XXI SEMEAD
Seminários em Administração

novembro de 2018
ISSN 2177-3866

Internet das Coisas (IoT) e privacidade de dados dos usuários: uma questão atendida pelas leis brasileiras?

DANIELA ASSIS ALVES FERREIRA
UNIVERSIDADE FUMEC (FUMEC)

RODRIGO MORENO MARQUES
UNIVERSIDADE FUMEC (FUMEC)

Internet das Coisas (IoT) e privacidade de dados dos usuários: uma questão atendida pelas leis brasileiras?

Área de Pesquisa: Tecnologia da Informação

1 INTRODUÇÃO

Desde a Revolução Industrial a tecnologia tem se desenvolvido contínua e exponencialmente, estando intimamente ligada à vida das pessoas, transformando a sociedade, modificando atitudes, criando tendências e redefinindo conceitos sociais. Especialmente após o advento da Internet, a tecnologia se tornou algo muito mais próximo ao cotidiano das pessoas, influenciando não só a vida profissional, como também a vida pessoal por meio de um acesso cada vez mais disponível nos grandes centros urbanos. O próximo passo esperado será fazer quase tudo de forma remota, e esse conceito já tem um nome: a Internet das Coisas (Internet of Things, em inglês). A Internet das Coisas (IoT) está relacionada à integração de objetos físicos, sensores e dispositivos móveis e aplicações na web. A IoT abrange inúmeras tecnologias, serviços e padrões e é vista por muitos como um conceito emergente na área de tecnologias de informação e comunicação (TICs).

A Internet das Coisas ou Internet of Things (IoT) desponta como uma evolução da internet e um novo paradigma tecnológico, social, cultural e digital, proporcionando aos objetos do dia a dia, com capacidade computacional e de comunicação, se conectarem à internet. Essa conexão viabiliza controlar remotamente os objetos, e acessá-los como provedores de serviços, que se tornam objetos inteligentes ou smart objects. Os objetos inteligentes possuem capacidade de comunicação e processamento aliados a sensores. Assim, a Internet das Coisas revolucionará os modelos de negócios e a interação da sociedade com o meio ambiente, por meio de objetos físicos e virtuais, em que esses limites se tornam cada vez mais tênue (LACERDA; LIMA-MARQUES, 2015).

Atualmente, além de computadores conectados à internet, diversos equipamentos, tais como TVs, laptops, geladeira, fogão, eletrodomésticos, automóveis, smartphones, entre outros, também já podem ser acessados via web. Assim, previsões indicam que mais de 50 bilhões de dispositivos estarão conectados até 2020 (EVANS, 2011). Essas novas habilidades dos objetos inteligentes gerarão um grande número de oportunidades de pesquisas e projetos no âmbito acadêmico e empresarial.

Com o avanço da utilização dessa nova tecnologia, é possível perceber que uma das tensões centrais da Internet das Coisas (IoT) é relativa ao dilema do gerenciamento da privacidade versus a conveniência. Isso se deve ao substancial aumento da quantidade de dados relacionados ao consumidor e seu acesso via Internet, expondo informações e revelando segredos mais frequentemente.

Para Weinberg et al. (2015), o advento da IoT levará as pessoas a compartilharem e exporem mais informações, podendo afetar o sigilo em diversas situações. Os autores explicitam que na IoT os dispositivos, tais como computadores, laptops, servidores, smartphones, tablets, entre outros, estão conectados a Web e seus usuários podem receber ou transmitir dados através de um navegador, permitindo que o mundo físico e natural esteja integrado e acessível através da Internet. Desta forma, em um ambiente baseado em IoT, os dispositivos monitoram e gravam dados relacionados ao comportamento do usuário em seu ambiente natural e não por

interações online em um mundo digital, fazendo com que o usuário não precise participar ativamente para que o dispositivo colete seus dados, sendo isso feito pelos dispositivos de IoT que por si só monitoram e recuperam dados relevantes do meio ambiente e de uma pessoa. Assim, os dispositivos IoT aprendem sobre os comportamentos dos usuários no mundo natural e físico ao observar seus hábitos, tendências e preferências, extrapolando os dados comportamentais relacionados ao mundo estritamente online (WEINBERG ET AL., 2015).

Diante do exposto, os autores indicam que a privacidade é apenas uma das preocupações advindas do uso da IoT, mas também é possível sinalizar outras questões difíceis de gerenciar, tais como o grande volume de dados que serão gerados e demandarão novas tecnologias e algoritmos para processamento e armazenamento dos mesmos. Além dessas questões, também são apontadas preocupações relacionadas à propriedade, interoperabilidade, comunicação e padrões dos dados.

Portanto, diante das atuais discussões sobre o tema, a questão orientadora deste artigo é: o que dizem as leis existentes atualmente no Brasil sobre a privacidade de dados pessoais para os sistemas de Internet das Coisas IoT?

Assim, com base nas leis existentes sobre o tema, este artigo tem como objetivo discutir as leis que tratam a questão de privacidade de dados pessoais para os usuários em um contexto de IoT no Brasil.

Diante do exposto, este artigo se justifica por visar estudar um tema atual e que demonstra ser uma preocupação tanto para a sociedade civil, como para empresas e governos. O levantamento mostrou que o mesmo se encontra no centro das discussões e em um especial momento de efervescência, devido à conclusão do estudo promovido pelo BNDES, assim como a tramitação da Lei de Proteção de Dados Pessoais no Congresso Nacional e da aprovação do Regulamento Geral de Proteção de Dados (RGPD) por parte do Parlamento Europeu.

Portanto, a seguir será apresentado o conceito de Internet das Coisas (IoT) e como o tema tem sido tratado no Brasil, bem como levantar as leis disponíveis sobre a privacidade de dados pessoais para os usuários da web. Após a discussão do tema, conclui-se que o Brasil ainda não dispõe de uma lei específica de proteção de dados pessoais que circulam na Internet, quanto mais alguma lei específica para a IoT.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Internet das Coisas (IoT)

A expressão Internet das Coisas (IoT) foi utilizada pela primeira vez em 1999 pelo cientista Kevin Ashton, pesquisador britânico do Massachusetts Institute of Technology (MIT), que apresentou o termo como "um conceito tecnológico em que todos os objetos da vida cotidiana estariam conectados à internet, agindo de modo inteligente e sensorial" (FONSECA, 2017, p. 12). Kevin Ashton começou sua carreira na Procter & Gamble, onde comandou um trabalho pioneiro sobre identificação de produtos por radiofrequência; é cofundador do Auto ID-Center no MIT e criador de três start ups de sucesso. Para Ashton (2009), "The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so"[i].
O conceito primordial associado à Internet das Coisas (*IoT - Internet of Things*) relaciona-se à capacidade que os objetos possuem de se comunicar, reportando informações acerca de seu

estado e funcionamento. Segundo Serafim (2014), esta tecnologia consiste em interligar os objetos de uso cotidiano do ambiente real com a Internet, tornando-os então objetos inteligentes. O termo Internet das Coisas, destaca Gogliano (2013), refere-se a um novo paradigma, que tem por premissa a integração entre objetos de uso cotidiano e a Internet. Contudo, sustenta o autor, para muitos esse conceito demonstra-se abstrato, e muitas vezes de difícil compreensão, no que tange à maneira de como se procede a essa integração.

A Internet das Coisas, segundo Lacerda (2015), provê vários benefícios para a sociedade, concebendo efeitos significativos nas áreas de meio ambiente, saúde, comunicação, segurança, comodidade e urbanismo, uma vez que as aplicações são tantas quantas forem possíveis de se imaginar ao associar-se objetos com informações. A IoT tem por objetivo a conexão de dispositivos em tempo real na rede, para que desta forma várias pessoas de vários locais, de fuso horários diferentes possam estar conectados simultaneamente em tempo real, realizado a integração e troca de informações de qualquer tipo de sistema e objeto físico desenvolvido por qualquer tipo de software. Em entrevista a Fonseca (2017), João Resende, vice-presidente para desenvolvimento de produtos da WeDo Technologies, acredita que tudo será rastreado digitalmente, e com a IoT "vamos ter um mapeamento em algo digital, com sensores em nossos corpos, nossos carros, nossas casas. Serão os nossos gêmeos digitais. Será a internet de tudo, não só das coisas". Quanto à questão da privacidade, João Resende ainda aponta que:

> Sociedades diferentes terão posturas diferentes. Uma maior conveniência parte do pressuposto de uma menor privacidade. Nos Estados Unidos, as pessoas privilegiam mais a conveniência em detrimento da privacidade, ao contrário dos europeus, que geralmente preferem ficar menos expostos. Se for para aumentar a segurança, todos pensam que é melhor uma menor privacidade, diferentemente do marketing, em que o excesso de informações disponíveis para uma empresa costuma irritar o cidadão (FONSECA, 2017, p. 12).

Assim, é possível perceber que as aplicações da IoT são diversas, tais como: melhorar a mobilidade urbana, auxiliar na segurança, no monitoramento de plantas e animais, além de integrar de forma mais eficiente as cadeias produtivas e o setor industrial como um todo. No entanto, ainda há muito a ser debatido sobre como evitar uma possível vigilância excessiva e garantir a privacidade das pessoas. Segundo Lacerda e Lima-Marques (2015), as questões ligadas à IoT são tratadas na literatura com o viés sociocultural, econômico, filosófico e predominantemente tecnológico. Mas existem outras questões ligadas à privacidade, usabilidade e consentimento que também afetam o indivíduo e a sociedade. A privacidade em um contexto IoT, portanto, parece ser um tema capaz de evocar bastantes discussões.

No Brasil, essas questões também já suscitaram várias discussões que, segundo Singer (2012), tiveram início durante o 1º Congresso de Tecnologia, Sistemas e Serviços com RFID, que aconteceu em Salvador, em agosto de 2010. No ano seguinte, a segunda edição do evento mudou de nome para Congresso Brasileiro de Internet das Coisas e RFID, mas manteve o foco empresarial e industrial nas discussões sobre as aplicações dessa tecnologia. Singer (2012) ainda destaca o início da utilização da IoT que,

> além do congresso, 2010 marcou a implantação do Centro de Operações do Rio (COR), quartel general da prefeitura da cidade do Rio de Janeiro que opera com tecnologia de cidades inteligentes da IBM. No COR um telão de 80 m² mostra o mapa da cidade com camadas de informação e imagens de câmeras que permitem visualizar o trânsito, condições climáticas e ocorrências diversas.

No ano de 2015, diversos sites de notícias alertaram sobre a intenção do governo federal em elaborar uma política específica para a IoT, visando nortear a implementação dessa tecnologia no país. O projeto foi iniciado pela Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas Máquina a Máquina, um grupo "composto por membros de ministérios, da Agência Nacional de Telecomunicações (Anatel), além de representantes da indústria, das prestadoras de serviço em telecomunicações, de instituições de ensino e desenvolvedores" (OLIVEIRA, 2015).

Peduzzi (2015) entrevistou o analista de Infraestrutura e chefe do Núcleo de Internet das Coisas do Ministério das Comunicações, Guilherme Corrêa, que afirmou que "A internet das coisas inevitavelmente será usada para auxiliar a administração pública a ampliar e melhorar suas políticas públicas". O analista ainda apontou estudos que indicam que até 2020 haverá cerca de 50 bilhões de dispositivos conectados à IoT no mundo. Peduzzi (2015) também sinalizou que o governo federal pretende acionar órgãos e ministérios com potencial de uso da tecnologia para o desenvolvimento de políticas públicas.

Também preocupada com os rumos que esse tema tem tomado diante dos avanços das TICs, e principalmente após a aprovação do Regulamento Geral de Proteção de Dados (RGPD)[ii] por parte do Parlamento Europeu em 25 de maio de 2016, a Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) organizou em 3 de novembro de 2016 a conferência "Novo Regulamento de Proteção de Dados - Preocupações, desafios e oportunidades para as empresas". O novo RGPD determina novas obrigações de impacto considerável para as organizações públicas e privadas, e sua aplicação na prática se deu a partir de 25 de maio de 2018.

Em março de 2016, o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) abiu uma Chamada Pública BNDES/FEP Prospecção nº 01/2016 – Internet das Coisas (*Internet of Things* - IoT) e Seleção para a realização de estudos técnicos independentes com objetivo de "avaliar o estágio e as perspectivas de implantação da IoT no mundo e no país, com vistas à proposição de políticas públicas que potencializem tanto os impactos econômicos, tecnológicos e produtivos, como aqueles ligados ao bem-estar da sociedade brasileira" (BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL, 2016). O estudo foi dividido em quatro grandes fases:

- Fase I: Diagnóstico Geral do impacto da IoT no Brasil (janeiro a março de 2017);
- Fase II: Seleção de temas verticais e horizontais a serem aprofundados na etapa seguinte (abril a maio de 2017);
- Fase III: Aprofundamento nas verticais priorizadas, e elaboração de visão para IoT para cada vertical e elaboração de Plano de Ação 2018-22 (junho a setembro de 2017);
- Fase IV: Suporte à Implementação do Plano de Ação 2018-22 (outubro de 2017 a março de 2018).

A primeira etapa objetivou obter uma visão geral do impacto de IoT no Brasil, entender competências de TIC do País e as aspirações iniciais para IoT no Brasil. A segunda fase definiu critérios chaves para a seleção de temas verticais e horizontais. Já a terceira etapa visou aprofundar-se nas verticais escolhidas, elaborar a visão para IoT para cada vertical e elaborar um Plano de Ação 2018-22. A última etapa apresentou um detalhamento dos 3 projetos mobilizadores do Plano de Ação, assim como o desenho de modelo de governança para o PNIoT e da estrutura de monitoramento (PMO). O estudo teve início em dezembro de

2016 e foi conduzido pelo consórcio McKinsey/Fundação CPqD/Pereira Neto Macedo. Ao longo das quatro fases foram produzidos quatorze relatórios, conforme o Plano de Trabalho e Governança elaborado pelo Consórcio.

Durante o período de elaboração deste estudo a expectativa foi grande e amplamente noticiada, pois uma pesquisa sobre as oportunidades para o país definir as estratégias possíveis de ofertante de produtos e serviços, assim como a definição de políticas públicas para IoT, é de grande importância, tanto para Estado quanto para a sociedade civil. Mas a escolha de uma empresa de capital estrangeiro para o estudo financiado pelo BNDES também foi criticada, pois, conforme aponta Duarte (2016),

> Se a chamada do BNDES tivesse como objeto apenas o estudo, talvez, fosse possível concordar com a escolha. Pois de um estudo para a proposição e implementação de políticas públicas há um caminho longo a ser percorrido. Um caminho que poderia envolver a participação de um conjunto maior de atores, incluindo na busca de soluções e consenso empresas interessadas em ofertar soluções para a IoT e cidadãos que serão por ela impactados. Mas deixar sob responsabilidade de uma empresa de capital estrangeiro um pacote com várias incumbências, ou seja, desenvolver o estudo, propor políticas públicas e apoiar a sua implementação, parece demais. Especialmente considerando que se trata da construção de um plano nacional de ação para um assunto com tal potencial de mudanças, como é o caso da Internet das Coisas.

A construção de um plano de ação para acelerar o desenvolvimento da IoT no Brasil definiu quatro frentes de trabalho: Cidades, Saúde, Rural e Indústrias. Para organizar as medidas a serem implementadas dentro de um plano de ação, foram estruturadas diversas iniciativas de acordo com os temas transversais a todos os ambientes de IoT: (1) Capital humano, (2) Inovação e inserção internacional, (3) Infraestrutura de conectividade e interoperabilidade, (4) Regulatório, segurança e privacidade.

Este último tema, foco deste estudo, definiu que o Regulatório, segurança e privacidade será um elemento habilitador importante para impulsionar a adoção de IoT. Seus objetivos são: endereçar barreiras da regulamentação de telecomunicações, com vistas a acelerar o desenvolvimento de aplicações IoT; criar um marco regulatório de proteção de dados pessoais adequado para fomentar a inovação e a proteção aos direitos individuais; identificar e tratar questões regulatórias específicas nas verticais priorizadas; e estabelecer desenho institucional adequado para enfrentar os desafios em privacidade e segurança para IoT.

O estudo aponta que os temas de privacidade e proteção de dados pessoais e de segurança da informação são os atuais gargalos na regulamentação de telecomunicações, sendo apontado como um desafio maior do que a próprio ambiente de IoT. Com o aumento de novos dispositivos conectados à Internet e capazes de armazenar, coletar e tratar uma grande quantidade de dados, a discussão sobre os usos legítimos dos dados e sobre as vulnerabilidades das bases de dados gerados tem intensificado. Assim, o desenvolvimento de soluções de IoT demanda o desenvolvimento de normas sobre proteção de dados pessoais para lidar com a complexidade e as nuances do contexto tecnológico, a definição de uma autoridade central independente para a proteção de dados pessoais, e que seja capaz de trazer segurança jurídica diante dos novos desafios da atual sociedade da informação.

O próximo tópico apresenta as leis que estão em vigor relacionadas à privacidade e proteção de dados pessoais no Brasil.

2.2 Privacidade de dados

Desde o surgimento da Internet, a discussão sobre o impacto das TICs na sociedade tem sido uma constante. Com a crescente popularização de seu uso e do acesso a diversos tipos de informações, questões como privacidade e liberdade de expressão em ambientes digitais tem suscitado debates em busca de uma melhor compreensão do tema e como uma forma de assegurar a preservação do direito do cidadão.

Polido et al (2018) indicam que o artigo 21 do Código Civil de 2002 apresenta o direito à privacidade, mas não aborda a questão de proteção de dados pessoais, não considerando o amplo e complexo aspecto ligado à atual sociedade da informação, sempre conectada às diversas TICs.

A regulamentação do uso da internet no Brasil teve início com a sanção da Lei nº 12.965, de 23 de abril de 2014, mais conhecida por Marco Civil (MCI) e visa estabelecer uma regulamentação sobre os direitos e deveres dos usuários, provedores de serviços e conteúdos e demais envolvidos com o uso e disponibilidade da Internet no Brasil. Esta lei trata dos princípios, garantias, direitos e deveres de quem usa a rede e determina diretrizes para atuação do Estado e é considerada uma das legislações mais avançadas do mundo na regulação da internet e na garantia da neutralidade da rede. O texto do MCI foi resultado de uma série de discussões iniciados em 2009, quando havia naquele momento 26 propostas no Congresso Nacional a respeito do tema.

Os pontos que geraram maiores discussões durante a sua tramitação foram sobre liberdade, privacidade e neutralidade da rede. Em relação à questão da privacidade do usuário, foco desse artigo, já no seu artigo 3º, III, o Marco Civil indica o princípio de proteção dos dados pessoais para o uso da internet no Brasil. O MCI visa garantir a privacidade ao evitar que informações pessoais sejam disponibilizadas sem a prévia autorização do usuário pelos provedores de aplicações, assim como a preservação do sigilo nas comunicações feitas online pelo mesmo. Deste modo, os provedores de aplicações deverão possibilitar ao usuário, de forma clara, o direito de permitir ou não a transferência a terceiros de seus dados pessoais, podendo isso ser revogado a qualquer momento (BRASIL, 2014).

O Artigo 7º da Lei nº. 12.965 estabelece os direitos e garantias dos usuários da Internet no Brasil e indica que o acesso à internet é essencial ao exercício da cidadania, e ao usuário é assegurado o direito de inviolabilidade da intimidade e da vida privada, sigilo do fluxo de suas comunicações pela internet e de suas comunicações privadas armazenadas. Art. 8 também aponta "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet" (BRASIL, 2014).

Em relação à proteção dos registros, dos dados pessoais e das comunicações privadas, o artigo 11 da Lei 12.965/2014 indica que:

> Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (BRASIL, 2014).

A Lei também determina que "os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações" (BRASIL, 2018), visando, assim, criar mecanismos para assegurar proteção dos dados pessoais e registros de conexão.

Um dos problemas da proteção dos dados pessoais é que a internet é em escala mundial. A própria estrutura da internet permite que as violações da lei possam ocorrer de qualquer lugar do mundo, onde o Brasil não tem jurisdição. Tomasevicius Filho (2016) afirma que apesar das punições severas previstas na lei, que podem chegar até a 10% do faturamento da organização no Brasil ou proibição do exercício da atividade, o efeito normativo desta é praticamente inócuo já que o Brasil não tem jurisdição para controlar as atividades dessas empresas no exterior ou até mesmo proibir o exercício da atividade, pois seria inconstitucional.

Marques e Kerr Pinheiro (2014) apontam que o Projeto de Lei Marco Civil da Internet no Brasil, assim como outras leis e regulamentos que compõem as políticas de informações, tem como desafio mediar os diversos conflitos de interesses que surgem sobre o tema. Segundo os autores, "a neutralidade da rede" e a "coleta massiva de informação dos usuários" são pontos "cruciais para a manutenção ou abolição do caráter livre e isonômico que foi atribuído à web, quando da sua concepção" (MARQUES; KERR PINHEIRO, 2014, p. 235). A coleta massiva de informações de usuários é realizada por meio de pesquisas de marketing e rastreamento online dos acessos realizados pelos usuários na rede, e ignoram o princípio do direito à privacidade dos internautas. "Mas esse tipo de prática não é empregado apenas para fins econômicos. Sua adoção é defendida por instituições governamentais que alegam a necessidade de combater o crime e promover a defesa nacional" (MARQUES; KERR PINHEIRO, 2014, p. 240).

> Além disso, as tecnologias de rastreamento digital ganham força na sociedade da informação, tanto na esfera do mercado, quanto do Estado. Paradoxalmente, é a plena liberdade na internet que permite o monitoramento dos internautas por empresas e por governos. Portanto, é preciso que a defesa de uma rede aberta, livre e igualitária seja também acompanhada pela reivindicação do controle social da coleta massiva de informações dos usuários (MARQUES; KERR PINHEIRO, 2014, p. 249).

Em um ambiente de Internet das Coisas (IoT), Weinberg et al. (2015) indicam que o compartilhamento de informações sobre o comportamento do consumidor na web geralmente é realizado internamente nas organizações ou externamente com terceiros ou parceiros. Dessa forma, por meio de dispositivos conectados à IoT, fornecedores e comerciantes aprendem sobre os hábitos, tendências e preferências dos consumidores com base em suas atividades dentro do mundo digital, como comprar on-line e usar mídias sociais. Os autores advertem que questões relacionadas à privacidade é o ponto principal da experiência do consumidor com a IoT, uma vez que os mesmos devem refletir sobre as conveniências oferecidas pela IoT e a perda de sua privacidade.

Aqui no Brasil a Lei de Proteção de Dados Pessoais está em discussão pela sociedade civil desde 2010, tramita no Congresso desde abril de 2016 e que uma das mudanças está na noção de "consentimento" dos usuários, uma das pautas presente no Marco Civil da Internet. "Para fazer uma atualização no celular, hoje, o usuário precisa consentir com isso. Fazer o mesmo com qualquer objeto da internet das coisas pode torná-la inviável. Precisamos repensar isso" (ASSOCIAÇÃO NACIONAL DE PESQUISA E DESENVOLVIMENTO DAS EMPRESAS

INOVADORAS, 2017). A Câmara dos Deputados aprovou no dia 29 de maio de 2018 o parecer do deputado Orlando Silva (PC do B/SP) ao PL 4.060/2012, que trata da proposta de Lei de Proteção de Dados Pessoais, e será enviada ao Senado, que paralelamente discute o Projeto de Lei do Senado (PLS) 330/2013, que também estabelece regras de proteção, tratamento e uso de dados pessoais e foi aprovada com requerimento de urgência no dia 23 de maio de 2018. Segundo Possebon (2018), "o projeto aprovado pela Câmara prevê que a atividade de tratamento de dados pessoais (ou seja, quem utiliza as informações) é atividade de risco e, portanto, implica responsabilidade objetiva ao agente de tratamento". Entretanto, ainda paira muita incerteza sobre qual texto prevalecerá, pois as duas casas apresentaram requerimento de urgência para acelerar a tramitação de suas respectivas propostas. O principal ponto do projeto trata dos direitos dos titulares sobre os dados, da necessidade de consentimento inequívoco para a coleta de dados, assim como do seu cancelamento a qualquer tempo.

Já no dia 3 de julho de 2018, a Comissão de Assuntos Econômicos do Senado aprovou o Projeto de Lei da Câmara nº 53, de 2018, que dispõe sobre a proteção, o tratamento e o uso de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. A nova regulamentação europeia para a proteção de dados pessoais, ou General Data Protection Regulation (GDPR), foi apontada como a inspiração para atualização de acordo com o que foi discutido na União Europeia, visa garantir a possibilidade de transferência internacional de dados. A proposta foi aprovada por unanimidade e segue em regime de urgência para tramitação, previsto para iniciar em 18 de julho.

Por fim, Califano (2013) afirma que a internet ainda apresenta desafios regulatórios devido ao grande volume de dados circulantes e, justamente por isso, o autor indica a necessidade de intervenção dos governos por meio de leis específicas para assegurar o direito à privacidade de dados pessoais de quem utiliza a rede.

3 DISCUSSÃO

Atualmente, a proteção de dados pessoais no Brasil é tratada superficialmente pelo Marco Civil da Internet. A Lei 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, e pelo Decreto nº 8.771/2016, de 11 de maio de 2016, que regulamenta o Marco Civil da Internet. Além destas leis, o tema tem sido tratado por diferentes projetos de lei no Congresso Nacional:

- Projeto de Lei do Poder Executivo 5.276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.
- Projeto de Lei do Senado Federal 330/2013, que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências.
- Projeto de Lei da Câmara dos Deputados 4.060/2012, que dispõe sobre o tratamento de dados pessoais, e dá outras providências.
- Projeto de Lei da Câmara no 53, de 2018, que dispõe sobre a proteção de dados pessoais.

Essa falta de definição de uma lei única é apontada por Polido et al (2018, p. 25) ao afirmarem que

> A proteção dos dados pessoais no Brasil se aproxima do modelo europeu, uma vez que reconhece seu status de direito fundamental como desdobramento da tutela da privacidade. Contudo, o sistema jurídico brasileiro ainda prevê uma normativa fragmentária e insuficiente. Há lei - geral ou especial - que regule de forma abrangente a atividade de tratamento de dados pessoais realizada por entidades públicas e privadas, seja em ambiente interconectado em redes digitais ou não.

A coleta de dados dos usuários de Internet é uma preocupação atual, visto que no Brasil ainda não há uma lei de proteção de dados pessoais, e questões regulatórias devem ser tratadas como prioridade; ainda mais diante do aumento da utilização de dispositivos conectados à IoT e a possibilidade dos dados pessoais dos usuários serem utilizados pelas empresas que ofertarem os serviços. Essa indefinição normativa é preocupante não só para os cidadãos, mas também para o setor privado e para o próprio Estado.

O Plano Nacional de Internet das Coisas para o Brasil representa um marco em busca de uma visão estratégica sobre Internet das Coisas ao permitir uma construção colaborativa entre os atores-chave dessa nova realidade, a saber: setores público e privado, associações empresariais e academia. A proposta é que o estudo do BNDES sobre Internet das Coisas apresentado no capítulo anterior sirva de base para o Plano Nacional de Internet das Coisas, por meio da identificação dos principais gargalos existentes atualmente para a expansão de IoT e proposta de iniciativas para que o país avance no desenvolvimento desta tecnologia.

Um dos pontos que merece atenção para o crescimento de IoT no Brasil é a garantia da privacidade e da proteção de dados pessoais por meio de legislações específicas. É preciso preparar o país para lidar com os crescentes riscos à segurança da informação e aperfeiçoar a regulação para facilitar o investimento na ampliação de rede no país. É imperativa a aprovação da Legislação de proteção de dados pessoais, sendo perceptível que há um consenso entre sociedade civil, empresas e governo sobre essa necessidade, mesmo diante das divergências sobre qual projeto lei prevalecerá, do Senado ou da Câmara dos Deputados.

No entanto, Silva, Pinheiro e Marques (2018, p. 87) apontam que

> A Internet se constitui atualmente como o principal domínio de criação e circulação da informação, sendo fundamental o desenvolvimento de uma estrutura normativa que alcance um equilíbrio entre direitos e responsabilidades de indivíduos e instituições, de forma a regular o impacto da rede mundial nos estágios da cadeia de produção informacional e, em última instância, nas dinâmicas socioeconômicas contemporâneas.

Assim, os autores afirmam que essa disputa de poderes e interesses dos diversos atores representa um desafio para alcançar o ordenamento da Internet. Corroborando essa ideia, Bezerra e Waltz (2014, 159) já indicavam que, mesmo com o aumento da democratização e da liberdade de expressão proporcionadas pela Internet, a privacidade estava ameaçada e a sua defesa, mesmo sendo defendida por quase todos os atores envolvidos na rede, mas violada por meio de ações de espionagem e vigilância de governos e grandes empresas. Desta forma,

> ao mesmo tempo em que as redes empoderam usuários com mais voz e capacidade de mobilização social, elas abrem uma importante lacuna à vigilância de governos e grandes corporações, possibilitando maior controle estatal sobre a vida dos cidadãos, violação da privacidade de indivíduos e de segredos empresariais, espionagem internacional e outros expedientes (BEZERRA; WALTZ, 2014, 161).

Um dos pontos necessário a ser analisado quanto à proteção de dados oferecidas em soluções de IoT em cidades inteligentes é relativa a expectativa de privacidade de cidadãos tanto em ambientes públicos quanto em ambientes privados. No entanto, ainda não há uma lei de proteção de dados pessoais para Internet, assim como não há uma lei direcionada especificamente para a Internet das Coisas.

Portanto, é possível indicar que os principais riscos jurídicos apresentados pela utilização de sistemas baseados em IoT são o desconhecimento dos usuários em relação à coleta de dados, visto que nem sempre existirá um aviso indicativo que os seus dados estão sendo coletados, e o monitoramento a que as pessoas estão sujeitas sem que saibam que os seus dados podem estar sendo gerados e coletados por terceiros.

4 CONCLUSÃO

É possível concluir que a Internet das Coisas surge como um processo de automatizar os processos diários os quais são executados por ações humanas. Porém como analisado, todo este processo de execução destas tarefas ainda carece da definição de leis sobre a privacidade e proteção de dados pessoais para que essa tecnologia possa atender a todos os seus usuários satisfatoriamente.

A coleta de dados pessoais faz parte do dia-a-dia de qualquer empresa, seja numa lógica comercial, de recursos humanos, financeira ou de comunicação e marketing, sendo impossível tratar desse tema sem levantar questões relativas à privacidade dos mesmos. A definição de uma lei de privacidade e proteção de dados pessoais deve ser capaz de assegurar maior controle sobre os dados pessoais de usuários de sistemas de IoT, assim como proporcionar transparência às operações de coleta, manutenção e tratamento desses dados.

O Marco Civil foi o ponto de partida no Brasil para a definição de direitos na Internet, mas há muito ainda a avançar e debater em relação a questões legais, técnicas, políticos e sociais. Mais ainda há muitos pontos que necessitam reflexões e discussões que envolvam indústria, governo e sociedade civil. Uma delas é a definição dos requisitos mínimos para uma legislação de proteção de dados pessoais que promova segurança jurídica para usuários e empresas. Mesmo representando um avanço em sua época, ainda há muito a ser discutido e atualizado, para que suas lacunas sejam adequadas às novas exigências, não só nacionais, como internacionais.

Portanto, a falta de uma clara definição quanto aos direitos à privacidade e proteção de dados pessoais e a falta de valorização da privacidade percebida na sociedade brasileira se mostra como um desafio atual. É preciso colocar o indivíduo no controle efetivo dos seus dados pessoais, visto que esses são importantes insumos para a atividade econômica em todos os setores da sociedade, assim como ampliar a conscientização das pessoas sobre métodos de coleta, consentimento, tratamento, compartilhamento, guarda e exclusão de dados pessoais.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **APDSI co-organiza a conferência "Novo Regulamento de Proteção de Dados - Preocupações, desafios e oportunidades para as empresas"**. 27 out. 2016. Disponível em: <http://www.apdsi.pt/index.php/news/1029/191/APDSI-co-organiza-a-conferencia-Novo-Regulamento-de-Protecao-de-Dados-Preocupacoes-desafios-e-oportunidades-para-as-empresas.html>. Acesso em: 26 nov. 2017.

ASHTON, Kevin. **That 'Internet of Things' thing**: in the real world, things matter more than ideas. 22 Jun. 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986>. Acesso em: 15 nov. 2017.

BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL. **Chamada Pública BNDES/FEP Prospecção nº 01/2016**. Chamada pública de seleção de estudo técnico para diagnóstico e proposição de políticas públicas no tema Internet das Coisas (Internet-of-Things - IoT). 24 mar. 2016. Disponível em: <https://www.bndes.gov.br/wps/portal/site/home/conhecimento/estudos/chamada-publica-internet-coisas/chamada-internet-das-coisas>. Acesso em: 15 nov. 2017.

BEZERRA, Arthur Coelho; WALTZ, Igor. Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do marco civil. **Revista Eletrônica Internacional de Economia Política da Informação da Comunicação e da Cultura**, v. 16, n. 2, p.161-175, maio/ago. 2014. Disponível em: <http://ridi.ibict.br/handle/123456789/858>. Acesso em: 10 jul. 2018.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. Código Civil. Disponível em: <http://www.planalto.gov.br/CCivil_03/Leis/2002/L10406.htm>. Acesso em: 10 jul. 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 1 jul. 2018.

CALIFANO, Bernadette. Políticas de Internet: la neutralidad de la red y los desafíos para su regulación. **Revista de Economía Política de las Tecnologías de la Información y Comunicación**. v.15, n. 3, p.19-37, set./dez 2013. Disponível em: <http://www.seer.ufs.br/index.php/eptic/article/viewFile/1353/1351>. Acesso em: 7 jul. 2018.

DUARTE, Virgínia. **Políticas públicas para Internet das Coisas (IoT)**. TIC em foco, 23 nov. 2016. Disponível em: <http://ticemfoco.com.br/politicas-publicas-para-internet-das-coisas-iot/>. Acesso em: 16 nov. 2017.

EVANS, D. **The internet of things**: how the next evolution of the internet is changing everything. CISCO white paper, 2011. 11 p. Disponível em: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>. Acesso em: 6 jul. 2018.

FONSECA, Roberto. Cidade conectada. **Jornal Estado de Minas**, Belo Horizonte, 10 nov. 2017. Ciência & Saúde, p. 12.

GOGLIANO SOBRINHO, Osvaldo. **Serviço de resolução e descoberta de informações sobre objetos em sistemas baseados em RFID**. 2013. Tese (Doutorado em Sistemas Digitais) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2013. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3141/tde-16102013-162918/pt-br.php> . Acesso em: 12 jun. 2018.

LACERDA, Flávia. **Arquitetura da Informação Pervasiva**: projetos de ecossistemas de informação na Internet das Coisas. 2016. 226 f. Tese (Programa de Pós-Graduação em Ciência da Informação) - Faculdade de Informação, Universidade de Brasília, Brasília, 2016. Disponível em: <http://repositorio.unb.br/bitstream/10482/19646/1/2015_FlaviaLacerda.pdf>. Acesso em: 4 jul. 2018.

LACERDA, Flávia; LIMA-MARQUES, Mamede. Da necessidade de princípios de arquitetura da Informação para a Internet das Coisas. **Perspectivas em Ciência da Informação**, v.20, n.2, p.158-171, abr./jun. 2015. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2356>. Acesso em: 4 jul. 2018.

MARQUES, Rodrigo Moreno, KERR PINHEIRO, Marta Macedo. Marco Civil da Internet: uma análise sob a ótica da razão jurídica. In: MOURA, Maria Aparecida (Org.). **A construção social do acesso público à informação no Brasil**: contexto, historicidade e repercussões. Belo Horizonte: Editora UFMG, 2014, p. 235-250.

MARTINS, Helena. **Governo espera que internet das coisas aporte US$ 50 bi na economia**. Agência Brasil, Brasília, 20 set. 2017. Disponível em: <http://agenciabrasil.ebc.com.br/pesquisa-e-inovacao/noticia/2017-09/governo-espera-que-internet-das-coisas-aporte-us-50-bi-na>. Acesso em: 16 nov. 2017.

OLIVEIRA, Déborah. **Governo prepara plano para M2M e internet das coisas**. IT Forum 365, 25 jun. 2015. Disponível em: <https://itforum365.com.br/conectividade/internet-das-coisas/governo-prepara-plano-para-m2m-e-internet-das-coisas>. Acesso em: 16 nov. 2017.

PEDUZZI, Pedro. **"Internet das coisas" pode ser instrumento de política pública, diz especialista.** Agência Brasil, Brasília, 2 set. 2015. Disponível em: <http://agenciabrasil.ebc.com.br/print/974106>. Acesso em: 16 nov. 2017.

POLIDO, Fabrício B. Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves; MACHADO, Diego Carvalho; OLIVEIRA, Davi Teofilo Nunes. **GDPR e suas repercussões no direito brasileiro - Primeiras impressões de análise comparativa.** IRIS - Instituto de Referência em Internet e Sociedade, 2018. Disponível em: <http://irisbh.com.br/gdpr-e-suas-repercussoes-no-direito-brasileiro/>. Acesso em: 10 jul. 2018.

POSSEBON, Samuel. **Câmara aprova projeto de Proteção de Dados Pessoais**. 29 maio 2018. Disponível em: <http://teletime.com.br/29/05/2018/camara-aprova-projeto-de-protecao-de-dados-pessoais/?utm_source=akna&utm_medium=email&utm_campaign=TELETIME+News+-+30%2F05%2F2018+00%3A03>. Acesso em: 4 jul. 2018.

SERAFIM, E. **Uma estrutura de rede baseada em tecnologia IoT para atendimento médico a pacientes remotos.** 2014. 118 f. Dissertação (Mestrado em Ciência da Computação) - Faculdade Campo Limpo Paulista, Campo Limpo Paulista, SP, 2014. Disponível em: <http://www.cc.faccamp.br/Dissertacoes/Edivaldo_2014.pdf> . Acesso em: 12 jun. 2018.

SILVA, Hermann Bergmann Garcia; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. Política de informação para a Internet: regulação do zero-rating na união europeia. In: POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luiza Couto Chaves (org). **Tecnologias e conectividade**: direito e políticas na governança das redes. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. p. 87-101. Disponível em: <http://irisbh.com.br/wp-content/uploads/2018/03/Tecnologias-e-Conectividade-Direito-e-Pol%C3%ADticas-na-Governan%C3%A7a-das-Redes.pdf>. Acesso em: 10 jul. 2018.

SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. In: SIMPÓSIO EM TECNOLOGIAS DIGITAIS E SOCIABILIDADE, 2., 2012, Salvador. **Anais eletrônicos...** Salvador: Programa de Pós-Graduação em Comunicação e Cultura Contemporâneas da UFBA, 2012. Disponível em: <http://files.educacao-e-tics.webnode.com/200000031-3af843cee5/Internet%20das%20Coisas%20-%20IOT%20Talyta%20Singer.pdf >. Acesso em: 16 nov. 2017.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, São Paulo, v. 30, n. 86, p. 269-285, abr. 2016. Disponível em: <https://www.revistas.usp.br/eav/article/view/115093/112803>. Acesso em: 20 maio 2018.

WEINBERG, Bruce D.; MILNE, George R.; ANDONOVA, Yana G.; HAJJAT, Fatima M. Internet of Things: convenience vs. privacy and secrecy. **Business Horizons**, Kelley School of Business, Indiana University, v. 58, n. 6, p. 615-624, nov./dez. 2015. Disponível em: <https://doi.org/10.1016/j.bushor.2015.06.005>. Acesso em: 16 nov. 2017.

[i] "A Internet das coisas tem o potencial de mudar o mundo, assim como a Internet fez. Talvez ainda mais" (Tradução da autora).

[ii] O Regulamento Geral de Proteção de Dados se refere à proteção das pessoas físicas no que respeita ao tratamento dos dados pessoais e à livre circulação destes. Tem como principal efeito ser de aplicação direta em toda a Europa, sem necessidade de ser incorporado pelo ordenamento jurídico de cada estado membro e versa sobre os direitos de transparência, direitos de informação, direitos de acesso, direitos de retificação, direitos de eliminação ou direito ao "esquecimento", limitação do tratamento dos dados, portabilidade dos dados e direito à oposição.