PRIVACIDADE E SEGURANÇA NA INTERNET DAS COISAS

PRIVACY AND SECURITY ON THE INTERNET OF THINGS

Maria Gabriela de Oliveira Martins[1]
Guilherme Madeira Martins[2]

RESUMO

A internet vem tornando-se cada vez mais essencial na vida das pessoas nos últimos anos e cada vez mais indispensável ao bom desempenho dos negócios. Com o investimento nas infraestruturas de redes, a utilização da internet tornou-se uma plataforma global para deixar aparelhos e objetos inteligentes capazes de se comunicarem de modo autônomo. Esta possibilidade visa a permitir que todos serviços e conteúdos encontrem-se disponíveis e acessíveis para todas as pessoas, de forma a facilitar a comunicação. Isso aumenta o leque de novas aplicações, permitindo inovações no meio de trabalho remoto, de interação, de lazer e entretenimento, desenvolvendo um novo padrão de vida. Este novo padrão faz-se imaginável graças aos avanços das Tecnologias da Informação e Comunicação - TICs e de nova concepção definida como Internet of Things – IoT (internet das coisas). Todavia, com uma vasta e diversificada coleta de dados e conhecimentos, para incontáveis fins no cotidiano das pessoas, essa coleta autônoma dos dados e das informações torna o direito fundamental da privacidade um dos principais desafios em relação à IoT. Esse avanço vem junto com importantes vulnerabilidades sociais e materiais a serem tuteladas, visto que o ciberespaço expõe os seus usuários a novas condições de risco, ainda que já existam no mundo físico, potencializa no mundo virtual, posto que há uma maior exposição e abrangência que as tecnologias proporcionam. Diante disso, este artigo pretende discorrer em âmbito teórico a privacidade dos usuários da tecnologia da Internet das Coisas, diante de sua legalidade existente, explorando possíveis soluções neste cenário ainda em construção.

Palavras-chave: Internet das coisas. Privacidade. Informação. Segurança. Internet.

[1]Bacharelanda em Direito – Faculdades Doctum de Juiz de Fora – MG
[2] Doutor em Direito – Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio (2020)

ABSTRACT

In recent years the internet has become more and more an essential tool in people's daily lives and in turn indispensable for the smooth running of businesses. With the investment in network infrastructures the internet becomes a global platform to let devices and smart objects communicate autonomously. This possibility aims to make all services and content available and accessible to everyone, facilitating communication and increasing the range of new applications, allowing new ways of working, interacting and entertaining, developing a new standard of living and working. This new standard is made possible by advances in Information and Communication Technologies - ICTs to a new conception defined as Internet of Things - IoT. However, with a diversified collection of data and information, for countless purposes in people's daily lives, this autonomous collection of data and information makes privacy one of the main challenges in relation to IoT. This advance brings with it important social and material vulnerabilities, since cyberspace exposes its users to new risk conditions, which, although they already exist in the physical world, are heightened in the virtual world, due to the greater exposure and scope that technologies provide. In this context, this article aims to discuss in theoretical terms the privacy of users of Internet of Things technologies, in light of its legality, exploring possible solutions in this scenario still under construction.

Keywords: Internet of Things. Privacy. Information. Security. Internet.

1. INTRODUÇÃO

No Brasil, a Internet das Coisas cresce gradativamente conforme as mudanças significativas nas formas de acesso à rede. Isso fica perceptível quando pensamos na substituição de telefones celulares por smartphones e a centralização do acesso à Internet por meio de serviços de banda larga móvel (2G, 3G, 4G) em todas as regiões do país. (CETIC 2017).

Em 2017, foram mais de 188,9 milhões de acessos à Internet via dispositivos móveis em comparação a 27,8 milhões de acesso por banda larga fixa. (ANATEL 2017). As estimativas mais recentes da União Internacional de Telecomunicações,

relativas a outubro de 2021, mostram que 62,5% da população mundial estavam conectados à internet. Em virtude desde aumento, foi definido o Programa Temático 2205, denominado “Conecta Brasil”, cujo objetivo é promover o acesso universal e ampliar a qualidade dos serviços de comunicações do País, tendo como meta ampliar o acesso à internet em Banda Larga para os domicílios brasileiros de 74,68% para 91% em 2023. (ANATEL 2021).

As pessoas em todo o mundo utilizam a Internet como meio de comunicação, para acessar conteúdos e serviços multimídia, jogos, interagir em redes sociais e muitas outras aplicações. Com o crescimento das infraestruturas de redes e popularização em massa da internet de alta velocidade, emerge um avanço relacionado à utilização da internet tornando-a uma plataforma global para deixar máquinas e objetos inteligentes capazes de comunicarem-se de forma autônoma. (MIORANDI et al., 2012).

Gao e Bai (2014) ressaltam que durante a próxima década, a rede inter-existirá como um tecido sem costura de redes clássicas e objetos ligados em rede. Deste modo, os conteúdos e serviços deverão estar sempre disponíveis para todas as pessoas, facilitando a comunicação e abrindo o caminho para novas aplicações. Isso possibilitará diferentes formas de trabalho, de interação, de lazer, desenvolvendo um novo padrão de vida. Este novo padrão é conhecido como Internet of Things possibilita tais avanços.

A IoT é um modelo que integra as “coisas” do mundo real no mundo tecnológico. É um conceito que os aparelhos e objetos do nosso dia-a-dia são equipados com sensores capazes de comunicar entre si de forma inteligente. Uma “coisa”, no contexto da IoT, é um objeto conectado que pode ser, por exemplo, uma pessoa com um monitor cardíaco, um *smartwatch* conectado ao *smartphone*, um carro com sensores que avisam a pressão dos pneus, uma lâmpada de iluminação pública de uma cidade, uma tomada em casa, ou qualquer outro objeto natural ou construído pelo homem.

Com variedade e aumento de coleta de dados e informações diferentes, variam de objetos domésticos comuns a ferramentas industriais sofisticadas. Neste sentido, a coleta autônoma traz a privacidade como uma das maiores preocupações éticas com relação à Internet das Coisas.

É invisível a troca de dados e cada dia mais constante entre as coisas e as pessoas, e entre as coisas e outras coisas, ocorrendo de forma que os usuários e

criadores desses dados não sejam identificados. Assim, a tutela à privacidade é extremamente necessária para o regulamentar deste novo ambiente complexo.

Para um esse novo ambiente inteligente originado pela Internet das Coisas, onde as aplicações tornaram-se de fácil acesso e as informações estão sempre disponíveis de maneira muitas vezes imperceptíveis, a privacidade é geralmente percebida pelos usuários como uma perspectiva de estar em um estado de proteção sem ter que persegui-lo ativamente. Diante disso, a Internet das Coisas vem em uma crescente inovação tecnológica envolvendo questões de privacidade de dados e informações de usuários, ganha cada vez mais espaço nas legislações e discussões em meios acadêmicos e profissionais. Assim, visando contribuir para amplificação das discussões este texto visa ventilar, de modo conceitual, os relevantes elementos que compõem o acontecimento da IoT.

2. METODOLOGIA

No intuito de familiarizar-se com o conteúdo, foi realizado uma pesquisa do tipo exploratória, a fim de construir hipóteses e aprimorar ideias preliminares acerca do tema proposto. O método usado para alcançar tal finalidade, deu-se através de uma amostra de referencial teórico, já que conforme descreve Selltiz et al (1967 apud GILL, 2002), este é um dos métodos para se analisar um conteúdo: “Na maioria dos casos, essas pesquisas envolvem: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que estimulem a compreensão”.

Para alcançar o objetivo proposto, utilizou-se como critério a pesquisa bibliográfica, do tipo exploratória, pois conforme Gil (2002): “As pesquisas sobre ideologias, bem como aquelas que se propõem à análise das diversas posições acerca de um problema, também costumam ser desenvolvidas quase exclusivamente mediante fontes bibliográficas”.

A metodologia empregada para reunir os resultados da pesquisa, de forma sistemática e ordenada, deu-se pela seleção de livros que abordavam o tema, artigos e periódicos que estavam disponíveis na íntegra e em bases de dados confiáveis, como Legislação Brasileira atual, Cartilhas dos órgãos de comunicação e governamentais, Biblioteca Nacional Digital (BND), entre outros.

A pesquisa bibliográfica permite ao observador o acesso à um amplo conteúdo sem a necessidade de percorrer um determinado território e/ou população em busca de dados. No entanto, é necessário que o pesquisador se assegure de que os dados coletados sejam confiáveis para que não reproduzam erros e comprometa a qualidade da pesquisa. Para isso, os dados coletados foram tratados e analisados cuidadosamente, excluindo a possibilidade de levar ao leitor uma informação incoerente e que não condiz com a verdade.

Com a finalidade de proporcionar a familiaridade do observador com a área a ser pesquisada, foi essencial que o estudo fosse feito de maneira clara e precisa. De acordo com Gil (2002), essa familiaridade é entendida como um estudo exploratório, pois permite ao pesquisador delimitar o conteúdo de interesse.

Esta fase da pesquisa se deu pela seleção de fontes bibliográficas que foram feitas em meio eletrônico através de palavras chaves, estas foram então elencados por títulos que abordavam a temática proposta e agrupadas por categoria: livros, periódicos, monografias e dissertações e outros.

Após uma leitura flutuante dos resumos, foi feita a classificação dos artigos e só então realizado um estudo minucioso e exaustivo acerca do tema.

3. SURGIMENTO E CONCEITO DA IoT - INTERNET DAS COISAS

Ao crescimento da Internet em seus primeiros anos, essa tem sido empregada principalmente para conectar pessoas através de troca de e-mails e, cada vez mais, por meio de sites de redes sociais que colhem e distribuem dados e informações. A Internet transformou definitivamente o nosso dia-a-dia, proporcionando o acesso rápido a informações que até então não dispúnhamos. Percebe-se também que ultimamente a Internet é empregada para conectar dispositivos, máquinas e outros objetos, através de redes com e sem fio, criando um novo posicionamento tecnológico nomeado de Internet of Things. (DUTTON, 2014).

Contudo, se a Internet "das pessoas" é considerada uma verdadeira revolução, a IoT proporciona muito mais, pois visa a ampliar a capacidade de conexão constante de compartilhamento de dados, o controle, a distância, dentre outras capacidades para o mundo físico. Deste modo, permite que objetos físicos armazenem, enviem e recebam informações de maneira que possam transformar a

forma como as pessoas fazem as coisas e justificar a Internet das Coisas como um novo conceito tecnológico. (DUTTON, 2014).

Conforme aduz Ashton (2009), a expressão Internet of Things (IoT) surgiu em 1999, como título de uma apresentação de Kevin Ashton para a empresa Procter & Gamble. Segundo o autor, sua finalidade era apresentar uma realidade na qual os computadores colheriam dados e assim saberiam tudo sobre as coisas. O homem seria desnecessário nessa coleta, diminuindo os desperdícios, perdas e custos, através do rastreio e contagem de todas as coisas.

Com o aparecimento da IoT, todo o tipo de coisas físicas, desde termostatos e carros, até roupas, conseguem comunicar entre si e gerar dados, informação e ações que prometem transformar uma grande variedade de produtos e serviços.

Um exemplo atual é o uso da IoT nas casas e prédios inteligentes, o qual auxilia na redução do consumo de eletricidade e outros insumos, das despesas operacionais e no consequente aumento da satisfação dos moradores. Esse aumento é dado através do uso de sensores, que são uma peça-chave no monitoramento do consumo e na detecção das necessidades do usuário. No caso das cidades inteligentes, mostra-se possível a otimização do uso da infraestrutura da cidade e o aumento na qualidade de vida dos cidadãos quando usada em sistemas para controle de tráfego e estacionamentos, além do sensoriamento da qualidade do ar, com informações sendo mandadas diretamente para os órgãos de saúde. Além disso, é possível também a redução de calamidades, como grandes incêndios, uma vez que o monitoramento constante torna possível chamar o corpo de bombeiros ao menor sinal de fogo, evitando que esse tome grandes proporções.

Com o advento desta indústria, surgem inúmeras questões legais e sociais. As fundamentais áreas de legislação a serem afetadas pela IoT são a privacidade e a segurança. Pois a ideia de partilhar dados coletados para uma finalidade está repleta de novas pontos de ordem ética, de ordem política e de ordem prática, mas o fato de cada vez mais compartilhamento é fundamental para permitir que a IoT seja capaz de aumentar aplicações que envolvem o conhecimento do comportamento.

Combinar os dados de diferentes indivíduos torna-se a chave para o pleno funcionamento da IoT, contudo gera um desafio recorrente ainda maior em relação a privacidade e segurança dos seus usuários. (DUTTON, 2014).

Em relação à segurança, o ideal seria a introdução de protocolos de forma a garanti-la ao utilizador. A importância da privacidade também aumenta

exponencialmente, haja vista que a abundância de informação sobre a vida de uma indivíduo vai aumentar à medida que a quantidade de dispositivos conectados à IoT também aumenta. Os consumidores desses produtos irão exigir um maior controle sobre as suas informações privadas, enquanto as empresas vão querer armazenar essas informações para fins de marketing e comercial.

A Internet das Coisas (IoT) faz com sucesso a transição de um conceito futurista à realidade tangível, estando cada vez mais presente no dia a dia.

4. PRIVACIDADE, SEGURANÇA E PROTEÇÃO DOS DADOS

Um dos maiores desafios que causa evidente preocupação acerca da IoT é a privacidade e a forma como a segurança dos dados e dos próprios consumidores irá ser garantida. Assim como já ocorre com os equipamentos de medição inteligente e automóveis cada vez mais autônomos, há um amplo volume de dados provendo informações sobre o uso pessoal dos aparelhos que, se não forem seguros, pode abrir caminho para violações de privacidade. Isto é um desafio, pois a quantidade de informação gerada pela IoT é essencial para a melhoria serviços e comodidades aos usuários.

O termo privacidade pode ser definido em três áreas segundo Weber e Weber (2010) sendo elas: O espaço físico, que pode ser entendido como uma barreita contra objetos indesejados ou sinais, dessa forma a privacidade está perto de segurança de infraestrutura; A capacidade de tomada de decisão no que tange ao fluxo de informações com a finalidade de proteger a liberdade de uma pessoa a fazer escolhas a respeito de seus dados; E o controle de uma pessoa ou usuário sobre o processamento da informação envolvendo desde a aquisição, divulgação até uso de informações pessoais.

Nessa linha, Marx e Murky (2001) definiram quatro planos de privacidade perceptíveis pelas pessoas, também destacados por Chabrindon et al. (2014) para determinar a modo como as pessoas compreendem as violações a sua privacidade, sendo estes níveis nomeados como fronteiras: A fronteira natural obsta a sua presença, sentimentos ou emoções, de ser percebido através de um dos sentidos humanos, como paredes, portas, cartas privadas, telefone e e-mail; A fronteira da sociedade abrange expectativas das pessoas para alguns papéis sociais, por exemplo médicos, membros do clero, advogados, pois são profissionais que não vão divulgar

informações confidenciais; A fronteira espacial ou temporal separa a informação dos diversos períodos ou aspectos da vida da pessoa; E a fronteira dos efeitos efêmeros ou transitórios, que se fundamentam na ideia de que a interação e comunicação são esquecidas em breve.

Controlar os dados recolhidos por todos os artefatos conexos que compõem o espaço inteligente torna-se uma tarefa essencial para o desenvolvimento dessa nova realidade. (CHABRIDON et al., 2014). Porém, o controle deste novo espaço complexo, a troca de dados constante entre as coisas e as pessoas, e entre as coisas e outras coisas, precisa incidir de maneira anônima, de modo que os proprietários e criadores não tenham conhecimento desses dados. Entretanto, Chabrindon et al. (2014) asseveram que resguardar a privacidade através do isolamento não é mais uma opção no mundo de hoje, diante da expansão da informação e comunicação.

Solove (2006) aduz que nenhuma definição é capaz de satisfazer a todos os aspectos compreendidos pela privacidade, mas que existem diversas formas de privacidade, taxando uma visão geral das atividades que possam levar à sua violação, sendo elas:

• A coleta de informações, pois, ainda que a informação comumente seja recolhida com o consentimento do proprietário da informação, cobranças forçadas ou interrogatórios podem levar a violação da privacidade da pessoa;

• A disseminação da informação quando extrapolam a confidencialidade, podendo tal situação ser gerada de múltiplas formas;

• A divulgação pode acontecer com a publicação de fatos verídicos, no entanto, tais fatos podem afetar a reputação da pessoa, por meio da exposição de dados e informações privadas que possam vir a ser vinculados;

• A invasão que pode ocorrer nos dados pessoais, por meio do acesso intrusivo em sua pessoalidade e através da interferência decisória.

Como foi caracterizado por Krause (2009), apesar desta taxonomia pretender ser utilizada para proteção legal, poderá também ser útil para as tecnologias. Os fornecedores de tecnologia devem analisar sistematicamente se algum software ou tecnologia pode aumentar as chances de tal problema ocorrer, e buscar desenvolver soluções que possam mitigar tais chances. (CHABRIDON et al., 2014).

Este ambiente é composto por uma rede de dispositivos conectados com sensores. Esses dispositivos comunicam então a informação recolhida e eventos específicos a um servidor e essa comunicação pode ser realizada por meio de uma

comunicação fixa ou móvel. A privacidade deve então ser protegida ao nível do dispositivo, durante a comunicação com o servidor, em seu armazenamento e no processamento. No primeiro caso, ao nível do dispositivo, os dados e informações coletadas podem ser roubados em caso de manipulação do *hardware* ou do *software* do próprio dispositivo. Por exemplo, no caso de um hacker entrar no sistema de luzes inteligentes de uma casa e analisar a rotina de uma família, esse pode juntar informações, encontrar padrões da rotina e saber quando a casa ou um cômodo estarão vazios.

Em relação à privacidade no armazenamento no servidor, deve ser realizada uma filtragem, a fim de armazenar o mínimo de informação possível, ou então apenas aquilo que o usuário consentir. Assim, o fornecedor de cada dispositivo poderá utilizar a informação recolhida para diversos propósitos como análise ou comercialização, desde que o utilizador saiba e consinta, ou não, com o uso dos seus dados, para que não sejam utilizados para uma finalidade distinta da inicial consentida. A WP29 (2014), um órgão europeu consultor em privacidade e proteção de dados, instituído pelo artigo 29 da diretiva 95/46 CE, emitiu um parecer específico sobre o conceito de que a IoT apresenta um extenso volume de desafios no que diz respeito a privacidade e proteção de dados, alguns já existentes e outros novos, mas que continuarão a aumentar simultaneamente com o avanço grandioso de processamento de dados, derivando da evolução contínua da IoT. São identificados alguns desafios de privacidade e proteção de dados na IoT pela WP29 (2014), sendo estes:

1. Falta de controle e assimetria da informação: A interação entre coisas que comunicam de forma automática, e entre os objetos e sistemas de *back-end* acarretará na geração de fluxos de dados que dificilmente podem ser controlados com as ferramentas habituais usadas para garantir a necessitada proteção dos interesses e direitos das pessoas em causa. Esta questão de falta de controle, diz respeito também a áreas como a *cloud computing* ou *big data*, e é ainda mais desafiadora quando se pensa que diferentes tecnologias emergentes podem ser utilizadas em combinação;

2. Qualidade do consentimento do usuário: Em diversos casos, o usuário não está realmente ciente do tratamento de dados realizado por certos dispositivos. A possibilidade de abdicar determinados serviços não é uma alternativa viável na IoT, e os mecanismos costumeiros usados para obter consentimento são difíceis de aplicar.

Logo, os fabricantes e criadores devem considerar novas formas de obtenção de consentimento por parte do utilizador dos aparelhos conectados;

3. Redefinição do processamento original dos dados: A acrescente quantidade de dados causada pela IoT, combinando com técnicas modernas de análise de dados e *cross-matching* dão origem a usos secundários desses mesmos dados, que podem ser relacionados ou não com a finalidade consentida para o compartilhamento inicial aos dispositivos. Ou seja, dados visivelmente insignificantes recolhidos de dispositivos podem valer-se para inferir informações com um propósito totalmente diferente do inicial;

4. Identificação de padrões e relações: Mesmo que cada dispositivo gere fluxos de dados isoladamente, a sua coleta e posterior análise pode facilmente revelar padrões de comportamento, preferências e hábitos específicos de uma pessoa. O conhecimento pode ser causado a partir de informações comuns, por meio de capacidade de *profiling* aos dados dos sensores;

5. Limitações sobre a possibilidade de manter o anonimato ao utilizar serviços: O total desenvolvimento das capacidades da IoT causa pressão sobre as possibilidades atuais do uso anônimo de serviços e restringem a possibilidade de se manter o anonimato.

O direito à privacidade, a proteção da privacidade individual livre de vigilância nacional e internacional, o rápido progresso alcançado no domínio das tecnologias da informação e, em particular, sobre a evolução, como as impressões digitais, monitoramento de rede, sistemas de bio-consciência, processamento eletrônico de dados, e criação extensas bases de dados, têm facilitado não só a coleta e armazenamento, mas também o processamento e interligação dos dados pessoais. (ROCHELANDET; TAI, 2012; SAXBY, 2015).

No entanto Weber e Weber (2010) apontam que a preocupação com a privacidade das informações faz com que o risco de um controle rigoroso por parte do proprietário possa colocar em risco a veracidade de certas atividades, ocultando informações que possam vir a indicar determinadas atividades criminosas. Nesta perspectiva a privacidade das informações pode, a longo prazo, não ser essencialmente indissolúvel portanto, o quadro jurídico deve ser elaborado para lidar com esse fenômeno e se adaptar a esta nova realidade.

5. PERSPECTIVAS LEGAIS DA IoT

Deste modo, a privacidade e vigilância estão entre uma série de riscos sociais e éticos ligados à Internet das Coisas (SPIEKERMANN, 2013). A população de grandes metrópoles já são monitoradas diariamente por câmeras de vigilância e o advento da IoT tem a capacidade de alargar ainda mais esse potencial de vigilância, pública e privada levando-a a locais ainda não alcançados pela indústria de segurança tradicional (WEBER; WEBER, 2010).

No que se refere à proteção à privacidade de dados a LGPD tem uma preocupação prioritária em evitar invasões de privacidade e utilização de dados de pessoas naturais de forma ilegal.

Na busca de melhores resultados operacionais, empresas investem em ferramentas com o objetivo de criar soluções que se encaixem em perfis predefinidos, fazendo com que o cliente sinta que o produto ou serviço foi elaborado de forma personalizada. Porém, como toda tecnologia mal utilizada, as empresas investem em captar clientes que, muitas vezes, não solicitaram ou não deram autorização.

Ao fazer uma conexão com a IoT, nota-se que o simples fato de coletar dados - como pulsação cardíaca (ligando esse batimento a um titular), biometria (coleta de impressão digital em portarias, pontos de funcionários), informações de carros ou máquinas que o levem a conhecer o condutor de um veículo (placa de carro, horário de trabalho) - já é considerado pela lei como tratamento de dados pessoais. Esses fatos podem levar as empresas (pessoas jurídicas) e até mesmo a pessoas físicas a responderem no âmbito jurídico por violação de dados pessoais.

Paralelo a isso, os projetos de IoT, assim como quaisquer outros que contenham dados pessoais, deverão estar preparados para serem transparentes, pois a lei concede aos titulares o direito da autodeterminação informativa. A qualquer tempo, os titulares dos dados podem, desde que façam um pedido expresso, querer saber o que existe de dados sendo tratados pelas organizações. As ferramentas devem permitir a modificação de dados inexatos, acréscimo de dados inexistentes, exclusão dos dados que estão ali sem o prévio consentimento do titular e, ainda, em caso de uma episódio de abuso ou violação de dados, deve conduzir caminhos acessíveis que permitam saber o que aconteceu, quando, por que e quem violou os dados. Essa necessidade atenta-se ao fato de os responsáveis serem obrigados a

conhecerem estas informações para mitigarem ou resolverem o dano causado aos titulares usuários.

Entre os diversos desafios de curto prazo com o impacto sobre a nova realidade, destaca-se a obrigação de definir táticas de gerenciar redes e critérios para certificação e homologação de equipamentos e dispositivos em linha com as melhores práticas e diretrizes internacionais. Promover uma comunicação estruturada e eficaz de orientação aos agentes de mercado e usuários sobre as competências e atribuições, visando assegurar a resolução ágil e eficiente dos problemas por eles enfrentados.

No médio prazo, os desafios calculados (ANATEL, 2021) podem ser divididos em três tópicos:

- A fiscalização da conformidade dos entes regulados em relação às regras definidas pela Anatel e outros órgãos com jurisprudência sobre temas de cibersegurança e proteção de dados;
- A identificação contínua de vulnerabilidades de rede internamente, de modo a proteger dados armazenados pela Agência, e externamente, por meio do acompanhamento, junto aos agentes de mercado, do consumo de dados pela população e da manutenção de infraestruturas de telecomunicações por parte das empresas do setor;
- A garantia da execução da Lei Geral de Proteção de Dados Pessoais (LGPD) em relação ao uso de dados em redes em tempo real, que tende a se tornar ainda mais comum com a implantação de tecnologias 5G e o consequente crescimento e popularização de diferentes serviços e soluções.

Finalmente, no longo prazo os principais desafios a serem enfrentados concentram-se na necessidade de monitoramento das evoluções tecnológicas e seus eventuais riscos aos usuários de internet e à segurança de seus dados. Isso porque se deve traçar possíveis exigências regulatórias e fiscalizatórias geradas pela maior complexidade do ecossistema nacional de telecomunicações, impactado pelo aumento da quantidade de participantes no fornecimento de infraestrutura em função da oferta de soluções diversas. (ANATEL 2021)

No Brasil, a legislação tenta acompanhar o avanço da IoT, sendo essa definida pelo artigo 2º do Decreto nº 9854/2019, como “*a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou*

virtual de objetos com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade.".

Depreende-se que para que "objetos" e "dispositivos" passem a integrar o universo IoT, é necessário que esses: (BNDS, 2018)

- Recebam dados digitais vindos de sensores e/ou indo para atuadores;
- Estejam conectados com uma rede fora do objeto;
- Sejam capazes de processar dados sem intervenção humana.

Assim, a capacidade de comunicação, bem como a aplicação adicional de sensoriamento, de atuação, de coleta, de armazenamento ou de processamento de dados, permitem definir as aplicações IoT como um serviço de valor adicionado, na medida em que acrescenta ao serviço de telecomunicações que lhe dá suporte, essas novas utilidades. (BRASIL, Decreto nº 9.854, de 2019, Art. 2º, I, c/c Art. 61, caput, da LGT).

Com o mundo cada vez mais conectado, distintas soluções tecnológicas de IoT têm surgido e é crescente a possibilidade de novas aplicações.

Neste sentido, Governo Federal aprovou o Plano Nacional de Internet das Coisas (Decreto nº 9.854, de 25 de junho 2019), visando a implementar e desenvolver a Internet das Coisas no país, com base na livre concorrência e na livre circulação de dados. Além disso, a norma destaca explicitamente os ambientes prioritários de estímulo para desenvolvimento: saúde, cidades, indústrias e rural, buscando expandir as redes de telecomunicações no Brasil para os bilhões de novos dispositivos que aumentam cada dia mais e precisarão de conexão a qualquer hora e em todos lugares. (GOVERNO FEDERAL, 2020)

Com o aumento de dispositivos e a ampliação do uso da internet, a IoT apresenta vários desafios para que seu funcionamento seja eficiente já que buscam conectar bilhões de dispositivos.

A Agência Nacional de Telecomunicações - ANATEL vem adotando vários meios para regularizar a utilização de tais dispositivos na rede, dentre as quais podem-se citar a redução da carga regulatória para Prestadoras de Pequeno Porte; a dispensa de outorga para a prestação do Serviço Limitado Privado – SLP nos casos em que as redes de telecomunicações de suporte à exploração do serviço utilizem exclusivamente meios confinados e/ou equipamentos de radiocomunicação de

radiação restrita, a revisão do modelo de outorgas, aprovado pela Resolução nº 720/2020, do licenciamento de estações, aprovado pela Resolução nº 719/2020, e da avaliação da conformidade de produtos, aprovado pela Resolução nº 715/2019; além de projetos ainda em andamento que procuram promover o desenvolvimento da IoT no Brasil, como a previsão na Agenda Regulatória de Edital de Licitação para a disponibilização de espectro de radiofrequências para a prestação de serviços de telecomunicações por meio de tecnologia de quinta geração (5G), o projeto da revisão do regulamento de numeração de serviços, entre outras. (ANATEL 2020)

Estes desenvolvimentos proporcionam benefícios abundantes em termos de eficiência e produtividade, mas ao mesmo tempo provoca riscos potenciais. A tecnologia moderna traz, em questão de segundos, o acesso a ilimitados dados pessoais e constitui a possibilidade de criar perfis dos usuários, através da combinação de diferentes arquivos de dados, este é facilitado pela tecnologia de vigilância, podendo causar um aumento considerável no desrespeito a privacidade individual (GREER, 2006). Desta forma, múltiplos organismos internacionais atentam-se com tais riscos definido em suas legislações o direito à privacidade, como o apresentado pelo art. 12 da Declaração Universal dos Direitos Humanos - DUDH, Art. 17 do Pacto Internacional sobre os Direitos Civis e Políticos - PIDCP, bem como o art. 8º da Convenção Europeia dos Direitos do Homem - CEDH (ALVES, 1999; PIOVESAN, 2006; COMPARATO, 2010). Na sociedade da informação a tutela dos dados pessoais devem ser consideradas uma questão-chave, especialmente levando em consideração que o direito de privacidade a proteção dos dados deve ser uma garantia essencial para o equilíbrio entre a vida privada, no que tange as liberdades individuais e as exigências de segurança, e à necessidade de existir informações disponíveis (WEBER, 2010). Dentro desse contexto Steffek e Nanz (2008) expõem uma concepção de liberdade para a IoT, defendendo que os usuários devem ter absoluto controle sobre etiquetas e sensores, podendo desativá-los e ativa-los a qualquer tempo, sempre que desejarem, a fim de dominar a maneira como seus dados são coletados e utilizados. Portanto, parte-se do princípio que é da sociedade civil organizada que terá que surgir as iniciativas de regulamentação da privacidade na IoT (COMPARATO, 2010).

6. PROBLEMAS DE SEGURANÇA *OFF-LINE*

Desconectar os dispositivos da Internet não é a solução para a segurança desses universo. A basilar característica das “coisas” da IoT é sua habilidade de transmitir e receber dados. Mas, para isto, não precisam de uma conexão à Internet, (ENISA 2017) ou seja, não estão sujeitos ao endereçamento IP para se comunicar. Este é o caso de identificadores por radiofrequência RFID (JIA et al 2012) e Comunicação por Campo de Proximidade (NFC). O RFID é um pequeno adesivo de identificação utilizado para conduzir dados via comunicação *wireless*. Dado o seu tamanho e finura, o identificador possibilita novas aplicações, tais como o uso de cartões sem chip (*contactless*), chaves de hotéis, rastreamento de gado, entre outras. (SHEA 2017). No panorama das IoT, esse conjunto de indicadores pode ser empregado para ampliar o monitoramento, rastreamento e supervisão de objetos. (JIA et al. 2012; MIRANI 2014). A segurança das comunicações *off-line* precisam de mecanismos de autenticação próprios para este cenário para que haja o armazenamento seguro de mensagens direcionadas aos aparelhos até que possam se conectar à Internet, autenticar-se rede e recebê-las. (MICROSOFT 2018). Contudo, esse desafio vai além da comunicação *off-line*, mas de unificar tecnologias e, ao mesmo tempo, evitar que colaborem para vigilância em massa. Segurança, neste caso, é composta por camadas - *software, hardware, middleware*, - infraestrutura, extremidades da rede e servidores. Agregar diferentes tecnologias operacionais e de informação também significa combinar suas respectivas inseguranças em um novo plano de interação comunicacional (*on-line* e *off-line*) por meio da IoT. (INSTITUTO IGARAPÉ, 2018).

Diante disso, é preciso pensar com muito critério em segurança e conhecer a fundo a LGPD, e as demais leis que a complementam como por exemplo: Código Civil, Marco Civil da Internet, Código de defesa do Consumidor, Constituição Federal e as demais normas citadas no tópico acima, sempre seguindo os regulamentos e boas práticas da segurança da informação. Isso permitirá criar soluções, que da mesma maneira atendam às necessidades levantadas, porém sem que haja invasão da privacidade de nenhum cidadão, e até mesmo do capital intelectual ou do segredo industrial contido em cada solução.

7. IoT NO CENÁRIO JURÍDICO BRASILEIRO

A Constituição Federal Brasileira, em seu artigo 5º resguarda os direitos e garantias fundamentais, tais como a vida, a igualdade, a privacidade e a intimidade, garantindo a todos a dignidade, possibilitando a vida em ambiente de respeito e liberdade. Preceitos legais também estabelecidos na Lei Geral de Proteção de Dados:

> "Art. 2º: A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> II – a autodeterminação informativa;
>
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> V – o desenvolvimento econômico e tecnológico e a inovação;
>
> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

Neste sentido, os atos ligados ao respeito a privacidade possuem maior impacto nos casos práticos em relação à IoT. O conceito de privacidade acaba flexibilizado pelos legisladores necessitando intervenção do judiciário para regulamentar tais situações.

Como exemplo, o julgamento do Agravo Regimental em Recurso Especial 1871660 / RO, pelo Superior Tribunal de Justiça, afastou multa e negou provimento a decisão do Juízo de primeiro grau, que com o objetivo de subsidiar investigação de delito de tráfico ilícito de entorpecentes, determinou de quebra de sigilo de dados, para fornecer dados telemáticos, agenda, grupos, registros de acesso, chamadas, arquivos de áudio, vídeo e mensagens intermediadas por meio do aplicativo de telefonia móvel *Whatsapp*, sob pena de multa diária a cada ordem de interceptação, que somam o valor máximo de R$ 30.000.000,00 (trinta milhões de reais), além de bloqueio de fundos e responsabilização criminal.

> PENAL E PROCESSO PENAL. AGRAVO REGIMENTAL NO RECURSO ESPECIAL. INTERCEPTAÇÃO DE

> DADOS. CRIPTOGRAFIA DE PONTA A PONTA. IMPOSSIBILIDADE FÁTICA DE CUMPRIMENTO DE ORDEM JUDICIAL. ASTREINTES. DESCABIMENTO. AGRAVO REGIMENTAL A QUE SE NEGA PROVIMENTO.
>
> 1. A Terceira Seção do Superior Tribunal de Justiça, ao apreciar o RMS n. 60.531/RO, decidiu pelo afastamento de multa cominatória aplicada por descumprimento de ordem judicial em caso de impossibilidade fática decorrente da utilização de criptografia ponta a ponta.
>
> 2. Não obstante possa significar prejuízos para investigações criminais, feita a ponderação de valores, concluiu o colegiado que os benefícios advindos da criptografia ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia.
>
> 3. Agravo regimental a que se nega provimento.
>
> (AgRg no REsp n. 1.871.660/RO, relator Ministro João Otávio de Noronha, Quinta Turma, julgado em 7/12/2021, DJe de 14/12/2021.)

Em um segundo caso, foi instaurada Ação Direta de Inconstitucionalidade 4924 em face da Lei 17.107/2012 do Estado do Paraná que dispunha no dispositivo impugnado, art. 2º, caput, e § 1º, a determinação para as prestadoras de serviço telefônico serem obrigadas a fornecer, sob pena de multa, os dados pessoais dos usuários de terminais utilizados para passar trotes aos serviços de emergência.

Transitada em julgado recentemente, em 06 de abril de 2022, foi determinado Conhecimento Parcial da ação, julgando a inconstitucionalidade apenas em relação ao art. 2º, caput, e § 1º por se tratar de invasão da competência da União para legislar sobre telecomunicações e violação à vida privada e à proteção de dados.

Em outro cenário, tramita no Supremo Tribunal Federal, Ação Direta de Inconstitucionalidade 5527 em face de alguns dispositivos da Lei 12965/2012, conhecida como Marco Civil da Internet.

A propositura da ação tem como objetivo pelo partido autor declarar a inconstitucionalidade dos incisos III e IV do art. 12 da Lei n. 12.965/14 (Marco Civil), que prevê sanções como “suspensão” e “proibição” a provedores, juntamente com art. 10, §2º, que dispõe sobre a disponibilização de conteúdo de mensagens mediante ordem judicial. Conforme exposto, o partido aduz que os artigos impugnados

conferem suporte jurídico à aplicação das penalidades de suspensão temporária e de proibição do exercício de atividades dos serviços de trocas de mensagens pela internet, pois, lidas de forma combinada, elas parecem autorizar as decisões judiciais que determinam a suspensão das atividades de serviços de troca de mensagens pela Internet do aplicativo *What's App* em todo território nacional quando a empresa responsável pelo aplicativo se recusa a disponibilizar à autoridade judiciária o conteúdo de mensagens privadas trocadas por usuários submetidos a investigação criminal.

Ao curso da ação, já foram apresentadas diversas manifestações como da Câmara dos Deputados, Senado Federal e da AGU. Esses entes não concordam com a inconstitucionalidade na Lei do Marco Civil da Internet, discorrem que o art. 12 prevê sanções para o descumprimento das normas de proteção, não podendo suspender ou proibir – bloquear – completamente serviços; apenas determinadas atividades ilegais. Alegam então que o problema se encontra no campo da aplicação da lei e nas próprias determinações de bloqueio ordenadas que interpretam inadequadamente o Marco Civil.

A ministra Rosa Weber, relatora da ADI, em seu voto aduziu que qualquer tipo de bloqueio de serviço aos provedores de internet somente podem ser autorizados quando as plataformas violam a privacidade do cidadão e não o contrário. Isso porque o objeto especificado no Marco Civil da Internet é a proteção das garantias de privacidade.

A relatora constatou ainda que a Constituição assevera a inviolabilidade do sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas, exceto por ordem judicial, nas investigações criminais e persecuções penais. Ressaltou também que o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e é "amplamente celebrado, inclusive no âmbito internacional, por situar nosso país em posição de vanguarda no tocante à proteção dos direitos e à previsão de deveres para os usuários da rede mundial de computadores". (WEBER, 2020)

Diante disso, temos que o direito fundamental a privacidade não deve ser relativizado posto que é uma garantia estendida a todos.

"Mais do que estações para fazer e receber chamadas, ou meros espelhos negros quando inativos dentro dos bolsos e bolsas, os telefones celulares, uma vez

ativados em nossas mãos, convertem-se em janelas luminosas para a nossa intimidade”. (WEBER, 2020)

8. CONCLUSÃO

Diante de tudo que foi exposto e evidenciado, conclui-se que há uma grande preocupação em regularizar a normatização, diretrizes que orientam e dão manutenção, tanto aos usuários dos dispositivos quanto aos seus fornecedores.

A LGPD trouxe para o mercado uma preocupação antiga, mas que agora ganha força perante a necessidade legal de segurança da informação. Os projetos de IoT em especial, no primeiro momento, focavam em coletar os dados e criar soluções com a utilização desses dados coletados.

Por esses motivos, a fim de preservar a privacidade e a segurança das informações pessoais, é preciso encarar questões complexas do ponto de vista regulatório: como será monitorado e regularizado o acesso aos dados, como os usuários poderão optar por não terem seus dados coletados, ou quais dados poderão ser compartilhados e por quanto tempo a informação será mantida, e ainda, como os abusos serão punidos, como os dados serão efetivamente anônimos, entre outras (GOLDSMITH; CRAWFORD, 2014).

Mas há outros lados que precisam estar em destaque juntamente com os aspectos regulatórios. Uma deles se refere à conscientização dos cidadãos e usuários no que tange ao valor de sua privacidade e do modo como os fornecedores de serviços e os órgãos governamentais responsáveis lidam com essa questão. Além de promover políticas de transparência e informação sobre coleta e a utilização de dados, a administração pública e entidades privadas deve promover campanhas e materiais orientem e preparem os indivíduos para essa realidade, especialmente diante das influentes redes sociais que disseminam as “*fake news”*.

Finalmente, cabe destacar a necessidade de engajamento com a comunidade técnica e de desenvolvedores, que podem aliar as tecnologias e produtos utilizados tornando mínimos os riscos de violações e abusos aos dados dos cidadãos e propondo soluções de compartilhamento que adotem técnicas reforçadas de segurança da informação, como a criptografia forte, e ainda métodos sofisticados de anonimização de dados pessoais. Mesmo que crescente, as tecnologias de coleta e

análise de dados ainda são relativamente novas, este é o momento oportuno para lidar com as implicações de privacidade, para que no futuro não incorram em erros do passado.

REFERÊNCIAS

1. ALVES, José Augusto Lindgren. A declaração dos direitos humanos na pós-modernidade. Os direitos humanos e o direito internacional. Rio de Janeiro: Renovar, p. 139-166, 1999

2. ANATEL, 2017. Relatório anual. Disponível em: <https://sistemas.anatel.gov.br/anexar-api/publico/portal-publicar/documentos?numeroPublicacao=348639> Acesso em: junho de 2022.

3. ANATEL, 2020. Cartilha orientativa sobre aspectos regulatórios da Internet das Coisas (IoT) e dos Sistemas de Comunicação Máquina a Máquina. Disponível em: <https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/a028ab5cc4e3f97442830bba0c8bd1dd> Acesso em: junho de 2022

4. ANATEL, 2021. RELATÓRIO ANUAL DE GESTÃO. Disponível em: <https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO7aDSQqqzWEJuAhvQ7vBZ6bhePEKS7H7K2efSWLiiXPuEib2Qdl3GibsRtMqCa1dRhDvWTMgvRVhLgrlYJgxIJ9> Acesso em: junho de 2022.

5. ASHTON, Kevin. That ‘Internet of Things’ Thing. RFID Journal, 2009.

6. BNDS. Cartlha de Cidades, 2018. Disponível em: <bndes.gov.br/wps/wcm/connect/site/db27849e-dd37-4fbd-9046-6fda14b53ad0/produto-13-cartilha-das-cidades-publicada.pdf?MOD=AJPERES&CVID=m7tz8bf> Acesso em: junho de 2022

7. BRASIL. Decreto Nº 9.854, de 25 de junho de 2019**,** Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas.

8. BRASIL. LEI Nº 9.472, de 16 de julho de 1997, Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995.

9. BRASIL. Superior Tribunal de Justiça. AGRAVO REGIMENTAL NO RECURSO ESPECIAL 1871660/RO. T5 Quinta Turma.

Relator: Ministro João Otávio de Noronha. Disponível em: <https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202000952223&dt_publicacao=14/12/2021>

10. BRASIL. Supremo Tribunal Federal. ADI/DF 4924. Relator: Gilmar Mendes. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4382183>

11. BRASIL. Supremo Tribunal Federal. ADI/DF 5527. Relator: Ministra Rosa Weber. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282>

12. CETIC.br, 2017. TIC Domicílios 2017. CETIC.br. Disponível em: https://cetic.br/media/analises/tic_domicilios_2017_coletiva_de_imprensa.pdf Acesso em: junho de 2022.

13. CHABRIDON, Sophie et al. A survey on addressing privacy together with quality of context for context management in the Internet of Things. annals of telecommunications-annals des telecommunications, v. 69, n. 1-2, p. 47-62, 2014.

14. COMPARATO, FABIO KONDER. A AFIRMAÇAO HISTORICA DOS DIREITOS HUMANOS. 2010. Tese de Doutorado. Universidade de Coimbra

15. ENISA, 2017. “Baseline security recommendations for IoT in the context of critical information infrastructures”. Enisa. Disponível em: <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot> Acesso em: junho de 2022.

16. GAO, Lingling; BAI, Xuesong. A unified perspective on the factors influencing consumer acceptance of internet of things technology. Asia Pacific Journal of Marketing and Logistics, v. 26, n. 2, p. 211-231, 2014.

17. GOLDSMITH, S.; CRAWFORD, S. The Responsive City: Engaging Communities Through Data-Smart Governance. Nova York: Jossey Bass, 2014.

18. GREER, Steven. The European Convention on Human Rights: achievements, problems and prospects. Cambridge University Press, 2006.

19. H. DUTTON, William. Putting things to work: social and policy challenges for the Internet of things. info, v. 16, n. 3, p. 1-21, 2014.

20. INSTITUTO IGARAPÉ, 2018. Louise Marie Hurel e Luisa Cruz Lobato, NOTA ESTRATÉGICA 31 – Segurança e Privacidade para Internet das Coisas.

21. JIA, X. et al. 2012. “RFID Technology and its applications in Internet of Things (IoT)”. IEEE. p.1282-1285. Disponível em: <https://ieeexplore.ieee.org/document/6201508/> Acesso em: junho de 2022.

22. Martinho Guimarães Pires Pereira A, Benessia A, Curvelo Da Silva Campos Alves P. Agência na Internet das Coisas. 26459 euros. Luxemburgo (Luxemburgo): Serviço das Publicações da União Europeia; 2013. Disponível em: <https://publications.jrc.ec.europa.eu/repository/handle/JRC87270> Acesso em: junho de 2022

23. MARX, Gary T. Murky conceptual waters: The public and the private. Ethics and Information technology, v. 3, n. 3, p. 157-169, 2001.

24. MICROSOFT, 2018. *Microsoft Azure IoT reference architecture*. Disponível em: <https://azure.microsoft.com/en-us/resources/microsoft-azure-iot-reference-architecture/> Acesso em: junho de 2022.

25. MIORANDI, Daniele et al. Internet of things: Vision, applications and research challenges. Ad Hoc Networks, v. 10, n. 7, p. 1497-1516, 2012.

26. MIRANI, L. 2014. The ‘Internet of Things’ may not always need an internet connection.Quartz. Disponível em: <https://qz.com/228750/the-internet-of-things-may-not-need-aninternet-connection/> Acesso em: junho de 2022.

27. PIOVESAN, Flávia. Direitos humanos. Curitiba: Juruá, v. 1, p. 15-37, 2006.

28. ROCHELANDET, Fabrice; TAI, Silvio HT. Do privacy laws affect the location decisions of internet firms? Evidence for privacy havens. European Journal of Law and Economics, p. 1-30, 2012.

29. SAXBY, Steve. The 2014 CLSR-LSPI Lisbon seminar on ‘the digital citizen’–Presented at the 9th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) 15–17 October 2014, Vieira De Almeida & Associados, Lisbon, Portugal. Computer Law & Security Review, v. 31, n. 2, p. 163-180, 2015.

30. SHEA, S. 2017. “RFID (Radio Frequency Identification)”. Tech Target. Disponível em: <https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequencyidentification> Acesso em: junho de 2022.

31. SOLOVE, Daniel J. A taxonomy of privacy. University of Pennsylvania law review, p. 477-564, 2006

32. STEFFEK, Jens; NANZ, Patrizia. Emergent patterns of civil society participation in global and European governance. Civil society participation in European and global governance: A cure for the democratic deficit, p. 1-29, 2008.

33. WEBER, Rolf H.; WEBER, Romana. Internet of Things. New York: Springer, 2010.

34. WP29, 2014. Opinion 8/2014 on the on Recent Developments on the Internet of Things. Disponível em: <http://ec.europa.eu/justice/data-protection/article-> Acesso em: junho de 2022.