CONSULTORIA LEGISLATIVA

INTERNET DAS COISAS (IOT) – DIFICULDADES PARA A REGULAÇÃO

Guilherme Pereira Pinheiro
Consultor Legislativo da Área XIV
Ciência e tecnologia, Comunicação Social, Informática, Telecomunicações e Sistema Postal

ESTUDO

OUTUBRO DE 2022

RESUMO EXECUTIVO

O presente texto tem o objetivo de explicitar um conjunto de questões que dificultam a aplicação da legislação de proteção de dados pessoais a serviços e produtos que se valem da Internet das Coisas (IoT). Nesse sentido, o trabalho analisa os seguintes problemas: (i) a falta de interface apropriada para interação com o usuário de muitos equipamentos de IoT: (ii) dispositivos de IoT utilizados por múltiplos titulares de dados; (ii) a complexidade do ecossistema de mercado da IoT, com relações contratuais sobrepostas; (iv) dificuldade, em muitos casos, de se definir a natureza do dado tratado em sistemas de IoT; e (v) dificuldades no uso prático de algumas aplicações de IoT por causa da obrigação de isonomia em relação aos pacotes de dados, graças ao princípio da neutralidade de rede.. Diante de cada item, iremos abordar brevemente uma possível solução ou encaminhamento da questão.

Palavras-chave: Internet das Coisas; Regulação; Dificuldades

SUMÁRIO

1. INTRODUÇÃO 5
2. O QUE É A INTERNET DAS COISAS 6
3. PRINCIPAIS PROBLEMAS REGULATÓRIOS DA IOT 8
3.1 PROBLEMAS DA INTERFACE LIMITADA COM OS USUÁRIOS NA IOT . 8
3.2 OS MÚLTIPLOS USUÁRIOS NA IOT 9
3.3 COMPLEXIDADE DO ECOSSISTEMA DE MERCADO DA IOT 10
3.4 DIFICULDADE NA IDENTIFCAÇÃO DO TIPO DE DADO 11
3.5 NEUTRALIDADE DE REDE NA IOT 12
CONCLUSÕES 14
REFERÊNCIAS 14

1 INTRODUÇÃO

O presente trabalho tem por objetivo explicar os principais aspectos técnicos e jurídicos da Internet das Coisas (IoT[1]), apontando para os problemas centrais que decorrem de sua utilização e algumas propostas legislativas ou regulatórias possíveis, inclusive algumas em discussão no Parlamento brasileiro.

Há hoje a previsão de que existem mais de 29 bilhões de equipamentos conectados à Internet, dentre os quais mais de 18 bilhões cujas conexões podem ser caracterizadas como de IoT[2]. É nessa multiplicidade de conexões que são geradas, armazenadas e transferidas quantidades incalculáveis de dados pessoais e outras informações, cuja possibilidade de uso vai desde aspectos que podem facilitar ações do dia a dia e melhorar a qualidade de vida até aqueles que, potencialmente, representam uma ameaça à privacidade, à vida, à liberdade e a outros direitos fundamentais.

Tal quantidade de equipamentos e plataformas de IoT, por sua vez, é capaz de tratar dados pessoais em uma velocidade, variedade e volume cada vez maiores. Isso leva a maiores níveis de veracidade, ou acurácia, na qualidade da informação extraída, o que gera um valor significativo de retorno sobre esses dados[3]. A situação torna-se mais delicada quando consideramos a crescente capacidade de processamento num contexto de Big Analytics. O Big Analytics é a expansão da capacidade de analisar dados e possui, simultaneamente, três perspectivas: (i) a análise descritiva, que peneira e prepara o conjunto de dados que será utilizado, o material para fins de avaliação; (ii) a análise preditiva, que identifica os melhores indicadores a serem empregados numa possível relação causal; e (iii) a análise prescritiva, que elabora recomendações de ação, valendo-se dos conhecimentos descritivos e preditivos para finalidades específicas[4].

Na última década, saímos de uma situação em que informações eram acessadas por meio da internet para outra em que existe uma progressiva quantidade de

[1] O termo Internet das Coisas é uma tradução literal da expressão em inglês *Internet of Things*, de onde deriva a sigla IoT.
[2] Ver em: https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/ushering-in-a-better-connected-future . Acesso em 13/09/2022.
[3] São os chamados 5Vs do Big Data: velocidade, volume, variedade, veracidade e valor. Vide em: Burri, Mira. Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer (in) New Developments in Competition Behavioural Law and Economics (coord. Klaus Mathis and Avishalom Tor). Cham: Springer, 2019, p. 242.
[4] Hoffmann-Riem, Wolfgang. Teoria Geral do Direito Digital. Transformação Digital e Desafios para o Direito Digital. São Paulo: Forense, 2022, p. 21.

serviços e equipamentos conectados, geralmente sem nossa intervenção e conhecimento[5]. Em estudo recente, mostrou-se que dispositivos de IoT rotineiramente transferem e compartilham dados de maneira pouco segura ou transparente. Assim, dentre 34 mil equipamentos considerados no levantamento, incluindo smart TVs, assistentes digitais, equipamentos de streaming, campainhas caseiras com vídeo embutido, entre outros, apenas 72 fizeram contato com mais alguém além dos fabricantes aos tratar dados pessoais[6].

Com a expansão da IoT, o emprego de sensores será ubíquo, cercando e monitorando as pessoas 24 horas por dia, num ecossistema inteligente que colhe constantemente os dados passivos dos titulares, permitindo um nível profundo de perfilização e personalização de serviços[7]. Oportuno notar, inclusive, que o 5G da comunicação móvel foi projetado tendo como um dos seus pilares servir de suporte para a IoT.

Tudo isso torna mais difícil aplicar o princípio da necessidade, previsto na Lei Geral de Proteção de Dados Pessoais – LGPD, e que prescreve o minimalismo na coleta e processamento dos dados. De fato, a regra de que deveriam ser tratados apenas os dados pessoais absolutamente indispensáveis para se atingir um objetivo pré-determinado e estritamente delimitado é cada vez mais difícil de ser cumprida.

Nesse contexto, iremos analisar alguns dos principais desafios que se colocam na regulação da IoT. Na sequência, após definir o que vem a ser a IoT e identificar algumas de suas aplicações essenciais, analisaremos os principais problemas que incidem atualmente no uso da tecnologia, especialmente em relação a questões atinente a privacidade e proteção de dados pessoais.

2 O QUE É A INTERNET DAS COISAS

A União Internacional de Telecomunicações – UIT definiu a Internet das Coisas como uma "infraestrutura global da sociedade da informação, que possibilita o uso

[5] Swan, Edward. Internet Law. A Concise Guide to Regulation Around the World. Corydon: Wolters Kluwer, 2022, p. 136-137.
[6] Trata-se de estudo elaborado pela Northwestern University com o Imperial College of London. Dubois, Daniel *et al.* Information Consumer Exposure from IoT Devices. IMC '19, Outubro, 2019, pp. 21–23. Vide em: https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf . Acesso em 19/09/2022.
[7] Riva, Gianluigi et al. Net Neutrality Matters. Privacy Antibodies for Information Monopolies and Massa Profiling. Revista Publicum Rio de Janeiro, v. 5, n. 2, 2019, p. 14.

de serviços avançados"[8], por meio do emprego de tecnologias móveis e sem fio, da nanotecnologia, do uso de sensores inteligentes e de mecanismos de identificação por radiofrequência[9]. Tais tecnologias, quando combinadas, podem produzir uma espécie de "internet" de dispositivos eletrônicos, com a comunicação direta e intensa troca de informações entre equipamentos[10].

Andrew Murray explica que a IoT – ao contrário do caráter evolutivo da web 2.0 em relação à Web 1.0, caracterizado pela maior democratização na participação dos usuários na rede – tem caráter mais revolucionário, provocando o surgimento de uma rede inteligente, em que as máquinas são capazes de analisar todos os dados, incluindo links, conteúdos e transações entre pessoas e computadores. É o que se chama de Web semântica, cuja marca é o aumento exponencial da interface humano-máquina, permitindo a personalização de serviços via assistentes digitais e inteligência artificial[11].

A IoT pode ser utilizada para inúmeras aplicações, como, por exemplo, a gestão de irrigação para agricultura, controlando modos de qualidade, quantidade e tempo do uso da água[12], em casas inteligentes, por meio do controle de ar condicionado e calefação e da iluminação[13], em veículos autônomos para fins de segurança automotiva[14], na implementação e aplicações de cidades inteligentes, no gerenciamento de lixos e dejetos, *inter alia*. Com isso, aplicações de IoT podem aumentar a eficiência no uso de recursos escassos, reduzindo o desperdício, e incrementando a capacidade de pesquisa com o acúmulo de dados. Por consequência, a precisão das políticas públicas que decorrem de informações obtidas com o uso de IoT permite, ainda, uma otimização de seu monitoramento e reavaliação.

---

[8] ITU-T Recommendation Y.2060, note, s.8.4.

[9] Trata-se da chamada Radiofrequency Identification (RFID)

[10] Harnessing the Internet of Things for Global Development. ITU. Ver em: https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf Acesso em 12/09/2022.

[11] Outros exemplos são os de realidade virtual e realidade aumentada. Ver mais em: Murray, Andrew. Information Technology Law. The Law and Society. Oxford. Oxford Universoty Press. 2016, pp. 634-635.

[12] Garcia, Laura; et al. IoT-Based Smart Irrigation Systems: An Overview on the Recent Trends on Sensors and IoT Systems for Irrigation in Precision Agriculture. *Sensors* 20, no. 4: 1042. Disponível em: https://www.mdpi.com/1424-8220/20/4/1042 . Acesso em 12/09/2022.

[13] Zaidan, B.B; et al. A review of smart home applications based on Internet of Things. Journal of Network and Computer Applications. Vol. 97, 1 November 2017, Pages 48-65. Disponível em: https://www.sciencedirect.com/science/article/pii/S1084804517302801 Acesso em 12/09/2022.

[14] Ver em: https://www.businessinsider.com/autonomous-cars-and-the-case-against-net-neutrality-2017-7 ACesso em 13/09/2022.

Ademais, os custos de armazenamento de informações caíram significativamente nos últimos anos, gerando fortes incentivos à guarda indiscriminada de dados, sejam eles pessoais ou não[15]. De fato, torna-se mais barato guardar dados de forma genérica do que desenvolver sistemas que se adequem efetivamente aos regimes jurídicos de proteção.

Junto às variadas vantagens tecnológicas, o uso da IoT carrega, portanto, um conjunto de problemas jurídicos. Países ao redor do mundo reconhecem, já há algum tempo, as dificuldades que se originam dessas situações, com desafios para a proteção de dados pessoais e sistemas de segurança da informação[16], por exemplo. A seguir, iremos explorar alguns desses problemas e apontar suscintamente possíveis soluções.

3 PRINCIPAIS PROBLEMAS REGULATÓRIOS DA IOT

Neste item, iremos concentrar nossos esforços em vislumbrar as principais questões e eventuais soluções em relação a vários aspectos da IoT. Muitos desses problemas têm relação direta com as características únicas dessa tecnologia.

Parte da dificuldade decorre do fato de existir uma grande variedade de dispositivos de IoT, com capacidades de armazenamento e processamento de dados que variam enormemente. Desde um mero sensor que capta a quantidade de chuva e envia os dados para uma central, passando por um monitor de medição automática de pressão sanguínea que compartilha os dados com um aplicativo, até um carro conectado que registra informações sobre o uso da navegação e a otimização do motor, ou que envia informações de falhas para a concessionária, são inúmeros exemplos.

Essa diversidade cria dificuldades adicionais para uma regulação efetiva da IoT, com riscos, de um lado, para o excesso regulatório, com normas pormenorizadas e vedações amplas e descabidas, e, de outro, para a simples ineficácia de uma norma geral,

[15] Ver em: https://www.computerweekly.com/feature/Storage-now-cheaper-than-ever Acesso em 14/09/1979.

[16] Government Office for Science (2015) The Internet of Things: Making the Most of the Second Digital Revolution, p. 6. Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf . Acesso em 13/09/2022.

incapaz de apreender as especificidades de cada sistema de IoT e, portanto, fornecer uma resposta efetiva aos problemas trazidos pela tecnologia.

3.1 – Problemas da Interface Limitada com os Usuários na IoT

Um primeiro problema é que, como os dispositivos de IoT podem ser simples e de baixo custo, é menos provável que eles tenham um display ou mecanismo que permita a interação direta com o usuário. Ou seja, a interface do dispositivo de IoT pode não ser apropriada, como são os tablets, smartphones ou laptops, para interagir com o usuário e expor com transparência as políticas de privacidade e tratamento de dados pessoais. Com isso, ações como a manifestação do consentimento a termos e condições de tratamento de dados, bem como as respectivas alterações dessas condições, são fatores de preocupação no contexto do uso de dispositivos de IoT.

Para combater esse problema, seria importante que equipamentos mais simples de IoT, que coletem dados pessoais, tragam instruções por escrito nas caixas ou embalagens, admitindo algum tipo de ação que permita a existência de uma base legal para o tratamento de dados pessoais, dentro das previsões do art. 7º e 9º da LGPD[17]. Além disso, nesses casos, são essenciais soluções de *privacy by design*, que empregam metodologia que visa à privacidade desde a concepção de qualquer sistema ou produto de IoT, prevendo, desde o início do desenvolvimento do produto, uma interface amigável para o usuário exercer suas opções de tratamento de dados, e de *privacy by default*, em que se adota por padrão, no sistema de IoT, a configuração de privacidade mais restritiva.[18]

3.2 – Os Múltiplos Usuários na IoT

Outra particularidade da IoT está no fato de que, ao contrário de telefones móveis e tablets, que geralmente pertencem e são manuseados sempre por um só indivíduo, dispositivos de IoT são utilizados por múltiplos usuários. É o caso de carros inteligentes de propriedade do pai ou da mãe, mas usados por toda a família, ou que foram deixados num

[17] Os artigos 7º e 9º trazem as bases legais que permitem o tratamento de dados pessoais e de dados pessoais sensíveis, respectivamente.
[18] Jimene, Camila do Vale. Reflexões sobre Privacy by Design e Privacy by Default: da Idealização à Positivação. (in) Comentários ao GDPR: Regulamento geral de Proteção de Dados da União Europeia (coord. Viviane Nóbrega; Renato Blum). São Paulo: Thomson Reuters, 2018, p. 174.

manobrista ou numa loja especializada e podem ter seus dados acessados. Ou um apartamento alugado, que conta um sistema de segurança e monitoramento de IoT, com informações do locador passíveis de acesso por parte do locatário. Ou, ainda, um equipamento médico que monitora sinais cardíacos e é utilizado por vários pacientes ao longo de sua vida útil, armazenando tal informação para controle médico.

Um exemplo simples ajuda a compreender esse ponto. Tome-se um eventual sistema de IoT que monitora quantidades de comida na geladeira de uma residência. A geladeira é usada por todos os membros da família e empregados que eventualmente lá trabalhem. Nesse caso, quem deverá fornecer o consentimento para a coleta de dados, a fim de que o equipamento passe a funcionar? Todos da família? Alguns? Cada um deles poderá personalizar suas escolhes e alterá-las a todo momento? E quando houver alterações nos termos e condições, novamente todos deverão manifestar uma nova aceitação, um novo consentimento?

A LGPD parece ter sido desenhada pensando apenas no uso de serviços ou produtos que tratam dados pessoais por um titular a cada vez. Como se houvesse uma relação jurídica única e unidirecional entre o titular e o respectivo controlador. Esse desenho jurídico dificulta bastante a compreensão dos usuários em situações em que vários usuários manuseiam um mesmo dispositivo de IoT.

3.3 – Complexidade do Ecossistema de Mercado da IoT

Uma terceira dificuldade da relação entre IoT e proteção de dados pessoais está na complexidade do ecossistema de mercado que envolve os usos e aplicações dessa tecnologia.

Vejamos um exemplo. Imagine-se um serviço automatizado com IoT, que controle a segurança e o acesso a um prédio. Nesse cenário, teremos uma intrincada relação jurídica que envolve a coleta, recepção, distribuição, processamento e arquivamento de dados entre: (i) o proprietário do prédio; (ii) a empresa que presta o serviço de segurança e que é a dona do dispositivo de IoT; (iii) o provedor de telecomunicações que permite o envio e recebimento dos dados no âmbito do sistema de IoT; (iv) o fabricante do dispositivo; (v) o provedor do serviço de nuvem onde os dados são armazenados ou processados; (vi) a

empresa que desenvolve o software ou as aplicações utilizadas pelo equipamento; (vii) as empresas ou pessoas que alugam salas no edifício, utilizam o serviço, etc.

Nesse panorama, embora certamente haja relações contratuais que permitam o tratamento de dados pessoais entre alguns dos atores mencionados, é provável que inexista qualquer "projeto unificado" que uniformize as permissões, consentimentos e vedações ao tratamento, gerando potenciais descompassos no entrelace dos contratos bilaterais ou na cadeia de consentimentos, por exemplo[19].

Nesses casos, o foco deve estar na aplicação do princípio da prevenção, ou seja, na adoção de medidas para evitar a ocorrência de danos em virtude do tratamento de dados pessoais nos moldes previstos pela LGPD, com o emprego de programas de governança em privacidade que, além de serem adaptados à estrutura, escala e volume das operações, também prevejam mecanismos de supervisão internos e externos

3.4 – Dificuldade na Identificação do Tipo de Dado

Uma quarta dificuldade relaciona-se à espécie de dado tratado. Como a IoT expande o universo de dados coletados, é possível o surgimento de dúvidas acerca da natureza desses dados, se são pessoais ou não.

Imagine-se um equipamento de IoT utilizado em uma fazenda e que colhe informações sobre as características do solo, a fim de saber sua composição mineral, seu nível de umidade, seu potencial para o cultivo de determinadas culturas e que tipo de adubo, fertilizante ou outros produtos podem ser usados para melhorar a qualidade do solo e torná-lo mais propício ao plantio.

Nesse caso, poder-se-ia indagar se os dados hauridos do solo pelos dispositivos de IoT deveriam ser considerados ou não dados pessoais. Por um lado, é possível arguir que são dados do solo, da natureza, não estando relacionados diretamente à pessoa natural do proprietário. No entanto, se tais dados fossem vazados, poderiam ser usados por um eventual comprador como argumento para desvalorizar a terra, já que podem ser utilizados para aferir sua produtividade. Disso resultaria severo impacto nos bens

[19] Protecting Data Privacy in the Internet of Things. Considerations and Techniques for Big Data, Machine Learning and Analytics. GSMA Report, 2019, p. 14. Vide em: https://www.gsma.com/iot/wp-content/uploads/2019/06/Protecting-Privacy-big-data-report-gsma.pdf Acesso em 19/09/2022. Acesso em 19/09/2022.

patrimoniais do proprietário da fazenda. Por outro lado, poder-se-ia também sustentar serem os dados do solo da fazenda protegidos por segredo comercial, mas que não seriam propriamente dados pessoais.

Por outro lado, seria possível argumentar serem os dados do solo efetivamente dados pessoais, já que estão relacionados, ao menos indiretamente, à pessoa do proprietário, perfazendo os requisitos contidos na definição do art. 5º, inciso I, da LGPD. Nesse caso, as características minerais do solo, coletadas pelos equipamentos de IoT, passariam a ser consideradas dados pessoais. Esse problema, de enquadramento ou não de um dado como pessoal, será cada vez mais frequente com a disseminação do uso da IoT. A quantidade absurda desses dados irá gerar confusão sobre a natureza de determinadas espécies de informações, gerando dúvida se se enquadram ou não na LGPD.

Nesse ponto, alguns autores já defendem ser necessária uma redefinição do conceito de dados pessoais, ampliando-o. Como na hipótese de dados que não são diretamente coletados de uma pessoa específica, mas que podem ser usados para - identificá-la, quando cruzados. Nesse ponto, argumenta-se que os processos de anonimização são cada vez mais raros, devido às técnicas mais apuradas de desanonimização e à capacidade de processamento[20].

Em linha semelhante, o Tribunal de Justiça da União Europeia decidiu recentemente que os dados pessoais possuem natureza expansiva, devendo ser considerado como dado pessoal sensível toda e qualquer informação que leve à conclusão sobre algum dado sensível do titular[21].

3.5 – Neutralidade de Rede na IoT

Um quinto problema está relacionado com a aplicação do princípio da neutralidade de rede, prescrito no art. 9º da Lei nº 12.965/2014, o Marco Civil da Internet. De acordo com tal princípio, a empresa que provê a infraestrutura da internet, geralmente uma empresa de telecomunicações, deve tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. Tal

[20] HOFFMANN-RIEM, Wolfgang. Teoria Geral do Direito Digital. Transformação Digital e Desafios para o Direito Digital. São Paulo: Forense, 2022, pp. 132-133.
[21] O caso tratou de funcionários públicos na Lituânia, que tiveram seus o nome dos cônjuges publicizados, da onde foi possível inferir-se a sua orientação sexual. Trata-se do caso C-184/2020.

isonomia, contudo, pode trazer vários problemas para certas aplicações de IoT, principalmente aquelas que requerem um canal dedicado e com bastante capacidade disponível, como a comunicação entre veículos autônomos, por exemplo.

Caso seja vedada a priorização do tráfego de determinados tipos de dados, como no caso citado dos veículos autônomos ou mesmo em cirurgias feitas a distância e que requerem uma comunicação máquina-máquina, teremos um problema de difícil solução. Por exemplo, caso não fosse possível priorizar o tráfego da internet para as funções de IoT nos carros autônomos, uma criança dentro de um automóvel, jogando online, poderia causar um acidente, pois os dados de comunicação dessa aplicação de IoT disputariam preferência com os necessários para o jogo online.

Infelizmente, a legislação brasileira de neutralidade de rede não prevê claramente essas exceções, embora o Decreto 8871/2016 tenha excepcionado da regra da neutralidade o caso de serviços especializados. Para se enquadrar como serviço especializado, o serviço não deve se constituir um substituto à internet em seu caráter público e irrestrito, e deve ser destinado a grupos específicos de usuários com controle estrito de admissão. Não fica claro, no entanto, quais são os serviços que de fato se enquadram nessa exceção e mesmo se ela é legal, porquanto aparentemente contrária à letra do disposto no art. 9º do Marco Civil da Internet. Tudo isso gera enorme insegurança jurídica, o que se reflete potencialmente em menos investimentos.

Há inciativas legislativas, como o Projeto de Lei nº 2498/2019, de autoria do deputado Carlos Gaguim, que procuram resolver o problema, assegurando a não aplicabilidade do princípio da neutralidade de redes a serviços e aplicações críticas que se destinarem a dar suporte a sistemas de Internet das Coisas ou demandarem priorização de tráfego, seja por motivo de segurança ou por necessidade justificada de qualidade ou de velocidade assegurada de serviço.

Por fim, vale notar que outros problemas para o desenvolvimento do ecossistema de IoT no Brasil já foram, ao menos parcialmente, endereçados. É o caso, por exemplo, das taxas do Fundo de Fiscalização das Telecomunicações - FISTEL que incidiam sobre sistemas de comunicação máquina a máquina e que poderiam inviabilizar economicamente o uso e disseminação dos equipamentos de IoT. Para resolver tal problema, a Lei nº 14.108, de 2020, igualou a zero, para as estações de telecomunicações que integrem sistemas de comunicação máquina a máquina, as taxas de fiscalização de instalação e

funcionamento, o valor da Contribuição para o Fomento da Radiodifusão Pública e a Contribuição para o Desenvolvimento da Indústria Cinematográfica Nacional (Condecine).

4 CONSIDERAÇÕES FINAIS

Vimos que a IoT possui várias características específicas. É uma tecnologia cujos equipamentos muitas vezes não possuem interface apropriada para interação com o usuário. Há equipamentos que são utilizados por múltiplos titulares de dados. Existe um ecossistema complexo de mercado com intrincadas relações contratuais que permitem a transferência ou compartilhamento de dados pessoais. É um ecossistema em que há maior dificuldade para se definir a natureza do dado tratado, e em que a obrigação de isonomia em relação aos pacotes de dados, em razão do princípio da neutralidade de rede, pode trazer problemas sérios ao uso prático da tecnologia.

Diante dessas características, que dificultam a aplicação da atual regulação de proteção de dados e privacidade ao ecossistema da IoT, é oportuno repensar mais cuidadosamente a legislação, de modo a adequar alguns pontos à nova realidade tecnológica. Ademais, algumas regras atualmente existentes, como o princípio da neutralidade de rede, merecem ser revistas nos pontos em que oferecem barreiras não razoáveis para o desenvolvimento da IoT, sem cumprir a finalidade primeira para a qual foram concebidas.

5 REFERÊNCIAS

BURRI, Mira. Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer (in) New Developments in Competition Behavioural Law and Economics (coord. Klaus Mathis and Avishalom Tor). Cham: Springer, 2019.

DUBOIS, Daniel *et al.* Information Consumer Exposure from IoT Devices. IMC '19, Outubro, 2019, pp. 21–23. Vide em: https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf . Acesso em 19/09/2022.

GARCIA, Laura; et al. IoT-Based Smart Irrigation Systems: An Overview on the Recent Trends on Sensors and IoT Systems for Irrigation in Precision Agriculture. *Sensors* 20, no. 4: 1042. Disponível em: https://www.mdpi.com/1424-8220/20/4/1042 . Acesso em 12/09/2022.

GSMA Protecting Data Privacy in the Internet of Things. Considerations and Techniques for Big Data, Machine Learning and Analytics. GSMA Report, 2019, p. 14. Vide em: https://www.gsma.com/iot/wp-content/uploads/2019/06/Protecting-Privacy-big-data-report-gsma.pdf Acesso em 19/09/2022. Acesso em 19/09/2022.

HOFFMANN-RIEM, Wolfgang. Teoria Geral do Direito Digital. Transformação Digital e Desafios para o Direito Digital. São Paulo: Forense, 2022.

ITU. Harnessing the Internet of Things for Global Development. Ver em: https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf Acesso em 12/09/2022.

ITU-T Recommendation Y.2060, note, s.8.4.

JIMENE, Camila do Vale. Reflexões sobre Privacy by Design e Privacy by Default: da Idealização à Positivação. (in) Comentários ao GDPR: Regulamento geral de Proteção de Dados da União Europeia (coord. Viviane Nóbrega; Renato Blum). São Paulo: Thomson Reuters, 2018, p. 174.

MURRAY, Andrew. Information Technology Law. The Law and Society. Oxford. Oxford Universoty Press. 2016.

RIVA, Gianluigi et al. Net Neutrality Matters. Privacy Antibodies for Information Monopolies and Massa Profiling. Revista Publicum Rio de Janeiro, v. 5, n. 2, 2019, p. 14

SWAN, Edward. Internet Law. A Concise Guide to Regulation Around the World. Corydon: Wolters Kluwer, 2022.

ZAIDAN, B.B; et al. A review of smart home applications based on Internet of Things. Journal of Network and Computer Applications. Vol. 97, 1 November 2017, Pages 48-65. Disponível em: https://www.sciencedirect.com/science/article/pii/S1084804517302801 Acesso em 12/09/2022.

UK. Government Office for Science (2015) The Internet of Things: Making the Most of the Second Digital Revolution, p. 6. Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/1 4-1230-internet-of-things-review.pdf . Acesso em 13/09/2022.