A NECESSIDADE DE CRIAÇÃO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS DIANTE DA IMPLEMENTAÇÃO DA IOT

Tiffany Cunha de Jesus

Advogada (OAB/PR 61.411) fundadora do TJ Advocacia, especialista em Direito Digital e Compliance, com nano degree em Direito Aplicado para Startups, escritora e autora de artigos jurídicos e do livro "A Natureza Jurídica do Dispositivo Dotado de Inteligência Artificial Autônoma" pela editora Instituto Memória, palestrante nos temas de Direito e Tecnologia, e coordenadora do projeto voluntário "Cidadania Digital".

Resumo: O presente trabalho centra-se em analisar a necessidade da criação da Lei de Proteção de Dados Pessoais no contexto de implementação da Internet das Coisas.

Este artigo apresenta uma investigação teórica de Direito Digital e Compliance voltado aos aparatos tecnológicos aos quais estão acoplados sensores que coletam, armazenam, tratam, compartilham, entre outros, dados

pessoais, objetivando explicar e demonstrar a relevância e a necessidade da promulgação do texto legal.

Palavras-chave: Internet das Coisas, Privacy by design, Proteção de Dados e Privacidade.

1. Introdução

Com o advento da "Era da Tecnologia" após a segunda metade do século XX, em especial após a Segunda Guerra Mundial com a entrada da Guerra Fria e a batalha por aparatos tecnológicos mais modernos e avançados entre os dois países que polarizaram essa discussão, Estados Unidos e Rússia, os avanços tecnológicos foram contínuos e influenciaram toda a sociedade em todas suas áreas de atuação e influência, além da política, a educação, a família, a saúde, etc.

A chamada "Era da Tecnologia" está intimamente ligada às evoluções tecnológicas biométricas e digitais a partir da segunda metade do século XX, conforme já referido, através da criação e utilização da internet. E nessa era tecnológica há um fenômeno que se manifesta fortemente: o da "Internet das Coisas", pois a proliferação de dispositivos biométricos e digitais modificou a sociedade e sua forma de interação entre si e com o mundo externo a partir da utilização de aparatos tecnológicos que se conectam entre pessoas e entre si.

Apesar disso, para que aparatos tecnológicos se conectem entre pessoas e entre si, há a necessidade de cole-

ta de dados dos usuários desses dispositivos tecnológicos. Por exemplo, uma geladeira com sensores que coleta dados diários acerca da nutrição e alimentação de uma família e envia informações para o celular do responsável pelas compras de mercado da casa que está faltando o leite das crianças e o queijo do café da manhã.

A empresa que coleta e armazena os dados da geladeira tem acesso a informações sensíveis a respeito dos indivíduos dessa casa mencionada no parágrafo acima, sobre quantos são os membros da família, quem faz as compras, quantas vezes ao mês vai ao mercado, quais produtos consome, entre outros. É importante que esses dados estejam seguros e não sejam compartilhados sem anuência e concordância dos titulares dos dados, bem como é importante que os dados estejam seguros e não vazem. E quantas outras recomendações deveriam ser feitas para proteção dos dados e garantia do direito a privacidade dessa família que tem em casa essa geladeira.

Nesse contexto, imagine-se que fora a geladeira, o aquecimento da casa, a televisão, o GPS, as câmeras de segurança, e outros, também coletam dados sensíveis como esses dessa família, e aí está configurada em uma casa apenas o fenômeno da Internet das Coisas e da necessidade da proteção de dados.

Neste artigo buscaremos demonstrar a imperatividade de uma boa lei de proteção de dados pessoais diante da implementação da Internet das Coisas na so-

ciedade, em todos os seus níveis, bem como, nos valeremos da Lei de Proteção de Dados brasileira que foi sancionada no dia 14 de agosto de 2018 e que está em período de vacância legal e a ela faremos comentários para ilustrar melhor este trabalho.

2. Sobre a internet das coisas

Kevin Ashton, cofundador e diretor executivo do Auto-ID Center no MIT (Massachusetts/ EUA) mencionou o termo "Internet das Coisas" (IOT) pela primeira vez em 1999 em uma apresentação que fez para a empresa Procter & Gamble. Observe este trecho da sua fala no qual explica a importância e relevância do fenômeno da Internet das Coisas:

> Atualmente, computadores - e portanto, a internet - são quase totalmente dependentes de seres humanos para obter informação. Quase todos os 50 petabytes (um petabyte é 1,024 de terabytes) de dados disponíveis na internet foram captados e criados por humanos digitando, apertando um botão de gravar, tirando uma foto ou scaneando um rótulo. O problema é que pessoas possuem tempo, atenção e precisão limitados - o que significa que eles não são muito bons em captar dados sobre as coisas no mundo real. Se tivéssemos computadores que soubessem tudo que há para saber sobre as coisas - usando dados que juntaram sem qualquer ajuda de nós - nós seriamos capazes de acompanhar e contar todas as coisas e grandemente reduzir desperdício, perda e custo. Nós saberíamos

> quando as coisas precisam ser trocadas, consertadas ou fazer recall e se as coisas estão frescas ou ultrapassaram sua validade.[1]

Neste contexto encontramos a aplicabilidade da Internet das Coisas, mas não sua definição. Eduardo Magrani, estudioso brasileiro no tema em questão, explicou em sua tese de doutorado que a definição de IOT é um tema divergente, e que por isso não possui uma conceituação única, devendo, apesar disso, ser considerado como:

> …um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. O que todas as definições de IOT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade.[2]

Em outras palavras, a IOT é a utilização de objetos que estão conectados a outros objetos ou até mesmo pessoas, nos quais há um ou vários sensores acoplados que coletam, armazenam e fazem tratamento de dados.

---

1 ROUSE, Margaret. IOT Agenda: Internet of Things. Retirado de: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things--IoT> em 23 de junho de 2018.

2 Magrani, Eduardo. "A internet das coisas". Rio de Janeiro: FGV Editora, 2018, p. 21 e 22 .Retirado de: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf?sequence=1&isAllowed=y> em 18 de agosto de 2018.

Para facilitar a visualização do conceito trago o exemplo do "*Nest Learning Thermostat*"[3], que se trata de um termostato inteligente, controlado através de smartphone por meio de um aplicativo. Este aparato é conectado na parede da residência e aprende a temperatura que o usuário prefere ao longo do dia, se mais quente a noite e mais ameno pela manhã, por exemplo. Ainda, o sensor acoplado ao termostato permite saber quando o usuário está em casa e quando não está, desligando o aparelho que só volta a funcionar quando o usuário está próximo de casa, pois o termostato também está conectado ao smartphone para saber a precisa localização do usuário e iniciar funcionamento para que no momento em que o usuário chega em sua residência a temperatura esteja perfeita.

O aplicativo do termostato mostra ao usuário quanto de energia é gasta diariamente, de maneira que se pode controlar quando está sendo usada energia desnecessária e programar-se para economizar. E, ainda, para ajudar o usuário que busca economizar energia, com base nos dados que o termostato apresenta, o aparelho apresenta em sua interface uma folha, indicando sustentabilidade, todas as vezes que a alteração de temperatura economizou energia.

Deste modo, verifica-se que o termostato detém informações relevantes de não apenas como o usuário quer

3 Nest Learning Thermostat. Retirado de <https://nest.com/thermostats/nest-learning-thermostat/overview/> em 24 de junho de 2018.

a temperatura da sua casa, mas também quando o usuário está em casa ou não, e a que horas. Estas informações são bastante pessoais e se expostas podem significar a violação da privacidade do usuário.

Em maior escala, temos o fenômeno das "*Smart Cities*" (Cidades Inteligentes), na qual, por exemplo, a segurança pública se vale de câmeras com a tecnologia de fazer reconhecimento facial e monitorar as atividades dos cidadãos, podendo identificar qualquer indivíduo que seja de seu interesse. A princípio é bastante benéfica essa medida para buscar pessoas que estão fugindo de responsabilidades perante o Estado, todavia, imagine que todas essas imagens estão sendo armazenadas em registros internos e, potencialmente, podem ser verificadas por qualquer indivíduo autorizado, imagens suas transitando pelas ruas da sua cidade que informam exatamente onde você está, quando e com quem.

A partir disso entendemos na prática a aplicação da Internet das Coisas e que é algo notadamente benéfico, sustentável, prático, entre outras qualidades. Todavia, isso apenas se torna possível em razão da coleta, armazenamento e tratamento de dados que o dispositivo captura, e neste contexto há o contraponto do perigo de vulnerabilidade na proteção dos dados coletados por estes dispositivos. Imagine a hipótese de uma invasão ilícita nos sistema mencionados do termostato ou da segurança pública, as informações são bastante sensíveis e inferem em invasão de privacidade de um indivíduo. Por outro lado, há informações que não

são aptas a colocar em risco a segurança ou a privacidade do usuário, pois não o individualizam.

Neste viés, há, portanto, a preocupação com a privacidade e proteção de dados a fim de proteger o usuário, a coletividade ou qualquer outro bem jurídico que possa ser visualizado e que mereça ser tutelado. O ponto é que informações sempre foram coletadas pelo Estado, por exemplo, a fim de monitorar atividades, não apenas para fins de segurança pública, mas também e inclusive para efetivar serviços públicos. Por exemplo, identificar em qual região de um bairro construir mais uma creche, o mais eficiente seria construi-la em área menos movimentada e talvez mais próxima a fábrica onde a maior parte das pessoas trabalha. São informações que individualizam e identificam indivíduos e suas famílias, e para a sua segurança já há legislação que discorra sobre a proteção das suas informações coletadas, armazenadas e tratadas pelo Estado.

Apesar disso, a IOT é um fenômeno em que as informações são coletadas, armazenadas e tratadas não por humanos, conforme o discurso inicial deste artigo feito por Kevin Ashton, e a tecnologia digital coleta dados com muito mais rapidez e os trata com a mesma velocidade, bem como, muito provavelmente, envia esses dados para armazenamento em alguma outra base de dados que não seja em seu depósito próprio, mas sim um de empresa terceirizada que talvez nem mesmo esteja localizada no mesmo país que o do usuário ou talvez nem mesmo no país da empresa que presta o serviço contratado. E na ver-

dade, de uma forma geral, é exatamente assim que a IOT funciona, o usuário fornece seu dado a um dispositivo, como o termostato, aqui no Brasil, e a empresa que armazena o mesmo se localiza nos Estados Unidos. E para sermos bastante sinceros, nem mesmo sabemos por certo quais informações estão sendo coletadas ou para quem estão sendo direcionadas. E, ainda, em caso de conflito de interesses, qual direito se aplica ao caso? O americano, porque é onde estão armazenados os dados, ou o brasileiro, porque os titular dos dados está no Brasil?

Um outro exemplo é o do monitor de batimentos cardíacos portátil, como o "*Alive Cor*", o usuário pode conectar o dispositivo com seu relógio inteligente, o qual monitora os batimentos cardíacos e os grava no aplicativo respectivo, indicando se há algo de errado com os batimentos e enviando um relatório de imediato, o qual pode ser direcionado ao médico do usuário pelo link direto de e-mail que aparece na interface do aplicativo. O aplicativo é inteligente e aprende com a gravação dos seus batimentos cardíacos, de maneira que se detecta durante o dia que seu batimento cardíaco naquele horário é incompatível com o nível de atividade indicado em seu relógio, uma notificação é enviada para fazer o teste do aplicativo e verificar a normalidade ou não dos batimentos.

Essas são informações sensíveis, sobre a saúde do usuário, imagine se não há limites para a utilização desses dados pela empresa que os coleta, armazena e trata, e os vende para terceiros, como por exemplo, para uma empre-

sa de plano de saúde. Talvez com base nos dados recebidos a empresa não tenha interesse em ter em seu quadro de clientes uma pessoa que tenha predisposição para doenças cardiovasculares. Isso notadamente fere os direitos do usuário, que não autorizou a venda dos seus dados e não pode afiliar-se a um plano de saúde em razão da informação que lhe foi passada ilicitamente por terceiros.

Deste modo, verifica-se a necessidade de tutela desse direito fundamental a privacidade que se manifesta na forma de proteção de dados. Seja pelo Direito, seja por órgão regulador, é imperiosa a intervenção de um terceiro para que se limite a atuação das empresas que se valem da tecnologia da IOT frente a uma possível violação de direitos.

3. A necessidade da lei de proteção de dados pessoais

Verifica-se que a necessidade da criação de lei de proteção de dados pessoais é imperiosa pela proteção a privacidade e intimidade do titular dos dados, entretanto, talvez alguém poderia dizer que não se importa em comercializar seus dados e receber vantagem econômica por isso, ou, ainda, em ceder seus dados e obter contraprestação em serviços que tornem suas atividades mais sustentáveis, produtivas e econômicas, desde que (e aqui entra o argumento mais relevante acerca deste tema) haja consentimento.

Todavia, os termos e condições de uso dos produtos e serviços que se categorizam como IOT, pela maneira que são redigidos e direcionados ao usuário, não permitem que

os usuários, ou "titular de dados", estejam cientes de que maneira serão acessados, coletados, armazenados e manipulados os seus dados, aliás, não há nem mesmo a consciência de que aquele documento é um contrato.

A carência de proteção de dados pessoais, seja pela ausência de consentimento do titular de dados sobre a própria coleta e armazenamento dos dados, em um primeiro momento, e, depois, sobre a utilização e manipulação dos seus dados em um segundo momento, evidentemente não está sendo suprida pelo consentimento tácito com um clique ao final de tantas páginas com letras pequenas de termos e condições de uso.

O que é interessante acerca deste tema é a defesa dos que coletam e armazenam dados com a justificativa do consentimento pelo clique. A máxima do consentimento é no sentido de que "*Não consente? Não utiliza o produto*." ("*E fica excluído da sociedade*.", essa parte não é dita, mas é subentendida). Este argumento traz o mesmo princípio de qualquer abuso, inclusive de autoridade, que possa existir, tal como, abuso sexual, no qual a vítima se cala porque não teria onde morar sem o arrimo do agressor, ou como um filho adolescente que concorda em se comportar em festa de família sob pena de ficar sem o seu telefone celular, ou, ainda, por que não, a hipótese de um policial escolher um cidadão para ser revistado sob pena dele ser preso se resistir. É difícil de acreditar que consentimento livre seja esse sob algum tipo de condição.

Neste sentido, ouso dizer que atualmente o consentimento de termos e condições de uso de produtos e serviços que se configuram como IOT não é totalmente livre e consciente, pois o titular de dados não tem conhecimento da coleta, armazenamento e manipulação dos seus dados, e, pior, desconhece completamente os riscos do mau uso, e nesse último, é que se encontra o real problema do consentimento viciado: a ausência de educação digital.

Há quem diga que não se importa se o governo ou empresas da iniciativa privada que visam vender seus produtos, tenham acesso a seus dados pessoais, e nisto incluindo conversas privadas em aplicativos de relacionamento, sob o argumento de que "*não estou fazendo nada de errado, não tenho nada a esconder*". O interessante deste argumento é que a partir dele há a presunção de que há pessoas más e pessoas boas, afinal, somente pessoas com algo para esconder é que estariam preocupadas por sua privacidade. Mas sob este prisma, vale ressaltar que quando estão sendo observadas, as pessoas tendem a agir da maneira que é esperado delas (por exemplo, experimente trabalhar na mesa ao lado do seu chefe).

Passando para um pensamento filosófico acerca do tema privacidade e proteção de dados, é interessante ressaltar a teoria panóptica idealizada por Jeremy Bentham (1748 - 1832, Londres, Reino Unido) popularizada por Michel Foucault. Brevemente explicando, o panóptico é uma estrutura arquitetônica projetada para prisões que permitiria a um único vigilante observar todos os prisio-

neiros, sem que esses tenham o conhecimento de quando estão sendo vigiados ou não, que inclusive proporcionava a economia de contratação de autoridades policiais[4]. A ideia central era de que o medo de não saber quando estão sendo observados os faça agir da maneira que deles era esperada. O filósofo mencionou na época da criação da sua estrutura que essa era ideal para qualquer outro lugar cuja base fosse a subordinação e controle, tal como fábricas, hospitais e escolas.

A teoria do panóptico amadurecida por Michel Foucault afirma que a sociedade atual reflete esse sistema, pois a vigilância em massa cria tamanho aprisionamento mental e impõe comportamentos nos cidadãos tendo por base o temor de punição[5]. Medida essa que se demonstra, tal como Bentham previu, mais econômica e eficaz para controle social e imposição de normas de comportamento.

Este panorama não necessariamente precisa estar somente na seara governamental, mas também na privada, com dispositivos conectados a pessoas e a internet, para controle parental. Sob o argumento de ordem, proteção e segurança, o mercado tem fornecido produtos e serviços a pais e responsáveis que visam o controle dos seus filhos. E nesta seara fica o questionamento de qual é o limite de

4 Pensar Contemporâneo: A teoria da panóptica de Michel Foucault. Retirado de: <https://www.pensarcontemporaneo.com/teoria-da-panoptica-de-michel-foucault/> em 25 de junho de 2018.

5 Surveillance. Retirado de: <http://studymore.org.uk/ybenfou.htm> em 25 de junho de 2018.

controle parental de maneira a não afetar a expressão individual de um ser humano em fase de desenvolvimento e conhecimento pessoal.

Quando tratamos do tema de privacidade e proteção de dados é impossível não mencionar o famoso livro de George Orwell, "1984", no qual, ao meu sentir, o temor daquela população não era o de estar sendo monitorada o tempo todo, mas a possibilidade de sê-lo. E é o que passa atualmente sem a devida regulação para proteção de dados pessoais.

Saindo novamente da esfera filosófica, tem-se na forma prática que seus dados pessoais são informações privadas e o titular de dados como titular dele tem a prerrogativa de dispor deles ou não, desde que de maneira consciente, o que já ressaltamos que não existe porque usuário nenhum lê os termos e condições de uso, e tampouco tem conhecimento de que aquele documento tem força contratual. Desta feita, qual a solução para que empresas não coletem, armazenem, tratem e, inclusive, disponham de dados pessoais de maneira indevida?

Por evidente que um bom brasileiro, tendo enraizado dentro dos seus padrões éticos e morais a *common law* e a hegemonia da lei escrita, sustenta que a grande solução seria uma legislação no tema. E sim, de fato a sanção da Lei de Proteção de Dados Pessoais foi de absoluta relevância e importância, de vários modos uma boa lei nos dá sólidas diretrizes.

Todavia, antes que se trate diretamente da Lei de Proteção de Dados Pessoais recém sancionada no Brasil, na data de 14 de agosto de 2018, passa-se a analisar acerca do escopo do tema "dados pessoais".

3.1 O que são dados pessoais

Para melhor se falar da necessidade de criação da lei específica de proteção de dados pessoais, primeiramente passa-se a tratar o que são esses dados.

A exposição de motivos do Regulamento Geral de Proteção de Dados europeu, que entrou em vigor em meio de 2018, de forma magistral explica a necessidade de uma legislação específica sobre o tema de proteção de dados, observe alguns trechos:

> A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

> Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.[6]

Verifica-se que o texto menciona "dados pessoais", o que quer dizer que não apenas são relevantes e importantes os dados, mas aqueles que são intrínsecos a um usuário e que podem identifica-lo e individualiza-lo, tal como a freqüência dos seus batimentos cardíacos ou o horário que está em sua casa ou não. Outros dados, a depender do contexto, talvez não sejam relevantes, vez que não violam ou potencialmente não podem vir a violar a privacidade de um indivíduo. Deste modo, passamos a analisar o que deve ser objeto de proteção pela legislação específica de proteção de dados.

Entende-se por "dados pessoais" as informações que individualizam ou são aptas a individualizar um indivíduo, isto é, "*conjunto de informações distintas que podem levar à identificação de uma determinada pessoa*"[7].

---

6 Reforma de 2018 das regras de proteção de dados da UE. Retirado de: <https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt> em 19 de Agosto de 2018.

7 Comissão Europeia. Legislação. Proteção de Dados. O que são dados

No Brasil, no plano legislativo, a Lei de Acesso a Informação (lei n° 12.527/2011) em seu artigo 4° identifica como "informação pessoal" aquela que está "*relacionada* à *pessoa natural identificada ou identificável*". O Marco Civil da Internet (lei n° 12.965/2014) apenas se referiu a dados pessoais, sem definir o que entende por isso, de maneira que o Decreto Presidencial n° 8.771/2016), publicado para regulamentar alguns aspectos do Marco Civil da Internet, em seu artigo 14 considerou como dado pessoal aquele "*dado relacionado* à *pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa*".

Por fim, ainda no Brasil, a recém sancionada Lei n° 13.709/2018, que dispõe sobre a proteção de dados e altera o Marco Civil da Internet, prevê no seu artigo 5°, inciso I que dado pessoal é "*informação relacionada à pessoa natural identificada ou identificável*"[8]. Interessante mencionar, ainda, que o inciso II do artigo 5° diferencia dado pessoal de dado sensível:

> …dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados

pessoais. Retirado de: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt> em 23 de junho de 2018.

8 Senado Federal. Projeto de Lei n. 53/2018. Retirado de: <https://legis.senado.leg.br/sdleg-getter/documentodm=7738646&ts=1529700780674&disposition=inline&ts=1529700780674> em 23 de junho de 2017.

> referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Para facilitar a visualização do que isso representa no âmbito virtual trago o seguinte exemplo: faça a busca na rede se valendo dos seguintes dados "Tiffany, advogada, Curitiba". Em um universo de mais de 7 bilhões de pessoas existentes no mundo, você muito provavelmente encontrará apenas uma pessoa com apenas essas três informações, que são nome, profissão e cidade.

Até que entre em vigor a Lei de Proteção de Dados Pessoais, atualmente, a proteção de dados obtidos de forma virtual é disciplinada genericamente pelo Marco Civil da Internet (Lei n. 12.965/2014) que é a lei que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, confira-se: a) O artigo 7º estabelece que ao usuário da internet é assegurado o direito de somente fornecer seus dados pessoais com consentimento livre, expresso e informado, e mediante apresentação de informações claras sobre a coleta, uso, armazenamento dos dados. O mencionado artigo também assegura a exclusão definitiva dos dados do usuário mediante requerimento quando do término da relação entre as partes; b) Ainda, o artigo 10 da Lei n. 12.965/2014 estipula que a disponibilização de dados pessoais somente pode ser fornecida mediante ordem judicial; c) E, por fim, o artigo 11 determina que os provedores de conexão e aplicações de internet deve-

rão prestar informações quanto ao cumprimento da legislação brasileira referente a coleta, armazenamento e tratamento de dados quanto ao respeito a privacidade e sigilo de comunicações.

4. A lei de proteção de dados pessoais brasileira

Conforme dito, a lei brasileira de proteção de dados pessoais foi sancionada no dia 14 de agosto de 2018 e aguarda período de vacância legal de 18 (dezoito meses), e explicada sua relevância, necessidade e importância, passa-se a analisar os pontos mais relevantes.

4.1 Aplicação da lei

A Lei n° 13.709/2018 que atualmente está no período de vacância:

> …dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.[9]

A lei tem aplicação a qualquer operação de tratamento de dados, independente do meio ou de onde estejam localizados os dados, desde que:

9 Senado Federal. Projeto de lei n. 53/2018. Retirado de: <https://legis.senado.leg.br/sdleg-getter/documentodm=7761294&ts=1532357490441&disposition=inline&ts=1532357490441> em 25 de junho de 2018.

> …I – a operação de tratamento seja realizada no território nacional; II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.[10]

De maneira que não se aplica a tratamento de dados que sejam realizados por pessoa natural para fins particulares e não econômicos, ou fins jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional, de segurança do Estado e de atividades de investigação e repressão de infrações penais, entre outras exceções.

Ou seja, a lei se aplicada a empresas que: a) têm estabelecimento no Brasil; b) oferecem serviços no Brasil; c) coletam e tratam dados pessoais de pessoas localizadas no país, de maneira que não é relevante o país sede da empresa, a localização dos dados e tampouco a nacionalidade do titular de dados.

4.2 Os princípios da lei de proteção de dados

Em seu artigo 6˚ a lei prevê que os princípios que imperam no processo de coleta e tratamento de dados são os da finalidade, adequação e necessidade, isto é:

> …somente pode ser requerido e mantido um dado em certa base conforme a finalidade a que ele

10 Ibidem.

> presta”[11]: “I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com esses propósitos; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com a utilização de dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.

Estes princípios se materializam em previsões como no artigo 15 na qual está previsto o acesso aos dados e a finalidade e forma de tratamento dos mesmos pelo titular.

Nesse sentido, temos, por exemplo, o termostato mencionado no início do artigo que precisa colher o dado referente a temperatura ambiente, o momento do dia (se manhã ou noite, por exemplo) e quando o usuário está em casa ou não, a fim de que tome decisões “inteligentes” com base nos dados armazenados, sem isso o dispositivo perde sua finalidade principal que é a de ser “inteligente”. Apesar disso, se o dispositivo colher dados sobre a sexualidade do usuário talvez seja algo desnecessário, e não primordial para o seu funcionamento, perdendo a finalidade na coleta desse dado. Mas se o termostato combinar o fato de ser um

11 Sampaio, Rodrigo Vaz. Preocupação com Dados nas Redes Sociais e Autodeterminação Informacional. Retirado de: <http://blogs.correiobraziliense.com.br/aricunha/urgente-preocupacao-com-protecao-de-dados-nas-redes-sociais-e-autodeterminacao-informacional/> em 25 de Junho de 2018.

usuário do sexo feminino com a idade de mais de 50 anos, quem sabe possa indicar qual a temperatura ideal para uma pessoa que atravessa a menopausa e apresentar um relatório de aumento e diminuição de temperatura que a ajude com um reporte médico.

4.3 Sobre alguns direitos previstos na lei

Os direitos que a lei vem garantir para o titular de dados são vários e estão elencados no artigo 8°[12] da lei alguns deles:

> Art. 8º O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I – confirmação da existência de tratamento;
>
> II – acesso aos dados;
>
> III – correção de dados incompletos, inexatos ou desatualizados;
>
> IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
>
> V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

12 Senado Federal. Projeto de lei n. 53/2018. Retirado de: <https://legis.senado.leg.br/sdleg-getter/documentodm=7761294&ts=1532357490441&-disposition=inline&ts=1532357490441> em 25 de junho de 2018.

> VI – eliminação dos dados tratados com o seu consentimento, exceto nas hipóteses previstas no art. 22 desta Lei;
>
> VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
>
> VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
>
> IX – revogação do consentimento, nos termos do § 5o do art. 14 desta Lei.

A normatização do "Direito ao Esquecimento" com a possibilidade de anonimização dos dados para preservar a imagem de uma pessoa jurídica ou física, como por exemplo, retirar uma informação do banco de dados do Google, é de aplicação bastante relativa e debatida nos tribunais europeus e também no brasileiro, mesmo antes da lei ser sancionada, vez que manifesta conflito de princípios e garantias constitucionais. Sobre o tema a Ministra Cármen Lúcia do Supremo Tribunal Federal:

> …o que é a memória de alguém, que precisa de ser resguardada e não pode ser discutida, e o que não pode ser guardado porque constitui não memória individual, mas memória coletiva (…) Eu acredito que nós encontraremos, com toda a certeza, o equilíbrio que é virtuoso para deixar que as liberdades garantam a dignidade, mas que a liberdade de um não se sobreponha à de todos os outros, de tal maneira que nós não tenhamos mais condições de saber qual é

> a nossa história, o nosso passado, para saber como queremos construir nosso futuro.[13]

Interessante mencionar que o artigo 22 prevê que com o término da finalidade do tratamento de dados, os mesmos serão eliminados, sendo autorizada sua conservação apenas para:

> I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.[14]

Um detalhe importante que vale rapidamente ser mencionado é sobre transferência internacional de dados é, alem do consentimento sobre isso, que o país ou organismos intencionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na lei em questão.

4.4 Consentimento

No que se refere ao consentimento, a lei trouxe em seu artigo 5°, inciso XIV a definição do que entende por isso,

13 Palestra da presidente do STF abre fórum sobre direito ao esquecimento e proteção à memória. Retirado de: <http://stf.jus.br/portal/cms/verNoticiaDetalhe.aspidConteudo=353151> em 19 de Agosto de 2018.

14 Senado Federal. Projeto de lei n. 53/2018. Retirado de <https://legis.senado.leg.br/sdleg-getter/documentodm=7761294&ts=1532357490441&disposition=inline&ts=1532357490441> em 25 de junho de 2018.

observe-se: "*consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para finalidade determinada*"[15]. Deste modo, somente é autorizado pela lei o tratamento de dados com o consentimento do titular, seja por escrito ou por alguma maneira que demonstre a não equívoca manifestação de vontade, e em sendo por contrato, devem estar destacadas de alguma forma essas cláusulas, a fim de que seja percebida essa disposição pelo titular[16]. Isto é, a lei aniquilou a realidade atual de coleta e tratamento de dados que é de forma genérica.

Como exemplo menciono os termos e condições de uso da IBM[17], ao se cadastrar no site da empresa temos que ler e concordar com dois termos separados, o de condições de uso e antes desse um específico (e bem longo e detalhado) sobre a coleta, uso, armazenamento de dados, entre outros.

4.5 Personas criadas pela lei

A lei prevê a figura do operador, a pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador, que é a quem compete as decisões

15 Senado Federal. Projeto de lei n. 53/2018. Retirado de <https://legis.senado.leg.br/sdleg-getter/documentodm=7761294&ts=1532357490441&disposition=inline&ts=1532357490441> em 25 de junho de 2018.

16 Artigo 14 da lei 13.709/2018.

17 Confira aqui nesse site: <www.ibm.com/privacy/br/pt/?lnk=flg-priv-usen?lnk=flg> em 19 de agosto de 2018.

referentes ao tratamento de dados pessoais, a saber, os agentes de tratamento (artigo 42). E a essas pessoas atribui a responsabilidade objetiva, pois

> …só não serão responsabilizados quando provarem: I – que não realizaram o tratamento de dados pessoais que lhes é atribuído; II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.[18]

Sendo solidária a responsabilidade do operador com a do controlador quando, respectivamente, não tiver seguido as instruções lícitas do controlador ou estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados. Apesar disso há a previsão de inversão do ônus da prova quando no caso concreto o juízo verificar hipossuficiência do titular de dados[19].

Ainda discorrendo sobre as personas trazidas pela legislação, o artigo 46 traz a pessoa da autoridade nacional, o qual "*poderá dispor sobre padrões técnicos mínimos para fins do disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia,*

18 Senado Federal. Projeto de lei n. 53/2018. Retirado de <https://legis.senado.leg.br/sdleg-getter/documentodm=7761294&ts=1532357490441&disposition=inline&ts=1532357490441> em 25 de junho de 2018.

19 Ibidem.

especialmente no caso de dados pessoais sensíveis"[20]. Todavia, a criação dessa Autoridade Nacional de Proteção de Dados (ANPD) foi vetada.

O Presidente Michel Temer vetou a criação do ANPD e justificou pelo suposto "vício de iniciativa", ou seja, por se tratar de agência reguladora, deveria ser criada pelo Poder Executivo e não pelo Congresso. O Presidente disse que vai se ocupar da criação da agência e que o texto continuará igual, suprindo o vício.

De todo modo, vale mencionar que a Autoridade Nacional de Proteção de Dados (ANPD) será "*integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça*"[21], composta pelo Conselho Diretor, como órgão máximo, e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além das unidades especializadas para a aplicação da lei[22].

4.6 Penalidades pelo não cumprimento da lei

Aos agentes de tratamento de dados quando responsabilizados administrativamente, após procedimento administrativo devido, podem ter como sanção, entre outros: a) suspensão parcial ou total do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6

20 Ibidem.

21 Ibidem.

22 Ibidem.

(seis) meses, prorrogável por igual período até a regularização da atividade de tratamento pelo controlador; b) multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, segundo artigo 52 da lei n. 13.709/2018.

5. Desafios legais e IoT

Entretanto, apesar da legislação ser um excelente norte, a educação digital continua sendo a maior porta para mudança de qualquer parâmetro de utilização de produtos e contratação de serviços. Imagine-se que os consumidores deixam de adquirir determinado produto em razão da vulnerabilidade dos seus dados coletados, por óbvio a empresa será estimulada a mudar sua política relativa a dados para a venda do seu produto. Isto é, com isso o consumidor educou o mercado, tal como as gomas de mascar com açúcar que perderam drasticamente seu mercado para as gomas sem açúcar e mais benéficas para os dentes, e com isso quero dizer que educando o consumidor é sim possível que esse eduque o mercado.

Da mesma forma a empresa e o mercado como um todo, também devem ser educados para que trabalhem a favor do consumidor, com transparência e tornando o consentimento de fato livre, para que a escolha acerca do uso ou não do produto dependa da qualidade e funcionalidade

desse, e não de abuso da empresa com relação a informações que o sensor acoplado no hardware possibilite coletar e usar como moeda de troca por outros produtos e serviços que não atingem o consumidor final.

Dito isso, para além da educação do consumidor e da empresa, tem-se que a legislação que é um fato iminente e por enquanto a solução mais imperativa que se encontra para o problema de privacidade e proteção de dados. E para que tenhamos a privacidade respeitada e nossos dados protegidos, conclui-se que a lei deve seguir os seguintes critérios: a) Transparência: de forma que o consumidor saiba exatamente quais dados estão sendo coletados, armazenados e tratados e qual a finalidade; b) Finalidade: como pilar o princípio da finalidade, de maneira que sejam coletados apenas dados referentes e inerentes ao serviço ou ao produto; b) Categorização: que seja mantida a categorização mínima entre dados pessoais e dados sensíveis[23], para que a tutela de dados que sejam aptos a individualizar ou a tornar o indivíduo alvo de preconceito ou de tratamento diferenciado em razão da sua condição social, econômica, física, entre outros, seja reforçada; c) Consentimento: que abarca todas as diretrizes anteriores, devendo o consumidor ter conhecimento acerca dos dados coletados, sua finalidade e qual a destinação dos mesmos, para que o consentimento seja de fato livre e consciente, e que essa informação seja cada vez mais simples e acessível, pensando muito mais na experiência do usuário (*user experience*) com relação ao seus direitos, do que transformar

23 Artigo 5°, inciso II da lei n. 13.709/2018.

a leitura dos termos e condições de uso em um contrato não lido porque de difícil compreensão.

No que se refere a categorização, a Lei n° 13.709/2018 diferenciou dados pessoais de dados sensíveis, o que já é um grande passo para a melhor tutela da privacidade e dos dados do usuário, observe-se:

> I – dado pessoal: informação relacionada à pessoa natural identificada ou identificável; II – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.[24]

Todavia, essa classificação ainda é bastante simples e contextual, explica-se. Tomemos por exemplo o escândalo do site "*Ashley Madison*"[25], site de relacionamentos extraconjugal do qual vazaram endereços de e-mail. Um endereço de e-mail pode não ser um dado pessoal sensível quando relacionado no site de uma empresa, mas quando referente a uma relação extraconjugal, definitivamente sim.

Outra hipótese em que a categorização de dados é insuficiente é no caso de *data mining:*

---

24 Artigo 5°, inciso II da lei n. 13.709/2018

25 BARANJUK, Chris Baraniuk. Ashley Madison: 'Suicides' over website hack. Retirado de: <https://www.bbc.com/news/technology-34044506> em 19 de agosto de 2018.

> As técnicas de big data e data mining permitem que, ao se submeter dados desconexos ou que não trazem informações sensíveis a um tratamento estatístico, nasça a possibilidade de revelação de novas informações (estas sensíveis). Na verdade, uma das formas mais comuns de data mining é a análise preditiva ou "predictive data mining".

Tal atividade é composta da exploração inicial de dados com a posterior construção de modelos envolvendo a identificação de padrões*"*[26].

Verifica-se a partir disso que talvez a solução para a privacidade e proteção de dados esteja muito mais em no *compliance* interno das empresas do que na regulação estatal da atuação dessas com o *compliance* interno.

5.1 Privacy by design

Ao unirmos os tópicos mencionados acima, a saber, transparência, com a finalidade, categorização e consentimento, tem-se a regra de *Compliance* Digital chamada "*Privacy by design*"[27] que designa uma "metodologia na qual a proteção de dados pessoais é pensada desde a concepção de sistemas, práticas comerciais, projetos, produtos

26 GOULART, Guilherme Damásio. Dados Pessoais e Dados Sensíveis: a insuficiência da categorização. Retirado de: <http://direitoeti.com.br/artigos/dados-pessoais-e-dados-sensiveis-a-insuficiencia-da-categorizacao/> em 25 de junho de 2018.

27 Ou "Privacidade Desde a Concepção" (tradução livre), metodologia criada na década de 1990 pela Comissária de Informação e Privacidade de Ontário/Canadá, Dra. Ann Cavoukian.

ou qualquer outra solução que envolva o manuseio de dados pessoais"[28], ou seja, uma forma para que as empresas incorporem os conceitos e princípios de privacidade em suas soluções tecnológicas.

O "*Privacy by design*" foi resumido pelo *Legal Ethics Compliance* em 07 (sete) princípios[29] básicos que devem ser norte para todos aqueles, seja pessoa física ou jurídica, que produzem e vendem aparatos que coletam, armazenam e tratam dados, confira-se: a) Prevenção: prever e antecipar eventos que possam comprometer a privacidade antes que eles ocorram; b) Configuração padrão: o titular dos dados não deveria ter que ajustar configurações para garantir privacidade e proteção aos dados, essa deveria ser a configuração padrão do aparato tecnológico; c) Privacidade incorporada ao projeto:

> …proteção dos dados pessoais deve ser pensada como parte indissociável do projeto de arquitetura do sistema ou de prática de negócio, pensada desde sua concepção, com isso, a privacidade passa a ser parte da própria solução e não um adendo.[30]

---

28 LEC: PROTEÇÃO DE DADOS PESSOAIS: PRIVACY BY DESIGN E COMPLIANCE. Retirado de: <http://www.lecnews.com.br/blog/protecao-de-dados-pessoais-privacy-by-design-e-compliance/?utm_campaign=-compliance_news_382018&utm_medium=email&utm_source=RD+Station> em 19 de agosto de 2018.

29 Ibidem.

30 LEC: PROTEÇÃO DE DADOS PESSOAIS: PRIVACY BY DESIGN E COMPLIANCE. Retirado de: <http://www.lecnews.com.br/blog/protecao-de-dados-pessoais-privacy-by-design-e-compliance/?utm_campaign=-compliance_news_382018&utm_medium=email&utm_source=RD+Sta-

d) Funcionalidade total: deve ser desenvolvido o aparato tecnológico de forma que sua funcionalidade não seja prejudicada de forma alguma pela escolha do usuário em garantir sua privacidade e proteger seus dados; e) Segurança de ponta a ponta:

> A segurança das informações pessoais deve ser garantida desde a coleta do dado até sua destruição ou compartilhamento com um terceiro (…) Podemos dizer que a polêmica envolvendo o Facebook e a *Cambridge Analytica* ocorreu, pois não se garantiu a proteção da informação durante uma das etapas de seu ciclo de vida, no caso, o compartilhamento.[31]

f) Visibilidade e transparência: seria a manifestação dos artigos de lei que preveem a necessidade de um termos e condições de uso específicos para a coleta, armanezamento, tratamento, compartilhamento e tantos outros associados aos dados; g) Solução centrada no usuário: "Toda a arquitetura e operacionalidade do sistema ou da prática de negócio devem ser centradas na privacidade do usuário"[32].

6. Considerações finais

Ou seja, o fenômeno da Internet das Coisas é proveniente de dispositivos que saem de empresas privadas para nossos lares, deste modo, é imperativo que o seja muito

---

tion> em 19 de agosto de 2018.

31 Ibidem.

32 Ibidem.

mais forte o controle do *Compliance* Digital interno diretamente nas empresas do que a imposição de legislação de proteção de dados posterior a sua coleta.

A despeito de críticas a legislação de proteção de dados, a texto normativo e sua promulgação são medidas imperativas, inclusive porque a discussão acerca do tema é tardia no Brasil frente a outros países, como Argentina que possui uma legislação pertinente desde o ano 2000.

De fato a tecnologia avança em passos mais largos que o Direito, conquanto, no Brasil, culturalmente falando, a legislação tem finalidade não apenas regulatória, mas também educativa. Quando é sancionada uma lei ela vem também para instruir cidadãos acerca dos seus direitos e deveres, o que é resultado muito positivo frente a invasão dos dispositivos que coletam dados e fazem parte da Internet das Coisas. Frente a isso é importante a intervenção estatal a fim de proteger os direitos e garantias fundamentais, inclusive de privacidade, intimidade e imagem, e também delimitar o dever de cada cidadão nesse mundo novo e conectado em que vivemos.

Referências bibliográficas

BARANJUK, Chris Baraniuk. Ashley Madison: 'Suicides' over website hack. Retirado de: <https://www.bbc.com/news/technology-34044506> em 19 de agosto de 2018.

Comissão Europeia. Legislação. Proteção de Dados. O que são dados pessoais. Retirado de: <https://ec.europa.

eu/info/law/law-topic/data-protection/reform/what-personal-data_pt> em 23 de junho de 2018.

GOULART, Guilherme Damásio. Dados Pessoais e Dados Sensíveis: a insuficiência da categorização. Retirado de: <http://direitoeti.com.br/artigos/dados-pessoais--e-dados-sensiveis-a-insuficiencia-da-categorizacao/> em 25 de junho de 2018.

LEC: PROTEÇÃO DE DADOS PESSOAIS: PRIVACY BY DESIGN E COMPLIANCE. Retirado de: <http://www.lecnews.com.br/blog/protecao-de-dados-pessoais--privacy-by-design-e-compliance/?utm_campaign=compliance_news_382018&utm_medium=email&utm_source=RD+Station> em 19 de agosto de 2018.

Magrani, Eduardo. "A internet das coisas". Rio de Janeiro: FGV Editora, 2018, p. 21 e 22 .Retirado de: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf?sequence=1&isAllowed=y> em 18 de agosto de 2018.

Nest Learning Thermostat. Retirado de <https://nest.com/thermostats/nest-learning-thermostat/overview/> em 24 de junho de 2018.

Palestra da presidente do STF abre fórum sobre direito ao esquecimento e proteção à memória. Retirado de: <http://stf.jus.br/portal/cms/verNoticiaDetalhe.aspidConteudo=353151> em 19 de Agosto de 2018.

Pensar Contemporâneo: A teoria da panóptica de Michel Foucault. Retirado de: <https://www.pensarcontemporaneo.com/teoria-da-panoptica-de-michel-foucault/> em 25 de junho de 2018.

Reforma de 2018 das regras de proteção de dados da UE. Retirado de: <https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt> em 19 de Agosto de 2018.

ROUSE, Margaret. IOT Agenda: Internet of Things. Retirado de: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT> em 23 de junho de 2018.

Sampaio, Rodrigo Vaz. Preocupação com Dados nas Redes Sociais e Autodeterminação Informacional. Retirado de: <http://blogs.correiobraziliense.com.br/aricunha/urgente-preocupacao-com-protecao-de-dados-nas-redes-sociais-e-autodeterminacao-informacional/> em 25 de Junho de 2018.

Senado Federal. Projeto de Lei n. 53/2018. Retirado de: <https://legis.senado.leg.br/sdleg-getter/documentodm=7738646&ts=1529700780674&disposition=inline&ts=1529700780674> em 23 de junho de 2017.

Surveillance. Retirado de: <http://studymore.org.uk/ybenfou.htm> em 25 de junho de 2018.