 Wash. & Lee L. Rev. Online 420 (2016). Disponível em: <https://cyber.law.harvard.edu/node/99428> Acesso em: 01 out. 2016.

---

[1] PALANZA, Sabrina. *Internet of things, big data e privacy:* la tríade del futuro. Publicado em: out. 2016. Disponível em: <http://www.iai.it/en/pubblicazioni/internet-things-big-data-e-privacy> Acesso em: 16 fev. 2017.

[2] PINHEIRO, Patrícia Peck. *Direito Digital*. 6. ed. São Paulo: Saraiva, 2016. p. 486.

[3] LEMOS, Ronaldo et al. *Marco Civil da Internet.* São Paulo: Atlas, 2014. p. 739-740.

[4] ENOMURA, Bianca Yuki. *Big Data:* A era dos grandes dados já chegou. Santa Catarina: Superinteressante, 2014. p. 07.

[5] MOREY, Timothy; FORBATH, Theodore; SCHOOP Allison. *Dados dos consumidores: modelos de transparência e confiança.* Harvard Business Review Brasil. Publicado em: fev. 2016. Disponível em: <http://hbrbr.com.br/dados-dos-consumidores-modelos-detransparencia-e-confianca/> Acesso em: 01 out. 2016.

[6] MARR, Bernard. *What is Big Data?* Linkedin. Publicado em: fev. 2014. Disponível em: <http://pt.slideshare.net/BernardMarr/140228-big-data-slide-share/4-From_the_dawn_of_civilization> Acesso em: 10 out. 2016.

[7] BUGHIN, Jacques; CHUI, Michael; MANYIKA, James. *Clouds, big data, and smart assets:* Ten tech-enabled business trends to watch. McKinsey Quartely. Publicado em: ago. 2010. Disponível em: <http://www.mckinsey.com/industries/high-tech/our-insights/clouds-big-data-and-smart-assets-ten-tech-enabled-business-trends-to-watch> Acesso em: 22 out. 2016.

[8] MARR, Bernard. *Big Data:* The 5 Vs. Linkedin. Publicado em: fev. 2014. Disponível em: <http://pt.slideshare.net/BernardMarr/140228-big-data-volume-velocity-variety-varacity-value/8-We_currently_only_see_thebeginnings> Acesso em: 10 out. 2016.

[9] *Cloud Computing* (Computação em Nuvem) é o acesso a recursos computacionais através da internet, ou seja, o usuário pode acessar, compartilhar informações, fazer backup, utilizar-se de serviços e recursos básicos como editor de textos, apresentação de slides, entre outros, tudo através da internet e sem a necessidade de ter algo instalado em seu computador. InfoWester. *O que é Cloud Computing?* Disponível em: <http://www.infowester.com/cloudcomputing.php> Acesso em: 18 nov. 2016.

[10] MCAFEE, Andrew; BRYNJOLFSSON, Erik. *Big Data:* The Management Revolution. Harvard Business Review. Publicado em: out. 2012. Disponível em: <https://hbr.org/2012/10/big-data-the-management-revolution> Acesso em: 05 out. 2016.

[11] ASHTON, Kevin. *That 'Internet of Things' Thing*. RFID Journal. Publicado em: jun. 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986> Acesso em: 20 out. 2016.

[12] ASHTON, Kevin. *That 'Internet of Things' Thing*. RFID Journal. Publicado em: jun. 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986> Acesso em: 20 out. 2016.

[13] Endereço IP (protocolo de internet) é o número de identificação de um dispositivo em uma rede. Ele é composto por 4 (quatro) números de até 3 (três) dígitos e separados por "." (ponto).

[14] CHAVES, Luis Fernando Prado; GOMES, Maria Cecília Oliveira. *Por que a Internet das Coisas revolucionará o Direito Digital?* Carta Capital. Publicado em: fev. 2017. Disponível em: < http://justificando.cartacapital.com.br/2017/02/20/por-que-internet-das-coisas-revolucionara-o-direito-digital/> Acesso em: 21 fev. 2017.

[15] *IoT Mais do que uma* onda. Revista Abinee. São Paulo, n. 86, p. 14, junho/2016.

[16] *Wearable* em tradução literal significa "vestível". Trata-se de tecnologia que se pode vestir, como as pulseiras, relógios, óculos, todos inteligentes, ou seja, contam com processador próprio e podem se integrar aos smartphones com facilidade.

[17] *IoT na visão das empresas*. Revista Abinee. São Paulo, n. 86, p. 23, junho/2016.

[18] *IoT na visão das empresas.* Revista Abinee. São Paulo, n. 86, p. 22, junho/2016.

[19] *Mckinsey*&Company. Disponível em: <http://www.mckinsey.com/global-themes/internet-of-things> Acesso em: 22 nov. 2016.

[20] CENICEROS, Matt. *The Internet of Things Ecosystem:* The Value is Greater than the Sum of its "THINGS". Business 2 community. Publicado em: abr. 2014. Disponível em: <http://www.business2community.com/business-innovation/internet-things-ecosystem-value-greater-sum-things-0829370#Kp8RD2G8kqMFAwbV.97> Acesso em: 01 nov. 2016.

[21] PRESSER, Mirko et al. *Inspirando a Internet das Coisas*. São Paulo: Agns, 2012. p. 02.

[22] PRESSER, Mirko et al. *Inspirando a Internet das Coisas*. São Paulo: Agns, 2012. p. 54.

[23] PRESSER, Mirko et al. *Inspirando a Internet das Coisas*. São Paulo: Agns, 2012. p. 54-55.

[24] DULL, Tamara. *Big data and the Internet of Things:* Two sides of the same coin? SAS Best Practices. Disponível em: <http://www.sas.com/en_sg/insights/articles/big-data/big-data-and-iot-two-sides-of-the-same-coin.html> Acesso em: 02 nov. 2016.

[25] LEONARDI, Marcel. *Tutela e Privacidade na Internet*. São Paulo: Saraiva, 2011. p. 38.

[26] *A IoT no setor público.* Revista Abinee. São Paulo, n. 86, p. 18, junho/2016.

[27] *A IoT no setor público.* Revista Abinee. São Paulo, n. 86, p. 19, junho/2016.

[28] InternetLAB. *Reporta*: Proteção de Dados Pessoais. Disponível em: <http://www.internetlab.org.br/pt/conjuntura/reporta-anteprojeto-de-lei-de-protecao-de-dados-pessoais/> Acesso em: 25 jan. 2017.

[29] InternetLAB. *Big Data:* quais proteções os titulares de dados tem a sua disposição? Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-em-um-mundo-de-big-data-quais-tipos-de-controle-temos-em-relacao-a-nossos-dados/> Acesso em: 25 jan. 2017.

[30] *A IoT no setor público.* Revista Abinee. São Paulo, n. 86, p. 19, junho/2016.

[31] ABRUSIO, Juliana et al. *Marco Civil da Internet:* Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. p. 140-141.

[32] ABRUSIO, Juliana et al. *Marco Civil da Internet:* Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. p. 141.

[33] ABRUSIO, Juliana et al. *Marco Civil da Internet:* Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. p. 141.

[34] PINHEIRO, Patrícia Peck et al. *Direito Digital Aplicado 2.0*. 2. ed. São Paulo: Revista dos Tribunais, 2016. p. 55.

[35] ABRUSIO, Juliana et al. *Marco Civil da Internet:* Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. p. 145.

[36] *Projeto de Lei e Outras Proposições*. Câmara dos Deputados. Publicado em: jun. 2012. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066> Acesso em: 15 nov. 2016.

[37] InternetLAB. *Big Data:* quais proteções os titulares de dados tem a sua disposição? Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-em-um-mundo-de-big-data-quais-tipos-de-controle-temos-em-relacao-a-nossos-dados/> Acesso em: 25 jan. 2017.

[38] InternetLAB. *Big Data:* quais proteções os titulares de dados tem a sua disposição? Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-em-um-mundo-de-big-data-quais-tipos-de-controle-temos-em-relacao-a-nossos-dados/> Acesso em: 25 jan. 2017.

[39] ABRUSIO, Juliana et al. *Marco Civil da Internet:* Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. p. 147-148.

[40] ABRUSIO, Juliana et al. *Marco Civil da Internet:* Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. p. 150.

[41] "Art. 5.º, VI – conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacote de dados".

[42] "Art. 5.º, VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet".

[43] "Art. 5.º, VII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP".

[44] LEMOS, Ronaldo et al. *Marco Civil da Internet.* São Paulo: Atlas, 2014. p. 624-625.

[45] *Diretiva Europeia 2006/24/CE*. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32006L0024> Acesso em: 02 dez. 2016.

[46] LEMOS, Ronaldo et al. *Marco Civil da Internet.* São Paulo: Atlas, 2014. p. 625.

[47] "Artigo 22 – A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet".

[48] "Artigo 23 – Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro".

[49] GLEESON, Mark; JOHNSON, Mark. *Data from the "Internet of Things" is personal data.* Publicado em: out. 2014. Disponível em: <http://www.lexology.com/library/detail.aspx?g=73bef0f2-3184-45db-bad6-6354dafe0889> Acesso em: 16 fev. 2017.

[50] CHAVES, Luis Fernando Prado; GOMES, Maria Cecília Oliveira. *Por que a Internet das Coisas revolucionará o Direito Digital?* Carta Capital. Publicado em: fev. 2017. Disponível em: < http://justificando.cartacapital.com.br/2017/02/20/por-que-internet-das-coisas-revolucionara-o-direito-digital/> Acesso em: 21 fev. 2017.

[51] PINHEIRO, Patrícia Peck et al. *Direito Digital Aplicado 2.0*. 2. ed. São Paulo: Revista dos Tribunais, 2016. p. 88-89.

[52] MILLS, Chris. *The FBI thinks ransomware victims should 'just pay up'*. Gizmodo. Publicado em: out. 2015. Disponível em: <http://gizmodo.com/the-fbi-thinks-ransomware-victims-should-just-pay-up-1738846246> Acesso em: 20 dez. 2017.

[53] NSA, sigla para *National Security Agency*, que significa Agência de Segurança Nacional dos Estados Unidos.

[54] *Five Eyes* Intelligence Alliance é uma aliança inteligente entre Austrália, Canada, Nova Zelândia, Reino Unido e Estados Unidos, na qual estão ligados pelo acordo UKUSA para interceptação de sinais. Disponível em: <https://en.wikipedia.org/wiki/Five_Eyes> Acesso em: 26 fev. 2017.

[55] *Documentos da NSA apontam Dilma Rousseff como alvo de espionagem*. G1. Publicado em: set. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-

dilma-rousseff-como-alvo-de-espionagem.html> Acesso em: 27 fev. 2017.

[56] *Yahoo é processado na Justiça por negligência em ataque hacker*. G1. Publicado em: set. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/09/yahoo-e-processado-na-justica-por-negligencia-em-ataque-hacker.html> Acesso em: 27 fev. 2017.

[57] GOEL, Vindu. *Yahoo! adia venda à Verizon após ataque de hackers*. Folha de São Paulo. Publicado em: jan. 2017. Disponível em: <http://www1.folha.uol.com.br/mercado/2017/01/1852637-yahoo-anuncia-adiamento-de-venda-a-verizon-apos-ataque-de-hackers.shtml> Acesso em: 24 fev. 2017.

[58] OLIVEIRA, Déborah. *Evolução de IoT acende alerta vermelho sobre segurança*. IT Forum 365. Publicado em: fev. 2017. Disponível em: <http://www.itforum365.com.br/conectividade/internet-das-coisas/evolucao-de-iot-acende-alerta-vermelho-sobre-seguranca> Acesso em: 23 fev. 2017.

[59] FONSECA, Mariana. *Site da Alezzia sofre invasão por Anonymous* Brasil. Exame. Publicado em: fev. 2017. Disponível em: <http://exame.abril.com.br/pme/site-da-alezzia-sofre-invasao-pelo-anonymous-brasil/> Acesso em: 23 fev. 2017.

[60] PINHEIRO, Patrícia Peck et al. *Direito Digital Aplicado 2.0*. 2. ed. São Paulo: Revista dos Tribunais, 2016. p. 89.

[61] PINHEIRO, Patrícia Peck. *Direito Digital*. 6. ed. São Paulo: Saraiva, 2016. p. 489-490.

[62] *European Data Protection Supervisor*. Disponível em: <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS> Acesso em: 25 jan. 2017.

[63] *Protecção dos dados pessoais*. EUR-Lex Access to European Union Law. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=URISERV%3Al14012> Acesso em: 20 jan. 2017.

[64] "Artigo 25, 1. Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adoptadas nos termos das outras disposições da presente diretiva, o país terceiro em questão assegurar um nível de proteção adequado."

[65] "Artigo 28, 1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adoptadas pelos Estados-membros nos termos da presente diretiva. Essas autoridades exercerão com total independência as funções que lhes forem atribuídas."

[66] MORGADO, Laerte Ferreira. *O cenário internacional de proteção de dados pessoais*. Necessitamos de um Código Brasileiro? Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336> Acesso em: 15 jan. 2017.

[67] TALBOTT, Amy. *Privacy Laws:* How the US, EU and others protect IoT data (or don't). Publicado em: mar. 2016. Disponível em: <http://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/> Acesso em: 16 fev. 2017.

[68] *Privacy at the Department of State*. US Department of State. Disponível em: <https://www.state.gov/privacy/> Acesso em: 26 jan. 2017.

[69] *Safe Harbor*, em tradução literal significa Porto Seguro.

[70] *Welcome to the US-EU & US-Swiss Safe Harbor Framework.* Companies Export. Publicado em: jan. 2017. Disponível em: <http://2016.export.gov/safeharbor/> Acesso em: 14 fev. 2017.

[71] "EU-US Privacy Shield", em tradução literal significa "Escudo de Proteção Estados Unidos-União Europeia".

[72] "Swiss-US Privacy Shield", em tradução literal significa "Escudo de Proteção Suíça-Estados Unidos".

[73] *Welcome to the US-EU & US-Swiss Safe Harbor Framework.* Companies Export. Publicado em: jan. 2017. Disponível em: <http://2016.export.gov/safeharbor/> Acesso em: 14 fev. 2017.

[74] *Israel's data protection laws given EU approval*. The Register. Publicado em: fev. 2011. Disponível em: <https://www.theregister.co.uk/2011/02/08/israel_data_protection_law_eu/> Acesso em: 16 fev. 2017.

[75] *Data protection laws of the world*. The Venture Alley. Publicado em: mar. 2015. Disponível em: <http://www.lexology.com/library/detail.aspx?g=1a6e9e6c-affc-4e40-9270-7256ac9cf2a4> Acesso em: 16 fev. 2017. p. 321.

[76] TALBOTT, Amy. *Privacy Laws:* How the US, EU and others protect IoT data (or don't). Publicado em: mar. 2016. Disponível em: <http://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/> Acesso em: 16 fev. 2017.

[77] MORGADO, Laerte Ferreira. *O cenário internacional de proteção de dados pessoais.* Necessitamos de um Código Brasileiro? Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336> Acesso em: 15 jan. 2017.

[78] TALBOTT, Amy. *Privacy Laws:* How the US, EU and others protect IoT data (or don't). Publicado em: mar. 2016. Disponível em: <http://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/> Acesso em: 16 fev. 2017.

[79] MORGADO, Laerte Ferreira. *O cenário internacional de proteção de dados pessoais.* Necessitamos de um Código Brasileiro? Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336> Acesso em: 15 jan. 2017.