UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE NACIONAL DE DIREITO

INTERNET DAS COISAS: UMA DISCUSSÃO SOBRE A APLICABILIDADE DO CONSENTIMENTO NO AMBIENTE DE CASAS INTELIGENTES

RAFAELLA SILVA COGLIATTI

Rio de Janeiro
2023

RAFAELLA SILVA COGLIATTI

INTERNET DAS COISAS: UMA DISCUSSÃO SOBRE A APLICABILIDADE DO CONSENTIMENTO NO AMBIENTE DE CASAS INTELIGENTES

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Guilherme Magalhães Martins.**

Rio de Janeiro

2023

RAFAELLA SILVA COGLIATTI

INTERNET DAS COISAS: UMA DISCUSSÃO SOBRE A APLICABILIDADE DO CONSENTIMENTO NO AMBIENTE DE CASAS INTELIGENTES

Monografia de final de curso, elaborada no âmbito da graduação em Direito na Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Guilherme Magalhães Martins.**

Data da Aprovação: 27 / 11 / 2023

Banca Examinadora:

Prof. Dr. Guilherme Magalhães Martins

Orientador

Prof. Dra. Andreia Fernandes de Almeida Rangel

Membro da Banca

Prof. Dr. Guilherme Antônio Balczarek Mucelin

Membro da Banca

Prof. Dra. Juliana de Sousa Gomes Lage

Membro da Banca

Rio de Janeiro

2023

CIP - Catalogação na Publicação

C676i

Cogliatti, Rafaella Silva
Internet das Coisas: uma discussão sobre a aplicabilidade do consentimento no ambiente de casas inteligentes / Rafaella Silva Cogliatti. -- Rio de Janeiro, 2023.
84 f.

Orientador: Guilherme Magalhães Martins.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2023.

1. internet das coisas. 2. casas inteligentes. 3. consentimento. 4. privacidade. 5. dados pessoais. I. Magalhães Martins, Guilherme, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

AGRADECIMENTOS

Se este é o único espaço deste trabalho acadêmico no qual me é permitido expressar opiniões pessoais, gostaria de deixar claro que não é a formação, nem títulos, cargos e origens que diferenciam o grau de importância de alguém na vida de uma pessoa. E falar isso em um curso no qual muitos se colocam - ou são colocados - em uma posição de superioridade pelo simples fato de cursar Direito, é de prima importância.

A formação jurídica pode até ser um meio para fazer a diferença prática na vida de alguém, mas o agir e a forma como se trata os demais é o que de fato marca uma trajetória individual. E se hoje tenho orgulho de estar me formando na Universidade Federal do Rio de Janeiro (UFRJ), foi porque pessoas construíram esse caminho junto comigo, cada uma na sua medida e intensidade. Então, deixo aqui os agradecimentos àqueles que marcaram esta etapa.

Aos meus pais, Alessandro e Alessandra, pelo amor incondicional. Minhas lembranças ainda estão vivas de quando, com o coração apertado mas cheio de orgulho, me deixaram na rodoviária para que eu embarcasse nessa jornada que foi estudar na UFRJ. À minha irmã, Manuella, pelo verdadeiro amor fraterno e pela companhia de vida. Em vocês, eu encontro a referência do que são pessoas com quem se pode contar, mesmo quando não podemos estar fisicamente juntos.

Agradeço também ao meu irmão peludo, Denny, e ao de pena, Floquinho, por completarem a minha família e pela alegria que trazem no nosso dia a dia.

Ao meu grande amor, Pedro, por ser a extensão do meu lar e pela parceria ao longo de todo o tempo que estamos juntos. Obrigada por acreditar em mim e me encorajar nas minhas escolhas.

À minha avó, Sidnea, por me abrigar em sua casa nas primeiras semanas no meu retorno ao Rio de Janeiro. Ao meu padrinho, Ubiratan, por fazer jus aos poderes de uma procuração, se deslocar até ao Fundão para realizar a minha matrícula. Estendo meus agradecimentos a sua família, por também me acolher em sua casa durante alguns meses.

Aos demais familiares no Rio, pela ajuda nos problemas típicos de alguém inexperiente como eu, morando sozinha pela primeira vez.

Às amizades que encontrei na faculdade. Mais do que companhia para aulas, palestras, passeios no Saara e festas, com meus amigos compartilhei momentos únicos de risadas e divisão de angústias, desejos e frustrações. Juntos e com muito esforço, sobrevivemos a uma difícil trajetória acadêmica marcada por uma pandemia que, apesar de ter nos deixado 2 anos distantes, apenas fortaleceu nosso vínculo. Anna, Beatriz, Joana e Letícia, obrigada por tanto.

Ao Corpo Docente e Social da Universidade, pelo trabalho educacional, administrativo e de segurança. Reservo aqui um agradecimento especial ao Robinho, que sempre de muito bom humor às 08h00 da manhã, nunca deixou que houvesse um arranhão em um Honda Fit de mala amassada estacionado no nº 8 da movimentada rua Moncorvo Filho.

Não posso deixar de reconhecer a oportunidade conferida pela UFRJ de estudar na Universidade de Bologna. Na Itália, vivi uma experiência ímpar para a minha vida acadêmica, profissional e pessoal.

Encerrando, preciso dizer que um dos privilégios que tive por estudar em uma universidade pública foi poder sair da zona de conforto e viver a pluralidade de ideias e histórias que formam o nosso país. Em meu primeiro dia na Faculdade de Nacional de Direito me lembro de ler nos corredores que "O Direito não é neutro. A Justiça não é cega". Mas, se dependesse somente de algumas pessoas que lá conheci, hoje tendo a acreditar que a realidade poderia ser outra.

Se a conclusão de qualquer etapa sempre nos faz relembrar do percurso, é porque este último é o que realmente importa. Sou muito grata a todos que fizeram história na minha história com a UFRJ e por estarem nas já saudosas lembranças de uma eterna caloura da Minerva.

“A educação é a arma mais poderosa que você pode usar para mudar o mundo.”

Nelson Mandela, 2003.

RESUMO

O objetivo desta pesquisa é discutir a aplicação do consentimento no ambiente de casa inteligente. Como os dispositivos domésticos estão se tornando cada vez mais inteligentes devido ao crescimento da internet das coisas, preocupações jurídicas sobre a proteção dos dados pessoais coletados tendem a aumentar. Com base na literatura produzida no campo do direito e da tecnologia, esta pesquisa revela certa fragilidade no fundamento jurídico do consentimento em ambientes inteligentes. A internet das coisas já é uma realidade que o direito deve enfrentar para assegurar a proteção dos direitos humanos básicos, principalmente o direito à privacidade.

Palavras-chave: internet das coisas; casas inteligentes; consentimento; privacidade e dados pessoais

ABSTRACT

The purpose of this research is to discuss the enforcement of the consent in the smart home environment. Since domestic devices are becoming more and more smart due to the increase of the internet of things, legal concerns regarding the protection of the personal data collected tend to appear. Based on the literature produced in the field of law and technology, this research reveals a certain fragility in the legal ground of consent in smart environments. The internet of things is already a reality that law must face in order to assure the protection of basic human rights, mainly the right to privacy.

Keywords: *internet of thing; smart home; consent; privacy and personal data*

LISTA DE ABREVIATURAS E SIGLA

ABINC	Associação Brasileira de Internet das Coisas
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
CDC	Código de Defesa do Consumidor
CERN	*Conseil Européen pour la Recherche Nucléaire* (Organização Europeia para Pesquisa Nuclear)
CIJ	Corte Internacional de Justiça
CNIL	*Commission nationale de l'informatique et des libertés* (Comissão Nacional de Informática e Liberdades)
DNS	*Domain Name System* (Sistema de Nomes de Domínio)
EDPB	*European Data Protection Board*
EPC	*Eletronic Product Code* (Código Eletrônico do Produto)
ERP	*Enterprise Resource Planning*
ESG	*Environmental, Social and Governance* (Ambiental, Social e Governança)
GDPR	*General Data Protection Regulation* (Regulamento Geral Europeu de Proteção de Dados)
ICANN	*Internet Corporation for Assigned Names and Numbers* (Corporação da Internet para Atribuição de Nomes e Números)
IDEC	Instituto Brasileiro de Defesa do Consumidor
IETF	*Internet Engineering Task Force* (Força-Tarefa de Engenharia da Internet)
IoE	*Internet of Everything* (Internet de Todas as Coisas)
IoNT	*Internet of Nano Things* (Internet das Coisas Pequenas)

IoopT	*Internet of other people's thing*s (Internet das Coisas de Outras Pessoas)
IopT	*Internet of People's Thing* (Internet das Coisas das Pessoas)
IoT	*Internet of Things* (Internet das Coisas)
IP	*Internet Protocol* (Protocolo de Internet)
IPv6	*Internet Protocol version 6* (Protocolo de Internet versão 6)
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
OMC	Organização Mundial do Comércio
ONU	Organização das Nações Unidas
PETs	*Privacy Enhancing Technologies* (Tecnologias de Aprimoramento de Privacidade)
RFID	*Radio Frequency Identification* (Identificação por Radiofrequência)
TICs	Tecnologias da Informação e da Comunicação
UIT	União Internacional de Telecomunicações
WWW	*World Wide Web* (Rede Mundial de Computadores)

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Muitas pessoas certamente já ouviram falar em *smartphone*, afinal, é por meio dele que realizamos a maioria dos atos do dia a dia, seja uma troca de e-mails, uma rápida pesquisa na internet, conversa com amigos ou checagem em redes sociais. Porém, talvez poucos saibam que esse moderno celular conversa com um tipo de tecnologia conhecida em inglês como *Internet of Things* (IoT), ou Internet das Coisas em português.

De forma bem simples, IoT é uma rede de dispositivos interconectados e que interagem com o ambiente onde se encontram por meio da troca de dados. Destaca-se o fato de que, quando o primeiro celular foi lançado, ele cumpriu a finalidade para a qual foi criada, isto é, permitir a comunicação móvel e a distância entre pessoas. Contudo, ao atribuir ao celular a capacidade de se conectar com a internet, suas funcionalidades também foram ampliadas.

O mesmo vem acontecendo com outros produtos, como TVs inteligentes (*smart tv*) que oferecem serviços de *streaming*, geladeiras inteligentes (*smart fridge*) que gerenciam os alimentos, relógios inteligentes (*smartwatches*) que monitoram a saúde física, entre outros[1]. Assim, pode-se dizer que quando um produto recebe o adjetivo "inteligente" (*smart*), significa não só que possuem a capacidade de conectar com a internet, mas também com outros dispositivos, o que permite a criação de verdadeiros ecossistemas, a exemplo do que seria uma cidade inteligente (*smart city*), escola inteligente (*smart school*), ou casa inteligente (*smart house*).

Se por um lado muitos são os benefícios trazidos com advento da IoT, como a automatização de tarefas de monitoramento, gestão de dados, melhoria na comunicação para torná-la rápida e eficiente, possibilidade de novas técnicas na área da saúde, na indústria, nas cidades, no campo, entre outras; por outro, essa tecnologia traz desafios sobretudo de

[1] Milena Garcia, em um texto escrito para o TechTudo em 28 de junho de 2021, narra situações em que um relógio inteligente contribuiu para salvar vida de pessoas, como o caso em que o dispositivo avisou a mãe de um menino vítima de uma queda de penhasco e do brasileiro que descobriu problemas cardíacos. Disponível em: https://www.techtudo.com.br/listas/2021/08/apple-watch-veja-7-vezes-em-que-o-relogio-salvou-a-vida-das-pessoas.ghtml. Acesso em: 08 jul. 2022.

infraestrutura, sustentabilidade, privacidade e dados pessoais[2]. É o que fica evidenciado no final da série norte-americana *Modern Family,* ou Família Moderna, em português.

Brevemente, com o fim de trazer modernização aos seus produtos, a empresa de fabricação closets decidiu, em parceria com uma startup, criar um guarda-roupa inteligente (*smart closet*) no qual as pessoas experimentam as roupas virtualmente. O negócio fica estremecido quando descobrem um vazamento de dados, incluindo fotos e vídeos de pessoas que utilizaram o produto. A situação se agrava pelo fato de que o closet possuía uma câmera com a finalidade de escanear o corpo humano, porém, tudo era feito sem que a pessoa soubesse que estava sendo gravada.

Apesar de ser apenas um episódio de uma série fictícia, a verossimilhança precisa ser reconhecida, visto que já se pode encontrar residências estruturadas nesse sentido. No Brasil, a casa inteligente já foi, inclusive, motivo de reportagem no ano de 2022, em que um morador relata a experiência de viver em um ambiente automatizado, controlado por comandos de voz e aplicativos instalados no celular[3]. Não é à toa que grandes empresas do ramo de tecnologia, conhecidas como *Big Techs*, já possuem um setor dedicado exclusivamente a produtos inteligentes voltados, sobretudo, para vestimentas e uso doméstico.

Tudo isso provoca questionamentos no sentido de saber se as normas jurídicas de hoje estariam de fato preparadas para abarcar as novas formas de uso de tecnologias alimentadas por dados, inclusive pessoais, tal como ocorre em residências tomadas por aparelhos domésticos inteligentes. Sendo no mínimo preocupante o fato de indivíduos sequer terem conhecimento sobre o manuseio de suas informações pessoais, indaga-se sobre quais são os limites de aplicabilidade do instituto jurídico do consentimento enquanto base legal para o tratamento de dados pessoais no ambiente de casas inteligentes.

Com o objetivo de atribuir profundidade e qualidade à pesquisa, dentre os diversos cenários que envolvem a Internet das Coisas, a casa inteligente foi o objeto escolhido para ser analisado. Quanto à metodologia, o estudo se constrói com base no método dedutivo, com a técnica da revisão bibliográfica e documental tanto de autores que abordaram os aspectos

---

[2] MAGRANI, Eduardo. *A Internet das Coisas*. Rio de Janeiro: FGV Editora, 2018. 192 p. Disponível em: http://eduardomagrani.com/livro-internet-da-coisas-2018/; Acesso em: 13 dez. 2022.

[3] Reportagem produzida pelo Domingo Espetacular em novembro de 2022 sobre as grandes empresas de tecnologias. Disponível em: https://www.youtube.com/watch?v=5yJRCI6RcuM&t=0s. Acesso em: 14/08/2023.

técnicos da IoT quanto daqueles que estudam sua relação com o direito, o que permite compreender como os dois campos interagem entre si.

De início, reconhecendo a característica multidisciplinar que permeia o tema deste trabalho, foi fundamental obter referências nas áreas de engenharia e ciência da computação. Isso porque, se uma das funções do direito é regular para manter a ordem, é imprescindível que se conheça o mínimo daquilo que se pretende regular[4]. Dessa forma, uma vez compreendido o funcionamento dos produtos desenvolvidos com a tecnologia IoT, o diálogo com o conhecimento jurídico tende a ser mais concreto e menos abstrato.

Em seguida, o estudo cuidou de analisar o instituto jurídico do consentimento pelo viés da aplicabilidade no âmbito da internet das coisas, mais especificamente no ambiente de casas inteligentes. Tendo em vista a influência global, extraterritorial e transacional do campo de estudo abordado, foi preciso olhar para o direito como um todo, seja nas suas formas internas, estrangeiras e internacionais, para chegar às possíveis respostas quanto à aplicabilidade do consentimento. Contudo, considerando que o Brasil é lugar de produção da pesquisa, em primeiro lugar, parte-se de uma análise jurídica nacional para que, então, se alcance perspectiva regulatória estrangeira e internacional quando se trata de IoT.

Vale ressaltar que tanto as observações jurídicas como as de viés computacional tiveram suporte também nos estudos acadêmicos do intercâmbio realizado no primeiro semestre de 2023 na Universidade de Bolonha, na Itália. Durante este período foi possível não só aprofundar o conhecimento jurídico no que diz respeito ao direito internacional, como também ter mais familiaridade com conceitos de ciência da computação e programação[5].

Em última instância, trata-se de um trabalho com uma abordagem predominantemente qualitativa e descritiva que objetiva a produção de um conhecimento científico relevante para a academia e sociedade, sendo uma forma de retribuir o investimento feito na educação

---

[4] Depreende-se da tese de Adriana Cansian (2022, p. 13) que: "O caráter multidisciplinar que permeia a atividade de todo operador do direito em qualquer parte do mundo atual, sobretudo no que diz respeito à interface tecnológica, é claramente uma demonstração de que sem se debruçar sobre outras ciências, notadamente a engenharia da computação e todos os seus desdobramentos, será muito difícil extrair um entendimento cristalino da natureza factual que desafia os seculares institutos jurídicos."

[5] O intercâmbio acadêmico foi realizado no primeiro semestre do ano de 2023 e os cursos de direito internacional e programação para advogados foram essenciais para o desenvolvimento deste trabalho de pesquisa. Mais informações sobre a Universidade podem ser encontradas no site https://www.unibo.it/it/homepage. Acesso em: 10 ago. 2023.

pública e gratuita de ensino superior. Com ele, se espera que seja possível encontrar dados e informações que contribuam com a melhoria do sistema jurídico brasileiro no que se refere à regulação no campo de Direito e Tecnologia, mais precisamente com relação à Internet das Coisas.

1. PANORAMA SOBRE INTERNET DAS COISAS E CASAS INTELIGENTES

1.1. O caminho até a IoT

A internet das coisas é mais uma etapa da evolução da internet e de um mundo hiperconectado. Nela, objetos ("coisas") adquirem a capacidade de se conectarem à internet.

Desenvolvida na Organização Europeia para Pesquisa Nuclear (CERN) pelo cientista britânico Tim Berners-Lee, a web, ou WWW (*World Wide Web*), é um protocolo de acesso a uma rede mundial de computadores interligados que permite a troca global de dados e informações[6]. A internet é, portanto, uma grande rede que pode ser acessada de diferentes formas, sendo a web uma delas. Eduardo Magrani reforça que "o principal acesso à internet hoje no mundo se dá por meio da web, que acabou se tornando, usualmente, sinônimo da própria internet, mas que não deve ser confundido com esta" e completa dizendo que "a web usa a internet, mas ela em si não é a internet"[7].

Com o aprimoramento da rede, tornou-se comum o uso de termos como web 1.0, web 2.0, web 3.0 e web 4.0 para diferenciar os momentos em que as capacidades da rede são exploradas. Assim, enquanto a primeira geração (web 1.0) estaria associada a conexões feitas apenas na forma de leituras estáticas e sem interações mais profundas, a web 2.0 já possui características que permitem interações com os usuários[8]. O exemplo dado por Magrani são os sites de comércio eletrônico, que passaram a permitir a interação com consumidores através

---

[6] CONSEIL EUROPÉEN POUR LA RECHERCHE NUCLÉAIRE. *A short history of the Web: the Web has grown to revolutionise communications worldwide*. Homepage. Genebra. Disponível em: https://home.cern/science/computing/birth-web/short-history-web. Acesso em: 07 jul. 2022.

[7] MAGRANI, Eduardo. *A Internet das Coisas*. Rio de Janeiro: FGV Editora, 2018. P. 63. Disponível em: http://eduardomagrani.com/livro-internet-da-coisas-2018/; Acesso em: 13 dez. 2022.

[8] *Ibid*., p. 64-66.

de avaliações ou comentários (web 2.0) ao invés de apenas exibirem um catálogo de produtos disponíveis para compra (web. 1.0)[9].

Já a versão 3.0 da internet seria aquela baseada na coleta, cruzamento e interpretação de dados, com o fim de fornecer informações mais precisas e específicas[10]. É o que se vê muito nas redes sociais e plataformas de streaming, em especial quando recomendam algo ou utilizam de recursos como a publicidade direcionada.

Por outro lado, a chamada web 4.0 é marcada pelo potencial de conectar não só pessoas à internet, mas também objetos e coisas, permitindo então o desenvolvimento do cenário da Internet das Coisas[11]. Existe, inclusive, a ideia de uma indústria 4.0, ou quarta revolução industrial, viabilizada justamente pela IoT e que promete um novo modelo de produção com a ajuda de dispositivos inteligentes conectados a internet em fábricas automatizadas[12].

Dado o atual potencial de conectividade, a fabricação de dispositivos inteligentes permite o desenvolvimento de verdadeiros ambientes inteligentes, como casas, cidades, escolas, fábricas, empresas, entre outros. Por isso, também se fala na expressão "internet de todas as coisas", ou *internet of everything* (IoE), em inglês[13]. Afinal, para que se crie ambientes inteligentes, é imprescindível que haja um alto número de sensores e dispositivos conectados à rede. Eduardo Magrani destaca que:

> A internet das coisas é muito mais que uma geladeira conectada. É a progressiva automatização de setores inteiros da economia e da vida social com base na comunicação máquina-máquina: logística, agricultura, transporte de pessoas, saúde, produção industrial e muitos outros. Para isso é necessário um ambiente favorável ao acesso de um número cada vez maior de dispositivos.[14]

Além da conectividade, outras ferramentas e tecnologias também estão presentes na IoT, como os sensores, a computação em nuvem, o aprendizado de máquinas (*machine learning*) e o processamento de linguagem natural em inteligência artificial (IA). Tais pontos

[9] MAGRANI, 2018, p. 66.
[10] *Ibid*., p. 68-71.
[11] *Ibid*., p. 79.
[12] *Ibid.*, p. 79
[13] *Ibid.*, p. 73.
[14] *Ibid.*, p. 15-16.

foram elencados pela empresa de tecnologia Oracle como fundamentais para o desenvolvimento da IoT[15]. Em complemento, não se pode esquecer do desenvolvimento de aplicações e a interface gráfica na interação com o usuário, já que o controle dos dispositivos muitas vezes é feito através de aplicativos[16].

Evidentemente, toda transformação com impacto na vida cotidiana também reflete na ordem jurídica, afinal, conflitos podem surgir e o sistema jurídico deve estar preparado para dirimi-los e enfrentá-los. Nesse sentido, o governo brasileiro parece estar atento às implicações tecnológicas e, em 2019, instituiu um Plano Nacional de Internet das Coisas com o objetivo de garantir o desenvolvimento da tecnologia no país[17].

Contudo, antes de aprofundar na temática jurídica relacionada à IoT, é preciso compreender o seu funcionamento técnico bem como os efeitos concretos do uso da tecnologia, sobretudo no ambiente doméstico.

1.2. Da fabricação ao consumo de produtos e dispositivos IoT

Sabendo que a IoT funciona por meio da coleta e troca de dados e informações, sua arquitetura é baseada em tecnologias de comunicação[18] e é dividida em três principais camadas, conforme a **Figura 1**: (i) camada de percepção; (ii) camada de rede; (iii) camada de aplicação[19].

---

[15] O que é IoT?. Oracle. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/#industries-iot. Acesso em: 24 ago. 2023.

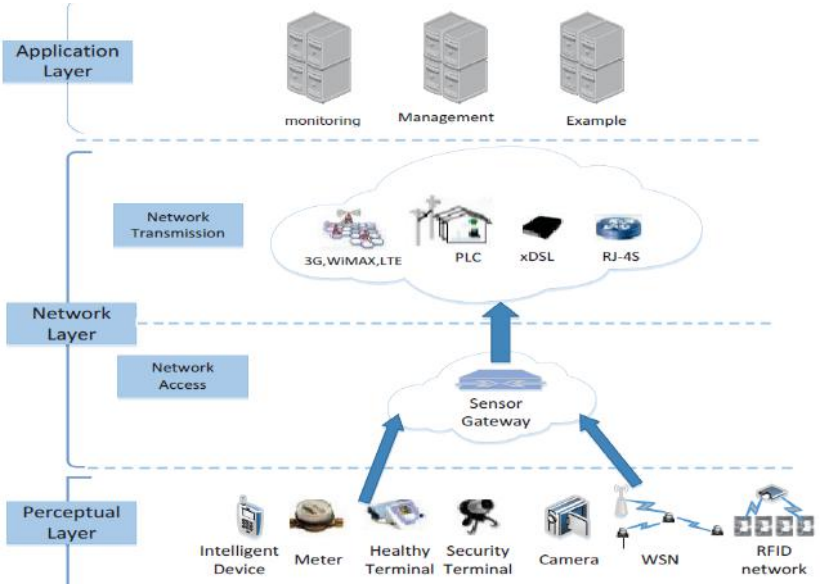
[16] O que é a IoT?. Amazon. Disponível em: https://aws.amazon.com/pt/what-is/iot. Acesso em: 24 ago. 2023.

[17] BRASIL, Decreto nº 9.854, de 25 de junho de 2019. Plano Nacional de Internet das Coisas. Brasília, 25 jun. 2019.

[18] WEBER, Rolf H.; WEBER, Romana. *Internet of Things: Legal Perspectives*. Springer Berlin, Heidelberg, 2010. P. 2. Disponível em: https://www.dhi.ac.uk/san/waysofbeing/data/governance-crone-weber-2010.pdf. Acesso em: 26 jul. 2023.

[19] LINS, Theo. Indústria 4.0 E IoT – Internet Das Coisas E Automação. Laboratório iMobilis, 22 set. 2015. Disponível em: http://www2.decom.ufop.br/imobilis/industria-4-0-e-iot/. Acesso em: 30 ago. 2023.

Figura 1 - Ilustração das camadas da arquitetura IoT



Fonte: Laboratório iMobilis[20]

1.2.1. Camada de percepção

Sabendo que a internet das coisas interage com um ambiente ou espaço físico, a camada de percepção é justamente a fase em que há a interação entre os componentes eletrônicos e os dados disponíveis no ambiente[21]. No setor automotivo, por exemplo, sensores captam possíveis falhas nos veículos, que por sua vez recomendam ou mesmo já tomam alguma decisão no sentido de evitar algum acidente e até notificar familiares sobre a ocorrência[22]. No mesmo sentido, sensores em estoques com produtos sensíveis a variações do ambiente, como fármacos, monitoram e alertam para perigos ou riscos[23].

Sensores são os componentes eletrônicos que captam os dados a serem transmitidos e utilizados na tomada de decisão[24]. Por isso, segundo Emiliano Leite *et. al* tais componentes são vistos como sendo os "geradores básicos de informações"[25]. Em seguida, o autores

[20] LINS, 2015, online.

[21] *Ibid.*, online.

[22] O que é IoT?. Oracle. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/#industries-iot. Acesso em: 24 ago. 2023.

[23] *Ibid.*, online.

[24] O que é a IoT?. Amazon. Disponível em: https://aws.amazon.com/pt/what-is/iot. Acesso em: 24 ago. 2023.

[25] LEITE, JR Emiliano; MARTINS, Paulo S.; URSINI, Edson L. A Internet das Coisas (IoT): Tecnologias e Aplicações. *In*: *Brazilian Technology Symposium*. 1., Campinas, dezembro de 2017. P. 4. Disponível em: https://lcv.fee.unicamp.br/images/BTSym-17/Papers/76926.pdf. Acesso em: 30 ago. 2023.

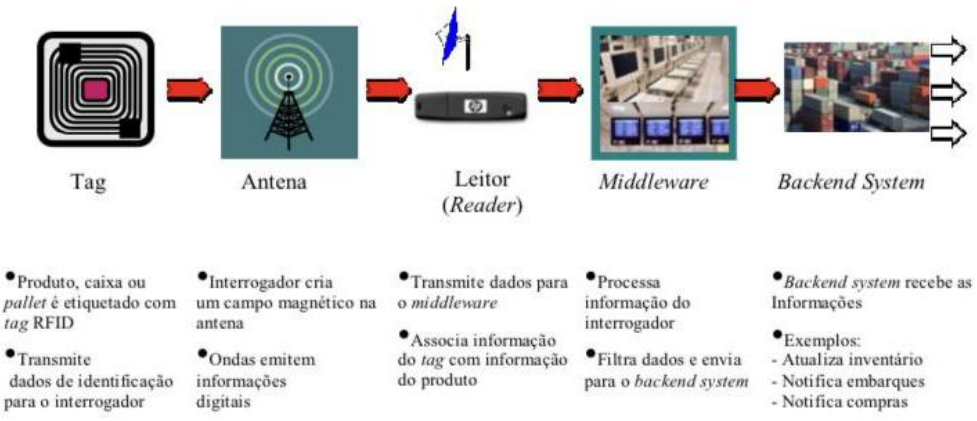
explicam que:

> Por sua simplicidade, só conseguem gerar informações específicas de Temperatura, Pressão, Umidade, Claridade,etc; o tráfego dessas informações é feito através das Redes de Sensores que podem ser Fixas ou Móveis Adhocs. Já existem sensores capazes de gerar diversas dessas informações conjuntamente e outros sensores embutidos em Etiquetas RFID evitando o uso de bateria[26].

A etiqueta RFID (*Radio Frequency Identification*) mencionada acima, é uma das diversas tecnologias tecnologias que viabilizaram a IoT. Trata-se de um sistema de identificação de objetos por meio de radiofrequência (RFID), no qual o objeto é identificado por um transponder (uma etiqueta/*tag* ou chip) e pode ser usado em comunicação de rede sem fio (*wireless/wifi*) com sistemas gerenciais de interface com o usuário[27] .

Um caso de uso comum baseado em RFID é o controle de estoques no varejo, mas a tecnologia também se aplica para pagamentos, rastreamento, restrição e controle de acessos entre outras possibilidades[28]. Basicamente os componentes de um sistema RFID são: a etiqueta *(tag*), antena, leitor, *middleware* e sistemas de *backend*.

Figura 2 - Funcionamento do sistema RFID



Fonte: NEMOTO, Miriam[29]

---

[26] LEITE, JR Emiliano; MARTINS, Paulo S.; URSINI, Edson L. A Internet das Coisas (IoT): Tecnologias e Aplicações. *In*: *Brazilian Technology Symposium*. 1., Campinas, dezembro de 2017. P. 4. Disponível em: https://lcv.fee.unicamp.br/images/BTSym-17/Papers/76926.pdf. Acesso em: 30 ago. 2023.

[27] WEBER, Rolf H.; WEBER, Romana, 2010, p. 2-3.

[28] NEMOTO, Miriam Christi Midori Oishi. *Inovação tecnológica: um estudo exploratório de adoção do RFID (Identificação por Radiofrequência) e redes de inovação internacional.* 2009. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2009. Disponível em: http://www.teses.usp.br/teses/disponiveis/12/12139/tde-18122009-105036/. Acesso em: 24 ago. 2023.

[29] *Ibid.,* p. 46.

Durante o funcionamento do sistema RFID (**Figura 2**), Miriam Nemoto explica que o objeto recebe uma *tag* que transmite dados conforme a frequência para uma antena que, por sua vez, recebe e envia para o leitor na forma de EPC (*Eletronic Product Code* - Código Eletrônico do Produto), um número de identificação único[30]. Uma vez recebidos os dados pelo leitor, este os envia ao *Middleware*, responsável pelo tratamento e filtragem dos dados a serem enviados para o último ponto: o sistema de *backend* pertencente a quem lida e gerencia as informações transmitidas[31]. Assim, uma empresa do setor de logística dotada de um ERP ("*Enterprise Resource Planning*" - sistema de gestão integrado), por exemplo, consegue notificar o seu cliente sobre a entrega de um produto.

Sem a camada de percepção, onde atua os sensores, o sistema RFID e outras ferramentas de comunicação, seria difícil ou mesmo inviável a captação dos dados necessários para o funcionamento esperado da tecnologia. Em São Paulo, no início do ano de 2023, semáforos inteligentes com algoritmos e sensores de monitoramento de tráfego foram instalados para ajustar o tempo do semáforo com o fluxo de veículos, melhorando assim a qualidade do tráfego na cidade.[32]

1.2.2. Camada de rede

A camada de rede em uma arquitetura IoT é onde se encontra a característica da conectividade, pois é nela que ocorre a transmissão dos dados obtidos no nível sensorial (camada de percepção)[33]. A **Figura 3** ilustra como as duas camadas integram o mundo físico e virtual.

---

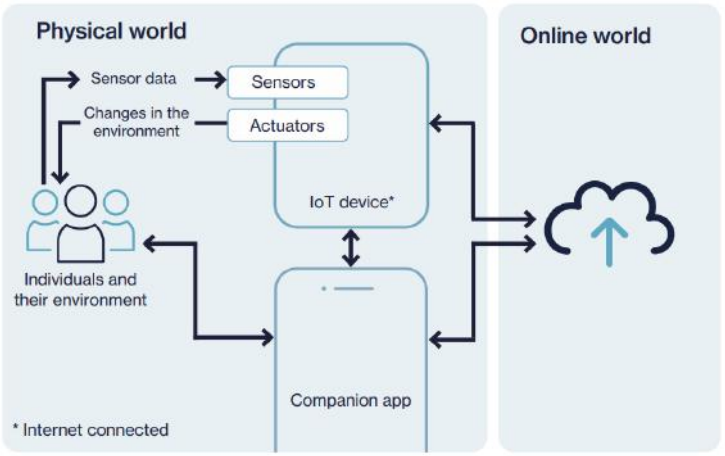
[30] NEMOTO, 2009, p. 46.

[31] *Ibid*., p. 45-50.

[32] SOUZA, Erick. São Paulo instala semáforos inteligentes; entenda como funcionam. *Estadão* [online], São Paulo, 23 ago. 2023. Disponível em: https://mobilidade.estadao.com.br/mobilidade-com-seguranca/transito/semaforos-inteligentes-sao-paulo/. Acesso em: 28 ago. 2023.

[33] LINS, 2015, online.

Figura 3 - Relação do mundo físico com o digital na IoT



Fonte: HUDIG, Anna *et al.*[34]

Tendo em vista a hiperconectividade como marca da IoT, o setor de telecomunicações exerce um papel fundamental, na medida em que, mais do que uma simples troca de dados e informações, o funcionamento de dispositivos inteligentes se dá com base na comunicação rápida. Nesse aspecto, além do wifi, a implantação da 5ª geração de internet móvel (5G) é essencial para o desempenho adequado da tecnologia IoT.

No Brasil, a Agência Nacional de Telecomunicações (ANATEL), é a instituição responsável por coordenar a introdução da nova geração de comunicação móvel que teve início no dia 06 de julho de 2022, em Brasília. Segundo a agência, trata-se de um passo a caminho de uma nova tendência tecnológica, da qual se espera ganhos econômicos com a introdução de novos produtos e serviços viabilizados pelo 5G[35]. No mesmo sentido, o atual presidente da Associação Brasileira de Internet das Coisas, Paulo José Spaccaquerche, ao citar os benefícios trazidos com o 5G, destacou o monitoramento de tráfego, iluminação e segurança pública em cidades; a saúde, com cirurgias remotas; processos automatizados em fábricas; transporte, a exemplo de veículos autônomos e também no campo, com uma agricultura mais eficiente.[36]

---

[34] HUDIG, Anna I.; NORVAL, Chris; SINGH, Jatinder. *Transparency in the consumer Internet of Things: data flows and data rights*. Reino Unido: University of Cambridge, Imperial College London, 2023. P. 11. Disponível em: http://www.iot-transparency.org/. Acesso em: 29 ago. 2023.

[35] AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Tecnologia 5G: Saiba mais sobre a tecnologia que vai revolucionar a conectividade. Gov.br: Ministério das Comunicações, 22 fev. 2021. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/5G/tecnologia-5g. Acesso em: 08 jul. 2022.

[36] SPACCAQUERCHE, Paulo. Aplicações de IoT que se tornaram viáveis com o 5G. *ABINC: Associação Brasileira de Internet das Coisas*, São Paulo, 29 de maio de 2023. Disponível em: https://abinc.org.br/aplicacoes-de-iot-que-se-tornaram-viaveis-com-o-5g/. Acesso em: 16 ago. 2023.

Falar em uma camada de rede significa, em outras palavras, que os dispositivos IoT se conectam à "rede das Redes"[37], ou seja, à internet. Em geral, a internet é organizada essencialmente pela (Corporação da Internet para Atribuição de Nomes e Números (ICANN - *Internet Corporation for Assigned Names and Numbers*), nos Estados Unidos. Trata-se de uma organização sem fins lucrativos que mantém e coordena os endereços de acesso a Internet com base em nomes e números[38]. Dessa forma, cada dispositivo que acessa a internet tem um endereço único que pode ser comparado ao funcionamento de um número de telefone[39]. Tal endereço é representado numericamente pelo IP (*Internet Protocol* - Protocolo de Internet) que, com base em regras preestabelecidas, gera um número de registro e identificação de dispositivos.[40]

A ICANN, então, gerencia todo o processo por meio do DNS (*Domain Name System*, ou sistema de nome de domínio), que permite aos usuários encontrarem o que procuram na rede[41]. Assim, ao invés de o usuário ter que digitar o número ou IP de cada endereço que deseja acessar, basta inserir o nome domínio, formado por um nome inicial e, em seguida, a identificação genérica do grupo ao qual o endereço pertence (gTLD - *generic Top-Level Domain*), como atividades comerciais (.com), governos (.gov), organizações (.org). O endereço pode ser ainda mais afunilado em um segundo nível de especificação, a exemplo da identificação de países pelo *country code Top-Level Domain* (ccTLD), .br, no caso brasileiro, .us para os Estados Unidos e assim por diante. É exatamente o que explica a instituição em seu glossário de termos técnicos e acrônimos utilizados na internet[42]:

> O Sistema de Nomes de Domínios (DNS) ajuda os usuários a encontrarem seu caminho pela Internet. Todo computador na Internet tem um endereço único - como um número de telefone - que é uma sequência complicada de números chamada de endereço IP (Protocolo de Internet). Endereços IP podem ser edifícios de serem lembrados. O DNS torna o uso da Internet mais fácil por permitir que uma sequência de letras familiar - dome de domínio - seja usada ao invés do arcano IP. Por exemplo, você precisa digitar apenas

[37] LEITE, JR Emiliano; *et al.,* 2017, p. 1.

[38]INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. *ICANN for Beginners.* Disponível em: https://www.icann.org/en/beginners. Acesso em: 29 ago 2023.

[39] INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. *ICANN Acronyms and Terms.* Disponível em: https://www.icann.org/en/icann-acronyms-and-terms. Acesso em: 29 ago 2023.

[40]SALUTES, Bruno. O que é IP. *CanalTech*, 21 out. 2023. Disponível em: https://canaltech.com.br/software/o-que-e-ip/. Acesso em: 29 ago. 2023.

[41] INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. *ICANN Acronyms and Terms.* Disponível em: https://www.icann.org/en/icann-acronyms-and-terms. Acesso em: 29 ago 2023.

[42] *Ibid.,* online.

> https://icann.org para encontrar o nosso website, ao invés do endereço de IP 192.0.43.7.
>
> Um único nome que forma a base de localizadores uniformes de recursos (URL) utilizados por pessoas para encontrar recursos na internet (e.g. páginas na web, servidores de email, imagens e vídeos). O nome de domínio identifica um endereço específico na Internet que pertence a um ente, como uma empresa, organização, instituição ou indivíduo. Por exemplo, na URL https://www.icann.org/public-comments, o nome de domínio icann.org direciona um navegador para o domínio da organização ICANN. O restante da URL direciona o navegador para um recurso específico no servidor www dentro do domínio da ICANN (neste caso, a página Comentários Públicos no site da organização da ICANN).
>
> O nome de domínio consiste em dois ou mais segmentos textuais separados por pontos. Por exemplo, no nome de domínio icann.org, a primeira parte do nome, icann, representa um domínio de segundo nível dentro da organização de domínio de nível superior. Os nomes de domínio também podem ter mais de dois segmentos, como em bbc.co.uk. Neste exemplo, bbc representa um subdomínio dentro do domínio de segundo nível ".co", que reside no domínio de nível superior ".uk." (Tradução nossa)[43].

Tudo isso se relaciona com a Internet das Coisas no sentido de que há quem defenda um domínio próprio para identificar o grupo de dispositivos IoT, ou seja, uma espécie de ".iot"[44]. Contudo, existem certas críticas em relação à falta de legitimidade, representação e transparência da ICANN, já que boa parte das questões concernentes a governança e organização da internet seriam tomadas por uma única autoridade central[45]. De acordo com Matthias Kettermann, a instituição foi o primeiro ente privado nascido de um processo não formal, não estatal, descentralizado e não internacional, mas que age em torno de um interesse global comum (tradução nossa)[46].

---

[43] No original: *The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address - just like a telephone number - which is a complicated string of numbers called its IP address (IP stands for Internet Protocol). IP addresses can be hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters - the domain name - to be used instead of the arcane IP address. For instance, you only need to type https://icann.org to reach our website, instead of the IP address 192.0.43.7. A unique name that forms the basis of the uniform resource locators (URLs) that people use to find resources on the Internet (e.g., web pages, email servers, images, and videos). The domain name itself identifies a specific address on the Internet that belongs to an entity such as a company, organization, institution, or individual. For example, in the URL https://www.icann.org/public-comments, the domain name icann.org directs a browser to the ICANN organization's domain. The rest of the URL directs the browser to a specific resource on the www server within ICANN's domain (in this case, the Public Comments page on the ICANN org website). A domain name consists of two or more textual segments separated by dots. For example, in the domain name icann.org, the first part of the name, icann, represents a second-level domain within the top-level domain org. Domain names can also have more than two segments, as in bbc.co.uk. In this example, bbc represents a subdomain within the second-level domain co, which resides in the top-level domain uk. In:* INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. *ICANN Acronyms and Terms.* Disponível em: https://www.icann.org/en/icann-acronyms-and-terms. Acesso em: 29 ago 2023.

[44] WEBER, Rolf H.; WEBER, Romana, 2010, p. 7.

[45] *Ibid.,* P. 73-74

[46] No original: *"ICANN is the first private entity borne out of a non-formal, non-statal, decentralized, and non-international (or international law-based) process to manage resources in the global common interest.* In: KETTERMANN, Matthias C. *Law and Governance of the Internet. In: _____. The Normative Order of the*

Além da ICANN, a Força-Tarefa de Engenharia da Internet (IETF - *Internet Engineering Task Force*) tem importante papel no desenvolvimento da internet das coisas. Como explica Bruno Santos *et al.*, "não se imaginou que a Internet cresceria e poderia ter dezenas de milhares de pontos finais em uma única sub-rede, tal como agora é previsto para a IoT"[47]. A solução veio com a criação do IPv6 (padrão 6LoWPAN) pela IETF. A nova versão permite que objetos inteligentes se comuniquem de forma mais eficiente com a rede, na medida em que melhora o envio de pacotes de dados por dispositivos com capacidade computacional limitada.[48]

Considerando o alcance transnacional da rede, seria, no mínimo, interessante debater sobre a necessidade de maior participação global dos Estados Nacionais. Ademais, no que diz respeito especificamente à governança da internet das coisas, Rolf Weber e Romana Weber defendem que empresas e clientes também são partes interessadas e que, por isso, devem poder participar do processo de governança da matéria[49]. Para tanto, sugerem os fóruns como sendo um ambiente propício para discussão e participação dos processos de tomada de decisão sobre IoT.[50]

De toda forma, fato é que graças ao acesso à internet os objetos dito inteligentes conseguem realizar a troca de dados que, por sua vez, serão processados no nível seguinte da arquitetura: a camada de aplicação.

Internet: A Theory of Rule and Regulation Online. Estados Unidos da América: Oxford University Press, 2020. P. 106-107. Disponível em: https://academic.oup.com/book/39694. Acesso em: 05 jul. 2023.

[47] SANTOS, Bruno P.; *et al.* Internet das Coisas: da Teoria à Prática. *In:* AUGUSTO, F. S.; LUNG, L. C.; GREVE, F. G. P.; FREITAS, A. E. S. F. (Org.). Livro de Minicursos. *XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*; Porto Alegre: SBC, 2016, P. 14. Disponível em: https://bps90.github.io/assets/files/MinicursosSBRC2016.pdf. Acesso em: 28 set. 2023.

[48] *Ibid.,* p. 15.

[49] WEBER, Rolf H.; WEBER, Romana, 2010, p. 74.

[50] *Ibid.,* p. 74-75.

1.2.3. Camada de aplicação

A terceira camada da arquitetura IoT compreende as aplicações, responsáveis pelo processamento de dados e interface com o usuário[51]. É nesse nível que ocorre a interação entre dois ou mais dispositivos conectados (“coisas”) e deles com as pessoas.

Com relação ao usuário, as aplicações são o meio pelo qual o indivíduo pode coordenar os aparelhos IoT. Para um médico, basta, por exemplo, desbloquear um *smartphone* ou um computador e dele mesmo, encaminhar um paciente ao hospital com base nas informações de saúde coletadas por aparelhos e recebidas em tempo real.[52]

No que tange ao ambiente doméstico, Emiliano Leite *et. al.* exemplificam a camada de aplicação pelo controle de luzes, portas e eletrodomésticos pelo *smartphone* do morador, que poderia até receber uma lista de compras da própria geladeira (*smart fridge*)[53]. O mesmo ocorre com o uso de comandos de voz através do processamento de linguagem natural visando a execução de tarefas, como o caso da Alexa, inteligência artificial desenvolvida pela Amazon.[54]

No entanto, essa interação com o usuário depende do processamento de dados. Segundo Santos *et al.*, a “razão de ser” da internet das coisas está em obter conhecimento e inferências com base nos dados coletados pelos sensores na camada de percepção[55]. Visando o funcionamento ideal da IoT, os autores explicam que é preciso se atentar a modelagem dos dados, o armazenamento e o pré-processamento para se alcançar o conhecimento buscado, afinal, os maiores problemas quando se lida com dados são a imperfeição e inconsistência das informações[56]. Nas palavras de Santos *et al.*:

---

[51] LINS, 2015, online.

[52] LEITE, JR Emiliano; *et al.,* 2017, p. 6.

[53] *Ibid.,* p. 5.

[54]CASA Inteligente com Alexa. **Amazon.** Disponível em: https://www.amazon.com.br/b?ie=UTF8&node=20000328011. Acesso em: 31 ago. 2023.

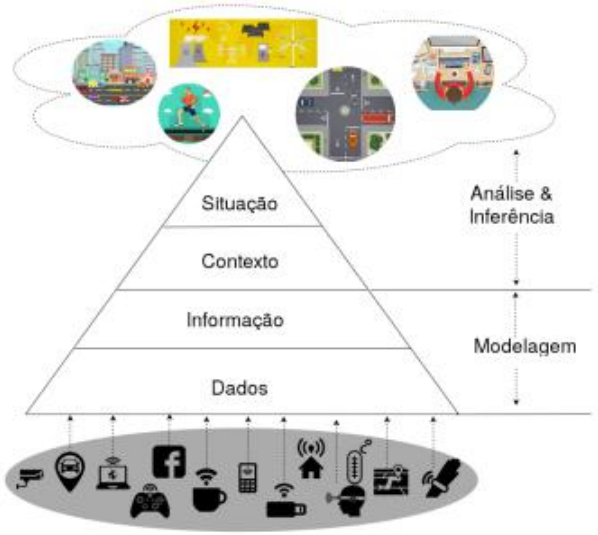
[55] SANTOS, Bruno P.; *et al.* Internet das Coisas: da Teoria à Prática. *In:* AUGUSTO, F. S.; LUNG, L. C.; GREVE, F. G. P.; FREITAS, A. E. S. F. (Org.). Livro de Minicursos. *XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*; Porto Alegre: SBC, 2016, P. 35. Disponível em: https://bps90.github.io/assets/files/MinicursosSBRC2016.pdf. Acesso em: 28 set. 2023.

[56] *Ibid.,* p. 39.

> Extrair um conhecimento refere-se a modelar e analisar dados definindo uma semântica de forma a tomar decisões adequadas para prover um determinado serviço [Barnaghi et al. 2012]. Tomando como exemplo o cenário de smart grids [Yan et al. 2013], uma arquitetura de IoT pode auxiliar a controlar e melhorar o serviço de consumo de energia em casas e edifícios. Por meio da IoT, as fornecedoras de energia podem controlar os recursos proporcionalmente ao consumo e possíveis falhas na rede elétrica. Isso acontece por meio das diversas leituras que são coletadas por objetos inteligentes e são analisadas para prevenção e recuperação de falhas, aumentando, assim, a eficiência e qualidade dos serviços.[57]

Em outras palavras, os dados coletados precisam ser lapidados antes de serem usados como referência na produção do conhecimento e futura tomada de decisão, conforme ilustrado na **Figura 4.**

Figura 4 - Processamento de dados para extração do conhecimento



Fonte: SANTOS, Bruno *et al.*[58]

Simbolizada acima pelo desenho de uma casa ( ), a configuração da casa inteligente (*smart home*), se dá justamente por uma rede de dispositivos domésticos interconectados e que será melhor aprofundado no tópico a seguir. Por enquanto, importa dizer, ainda, que a camada de aplicação será importante na discussão dos capítulos seguintes no que se refere à obtenção do consentimento.

[57] SANTOS, Bruno P.; *et al.,* 2016, p. 35.

[58] *Ibid.*, p. 36.

1.3. Considerações sobre aspectos regulatórios

Em virtude do caráter globalizado que pauta a internet como um todo, há quem defenda uma regulação internacional, seguindo justamente a lógica da estrutura transnacional da tecnologia. Isso porque a regulação individual da internet por cada Estado não seria tão efetiva, dado que a internet transcende os limites da soberania territorial.[59]

Segundo Kettermann, citando a doutrina alemã de Robert Uerpmann-Wittzack, a padronização mundial seria atingida com chamado direito internacional da internet, compreendido como sendo um denominador comum para todas as regras de direito internacional público referentes ao funcionamento e uso da internet[60]. Tanto Kettermann quanto Rolf H. Weber e Romana Weber defendem que a regulação da internet seja pautada pelo direito internacional. Entretanto, é preciso lembrar da predominância do caráter voluntário no momento de submissão dos Estados às normas de direito internacional. Nesse diálogo entre a soberania interna e externa[61], existe, atualmente, uma tendência dos países em repudiar o direito internacional em prol da jurisdição nacional.[62]

Por esse motivo, Kettermann chama atenção para as normas de governança, afinal, enquanto o direito internacional tradicional foca no binário do legal/ilegal, a governança permitiria conceituações e críticas aos regimes de responsabilidade[63]. De maneira geral, o autor entende que a governança da internet é a direção e a modelação, a coordenação e a integração de regras e expectativas normativas relativas ao desenvolvimento da internet.[64]

---

[59] KETTERMANN, Matthias C. *Law and Governance of the Internet. In: _____. The Normative Order of the Internet: A Theory of Rule and Regulation Online.* Estados Unidos da América: Oxford University Press, 2020. P. 60-61. Disponível em: https://academic.oup.com/book/39694. Acesso em: 05 jul. 2023.

[60] Tradução nossa. No original: *"The German equivalent of international law of the internet—Internetvölkerrecht or Völkerrecht des Netzes has been defined as "the common denominator for all rules of public international law pertaining to the functioning and use of the internet." In:* KETTERMANN, Matthias C. *Law and Governance of the Internet. In: _____. The Normative Order of the Internet: A Theory of Rule and Regulation Online.* Estados Unidos da América: Oxford University Press, 2020. P. 68. Disponível em: https://academic.oup.com/book/39694. Acesso em: 05 jul. 2023.

[61] TANZI, ATTILA. *A Concise Introduction to International Law.* 2. ed. Turim: Eleven international publishing, 2022. 285 p. P. 41-42.

[62] *Ibid.,* p. 152-159

[63] KETTERMANN, *op. cit.,* p. 129.

[64] Tradução nossa. No original: *"Internet governance is the steering and shaping, the coordinating and integrating of rules and normative expectations regarding the development of the internet." In:* KETTERMANN, Matthias C. *Law and Governance of the Internet. In: _____. The Normative Order of the Internet: A Theory of Rule and Regulation Online.* Estados Unidos da América: Oxford University Press, 2020. P. 104. Disponível em: https://academic.oup.com/book/39694. Acesso em: 05 jul. 2023.

Apesar de já existirem tentativas de estabelecer uma governança da internet, como ainda não há uma padronização normativa internacional voltada para a sua regulação global, por enquanto, as fontes do direito internacional assumem um caráter protetivo indireto, sobretudo quanto aos direitos humanos[65]. Conforme artigo 38 do Estatuto da Corte Internacional de Justiça (CIJ), princípios, costumes e tratados são as fontes que contribuem juridicamente, em alguma medida, para regulação internacional da internet.[66]

No Brasil, a norma mais próxima de regulação nacional da internet é a L. 12.965/14, conhecida como Marco Civil da Internet (MCI) ao passo que a IoT é tratada no Decreto nº 9.854 de 2019 que instituiu um plano nacional voltado para o desenvolvimento da internet das coisas. No entanto, como apenas a atuação interna do Estado não é suficiente dada as peculiaridades da tecnologia, urge pensar em soluções regulatórias que abrangem a característica de atuação transnacional dos serviços e produtos conectados à rede. Em outras palavras, regular a internet também significa considerar as tecnologias que surgem a partir dela, tal como a internet das coisas abordada neste trabalho.

Rolf H. Weber e Romana Weber, depositam expectativas na autorregulação da IoT ao invés da abordagem intergovernamental, pois não acreditam na possibilidade de um consenso em um futuro próximo[67]. Brevemente, a autorregulação ocorre quando os próprios destinatários do que poderia ser uma norma estatal já estabelecem as soluções e limites de atuação, de forma que o Estado apenas deveria intervir quando tais soluções não forem adequadas ou encontradas.[68]

Dito isso, caberia aos próprios fabricantes a regulação de seus produtos IoT, mas, dada a fraqueza deste modelo em razão da ausência de obrigatoriedade de suas provisões, não se afasta totalmente a atuação do governo através do estabelecimento de normativas basilares, que por sua vez deveriam ser tratadas em perspectiva internacional[69]. Seria, então, a chamada "autorregulação regulada", em que as normas estatais conferem certa liberdade para que os entes regulados estabeleçam suas regras, porém nos limites pré-estabelecidos pelo legislador.

---

[65] KETTERMANN, 2020, p. 121.

[66] *Ibid.,* p. 68.

[67] WEBER, Rolf H.; WEBER, Romana. *Internet of Things: Legal Perspectives*. Springer Berlin, Heidelberg, 2010. P. 26. Disponível em: https://www.dhi.ac.uk/san/waysofbeing/data/governance-crone-weber-2010.pdf. Acesso em: 26 jul. 2023.

[68] *Ibid.,* p. 23.

[69] *Ibid.,* p. 23.

Não se descarta a cooperação internacional e a participação de organismos intergovernamentais em longo prazo. Rolf H. Weber e Romana Weber cogitam que organizações já estabelecidas, como a Organização Mundial do Comércio (OMC) e a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), abriguem um comitê responsável pela governança da IoT como uma espécie de "legislador global"[70].

Seguindo o caminho da atuação das organizações internacionais na governança da internet das coisas, a União Internacional de Telecomunicações (UIT), agência da ONU especializada em tecnologias de informação e comunicação (TICs), sinaliza para a necessidade de uma taxonomia regulatória[71]. Em outros termos, estabelecer uma linguagem comum com dicionário para termos e definições chaves facilitaria a regulação do grande grupo das TICs, no qual se enquadram facilmente certos produtos da IoT, como o *smartphone*. A ITU lembra, ainda, da opção do sandbox regulatório na regulação de TICs alternativamente a regulação tradicional, pois este novo modelo consiste em promover um ambiente viável de teste e aprendizado de novas tecnologias para encontrar as melhores soluções regulatórias.[72]

1.4. "CLOME": o direito no ecossistema de casas inteligentes

Como visto, o espaço doméstico é mais um dos diversos ambientes com potencial de se tornarem inteligentes. Dados estatísticos estimam que até 2027 é esperado pouco mais de 500 milhões de usuários de produtos domésticos inteligentes[73]. Isso significa uma transformação do espaço doméstico para o que Alvi e Nabi chamam de "CLOME", um

---

[70] WEBER, Rolf H.; WEBER, Romana, 2010, p. 27-32.

[71] INTERNATIONAL TELECOMMUNICATION UNION. *Global Digital Regulatory Outlook 2023: Policy and regulation to spur digital transformation*. ITU Publications, 2023. P. 26-27. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2023-PDF-E.pdf. Acesso em: 31 ago.

[72] *Ibid.,* p. 69.

[73] STATISTA RESEARCH DEPARTMENT. *Number of households with smart home products and services in use worldwide from 2017 to 2025.* Disponível em: https://www.statista.com/statistics/1252975/smart-home-households-worldwide/#:~:text=The%20number%20of%20households%20worldwide%20using%20smart%20home,increase%20even%20further%20to%20more%20than%20530%20million. Acesso em: 25 ago. 2023.

acrônimo para *Cloud Home* (casa em nuvem)[74]. O termo está relacionado com a computação em nuvem, que facilita a infraestrutura de serviços essenciais para a IoT através da internet, como servidores, armazenamento de dados e desenvolvimento de software, possibilitando o acesso através de qualquer computador ou dispositivo móvel.[75]

Renato Opice Blum alerta para as implicações jurídicas relevantes que um ambiente como esse pode ter e exemplifica o direito contratual, pois não é difícil pensar em uma geladeira que realiza compras de forma automática conforme o estoque de produtos diminui[76]. Ademais, lembra-se da capacidade da tecnologia de detectar um padrão de consumo e preferências do morador (*profiling*), ou seja, um perfil comportamental formado e identificado por dados[77] que, no caso, pode revelar as preferências de consumo de gêneros alimentícios do indivíduo. Em outras palavras, o morador tem um serviço personalizado em troca do compartilhamento de suas informações pessoais.

Para uma melhor visualização do que de fato seria a casa inteligente, a **Figura 5** exemplifica uma residência onde existem diversos dispositivos domésticos fabricados por diferentes marcas e que estão conectados à internet. Nota-se que os aparelhos podem ser controlados pelo próprio celular do usuário (“user access and control”) e são fontes de produção de dados para negócios (“business data analysis”).

---

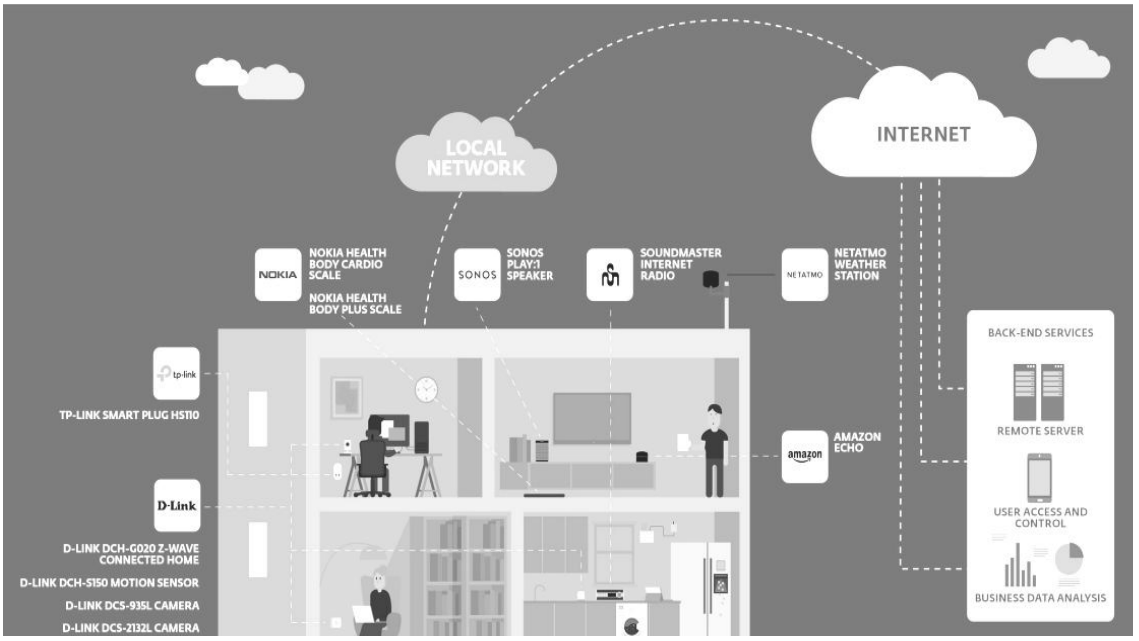
[74] ALVI, Atif; NABI, Zubair. *Clome: The Practical Implications of a Cloud-based Smart Home.* IBM Research Report**.** 2014. P. 1. Disponível em: https://dominoweb.draco.res.ibm.com/fea5c1645d95c27285257d02005c4ec1.html. Acesso em: 25 ago. 2023.

[75] WEBER, Rolf H.; WEBER, Romana, 2010, p. 16.

[76] BLUM, Renato Opice M. S. Internet das Coisas: A Inauguração do novo mundo e suas intercorrências jurídicas. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital, Direito Privado e Internet.* 4 ed. São Paulo: Editora Foco, 2021, p. 270.

[77] MARTINS. Guilherme Magalhães. A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e a sua principiologia. *Revista dos Tribunais*, São Paulo, v. 1027, p. 215, maio 2021.

Figura 5 - Ilustração de uma casa inteligente



Fonte: ANSCOMBE, Tony[78]

Basicamente, a tecnologia IoT, ocupa a casa com o compromisso de melhorar atividades cotidianas com base na utilização de dados e na comunicação entre os dispositivos, que podem automatizar tarefas diárias de limpeza e cozinha, encontrar itens perdidos e até gerenciar imóveis alugados[79]. Depreende-se do site da Amazon, fabricante e vendedora de produtos inteligentes, o potencial da IoT no ambiente doméstico, pois:

> Os dispositivos domésticos inteligentes concentram-se principalmente em melhorar a eficiência e a segurança da casa, além de melhorar as redes domésticas. Dispositivos como tomadas inteligentes monitoram o uso de eletricidade e termostatos inteligentes oferecem melhor controle de temperatura. Os sistemas hidropônicos podem usar sensores de IoT para gerenciar a horta, enquanto os detectores de fumaça de IoT podem detectar fumaça de tabaco. Sistemas de segurança doméstica, como fechaduras, câmeras de segurança e detectores de vazamento de água, podem detectar e prevenir ameaças e enviar alertas aos proprietários.[80]

Contudo, os produtos domésticos inteligentes já ultrapassam a funcionalidade de uso pessoal para otimização de tarefas diárias e segurança. Há relatos de que a caixa de som de hoje (“speaker” tal como ilustrado na **Figura 3**) poderia servir como meios de prova no

---

[78] ANSCOMBE, Tony. *IoT and privacy by design in the smart home*. Bratislava: Eset - enjoy safer technology**,** fev. 2018. Disponível em: https://iapp.org/resources/article/iot-and-privacy-by-design-in-the-smart-home/#:~:text=IoT%20and%20privacy%20by%20design%20in%20the%20smart,to%20the%20creation%20of%20a%20basic%20smart%20home. Acesso em: 13 set. 2023.

[79] O que é a IoT?. Amazon. Disponível em: https://aws.amazon.com/pt/what-is/iot. Acesso em: 24 ago. 2023.

[80] *Ibid.,* online.

âmbito do direito penal, na medida em que o objeto poderia ter registrado ruídos de um crime. É o que conta Renato Opice Blum sobre a investigação de um homicídio ocorrido nos Estados Unidos em que autoridades solicitaram o acesso a um dispositivo de som da Amazon (*Echo*) sob a justificativa de nele poderem encontrar informações sobre o crime[81]. Como diz o autor:

> Todo dispositivo com capacidade de armazenar dados tem uma história para contar. Logo, se câmeras de segurança e interceptações telefônicas não puderem elucidar os detalhes de um crime, objetos da nova geração poderão ter um importante papel. A guarda de registro de comandos de voz, transações, fruições e o próprio conteúdo armazenado podem ser absolutamente esclarecedores para investigações criminais. Desta feita, a popularização da IoT dá a vida, indiretamente, a um exército de milhares e milhares de testemunhas eletrônicas: câmeras, TVs, geladeiras, fogões, óculos, carros… Objetivas, precisas, imparciais e, potencialmente a serviço da Justiça.[82]

Assistência à idosos, pessoas com deficiência, enfermos ou com alguma doença limitadora também é um dos benefícios da internet das coisas. Um mapeamento feito na Universidade de São Paulo (USP) revelou que há uma série de pesquisas voltadas para acessibilidade através da IoT[83]. Sandra Rodrigues e Renata Fortes (2019) demonstraram que o uso da IoT para desenvolvimento de tecnologia assistiva (TA) é a solução que mais aparece nos estudos de acessibilidade[84].

O mapeamento mostrou a tendência do uso da IoT em ambiente doméstico para monitorar pessoas idosas, possibilitando, por exemplo, que cuidadores e parentes sejam alertados caso os sensores detectem uma atividade incomum ou mesmo ausência de atividade na residência, bem como localização de objetos perdidos no caso de pessoas com doenças cognitivas e automatização residencial por reconhecimento de voz para moradores com deficiência visual ou limitação de locomoção.

É preciso dizer que a assistência não se limita ao ambiente doméstico, se estendendo também ao espaço público. Pensando na IoT como tecnologia capaz de recriar ambientes, foi

---

[81] BLUM, 2021, p. 277.

[82] *Ibid.,* p. 277.

[83] RODRIGUES, Sandra Souza.; FORTES, Renata Pontin de Mattos. Uma revisão sobre acessibilidade no desenvolvimento de internet das coisas: oportunidades e tendências. *Revista de Sistemas e Computação*, Salvador, v. 9, n. 1, p. 19-40, jan./jun. 2019. Disponível em: https://revistas.unifacs.br/index.php/rsc/article/view/5708#:~:text=UMA%20REVIS%C3%83O%20SOBRE%20ACESSIBILIDADE%20NO%20DESENVOLVIMENTO%20DE%20INTERNET,um%20t%C3%B3pico%20de%20significativo%20interesse%20nos%20%C3%BAltimos%20anos. Acesso em: 22 set. 2023.

[84] *Ibid.*, p. 26.

encontrado um estudo voltado para implementação de supermercado inclusivo que se utiliza a IoT para auxiliar consumidores com deficiência visual a encontrar produtos[85], o que poderia ser feito através dos carrinhos inteligentes, já aderidos por alguns supermercados.[86]

A tecnologia, portanto, vai de encontro com a concretização de direitos consagrados no Estatuto da Pessoa Idosa (L. 10.741/03) e no Estatuto da Pessoa com Deficiência (L. 13.146/15), na medida em que promete conferir mais autonomia e melhor qualidade de vida. Contudo, é preciso ter cuidado na interação desses grupos com a tecnologia, sobretudo tendo em vista a hipervulnerabilidade sob a qual estão sujeitos, na medida em que além de figurarem por si só como grupo vulnerável, também são titulares de dados pessoais. O mesmo entendimento se aplicaria a crianças e adolescentes que vivem em ambientes inteligentes ou manuseiam produtos desta categoria.

Por outro lado, além dos benefícios que a tecnologia oferece, sobretudo no ambiente doméstico, a introdução dos dispositivos IoT no mercado gera preocupações acerca de sustentabilidade e consumismo na sociedade. Isso porque, não haveria utilidade em atribuir a tecnologia a um objeto que funciona bem sem ela, pois apenas o torna mais caro sem que ocorra de fato um aprimoramento relevante no produto[87]. Daí se tem a divisão do que seria uma internet das coisas "úteis" e "inúteis"[88].

Além da tendência de produtos inteligentes aumentarem o consumismo, existe o problema da sustentabilidade na perspectiva ambiental, visto que a IoT gera lixos eletrônicos potencialmente danosos sem o descarte correto. Sem falar da possibilidade de danos à saúde humana decorrentes da energia eletromagnética emitida pelos dispositivos eletrônicos.[89]

Isto posto, enquanto o consumismo encontra saída na propagação do consumo consciente, questões relativas à sustentabilidade podem ser amenizadas pelo emprego das práticas corporativas voltadas ao ESG (*Environmental, Social and Governance*, ou

---

[85] RODRIGUES, S.; FORTES, R., 2019, p. 29.

[86] GRATÃO, Paulo. Supermercado de SP adota carrinho inteligente, que soma e recebe o pagamento das compras. Pequenas Empresas & Grandes Negócios, 3 de maio de 2022. Disponível em: https://revistapegn.globo.com/Banco-de-ideias/Varejo/noticia/2022/05/supermercado-de-sp-adota-carrinho-inteligente-que-pesa-soma-e-recebe-o-pagamento-das-compras.html. Acesso em: 31 out. 2023.

[87] MAGRANI, 2018, p. 47.

[88] *Ibid.,* p. 47.

[89] WEBER, Rolf H.; WEBER, Romana, 2010, p. 98.

Ambiental, Social e Governança), o que deve ser empregado não só pelas empresas fabricantes de tecnologias IoT, como por aquelas que se utilizam dela em suas atividades operacionais[90].

A mudança de comportamento social, incentivado através da educação, seria a chave para o combate ao consumismo e alcançar melhorias no âmbito sustentável. Além disso, tanto Renato Opice Blum[91] como Rolf Weber e Romana Weber[92] defendem que o conhecimento básico dos usuários pode contribuir com a redução dos riscos de segurança e privacidade. Inclui-se aqui a educação digital como sendo fundamental para o desenvolvimento da IoT e, nesse aspecto, o governo brasileiro parece estar atento, posto que em janeiro de 2023 foi instituída a Política Nacional de Educação Digital.[93]

Relevante também é comentar a questão da desigualdade no acesso à internet no Brasil. Uma pesquisa do ano de 2022 do Instituto Cidades Sustentáveis mostrou que mais de um terço da população brasileira precisou e conseguiu ter acesso a algum serviço pela internet, como serviços públicos, serviços de saúde e de educação[94]. Se de fato, no futuro, a IoT terá caráter essencial e indispensável para o funcionamento da sociedade, tal como já ocorre com a internet como um todo[95], o problema da desigualdade precisa ser pelo menos minimizado. Afinal, como enfatiza Rolf H. Weber e Romana Weber (2010): "Superar a exclusão digital é uma questão de justiça social que abrange não apenas o acesso às redes de informação e comunicação, mas também dimensões da vida, desde cuidados de saúde e nutrição até educação e longevidade." (Tradução nossa)[96].

---

[90] PACETE. Luiz Gustavo. IoT amplia vendas de eletrônicos e expõe o desafio da sustentabilidade. **Forbes** [online], 30 set. 2022. Disponível em: https://forbes.com.br/forbesesg/2022/09/iot-amplia-vendas-de-eletronicos-e-expoe-o-desafio-da-sustentabilidade/. Acesso em: 09 out. 2023.

[91] BLUM, 2021, p. 266.

[92] WEBER, Rolf H.; WEBER, Romana, 2010, p. 65.

[93] BRASIL. Lei nº 14.533, de 11 de janeiro de 2023. Política Nacional de Educação Digital. Brasília, DF, 11 jan. 2023.

[94] INSTITUTO CIDADES SUSTENTÁVEIS. Pesquisa Cidades Sustentáveis: desigualdades. São Paulo, 2022. P. 24. Disponível em: https://www.cidadessustentaveis.org.br/paginas/pesquisas. Acesso em: 18 out. 2023.

[95] WEBER, Rolf H.; WEBER, Romana, 2010, p. 94.

[96] No original: *"Bridging the digital divide is a matter of social justice encompassing not only access to information and communication networks, but also dimensions of life from health care and nutrition to education and longevity.". In:* WEBER, Rolf H.; WEBER, Romana. *Internet of Things: Legal Perspectives*. Springer Berlin, Heidelberg, 2010. P. 101. Disponível em: https://www.dhi.ac.uk/san/waysofbeing/data/governance-crone-weber-2010.pdf. Acesso em: 26 jul. 2023.

O tópico da desigualdade se insere na análise das casas inteligentes, também na perspectiva do direito à moradia. Isso porque, enquanto se tem moradores e/ou proprietários de casas automatizadas e modernizadas, há quem sequer possui acesso à moradia digna. De acordo com o Instituto Cidades Inteligentes, 34% dos entrevistados perceberam um aumento de pessoas em situação de rua em 2022.[97]

Assim, o contexto da IoT torna ainda mais evidente uma disparidade do exercício de direitos, como o direito à moradia, direito de acesso à internet e à informação. Enfrentar os desafios expostos aqui é ir ao encontro dos Objetivos de Desenvolvimento Sustentável (ODS) da ONU, em especial os objetivos de número 9 ao 12, que buscam, respectivamente, o fomento à inovação e industrialização inclusiva e sustentável; a redução das desigualdades; cidades e comunidades sustentáveis e, por fim, um padrão sustentável de produção e consumo.[98]

Como visto, a comunicação entre os aparelhos e deles com o meio físico é o que faz a casa inteligente ser vista como tal. Nesse sentido, Bruno Bioni diz que:

> No cenário de uma casa inteligente, por exemplo, os seus respectivos objetos terão que conversar entre si para extrair as informações necessárias para automatizar e otimizar a vida dos seus moradores (da compra de alimentos e outras atividades domésticas até um consumo energético mais eficiente).[99]

No entanto, as "informações necessárias" às quais o autor se refere não se resumem apenas aos dados extraídos do ambiente em si, como variações de temperatura, luz, quantidade de produto etc., mas também aos dados pessoais. Isso porque, esse "microcosmo" (mundo pequeno) de computadores pessoais, *smartphones*, aplicações e sensores[100] possuem também a capacidade de monitorar e identificar padrões comportamentais ou identificar e detectar pessoas, a exemplo de sistemas de segurança que utilizam o reconhecimento facial para abertura automática de portas.[101]

---

[97] INSTITUTO CIDADES SUSTENTÁVEIS. Pesquisa Cidades Sustentáveis: desigualdades. São Paulo, 2022. P. 12. Disponível em: https://www.cidadessustentaveis.org.br/paginas/pesquisas. Acesso em: 18 out. 2023.

[98] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *The 17 Goals.* Disponível em: https://sdgs.un.org/goals. Acesso em: 5 out. 2023.

[99] BIONI, 2020, p. 196.

[100] ALVI; NABI, 2014, p. 1.

[101] *Ibid.*, p. 4.

A mera possibilidade de tratamento de dados pessoais, implica na necessidade de conformidade com legislações específicas da matéria que elencam as situações e sob quais condições o tratamento pode ocorrer. No Brasil, a Lei nº 13.709 ou Lei Geral de Proteção de Dados Pessoais (LGPD) dita as regras para aqueles que lidam com informações de cunho pessoal. Outros países, também possuem leis que, com suas particularidades, englobam a matéria, a exemplo dos Estados Unidos[102], China[103] e Argentina[104]. Mais recentemente, a Índia aprovou a lei de proteção de dados no país (*The Digital Personal Data Protection Act*)[105]. Já nos países europeus, o *General Data Protection Regulation* (GDPR)[106], ou Regulamento Geral Europeu de Proteção de Dados, é a principal referência normativa.

Para a lei brasileira, pessoal é o dado que traz uma "informação relacionada a pessoa natural identificada ou identificável" e são considerados sensíveis quando está atrelado a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico"[107].

A casa inteligente estaria, portanto, dentro do escopo de proteções jurídicas, sobretudo considerando que a privacidade dos indivíduos também é afetada, já que os dispositivos estão inseridos no espaço onde o morador exerce o direito à privacidade em sua mais restrita concepção, ou seja, na sua própria casa. Quanto a isso, Bruno Bioni explica a dicotomia entre atividades que seriam próprias do espaço público e outras do espaço privado:

> A habitação privada (casa) estabeleceria os contornos dessa dicotomia, sendo, por excelência, o espaço para que as pessoas se refugiassem do escrutínio público. Isso é simbolizado a partir da metáfora de que o indivíduo

---

[102] ESTADOS UNIDOS DA AMÉRICA. *California Consumer Privacy Act of 2018*. Califórnia, CA, 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 21 set. 2023.

[103] REPÚBLICA POPULAR DA CHINA. Lei de Proteção de Informações Pessoais. China, 2021. Disponível em: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm. Acesso em: 21 set. 2023.

[104] ARGENTINA. Proteccion de Los Datos Personales. Lei 25.326. Buenos Aires, 2000. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790. Acesso em: 21 set. 2023.

[105] ÍNDIA. *The Digital Personal Data Protection Act.* PRS - Legislative Research. Nova Deli, 2023. Disponível em: https://prsindia.org/acts/parliament. Acesso em: 23 set. 2023.

[106] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. (Regulamento Geral sobre a Proteção de Dados). Eur-Lex. Disponível em: Acesso em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. 11 set. 2023.

[107] Art. 5º, I e II, LGPD.

> tem a faculdade de se afastar da multidão (espaço público) para se recolher ao seu castelo (espaço privado).[108]

É tão significativo o valor atribuído a necessidade humana de estar só e de ter um espaço privado que o direito à privacidade é consagrado como um direito humano na Declaração Universal de Direitos Humanos da Organização das Nações Unidas (DUDH)[109]. Assim prevê o artigo 12º da DUDH:

> Artigo 12°. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.

Na mesma linha, apesar de a Constituição Federal de 1988 não prever literalmente a palavra "privacidade" no rol das garantias fundamentais, o direito está presente se analisarmos cuidadosamente o inciso XI do artigo 5º. Diz a Carta:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> XI - ***a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador,*** salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;

Ao viver em uma casa inteligente, o morador, consumidor dos produtos e titular dos dados pessoais está, de certa forma, abrindo mão de sua privacidade em prol das propostas de facilitação da vida cotidiana pela IoT. Ocorre que o indivíduo provavelmente sequer sabe que são as suas informações pessoais que podem ser expostas ao sistema. É o caso, por exemplo, do já mencionado *smart closet* (armário inteligente) do episódio da série que inspirou esta pesquisa, pois a personagem não sabia que o objeto fazia gravações suas.

Felizmente, a Emenda Constitucional nº 115 de 2022, reconheceu o status da proteção de dados pessoais como direito fundamental e hoje integra o rol do artigo 5º da Constituição Federal de 1988. Não obstante a importância de tal reconhecimento, seria

---

[108] BIONI, 2020, p. 103.

[109] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 1948. Disponível em: https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humano. Acesso em: 1 set. 2023.

ingênuo pensar que o simples fato de enquadrar a matéria nessa categoria de direitos resolveria eventuais brechas ou mesmo ausência de regulação para casos específicos de tratamento de dados.

Como adiantou Guilherme Martins, não seria adequado olhar para a proteção de dados pessoais somente sob a ótica dos direitos fundamentais à privacidade e intimidade[110]. Na verdade, proteger dados pessoais é também proteger o livre desenvolvimento da pessoa humana na dimensão dos direitos de personalidade, tendo em vista que um dado pessoal seria uma dimensão da figura do seu titular.[111]

Essa extensão da pessoa na forma de dados é o fenômeno da datificação, que transforma e ressignifica todos os aspectos da vida de uma pessoa com base nos dados[112]. Bioni explica que:

> O ser humano terá um prolongamento e projeção completa no ambiente digital, sendo todas as suas individualidades datificadas. Problematiza-se, mais ainda, o desafio da tutela dos dados pessoais como um novo direito da personalidade, já que muitos aspectos da vida de uma pessoa poderão ser decididos a partir dessa sua extensão eletrônica.[113]

Dos ensinamentos de Danilo Doneda, é fácil perceber a relação do consentimento com os direitos da personalidade em matéria de proteção de dados pessoais, pois:

> O consentimento para o tratamento de dados pessoais toca diretamente em uma série de elementos da própria personalidade, ainda que não no sentido exato da disposição desses elementos. Ele assume com mais propriedade as vestes de um ato do titular cujo efeito será de autorizar um determinado tratamento para os dados pessoais.[114]

Isso posto, cabe a esta pesquisa, através de amparo das normas jurídicas existentes, analisar como se dá a base legal do consentimento nos casos em que há tratamento de dados pessoais pela IoT, tendo como foco principal a casa inteligente. Por ora, é imprescindível

---

[110] MARTINS, 2021, p. 204.

[111] *Ibid.*, p. 204.

[112] BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento.* 2. ed. Rio de Janeiro: Forense, 2020. P. 101.

[113] *Ibid.*, p. 101.

[114] DONEDA, Danilo Cesar Maganhoto. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados.* 2. ed. São Paulo: Thomson Reuters Brasil, 2020. P. 296.

dissecar o instituto jurídico para, posteriormente, compreender sua aplicabilidade no cenário da internet das coisas (Capítulo 3).

2. O INSTITUTO JURÍDICO DO CONSENTIMENTO

2.1. "Quem cala, quando deveria se manifestar, consente?"[115]

Muito usada na sociedade brasileira, a frase popular "quem cala, consente" exprime uma ideia de que a ausência de posicionamento contrário a uma determinada situação implicaria em concordância[116]. Em outras palavras, optar pelo silêncio, ou seja, nada fazer ou dizer, pode ser interpretado como sendo uma forma de consentir.

Sinônimo de "concordar", "aprovar" e/ou "permitir", à primeira vista, pode parecer muito óbvio o que seja "consentir"[117], afinal, está nas atividades cotidianas, como o preenchimento de fichas para realização de exames em laboratórios ou tratamento médico, preenchimento de pesquisas, assinatura de contratos, compra de certos produtos e mercadorias, e até visita a sites na internet. Contudo, a depender da forma em que o consentimento é obtido - ou não -, pode ser necessária uma certa análise jurídica baseada no contexto e nas leis aplicáveis ao caso.

No direito, mais do que um ato de aprovação, anuência ou concordância[118], o consentimento muitas vezes é utilizado como um parâmetro jurídico ou critério de validade de determinado ato, sendo, portanto, um verdadeiro instituto jurídico no que se refere a declaração de vontade e está presente em diversos ramos. Dessa forma, é possível lembrar do direito civil, na formação de um negócio jurídico, na celebração de um casamento ou na

---

[115] Informação verbal do Prof. Simão Isaac Benjó transmitida durante a orientação do Prof. Guilherme Martins.

[116] RAPOPORT, Izabel Duva. A Curiosa Origem do Ditado "Quem cala consente". Aventuras na História, *UOL* [online], São Paulo, 24 jul. 2023. Disponível em: https://aventurasnahistoria.uol.com.br/noticias/almanaque/de-onde-vem-expressao-quem-cala-consente.phtml . Acesso em: 24 jul. 2023.

[117] De acordo com o Dicionário Online de Português, o verbo consentir significa dar autorização, concordar com algo, expressar a aprovação. Disponível em: https://www.dicio.com.br. Acesso em: 24 jul. 2023.

[118] Significado de "consentimento". Disponível em: https://www.dicio.com.br/consentimento/. Acesso em: 24 jul. 2023.

realização de um testamento[119]; do direito penal, no momento de classificação de certos tipos penais[120]; do direito processual[121], quando há necessidade de um dos cônjuges obter o consentimento do outro a depender da ação que deseja propor, entre tantos outros ramos.

Essas situações são exemplos que demonstram o ato de consentir como sendo essencial no ordenamento jurídico brasileiro e existem consequências dependendo da forma como ele é obtido. E não poderia ser diferente no campo de estudo do direito e tecnologia, que será abordado de forma mais profunda em momento oportuno, mais especificamente no tópico 2.3 deste Capítulo.

De toda forma, é possível adiantar que no ordenamento jurídico brasileiro, a Lei Geral de Proteção de Dados (LGPD) é a principal referência no que se refere ao tema deste trabalho e dela depreende-se também o consentimento, bem como seus requisitos de validade e aplicação. Cabe dizer que a lei brasileira teve forte influência da legislação europeia[122], o Regulamento Geral Europeu de Proteção de Dados (GDPR), que por sua vez é claro ao dispor que o silêncio ou inatividade não constitui consentimento.[123]

Em resumo e por tudo que foi exposto até aqui, é legítimo afirmar que, no âmbito jurídico, nem sempre quem cala, consente. Nem sempre o silêncio será interpretado como anuência ou concordância.

2.2. Consentimento como manifestação de vontade

Partindo do pressuposto de que na prática a principal função do consentimento é informar algo ao indivíduo para que ele concorde ou não com uma determinada situação, diversas são as formas de passar a informação e obter a manifestação de vontade. A simples

---

[119] Vide arts. 107-113; art. 1.514 e arts. 1.857 e 1.858 , todos do Código Civil de 2002.

[120] Vide o crime de aborto nos art. 124 - 129; o estupro contra vulnerável, no art. 217-a e art. 218-c, todos do Código Penal, decreto-lei nº 2.848, de 7 de dezembro de 1940.

[121] Vide art. 73 do Código de Processo Civil de 2015, que dispõe sobre a necessidade de consentimento do outro cônjuge propor ação que verse sobre direito real imobiliário.

[122] BLUM, 2021, p. 269.

[123] ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. P. 28. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021.

manifestação oral ou o comportamento de uma pessoa pode definir, juridicamente, se houve ou não uma violação à dignidade sexual, por exemplo.

Pensando no direito contratual, uma simples assinatura e firma são as formas tradicionais usadas para consentir, mas hoje já é possível identificar diversos meios de obtenção de consentimento, como um click em *checkbox* (caixa de seleção) e, recentemente, uma decisão de um magistrado no Canadá entendeu que o de "joinha", uma mão com o polegar para cima ("👍"), seria uma forma de expressar o consentimento.[124]

Na doutrina de Danilo Doneda depreende-se que o consentimento é um poder dado a um indivíduo para alterar a sua esfera jurídica[125]. No que tange ao direito civil, apesar de o instituto ter uma origem negocial, quando aplicado à proteção de dados, este aspecto de ser um instrumento para constituição de um "negócio jurídico" deve ser afastado em prol da visando a efetividade das normas[126]. Caso contrário, se estaria defendo a tese de que os dados pessoais teriam natureza jurídica de "bens" e, portanto, poderiam ser dispostos pelo titular, o que os inclui objetos a serem negociados.[127]

Corroborando com Danilo Doneda[128], essa corrente doutrinária que atribui a característica de propriedade aos dados pessoais natureza jurídica de "bens", não parece ser apropriada, na medida em que desconfigura a proteção de dados como direito fundamental, como será visto no tópico 3.2. Por enquanto, é preciso se atentar que:

> Em um sentido técnico, não parece apropriada a caracterização de uma natureza puramente negocial a esse consentimento. Se assim fosse, seria legitimada a inserção desse consentimento em estruturas contratuais, dificultando a sua valoração em função dos atributos da personalidade que estão em jogo.[129]

---

[124] A notícia versa sobre a decisão do magistrado que repercutiu em julho de 2023, ao decidir sobre um caso de compra e venda de produtos agrícolas. Na ocasião, a parte interessada em comprar os grãos foi respondida pelo agricultor com um emoji de "joinha" ao ter enviado o contrato assinado, gerando dúvidas se a resposta seria apenas um recebimento da oferta ou de fato a concordância com o contrato. Disponível em: https://veja.abril.com.br/mundo/%f0%9f%91%8d-emoji-de-joinha-firma-acordo-contratual-diz-tribunal-canadense/. Acesso em: 14 ago. 2023.

[125] DONEDA, 2020, p. 293.

[126] *Ibid.,* p. 295-296.

[127] *Ibid.,* p. 296.

[128] *Ibid.,* p. 296-297.

[129] *Ibid.*, p. 295-296.

Ademais, para além das diferentes maneiras que existem de expressar a declaração de vontade, é imprescindível que o ato de consentir seja feito por um indivíduo com devida capacidade para tanto. Isso porque existem pessoas mais vulneráveis que, no momento de exercer o consentimento, podem não compreender adequadamente o que está sendo feito, tal como crianças, idosos ou pessoas enfermas. Por isso, o direito brasileiro protege crianças e adolescentes até os 18 anos e aqueles que, por algum motivo, não exerçam as faculdades mentais em sua plenitude[130]. Assim, apesar de o consentimento ser um ato, em regra, personalíssimo, isto é, deve partir da pessoa a quem determinada situação se refere, podem existir situações em que a tomada de decisão ou expressão da manifestação de vontade parta de um terceiro, a exemplo dos responsáveis legais de menores de idade.

Em suma, é através do consentimento que um indivíduo pode manifestar a sua vontade em diversas situações da vida. Hoje, com o processamento massivo de dados e a importância deles, o instituto também se faz presente na matéria regulatória do tratamento de dados pessoais e se porta como sendo um dos "pontos mais sensíveis de toda a disciplina", alerta Danilo Doneda.[131]

2.3. Consentimento em proteção de dados pessoais: um diálogo entre legislações

Assim como outras normas jurídicas, a regulação dos dados pessoais surge da necessidade de equilibrar situações de assimetria de poder. No caso, o objetivo está em garantir a privacidade do indivíduo e proteger o uso dos dados pessoais no atual contexto de *Big Data* e processamento em massa por terceiros que não os seus próprios titulares.[132]

O fundamento básico por trás da regulação dos dados pessoais é a autodeterminação informativa[133], pela qual o indivíduo (titular dos dados pessoais) deve ter a capacidade controlar as suas informações pessoais, dado as consequências que o seu uso pode acarretar,

---

[130] O Código Civil (L. 10.406/02) dispõe sobre a capacidade das pessoas naturais entre os artigos 1º e 5º, parte geral.

[131] DONEDA, 2020*,* p. 292.

[132] BIONI, 2020, p. 184 - 188.

[133] *Ibid.,* p. 106.

como a formação e enquadramento de perfis comportamentais ou mesmo servir como guia nas decisões automáticas tomadas por máquinas e até discriminação.[134]

Tendo como primeira aparição na Alemanha[135], a doutrina da autodeterminação informativa ou informacional - como Bioni prefere chamar -, é fundamento explícito da LGPD[136] e sua existência é fruto do reconhecimento de uma hipervulnerabilidade dos titulares[137]. É nesse contexto de assimetria que Bruno Bioni defende a abordagem participativa dos indivíduos no que tange ao tratamento dos dados, colocando o consentimento como sendo aquilo que possibilita o protagonismo do titular dos dados pessoais.[138]

O autor explica que na medida em que "a própria noção do que seja um tratamento de dados pessoais justo e lícito é vinculada ao consentimento do indivíduo"[139]. Igualmente, Guilherme Martins vê o consentimento como o momento inicial do processamento dos dados pessoais e, consequentemente, a expressão da autonomia desse direito e do pressuposto da autodeterminação informativa.[140]

Isto posto, tamanha a importância do consentimento que a ele se atribui o status de base legal, isto é, uma das situações em que se justifica e autoriza o tratamento de dados pessoais. Trata-se de um entendimento comum presente tanto na legislação brasileira[141], mais especificamente na LGPD, como no Regulamento Geral de Proteção de Dados do Parlamento

---

[134] BIONI, 2020, p. 94.

[135] CANSIAN, Adriana Cardoso de Moraes. *Aspectos relevantes da internet das coisas (IoT): segurança e protenção de dados.* 2022. 142 p. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2022. P. 67.

[136] Art. 2º, II, LGPD.

[137] MARTINS, 2021, p. 221.

[138] BIONI, *op. cit.,* p. 150.

[139] BIONI, *op. cit.*, p. 150.

[140] MARTINS, 2021, p. 207.

[141] Artigo 7º da L. nº 13.709 (LGPD)

Europeu (GDPR)[142]. O mesmo ocorre na legislação chinesa[143], norte-americana[144] e indiana[145]. Na América Latina, a Argentina também dá destaque ao consentimento.[146]

O fato de ser possível encontrar a mesma percepção acerca do consentimento em diferentes jurisdições pode ser considerado um exemplo de uma tendência de padronização normativa das legislações de proteção de dados em todo mundo, como explica Guilherme Martins, pois:

> A lei brasileira é expressão da convergência internacional em torno de princípios básicos da proteção de dados pessoais no mundo, ensejando uma aproximação entre as diversas normas, em conteúdo e forma, para além das peculiaridades nacionais, trazendo consigo a identidade de um padrão normativo entre os diversos sistemas internacionais.[147]

Especificamente no cenário brasileiro, temos que consentimento é uma "manifestação ***livre***, ***informada*** e ***inequívoca*** pela qual o titular concorda com o tratamento de seus dados pessoais para uma ***finalidade determinada***" (grifo nosso).[148] Tal definição abrange os requisitos que, à luz da LGPD, devem ser observados no momento de obtenção do consentimento pelo agente de tratamento.

---

[142] Condições aplicáveis ao consentimento, art. 7º, GDPR.

[143] Depreende-se do artigo 13 lei chinesa: "*A personal information processor can process personal information of an individual only if one of the following circumstances exists: (1) the individual's consent has been obtained;" e o artigo 14 completa "Where personal information processing is based on individual consent, the individual consent shall be voluntary, explicit, and fully informed. Where any other law or administrative regulation provides that an individual's separate consent or written consent must be obtained for processing personal information, such provisions shall apply. In the case of any change of the purposes or means of personal information processing, or the category of processed personal information, a new consent shall be obtained from the individual.*".

[144] Definições, CCPA: *(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.*

[145] Na lei indiana, temos que: *(1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.*

[146] Da lei argentina, retira-se do artigo 5º: *"El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley."*

[147] MARTINS, 2021, p. 221.

[148] Artigo 5º, inciso XII da L. nº 13.709 (LGPD).

Em detalhe, uma manifestação ***livre*** significa dizer que o consentimento não pode ser obtido por meios forçados, de forma que a pessoa deve consentir por vontade e escolha própria[149]. Trata-se de mais um ponto em que as previsões do GDPR vão de encontro com a legislação brasileira, pois a lei europeia também determina que o consentimento deve ser dado de forma livre *(freely given)*.[150]

O consentimento será ***informado*** quando houver uma explicação cristalina, clara e detalhada sobre o tratamento de seus dados pessoais. Quanto à validade, Ina Elevant defende que a forma pela qual a informação é apresentada ao indivíduo é fundamental para garantir a compreensão da mensagem[151]. É nesse entendimento que se pode lembrar dos conceitos de *Legal Design* e seu segmento voltado para o *Visual Law.*

Pensar na solução de questões jurídicas para além do direito é justamente a proposta do *Legal Design*, que se utiliza de metodologias de resolução de problemas e recursos tecnológicos para trazer soluções mais apropriadas à realidade[152]. No caso de um aceite ou concordância para tratamento de dados pessoais carregado de conteúdo jurídico, uma linguagem clara, simples, de fácil entendimento e até mesmo com a aplicação de esquemas gráficos e visuais para apresentação de informações jurídicas (*Visual Law*), facilita a assimilação da mensagem pelas pessoas em geral.

A importância da forma pela qual se transmite a informação sobre o tratamento de dados pessoais também parece ser uma preocupação de Bruno Bioni, que defende uma abordagem mais amigável com o uso de recursos gráficos, animações e símbolos que facilitem a comunicação[153]. Isso porque haveria um "dever-direito de informar"[154], ou seja, ao mesmo tempo em que existe uma obrigação legalmente imposta àquele que trata os dados pessoais, é direito do titular saber como suas informações pessoais serão usadas (art. 18,

[149] ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 24.

[150] Condições aplicáveis ao consentimento, art. 7º, GDPR.

[151] ELEVANT, *op. cit.,* p. 27.

[152] COELHO, Alexandre Zavaglia; HOLTZ, Ana Paula Ulandowski. Legal Design | Visual Law: comunicação entre o universo do Direito e os demais setores da sociedade. *Thomson Reuters.* Ed eletrônica. 2020. P. 11. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/legal-one/biblioteca-de-conteudo-juridico/legal-design-visual-law.html. Acesso em: 11 set. 2023.

[153] BIONI, 2020, p. 199-201.

[154] *Ibid.,* p. 198.

LGPD). Nesse sentido, o consentimento informado se relaciona estritamente com o princípio da transparência previsto no artigo 6º, inciso VI da LGPD e, como antecipou Bioni:

> O dever-direito de informação deve propiciar, portanto, ao usuário os elementos necessários para o início de um processo de tomada de decisão no que tange ao fluxo de seus dados. A prestação de uma informação clara, adequada e suficiente é o portal de entrada para capacitar o cidadão com o controle dos seus dados, sendo o próprio adimplemento (satisfatório) do dever-direito de informação.[155]

Não coincidentemente, a transparência é também parâmetro para o direito do consumidor, que por sua vez é fundamento da LGPD[156]. O artigo 31 do Código de Defesa do Consumidor (CDC) prevê:

> Art. 31. A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores.

Entendendo que dispositivos de tecnologia IoT se enquadram na oferta de produtos e serviços, seus fabricantes são obrigados por lei a prestar toda a informação sobre os dispositivos se desejam colocá-los a venda no mercado e isso inclui informar sobre o tratamento de dados pessoais[157]. Assim, sendo as soluções IoT um produto/serviço com funcionamento baseado na utilização de dados pessoais, fica clara a incidência tanto da legislação consumerista, em uma relação de fornecedor e consumidor quanto da proteção de dados pessoais, em que se tem de um lado os agentes de tratamento e do outro titular dos dados. Tal raciocínio encontra amparo na doutrina de Claudia Lima Marques e Bruno Miragem.[158]

À luz do direito consumerista, existe um ônus do fornecedor em prover ao consumidor todas informações necessárias sobre o produto ou serviço. Seguindo o mesmo raciocínio, o

---

[155] BIONI, 2020, p. 200.

[156] Art. 2º, VI, fig. 3, LGPD.

[157] BLUM, 2021, p. 270.

[158] MIRAGEM, Bruno; MARQUES, Claudia Lima. O necessário diálogo entre a LGPD e o Código de Defesa do Consumidor e os novos direitos do consumidor-titular dos dados. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otávio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. P. 795-817. Disponível em: https://brunomiragem.com.br/artigos/026-o-necessario-dialogo-entre-a-lgpd-e-o-codigo-de-defesa-do-consumidor.pdf. Acesso em: 18 out. 2023.

artigo 42 da LGPD[159] adotou o regime de responsabilidade civil objetiva[160] aos agentes de tratamento de dados pessoais (controladores e operadores) para o caso de danos causados aos titulares[161]. Dessa forma, sendo o consentimento uma das normas estabelecidas, danos decorrentes de sua violação estariam sujeitos à reparação pelo agente de tratamento pelo simples risco assumido, sem a necessidade de comprovação da culpa.

Da necessidade de ser informado, depreende-se a exigência do consentimento ser ***inequívoco***, isto é, a informação será devidamente passada quando não houver espaço para dúvidas, obscuridade ou ambiguidades. A cautela de respeitar as exigências de obtenção do consentimento é fundamental para que, futuramente, este não seja considerado nulo e invalide o tratamento de dados pessoais.[162]

Em complemento, Ina Elevant explica que o ato de consentir deve partir de um comportamento ativo (ação) por parte do titular (*opt-in*)[163], e a mesma lógica se aplica quando o consentimento for retirado pelo titular. Assim, havendo o desejo de interromper o tratamento de dados pessoais quando autorizado via consentimento, o titular deve ter a mesma facilidade do momento em que concedeu a autorização[164]. Para Guilherme Martins, o direito de revogação do consentimento abarca a dignidade humana, pois é da natureza do pensamento humano mudar de ideia e esta liberdade deve ser garantida.[165]

A retirada do consentimento é um direito do titular presente não só na legislação brasileira[166], como também em legislações estrangeiras[167], o que demonstra mais uma vez a tendência de harmonização e padronização das leis de proteção de dados pessoais. Vale

---

[159] LGPD. Art. 42. "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."

[160] Código Civil. Art. 927. "Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem."

[161] MARTINS, 2021, p. 221.

[162] Art. 9º, §1º, LGPD.

[163] ELEVANT, 2021, p. 28.

[164] Art. 8º, §5º, LGPD.

[165] MARTINS, 2021, p. 207.

[166] Art. 15, III c/c art. 18, IX, LGPD.

[167] Temos a revogação no GDPR (art. 7º, (3)); no DPDP (5 (2) (b)); no art. 15 da lei chinesa; no art. 11, (2) da lei argentina; nos métodos de limitação de venda, compartilhamento e uso de informações pessoais e sensíveis do CCPA em (2), (1), (A);

destacar que é um ônus do agente de tratamento provar que obteve adequadamente o consentimento quando este for a base legal.[168]

Importa dizer que a revogação do consentimento não é um direito absoluto, pois a depender do caso concreto, podem existir outras bases legais aplicáveis e que, portanto, dão condição para a manutenção dos dados pessoais pelo agente de tratamento[169]. É o caso, por exemplo, de os dados serem tratados em função de uma obrigação legal ou regulatória, ou seja, quando existe um dever legal de manter as informações pessoais.

Porém, no que se refere a tratamento de dados sensíveis, o consentimento parece ter uma dimensão maior de importância, justamente pela natureza dos dados tratados. Nota-se que a própria estética da redação do artigo 11 parece ser um indicativo de que o legislador entende o consentimento em plano superior às demais bases legais. Isso porque, enquanto o primeiro é posto no inciso I, as demais hipóteses em que não há exigência do consentimento estão dispostas nas alíneas do inciso II.[170]

---

[168] Art. 8º, §2º, LGPD.

[169] LGPD. Art. 7º "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

[170] LGPD. Art. 11. "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."

Por fim, é indispensável que o tratamento tenha uma ***finalidade determinada***. Logo, não se admite autorizações genéricas de tratamento, ocorrendo esta hipótese, o consentimento será nulo[171]. Daí a importância de esclarecer com qual objetivo (para que) os dados pessoais serão utilizados, informando sobre qualquer mudança de finalidade que possa surgir após o consentimento[172], já que pode influenciar na decisão de o titular permanecer autorizando ou revogar o tratamento de suas informações. Nota-se uma amarração entre os dizeres legais, com direitos e obrigações que tornam mais forte, ao menos no âmbito teórico-jurídico, a proteção ao titular.

A relação entre titular e agentes de tratamento ou consumidores e fornecedores tem fulcro no princípio da boa-fé objetiva, no sentido de que se espera como sendo verdadeiras as informações apresentadas e as condutas praticadas. Guilherme Martins esclarece que:

> A boa-fé objetiva, decorrente da concepção da obrigação como processo, implica uma conduta de cooperação, lealdade e expectativas legítimas das partes, em especial o titular, face ao controlador (art. 10, II, LGPD), o que se delineia a partir das circunstâncias concretas em que se deu o consentimento, a finalidade de uso e o tratamento de dados indicado, assim como as informações prévias oferecidas.[173]

Seguindo, a finalidade tem dimensão principiológica[174] e deve limitar operações de tratamento como a coleta, o armazenamento e o compartilhamento de dados pessoais. Esse princípio, atua como limitação temporal para uso dos dados, de forma que as informações devem permanecer guardadas por um período de tempo necessário e adequado para os fins e objetivos estipulados, que por sua vez precisam ser determinados antes que ocorra qualquer tratamento.[175]

O requisito da finalidade determinada na obtenção do consentimento está em linha com os princípios da necessidade e adequação[176] que, com base no parâmetro da proporcionalidade[177], atuam como como guia em quantidade e qualidade para tratar apenas os dados tidos como suficientes. Tratar o mínimo necessário é mais uma maneira de garantir a

---

[171] Art. 8º, §4º, LGPD.
[172] Art. 9º, §2º, LGPD.
[173] MARTINS, 2021, p. 216.
[174] Art. 6º, I, LGPD.
[175] MARTINS, 2021, p. 217.
[176] Art. 6º, II e III, LGPD.
[177] MARTINS, 2021, p. 217.

autodeterminação e controle dos indivíduos sobre as informações que desejam ou não fornecer. Quanto a isso, incide a ideia de consentimento granular, isto é, o titular deve ser capaz de autorizar (ou não) de forma segmentada o uso dos seus dados.[178]

Importa dizer que mesmo quando se está diante de uma situação em que o consentimento é dispensado pela lei, o titular dos dados pessoais possui o direito de acesso a eles (princípio do livre acesso)[179], de forma que poderá solicitar a cópia das informações bem como esclarecimentos e correção dos dados[180]. Contudo, os titulares não são apenas pessoas adultas plenamente capazes, mas também crianças e adolescentes, indivíduos que por si só já recebem maior grau de proteção jurídica no geral. Seguindo a lógica da proteção ao vulnerável, a lei brasileira determina que o consentimento para tratamento desta categoria de titulares seja feito mediante autorização de pelo menos um dos pais ou responsável legal[181], e, assim como o GDPR, prevê o emprego de todos os esforços para verificar se procede como verdadeira a identidade de quem se deu como responsável pela criança.[182]

São muitas as exigências que o instituto jurídico do consentimento carrega e, pensando nisso, é curioso o fato de a lei indiana, aprovada recentemente em agosto 2023, determinar a existência de um "Consent Manager", ou Gerente do Consentimento, uma pessoa registrada na autoridade governamental da Índia ("Board") responsável por ser o ponto de contato com o titular no que tange a obtenção, gestão, revisão e retirada do consentimento através de uma plataforma acessível, transparente e interoperável[183]. É uma figura semelhante ao Encarregado de Dados na LGPD e ao *Data Protection Officer* no GDPR.

---

[178] BIONI, 2020, p. 200.

[179] Art. 6º, IV c/c art. 18, II, LGPD.

[180] MARTINS, 2021, p. 218.

[181] Art. 14, §1º, LGPD.

[182] Art. 14, §5º, LGPD e art. 8º, (2), GDPR.

[183] Diz o DPDP: *"g) "Consent Manager" means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform;".*

2.3.1. Tendência de internacionalização das normas de proteção de dados

Da mesma forma que a regulação da internet e, consequentemente, da IoT, precisam ser pensadas em perspectiva internacional (vide tópico 1.3), a proteção de dados também deveria seguir o mesmo caminho. Considerando que os dados - inclusive de cunho pessoal -, são os insumos das tecnologias de hoje e que não encontram barreiras geográficas, seria incoerente não elevá-los ao status de tutela internacional quando as próprias tecnologias alimentadas por eles deveriam estar submetidas ao direito internacional, conforme discutido anteriormente.

Apesar de já ser observada a repetição de certos padrões normativos entre algumas legislações, tal como a questão do consentimento, um argumento favorável à internacionalização da proteção de dados reside justamente na possibilidade de existirem obrigações incompatíveis ou concorrentes impostas por cada Estado, o que pode culminar em conflitos de leis e desestimular o fluxo internacional dos dados, impactando no próprio desenvolvimento da sociedade[184].

Ter os dados pessoais regidos por diplomas internacionais confere maior segurança jurídica para sociedades que hoje têm o seu funcionamento baseado em tecnologias digitais, seja no setor público ou privado. Nessa linha, Danilo Doneda reforça que:

> A proteção de dados pessoais é uma matéria que, pela sua natureza e, em especial, pela característica de dinamicidade do fluxo de informações, não se prestaria a assumir contornos específicos em cada ordenamento jurídico nacional, de forma a dificultar a harmonização para proporcionar segurança e proteção de direitos nos fluxos internacionais de dados pessoais. Qualquer normativa nacional a respeito deve levar em consideração os efeitos de sua inserção na sociedade globalizada e deve estar preparada para as consequências do tráfico internacional de dados, capaz, conforme o caso, tanto de tornar ineficazes medidas incompatíveis com padrões internacionais como de pressionar pela adoção de medidas mais enérgicas.[185]

Essa necessidade de cooperação internacional em matéria de proteção de dados pessoais encontra reflexo nas próprias legislações. Não é a toa que as a maioria delas

---

[184] BRANCHER, Paulo Marcos Rodrigues. Proteção internacional de dados pessoais. *Enciclopédia jurídica da PUC-SP*. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Internacional. Cláudio Finkelstein, Clarisse Laupman Ferraz Lima (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em: 23 ago. 2023.

[185] DONEDA, 2020, p. 317.

apresenta como característica comum o escopo de aplicação extraterritorial, tal como o art. 3º da LGPD[186]. Sobre isso, Paulo Brancher conta que:

> Com o decorrer do tempo, os reguladores perceberam que não atribuir um alcance extraterritorial às leis de proteção de dados frustraria o objetivo de normas dessa natureza, uma vez que a internet permite (i) que entidades tratem dados pessoais de indivíduos a partir de qualquer lugar do mundo, independentemente de onde estiverem estabelecidas fisicamente; e (ii) o fluxo de informações para além de fronteiras geográficas.[187]

Em razão da possibilidade de não correspondência de níveis ideais de proteção em outros territórios[188], as legislações se valem de requisitos rígidos para certos tratamentos de dados pessoais. Um exemplo é o caso de transferência internacional de dados que, para a lei brasileira, somente pode ocorrer para países ou organismos internacionais com grau adequado de proteção de dados pessoais ou quando o controlador oferecer e comprovar o cumprimento dos princípios e direitos dos titulares[189]. Sobre este ponto, vale citar o mapa desenvolvido pela autoridade francesa denominada de *Commission nationale de l'informatique et des libertés* (CNIL), ou Comissão Nacional de Informática e Liberdades, que facilita a identificação dos países que atribuem proteção jurídica aos dados pessoais;[190]

Segundo Brancher, o patamar de compatibilidade entre as normas jurídicas de diferentes países pode ser alcançado com a construção de um sistema de cooperação internacional[191]. Por meio dele, seria possível a comunicação entre as autoridades de proteção de dados dos países bem como pela implantação adequada de mecanismos de salvaguardas, a exemplo das cláusulas padrões do direito contratual e das normas corporativas, como procedimentos internos e códigos de conduta.[192]

Em resumo, defender a cooperação internacional para regular e governar os produtos resultantes da evolução da internet bem como proteger os indivíduos (usuários, consumidores e titulares) é medida essencial para garantir a efetividade das normas e o respeito aos direitos

---

[186] BRANCHER, 2022, p. 12-13.

[187] *Ibid.,* p. 12.

[188] *Ibid.,* p. 12.

[189] Art. 33-36, LGPD.

[190] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. *Data protection around the world*. Disponível em: https://www.cnil.fr/en/data-protection-around-the-world. Acesso em: 09 out. 2023.

[191] BRANCHER, 2022, p. 24.

[192] *Ibid.,* p. 24.

humanos básicos. Para tanto, se faz necessário considerar as limitações e capacidades técnicas dos produtos fabricados para traçar as melhores soluções jurídicas e regulatórias.

Como preconiza Adriana Cansian, "é fundamental que o Direito incorpore conceitos tecnológicos, dados empíricos e aprimore seus institutos para melhor atender às demandas sociais. Qualquer coisa diferente disso, será um exercício de prestação jurisdicional fictício"[193]. Logo, de nada adianta ter uma norma abstratamente rígida e ideal se no plano dos fatos, sua eficácia acaba sendo de aplicação limitada.

3. LIMITAÇÕES PRÁTICO-JURÍDICAS PARA APLICAÇÃO DO CONSENTIMENTO EM CASAS INTELIGENTES

3.1. Obstáculos ao consentimento na estrutura de dispositivos domésticos IoT

Sabendo que a casa é o ambiente onde o indivíduo é livre para exercer sua privacidade, a partir do momento em que se traz dispositivos inteligentes para dentro deste espaço privado, é possível dizer que o ambiente perde em parte a característica de intimidade e refúgio em razão do monitoramento constante do meio físico e das pessoas. Por isso a necessidade de informar e obter autorização delas antes de iniciar o funcionamento do objeto. No entanto, existem questões práticas e jurídicas detalhadas a seguir que levariam a possíveis vícios de consentimento e, por consequência, uma carência de efetividade por parte do instituto.

Por ora, destaca-se os motivos pelos quais a base legal do consentimento, na forma como é concebida e aplicada hoje, não se sustenta mais com as novas aplicações tecnológicas. Ina Elevant constatou que: **(i)** pessoas não leem nem compreendem as notificações de privacidade em razão da grande quantidade de conteúdo em linguagem difícil; **(ii)** a tomada de decisão é enviesada pela influência de modelos heurísticos muitas vezes imprecisos ou baseados em informações falsas, incompletas ou mal utilizadas; **(iii)** usuários são bombardeados de notificações de privacidade a todo momento por diferentes entes, o que

[193] CANSIAN, 2020, p. 85.

dificulta o controle e gestão da privacidade, além da falta de tempo e recursos apropriados; **(iv)** dados que aparentemente são insignificantes, podem ser combinados com outros dados no futuro, revelando novas informações até mesmo sensíveis; **(v)** não há espaço para negociação diante de um termo de consentimento, tendo em vista que as pessoas frequentemente apenas possuem a opção de aceitar as disposições previamente estipuladas se desejam utilizar o dispositivo; **(vi)** como o mercado é dominado por empresas gigantes de tecnologias, não há alternativas para o usuário trocar de serviço com facilidade, além da falta de padronização e interoperabilidade; **(vii)** na mesma proporção em que dispositivos inteligentes estão se tornando cada vez mais comum e os usuários ficam mais dependentes deles.[194]

Em consonância com os problemas expostos acima, a grande crítica que se faz ao consentimento é que, na prática ele não é concedido de forma livre nem é informado, o que não passaria de uma "ilusão"[195] com falsa sensação de controle dos dados pessoais. Na mesma linha, Adriana Cansian demonstra certa preocupação acerca do instituto no cenário de IoT e adverte que:

> Se, a partir dos meios cotidianamente utilizados a informação adequada e o consentimento deixam as especificações da legislação protetiva de dados à deriva, contemplase então que a IoT propõe desafios ainda mais específicos quanto à subsunção do fato à norma.[196]

Haveria, portanto, uma contradição entre o consentimento construído com base na doutrina da autodeterminação informativa e aquele que de fato é visto na realidade. Como adiantou Cansian:

---

[194] Tradução nossa, no original: "*(i) People do not read privacy notices: most people do not read privacy notices due to information overload and consent transaction overload. ii) People do not understand privacy notices: privacy notices are too long and difficult to understand. iii) Skewed decision making: human rationality is bounded, and individuals' decision making is influenced by mental models and heuristics. Mental models can be inaccurate due to being based on false information or misplaced assumptions. iv) Problems with scale: There are too many entities providing privacy notices and consent requests, which makes privacy management difficult due to lack of time and resources. v) Aggregation effect: data that might have seemed insignificant may be combined with other data in the future revealing new and possibly sensitive information. vi) No room for negotiations: When confronted with a consent request people often have a choice to accept the terms of the privacy notice or not to engage with the device. vii) No alternatives: There are no privacy respecting alternatives on the market as the market is dominated by tech giants. The lack of standardization and interoperability in IoT makes it hard to switch service provider and/or device. viii) Dependency: Smart devices are becoming increasingly common, and users are becoming more and more dependent on such devices*." *In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 51. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[195] ELEVANT, 2021, p. 51.

[196] CANSIAN, Adriana Cardoso de Moraes. *Aspectos relevantes da internet das coisas (IoT): segurança e proteção de dados*. 2022. 142 p. Tese (Doutorado) - Universidade de São Paulo, São Paulo, 2022. P. 70.

> Não obstante a fenomenologia jurídica e sua história, sendo o objetivo do direito a busca pela efetivação material daquilo que disciplinou, pois não existe fora da sociedade, pois é 'um fato ou fenômeno social; não existe senão na sociedade e não pode ser concebido fora dela, a autodeterminação como medida abstrata é merecedora de atenção em suas aplicações, especialmente a partir de casos concretos.[197]

Em última análise, esta pesquisa constata uma fragilidade da ideia de controle dos dados pessoais no cenário de internet das coisas, sobretudo em decorrência da: (i) estrutura e interface dos dispositivos IoT; (ii) multiplicidade de titulares de dados e (iii) pluralidade de dispositivos conectados.

3.1.1. Estrutura e interface dos dispositivos IoT

Retomando o que foi discutido no Capítulo 1 sobre a arquitetura de objetos ligados a internet e relacionando com os apontamentos feitos em relação ao instituto no consentimento no Capítulo 2, a camada de aplicação seria o que viabiliza a comunicação do dispositivo com o usuário, uma vez que é nela onde se encontra elementos de interface gráfica e interação (*front-end*). É o que ocorre nas telas de *smartphones* e computadores, quando uma pessoa lê e aceita termos e condições de uso de um website ou aplicativo, por exemplo.

A obtenção do consentimento na camada de aplicação da IoT vai de encontro com as etapas proposta por Gerald Chikukwa, citado por Adriana Cansian[198], quais sejam a coleta de dados seguida pela coleta, gestão, execução e auditoria do consentimento. Em resumo, tem-se a estrutura de sensores coletando os dados a serem transmitidos por um *gateway* enquanto o consentimento deste processo deve ser feito através de login no *frontend* da aplicação, que além de ser o local onde o usuário pode encontrar informações sobre o tratamento de dados, também permitiria a interação com o *backend*, onde ocorre precisamente a manipulação dos dados a partir do momento em que o usuário decide sobre o tratamento[199]. Uma vez coletado, o consentimento deve ser devidamente gerenciado, o que engloba seu monitoramento e auditoria a fim de garantir a conformidade do processo com as exigências legais do instituto[200]. A estrutura, porém, não parece solucionar efetivamente o problema, pelo menos

[197] CANSIAN, 2022, p. 67.
[198] *Ibid.,* p. 72.
[199] *Ibid.,* p. 72.
[200] *Ibid.*, p. 72.

no que tange ao consentimento coletado por dispositivos IoT fabricados com telas pequenas, ou mesmo sem qualquer visor de interação, como adverte Ina Elevant:

> IoT traz consigo um conjunto único de problemas, já que a maioria dos dispositivos IoT carece de telas e métodos de entrada (*input*), dificultando o acesso aos avisos de privacidade e concessão do consentimento pelos indivíduos. A natureza discreta e onipresente da IoT torna invisível a atividade de coleta de dados. Os usuários muitas vezes desconhecem os sensores que os cercam e a ocorrência dos processos de coleta de dados, questionando, então, a existência de um consentimento significativo. Conforme dispositivos inteligentes vão se tornando cada vez mais comuns em espaços compartilhados, como lojas e transporte público, levanta-se questões sobre ***como*** as pessoas serão informadas sobre as finalidades do processamento de seus dados pessoais. (Tradução nossa, grifo nosso)[201]

A preocupação sobre como os usuários/titulares serão informados sobre cuidados com privacidade e dados pessoais reside no fato de que a forma tradicional de obtenção do consentimento não seria mais adequada na realidade da internet das coisas e uma das razões para isso seria a falta de tela ("*screenless*") e visualização gráfica em certos dispositivos[202]. Apesar de o *smartphone* ser em muitos casos o ponto chave de controle dos objetos ligados à internet - o que pode ser um argumento favorável à manutenção da forma como se obtém o consentimento hoje -, isso não necessariamente é uma regra. Basta lembrar da possibilidade de comando de voz sem a necessidade, *a priori,* de interação com aplicativos em celulares ou computadores.

Em outras palavras, o problema do instituto jurídico do consentimento aplicado a IoT é que a forma como ele se dá hoje seria própria para tecnologias tradicionais de websites e celulares, não sendo compatível com as peculiaridades de quando é um objeto ("coisa") que coleta dados pessoais. Quanto a isso, Ina Elevant diz:

> Como a regra parece se aplicar a dispositivos mais tradicionais, como computadores e smartphones, não está claro se, sob essa regra, os usuários, ao usar o seu novo dispositivo IoT, poderiam escolher suas configurações de

---

[201] No original: *"IoT also brings with itself a unique set of problems as most IoT devices lack screens and input methods making it hard for individuals to access privacy notices and provide consent. The unobtrusive and ubiquitous nature of IoT makes data collection activities invisible. Users are often unaware of the sensors surrounding them and the data collection processes taking place, thus questioning the existence of meaningful consent. As smart devices are becoming more and more common in shared spaces such as stores and public transportation, it also raises questions how people will be informed about the purposes of the processing of their personal data". In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 67. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[202] ELEVANT, 2021, p. 58.

> privacidade e se tais configurações iriam constituir consentimento. (Tradução nossa)[203]

Depreende-se da tese de Ina Elevant que as exigências legais de liberdade e informação na concessão do consentimento não são observadas na prática[204] , pois, enquanto o requisito de consentimento livre encontra obstáculo na assimetria de poder entre indivíduos e empresas[205], o consentimento informado é limitado pela assimetria de informação[206]. Se por um lado os titulares não sabem ao certo sobre o tratamento de dados pessoais, por outro, não detém de fato um poder de escolha, na medida em que o aceite, sem possibilidade de negociação, é condição para usufruir da tecnologia, não sendo, portanto, efetivamente livre. Nesse último aspecto, incide também o problema da pluralidade de titulares a ser explicada no tópico 3.1.3, pois o indivíduo sequer precisa ser o usuário principal da tecnologia para ter seus dados tratados.

Vale lembrar da necessidade de a camada de aplicação ser acessível, já que pessoas de grupos vulneráveis também são usuários da IoT e, por consequência, titulares de dados pessoais. Logo, a interface (*front-end*) deve atender estar adaptada a todas as categorias de titulares de dados, sejam eles crianças, adolescentes, idosos, pessoas enfermas e pessoas com deficiência.

---

[203] No original: *"As the rule seems to apply to more traditional devices such as computers and smart phones, it is unclear whether under this rule users could choose when starting to use their new IoT device their privacy settings and such settings would constitute consent.". In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 29. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[204] No original: *"This thesis has examined the problems related to consent in IoT. This thesis has shown that in practice consent is neither freely given nor informed." In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 66. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[205] No original: *"The problems with freely given consent arise from power asymmetries between individuals and companies. In practice, this means that dominant companies are able to exercise their power by one-sidedly imposing their practices on individuals." In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 67. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[206] No original: "*The problems with informed consent stem from the information asymmetries between individuals and companies. These asymmetries arise from personal data collection and analysis as individuals are not aware of what data is collected from them, how that data is being used and what inferences can be derived from that data, consequently calling into question the validity of informed consent*." *In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 66. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

Outro problema de infraestrutura e arquitetura com impactos jurídicos diz respeito à interoperabilidade. A falta de compatibilidade entre os dispositivos e padrões de fabricação definidos afeta a concretização, efetividade e exercício dos direitos dos titulares, encontrados no artigo 18 da LGPD[207]. Um deles é a portabilidade dos dados a outro fornecedor de serviço/produto e, sobre isso, explica Adriana Cansian:

> Haja vista que, conforme preconiza a legislação, a portabilidade determina que o controlador disponibilize os dados em formato utilizável por um terceiro, ao associar tal feito à IoT, entende-se que a padronização de estruturas e protocolos é de caráter imprescindível para cumprimento adequado do direito[208].

Apesar de algumas organizações estarem direcionando esforços para a construção de um padrão na IoT, ainda não há definições precisas sobre a arquitetura da tecnologia, que ainda está em processo de aperfeiçoamento[209]. Por isso, a pesquisadora aponta que, em termos de infraestrutura e arquitetura, estudiosos da área da ciência da computação ainda acreditam que "o sucesso da IoT está calcado na interoperabilidade, já que tal sistema é, por natureza, heterogêneo, por se tratar de um conjunto amplamente diversificado de dispositivos e recursos coletados em suas múltiplas camadas"[210]. O funcionamento coletivo de produtos da IoT é justamente o fenômeno da multiplicidade de dispositivos conectados, abordado a seguir.

3.1.2. Multiplicidade de dispositivos interconectados

Como visto, talvez o maior poder tecnológico da IoT seja a capacidade de transformar os ambientes a partir da conexão entre diversos dispositivos. Basta observar novamente a quantidade de objetos conectados à internet no retrato da casa inteligente

---

[207] LGPD. Art. 18. "O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei."

[208] CANSIAN, 2022, p. 75.

[209] *Ibid.,* p. 39.

[210] *Ibid.,* p. 39.

(**Figura 3**). Essa multiplicidade de dispositivos inteligentes conectados é o que caracteriza a formação de um ambiente inteligente como um todo.

Dessa forma, dada a quantidade de dispositivos que podem estar conectados ao mesmo tempo, torna-se impossível e inviável que os indivíduos tenham controle sobre suas informações pessoais. Como defende Ina Elevant, a mudança de meros dispositivos inteligentes para ambientes inteiramente inteligentes, move os indivíduos para além do domínio do controle (tradução nossa)[211] e destaca que:

> Existem muitos atores de processamento de dados pessoais, impossibilitando que uma pessoa controle e monitore todas essas entidades. Mesmo que todas elas forneçam aos indivíduos avisos e escolhas apropriadas para consentir com o processamento, uma pessoa comum não tem tempo ou recursos suficientes para gerenciar tais entidades; (Tradução nossa)[212]

Adriana Cansian parece corroborar com esse posicionamento ao dizer que:

> É um esforço sobre-humano controlar o compartilhamento de dados que se dá nos mais diferentes contextos e meios sem que para isso tenhamos dispositivos técnico-jurídicos que regulem esta prática, mormente quando se considera a economia digital e a importância que o compartilhamento e o consequente tratamento de dados ocupam hoje na sociedade contemporânea. Trata-se, em última análise, de um exercício necessário e urgente, sob pena de não conseguirmos atender não só o previsto na Lei 13.709/2018 – Lei Geral de Proteção de Dados, mas princípios constitucionais há muito dispostos na Carta Constitucional de 1988.[213]

Para além das dificuldades de infraestrutura, desafiador será também o trabalho de operadores do direito no momento de equacionar questões de proteção ao consumidor-titular com a livre concorrência - um dos fundamentos da LGPD[214] - e os segredos comercial e

---

[211] No original: *"The shift from mere smart devices into entire smart environments, moves individuals beyond the realm of control." In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 67. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[212] No original: *"there are too many information actors processing personal data, making it impossible for a person to control and monitor these entities. Even if all these entities would provide individuals with notice and appropriate choice whether to consent to such processing, a regular person does not have enough time or resources to manage such entities." In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 67. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[213] CANSIAN, 2022, p. 63.

[214] Art. 2º, VI, LGPD.

industrial, igualmente preservados ao longo da lei e que atua, inclusive, como um limitador do princípio da transparência.[215]

Dispositivos da IoT são produzidos por diferentes fabricantes do ramo da tecnologia e, quando minimamente compatíveis, efetuam a troca de dados e informações coletadas. Na **Figura 5** é possível observar pelo menos três grandes marcas atuando na conectividade da casa inteligente: Amazon, D-Link e Sonos. Mas o mercado também é abastecido pela Google, Samsung e Apple, que voltam seus produtos não só para casa inteligente, bem como vestimentas, acessórios entre outros.

Como não há um padrão definido pelo menos no que se refere a fabricação da IoT (vide tópico 3.1.1), cada produto é feito sob os procedimentos industriais, corporativos e de compliance definidos internamente por cada fabricante. Isso significa que, apesar de estarem submetidos aos parâmetros legais estabelecidos pela regulação de proteção de dados pessoais, na prática, a forma pela qual os dados são tratados, a informação é transmitida, o consentimento é coletado e os direitos são garantidos são, no fundo, uma escolha individual de cada empresa e, portanto, variam de uma para outra.

É claro que as empresas fabricantes da tecnologia, enquanto agente de tratamento, estarão sujeitas às consequências legais impostas em caso de não cumprimento ou violação de normas[216]. No entanto, é inegável que a falta de padronização (*standards*) para a IoT interfere na efetividade e concretização das normas jurídicas.

Nessa esteira, é interessante comentar, o estudo de Turner *et al.* citados por Cansian sobre a operacionalização do direito dos titulares à portabilidade em dispositivos IoT[217]. Os produtos domésticos *Amazon Echo* e *Google Home* estiveram entre os objetos integrantes da pesquisa que revelou, a partir de análises comparativas entre as políticas de privacidade e as normas do GDPR, a impossibilidade de exercício do direito de portabilidade.[218]

---

[215] LGPD. Art. 6º "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, ***observados os segredos comercial e industrial***;" (grifo nosso).

[216] Art. 52, LGPD.

[217] CANSIAN, 2022, p. 75.

[218] *Ibid.*, p. 75-77.

A mesma lógica de interferência da carência de padronização se aplica na obtenção do consentimento pelos dispositivos, pois, apesar de a lei determinar as condições e requisitos de validade, não há orientação acerca de como concretizar as exigências na prática. Tais orientações é um trabalho delegado pela lei à Autoridade Nacional de Proteção de Dados Pessoais (ANPD)[219], uma autarquia instaurada em 2022 para ser o órgão de fiscalização do cumprimento das normas de proteção de dados no Brasil, além de promover a educação à população.[220]

O trabalho educativo da ANPD pode ser visto através dos guias que vêm sendo divulgados para ajudar a compreender melhor como os agentes de tratamento devem atuar diante dos dados pessoais. Porém, até o momento de feitura deste trabalho, não foi encontrado nenhum guia que discutisse de forma específica e profunda a aplicação do instituto do consentimento, quiçá no detalhe da tecnologia IoT.[221]

Sendo assim, é legítimo o surgimento de dúvidas referentes à formação e constituição do consentimento, como o caso de um simples aceite das condições de uso do produto doméstico inteligente e políticas de privacidade ser ou não uma forma de consentir com a tecnologia e o processamento de dados. Indo além, há espaço para ser questionado se as empresas que fabricam aparelhos inteligentes de segurança e monitoramento de saúde poderiam se utilizar da base legal da proteção da vida ou incolumidade física do titular ou de terceiro[222] para processar os dados sem a necessidade de se submeter ao consentimento e seus requisitos de obtenção.

Não obstante, a experiência do continente europeu, pode servir de referência para o país. Por ter iniciado o processo de regulação antes do Brasil, o *European Data Protection Board* (EDPB) já possui diversas diretrizes (guidelines) quanto ao GDPR, sendo uma delas justamente sobre o consentimento[223]. Ainda na europa, a Corte de Justiça da União Europeia

---

[219] Art. 5º, XIX, LGPD.

[220] Art. 55-J, LGPD.

[221] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Publicações da ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em 28 set. 2023.

[222] Art. 7º, VII c/c art. 11, II, LGPD.

[223] EUROPEAN DATA PROTECTION BOARD. *Guidelines 05/2020 on consent under Regulation 2016/679.* Versão 1.1, maio de 2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt#:~:text=Diretrizes%2005%2F2020%20relativas%20ao%20consentimento%20na%20ace%C3%A7%C3%A3o%20do,2016%2F679%204%20May%202020%20Guidelines%2005%2F2020%20321.3%20KB. Acesso em: 29 set. 2023.

(CJEU) já proferiru decisões sobre o consentimento, esclarecendo que situações em que ele coletado digitalmente, caixas de seleção pré-selecionadas não estaria de acordo com o GDPR, dado a exigência de se ter a ação de consentir (*opt-in*) por parte do titular.[224]

A perspectiva crítica quanto a fragilidade da doutrina do controle de dados pessoais em ambientes inteligentes também encontra raiz na pluralidade de pessoas submetidas aos dispositivos IoT. A seguir, será analisada a dificuldade de conformidade do instituto do consentimento quando não se tem um efetivo controle nem por parte dos titulares nem dos agentes de tratamento e fabricantes dos produtos inteligentes.

3.1.3. Pluralidade de titulares de dados

No tocante a casa inteligente, nem sempre o processamento dos dados pessoais será restrito àqueles que moram na residência, pois existem momentos em que o espaço privado é compartilhado com outras pessoas, como funcionários e visitantes. Isso significa dizer que além do morador - usuário principal do sistema doméstico inteligente -, terceiros também são expostos a dispositivos IoT e, consequentemente, estão sujeitos a terem suas informações pessoais tratadas pela tecnologia. Por esse motivo, se fala em uma internet das coisas de outras pessoas (*Internet of Other People's Things* - IoopT) ou internet das coisas das pessoas (*Internet of People's Thing* - IopT)[225]:

> Ademais, dispositivos IoT, como rastreadores de vestimentas fitness, não apenas coletam informações sobre seus usuários, mas também de pessoas ao seu redor. É difícil ver como o modelo de aviso e consentimento poderia ser uma opção na "internet das coisas das outras pessoas". A mudança de meros dispositivos inteligentes para ambientes inteiros inteligentes, move os indivíduos além do domínio do controle. (Tradução nossa)[226]

---

[224] ELEVANT, 2021, p. 28.

[225] *Ibid.,* p. 50.

[226] No original: *"Moreover, IoT devices such as wearable fitness trackers do not only collect information about their user, but also from people around them. It is difficult to see how the notice and consent model could be an option in 'internet of other people's things'. The shift from mere smart devices into entire smart environments, moves individuals beyond the realm of control". In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 67. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

O fato de diversas pessoas terem suas informações tratadas ao mesmo tempo pelo sistema inteligente se traduz, para o direito, em uma verdadeira pluralidade de titulares dados pessoais[227], com implicações práticas sobretudo quanto à efetividade e aplicabilidade da base legal de tratamento. Afinal, pela regra, caberia a cada titular dos dados consentir (ou não) sobre o tratamento de seus dados pessoais em ambientes inteligentes, o que não se identifica na prática.

Contudo, os direitos dos titulares não se resumem apenas ao titular principal, qual seja, o usuário direto da tecnologia. Interpretando a LGPD, uma vez que há tratamento de dados pessoais, há titulares e a eles devem ser garantidos os direitos previstos no artigo 18. Assim, pensando nas hipóteses de compartilhamentos eventuais do espaço doméstico inteligente, deveria ser possível a um visitante requisitar informações sobre a existência de tratamento de seus dados pessoais, vide inciso I do artigo 18.

Ter a informação sobre a existência do tratamento e saber quais dados são tratados é um reflexo do princípio do livre acesso, pelo qual é garantido aos titulares, de forma gratuita e facilitada, a consulta sobre a forma e duração do tratamento além da integralidade dos dados.[228]

A pluralidade de titulares submetidos ao mesmo dispositivo IoT e ambiente inteligente não se limita ao espaço doméstico. Afinal, se assim como a casa pode ser transformada pela tecnologia, ambientes como escolas, hospitais, empresas, fábricas e até cidades têm capacidade de se tornarem inteligentes, como visto no Capítulo 1.

Dado os obstáculos prático-jurídicos na concretização da autodeteminação informativa através do consentimento, resta encontrar amparo na segurança, transparência e boa-fé dos agentes de tratamento e fabricantes de produtos da IoT. Aliás, a comportamento dos agentes servirá como parâmetro para definição de eventuais sanções decorrentes do não cumprimento regulatório e de violações de direitos dos titulares, conforme preconiza o artigo 52 da LGPD:

---

[227] LGPD, art. 5º, V - "titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento."

[228] LGPD. Art. 6º "As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;"

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> §1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> ***II - a boa-fé do infrator;***
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> ***VII - a cooperação do infrator;***
> ***VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados***, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> ***IX - a adoção de política de boas práticas e governança;***
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção (grifo nosso).

Dito isso, a postura dos agentes perante a transparência no tratamento de dados pessoais de uma infinidade de titulares encontra desafio no estabelecimento de uma boa política de compliance e prestação de contas.

3.2. Reflexão sobre alternativas ao consentimento para efetividade da proteção de dados pessoais em casas inteligentes

Como demonstrado anteriormente, a ideia de controle das informações pelos indivíduos perde forças no ambiente inteligente pela grande quantidade de dispositivos interconectados, possibilidade de existirem diversos titulares de dados em um só ambiente e pela própria arquitetura e infraestrutura sob as quais os dispositivos são produzidos. É necessário, portanto, repensar a forma pela qual a tutela dos dados pessoais será feita na IoT.

Observando dados empíricos produzidos pela pesquisa de Anna Hudig *et al.* em torno da transparência aos consumidores na internet das coisas, fica nítida a preocupação dos pesquisadores em torno do cenário doméstico de configurações pessoais e íntimas em que os dispositivos de consumo IoT operam[229]. A partir da seleção e análise de 43 produtos da

[229] HUDIG, Anna I.; NORVAL, Chris; SINGH, Jatinder. *Transparency in the consumer Internet of Things: data flows and data rights*. Reino Unido: University of Cambridge, Imperial College London, 2023. Disponível em: http://www.iot-transparency.org/. Acesso em: 29 ago. 2023.

tecnologia IoT de diferentes fabricantes, voltados essencialmente para o ambiente doméstico e *wearables*[230], foi constatado que diferentes tipos de dados são coletados e armazenados de várias maneiras ainda nebulosas e, apesar dos direitos relativos à transparência, não está claro o que acontece posteriormente com os dados.[231]

Os pesquisadores relatam uma baixa performance dos fornecedores aos pedidos de portabilidade, na medida em que não houve retorno de nove fornecedores quanto às requisições de direitos dos titulares e dos demais, quando houve, as respostas não consideraram os pedidos em sua totalidade. Além de terem um processo complicado, os retornos eram marcados por generalismo, inconsistência ou mesmo com uma complexidade desnecessária.[232]

À primeira vista, de todas as bases legais disponíveis pela legislação para justificar o tratamento de dados pessoais por dispositivos domésticos inteligentes, o consentimento parece ser o caminho que deveria ser seguido pelos fabricantes. Todavia, as observações feitas até aqui demonstram a dificuldade de concretização daquilo que de fato está por trás do instituto: a autodeterminação informativa.

As reflexões sobre os efeitos da aplicabilidade da base legal do consentimento e sua efetividade em torno de situações que envolvem dispositivos domésticos inteligentes estão em consonância com a identificação do instituto tanto no seu aspecto de autodeterminação como de instrumento de legitimidade para tratamento de dados pessoais[233]. Nas claras palavras de

---

[230] Os produtos se enquadram da categoria de: babás eletrônicas, relógios inteligentes para crianças, rastreadores fitness, sensores de movimento, iluminação inteligente, tomadas inteligentes, TVs com streaming, balanças inteligentes, câmeras de segurança, campainhas eletrônicas e assistentes de voz. *In:* HUDIG, Anna I.; NORVAL, Chris; SINGH, Jatinder. *Transparency in the consumer Internet of Things: data flows and data rights*. Reino Unido: University of Cambridge, Imperial College London, 2023. P. 18. Disponível em: http://www.iot-transparency.org/. Acesso em: 29 ago. 2023.

[231] HUDIG, Anna I. *et al., op. cit.,* p. 63.

[232] No original: "*Our experience indicates that IoT vendors generally perform inadequately when it comes to data transparency rights (Section 4). The response rates to data access and data portability requests were overall surprisingly low, with nine out of 43 product vendors not responding at all, and those that did respond often failed to directly nor fully address the points raised in our requests, even after reminders and follow-ups. We also found that the process of interacting with vendors to obtain a meaningful response to our rights requests was often cumbersome, while the form and format in which responses were returned was generally inconsistent, generic, or unnecessarily complex. Given that data transparency rights are a key aspect of data protection law, poor adherence to these rights by vendors in the consumer IoT is concerning and problematic." In:* HUDIG, Anna I.; NORVAL, Chris; SINGH, Jatinder. *Transparency in the consumer Internet of Things: data flows and data rights*. Reino Unido: University of Cambridge, Imperial College London, 2023. P. 63. Disponível em: http://www.iot-transparency.org/. Acesso em: 29 ago. 2023.

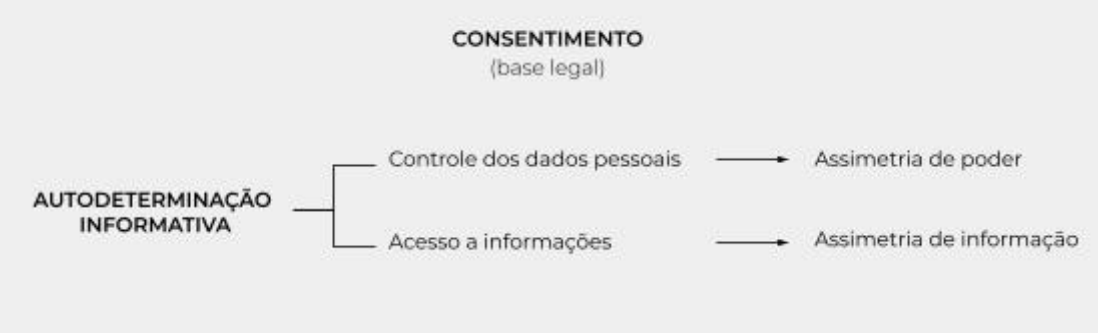
[233] DONEDA, 2020, p. 297.

Danilo Doneda:

> Neste momento, podemos voltar nossa análise para os efeitos do consentimento e então verificar como ponderar essa autodeterminação. E vemos que existem dois planos de análise possíveis: no primeiro, o consentimento é o instrumento por excelência dessa autodeterminação e, portanto, de um aspecto da tutela da pessoa. Em outro plano, porém, o consentimento representa o papel de instrumento de legitimação para que esses dados sejam, em alguma medida, utilizados por outra pessoa. E é preciso levar em conta que, muitas vezes, isso significa, conforme já ressaltamos, em alguma medida a transformação desses dados em uma determinada utilidade.[234]

Em resumo, a garantia do controle dos dados pessoais e o fornecimento de informações aos indivíduos são os dois aspectos do fundamento da autodeterminação informativa que compõem a "ficção jurídica"[235] do consentimento. No entanto, enquanto o exercício do primeiro é limitado pela assimetria de poder, o segundo encontra obstáculo na assimetria de informação. Para melhor visualização, a **Figura 6** demonstra o desenho da problemática em torno do consentimento.

Figura 6 - Esquema da problemática do consentimento



Fonte: Elaborado pela autora

Considerando a realidade da atual economia de dados bem como o fato de direitos fundamentais não serem absolutos, seria controverso defender que os titulares teriam de fato uma liberdade total de escolha sobre o uso de suas informações pessoais a ser exercida pelo consentimento. Sobre isso, Ana Frazão elucida:

> Como se vê, em que pese a LGPD exigir um consentimento qualificado, diversas características das negociações com dados dificultam o atendimento desse requisito, como já se viu anteriormente. Daí o ceticismo de alguns em relação a tais negociações, pois, como aponta Pasquale, não deixa de ser uma

[234] DONEDA, 2020, p. 296.

[235] *Ibid.,* p. 294.

> ficção achar que os consumidores podem e irão barganhar por privacidade ou simplesmente deixarem de contratar quando entenderem que seus direitos não estão sendo assegurados (o chamado opt out). Pelo contrário, em contextos de ausência de rivalidade e em que a aceitação da política de privacidade é condição sine qua non para o acesso ao serviço (as chamadas cláusulas take it or leave it), a legitimidade do consentimento sempre será discutível, mesmo que ele tenha sido informado.[236]

A própria LGPD, no mesmo artigo que prevê o consentimento, também cita outras hipóteses de tratamento de dados pessoais independentemente da anuência, ou concordância do titular, conforme explicado no Capítulo 2, tópico 2.3. Isso demonstra que, apesar de os dados revelarem informações pessoais, eles não podem ser vistos como propriedade única do indivíduo.

A posição doutrinária de que aborda os dados pessoais como bens jurídicos e, como tal, a escolha sobre a sua disposição recairia exclusivamente sob titular, é criticada por Danilo Doneda:

> Essa reflexão sobre a posição do mercado em relação ao uso de dados pessoais há de levar em conta, no entanto, que uma tutela dos dados pessoais em chave predominantemente proprietária seria incongruente com a própria consideração da proteção de dados como um direito fundamental, justamente pela incompatibilidade entre os meios de tutela e o exercício de um direito real sobre os dados pessoais. Assim, considerar os dados pessoais, a priori, como "bens" jurídicos teria como efeito basear o debate sobre a matéria a partir de paradigmas nos quais a pessoa humana estaria prejudicada já de início, e com parcas chances de fazer valer o valor do desenvolvimento de sua personalidade como prioritário. Assim, a possibilidade que parece ser mais palpável seria o enfoque no estabelecimento de mecanismos capazes de legitimar a inserção de dados pessoais no mercado, nos quais estaria inserida a valoração dos interesses e direitos fundamentais em questão, com os devidos limites e contrapesos.[237]

De fato, o consentimento é um mecanismo que torna legítimo a inserção dos dados e sua importância para o ordenamento jurídico não é negada. No entanto, persistir na aplicabilidade de um instituto que não está na mesma harmonia da tecnologia aqui estudada afeta não só a validade do próprio instituto, como também as demais normas que a ele estão associadas, a exemplo da questão da responsabilidade objetiva. Afinal, se a lei prevê que agentes de tratamentos estão sujeitos a sofrerem sanções e a repararem danos causados em razão de violação das normas nela previstas, seria ao menos contraditório punir o fabricante

---

[236] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* São Paulo: Ed. Thomson Reuters, 2019, p. 124.

[237] DONEDA, 2020, p. 288.

de IoT que a princípio é obrigado legalmente a coletar o consentimento, mas que, como visto, a própria natureza da tecnologia impede que ele seja obtido em conformidade legal.

Resta nítido, portanto, a necessidade de diálogo entre os campos do conhecimento humano para tornar a tutela do titular mais efetiva, pois, como antecipou Adriana Cansian, "a ciência jurídica por ela mesma não dará conta de explicar, tampouco solucionar a complexidade das relações humanas atuais"[238]. Depreende-se que há necessidade de se afastar um pouco das abstrações da norma jurídica e pensar em como de fato garantir os direitos com as ferramentas tecnológicas que se tem hoje.

3.2.1. Responsabilização e prestação de contas aos consumidores-titulares

Uma vez que o atual modelo de consentimento não é adequado para responder à evolução da realidade tecnológica[239], conforme preconiza Ina Elevant, urge explorar outras alternativas para proteger os titulares de dados utilizados no contexto de IoT. Para a autora, uma possível solução seria a mudança de paradigma do consentimento para a perspectiva de atribuir maior responsabilidade às empresas em lidar com a privacidade[240]. Assim, a carga é retirada do titular e é passada ao agente, que tem o ônus de assegurar a privacidade e as garantias jurídicas:

> A ênfase no controle e no consentimento coloca a responsabilidade nos indivíduos como tomadores finais da decisão. Isso implica em um fardo significativo sobre titulares de dados. Com o fim de reduzir essa carga nos indivíduos, o foco deveria ser desviado do consentimento. Muitas escolas e profissionais propuseram que o ônus da proteção de dados pessoais deveria ser posto mais nas empresas. Em razão da assimetria de informação, essa tese defende que as empresas poderiam ser postas de forma melhor para avaliar o impacto de seu tratamento de dados e implementar mitigações e salvaguardas adequadas. (Tradução nossa)[241]

---

[238] CANSIAN, 2022, p. 19.

[239] ELEVANT, 2021, p. 69.

[240] *Ibid.,* p. 68.

[241] No original: *"The emphasis on control and consent puts the responsibility on individuals as the ultimate decision makers. This places a significant burden on data subjects. In order to reduce the burden of individuals, the focus should be shifted away from consent. Several scholars and practitioners have proposed that the burden of data protection should be placed more on companies. Due to information asymmetries, this thesis argues that companies may be better placed to assess the impact of their data processing and to implement appropriate mitigations and safeguards." In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito,

Nessa linha, as empresas deveriam não apenas informar sobre a privacidade, como também inseri-la nos processos de desenvolvimento dos produtos[242]. Contudo, da mesma forma que melhorar a forma como a informação é passada não resolveria o problema da assimetria de poder, Ina reconhece o otimismo que seria depositar nas empresas a confiança de que elas prestarão contas a respeito do tratamento de dados, ainda mais considerando o valor comercial que eles carregam[243]. Por esse motivo que a autora conclui que a IoT escancarou os problemas concernentes ao consentimento, além de levantar novos questionamentos pela redução do espaço privado[244]. É o que acontece justamente em um ambiente doméstico infestado de dispositivos inteligentes.

De todo modo, prestar contas não é mero otimismo, mas sim uma obrigação legal. Trata-se de um princípio presente no inciso X do artigo 6º da LGPD pelo qual deve haver "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

Guilherme Martins explica que a eficácia de tal princípio reside no exercício da proteção coletiva, considerando a defesa do interesse difuso, direito coletivo ou direito individual homogêneo como direitos básicos do consumidor (art. 6º, VI e VII, CDC)[245]. Trata-se, portanto, de uma previsão legal de caráter essencial, sobretudo em razão do problema da pluralidade de titulares no contexto de ambientes inteligentes.

O foco na responsabilização e prestação de contas seria, portanto, uma alternativa diante da assimetria informacional que amedronta o instituto do consentimento. Como diz Ana Frazão:

> (...) diante da assimetria informacional que parece ser insolúvel, indaga-se em que medida vale a pena ainda valorizar tanto o consentimento, quando haveria outros mecanismos mais idôneos e exequíveis para assegurar os valores agasalhados pela LGPD, entre os quais as soluções tecnológicas, como o privacy by design, ou mesmo a transparência e a accountability.[246]

Universidade de Helsinki, Finlândia, 2021. P. 68. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[242] ELEVANT, 2021, p. 65.

[243] *Ibid.,* p. 68.

[244] *Ibid.,* p. 68.

[245] MARTINS, 2021, p. 221.

[246] FRAZÃO, 2019, p. 124.

Ina Elevant vai de encontro com o posicionamento anterior, pois defende que:

> Uma forma de transferir o ônus da proteção de dados para as empresas é o *Privacy by Design* e *Privacy by Default.* A privacidade por design e por padrão visa incorporar a privacidade no processo de design e engenharia do dispositivo inteligente, bem como nas práticas de negócios das partes interessadas. O *Privacy by Design* impõe um requisito de responsabilidade para os controladores. A introdução da responsabilização representa uma mudança de paradigma na proteção de dados. As empresas não são apenas obrigadas a fornecer informações de privacidade às pessoas, mas também são obrigadas a projetar dispositivos e processos com a privacidade em mente. (Tradução nossa)[247]

A ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviço (*Privacy by Design*), além de tê-la como padrão em suas configurações (*Privacy by Default*) é uma abordagem metodológica[248] que conversa com as chamadas PETs *(Privacy Enhancing Technologies),* tecnologias voltadas à facilitação e aprimoramento da privacidade, ajudam esse comportamento de garantia da privacidade[249]. Retomando a principal referência legislativa na elaboração da norma brasileira, o GDPR prevê o princípio do *accountability*, obrigando o controlador a estar em conformidade com a legislação. É nesse contexto que faz sentido o investimento em PETs com o fim de operacionalizar os programas de compliance voltados para proteção de dados pessoais.

No Brasil, a responsabilização e prestação de contas reverbera nos artigos 42 e entre os artigos 46 e 51 da LGPD[250]. O artigo 42 cuida da responsabilidade por danos causados, ao passo que o artigo 50 traz as boas práticas e governança como guias aos agentes de tratamento. A crítica que se faz a este último é que o uso da palavra "poderão" pelo legislador, ao invés de "deverão" parece esvaziar a força de obrigatoriedade:

---

[247] No original: *"One way of shifting the burden of data protection to companies is privacy by design and default. Privacy by design and default aims to embed privacy into the design and engineering process of the smart device as well as to business practices of the stakeholders. Privacy by design places an accountability requirement for controllers. The introduction of accountability represents a paradigm shift in data protection. Companies are not only required to provide privacy information to people but are also required to design devices and processes with privacy in mind.". In:* ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. P. 65. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

[248] JIMENE, Camilla do Vale. Capítulo VII - Da Segurança e das Boas Práticas: Seção I - Da segurança e do sigilo de dados. *In:* MALDONADO, Viviane Nóbrega; BLUM, Opice Renato (Coord.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019. P. 329-354.

[249] BIONI, 2020*,* p. 191

[250] LGPD. Capítulo VII - Da Segurança e das Boas Práticas.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, ***poderão*** formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (Grifo nosso).

Apesar das atecnicidades legislativas, o princípio se aplica, paralelamente, aos princípios da transparência e da segurança, o que reforça a necessidade de esclarecimento e informação através das boas práticas e governança sugeridas pelo artigo 50. Dito isso, a aplicação das referidas normas aos fornecedores e fabricantes de dispositivos inteligentes conversa com o objetivo central de incorporar a privacidade nos processos de desenvolvimento dos produtos, assim como nas práticas de negócios.[251]

Não menos importante, a abordagem do *Legal Design* corrobora na busca pelo atingimento de um nível adequado de conformidade, na medida em que atua na melhoria da comunicação e transparência na informação. Pensando nesse contexto, foi desenvolvido um rascunho do que poderia ser uma página na web para consulta dos usuários de dispositivos domésticos inteligentes, de forma que eles saibam se os seus direitos estariam (ou não) sendo respeitados[252]. A aplicação poderia facilmente ser utilizada por uma organização não-governamental, associação sem fins lucrativos ou até pela Agência Reguladora para consulta dos consumidores leigos, bem como servir de orientação em como eles devem proceder em caso de possíveis descumprimentos normativos.

Em última análise, prosseguindo com o viés da informação na problemática aqui abordada, é possível concluir que, enquanto a transmissão da informação pelo consentimento reside antes da coleta dos dados, a informação passada conforme a responsabilização e prestação de contas ocorre em momento posterior, isto é, quando já há tratamento de dados pessoais e os agentes precisam demonstrar a tutela conferida a eles. Logo, uma vez adotada a mudança de paradigma do consentimento para uma postura mais ativa por parte dos agentes,

---

[251] ELEVANT, 2021, p. 62.

[252] O código da página foi desenvolvido como avaliação da disciplina "Coding for Lawyers", cursada durante o intercâmbio na Universidade de Bologna no primeiro semestre de 2023. Construída com o básico de HTML, CSS e Javascript, o principal objetivo da página é transmitir informação aos usuários de IoT no contexto de casas inteligentes, além de indicar, com base no *input* do usuário, se os direitos estariam sendo respeitados. Para ter acesso, recomenda-se fazer o download do código e abrir em um navegador. Disponível em: https://github.com/rafacogliatti/Coding_for_LawyersUNIBO-96363-. Acesso em: 03 out 2023.

em caso de descumprimento das normas, as empresas seriam punidas não porque o consentimento não foi coletado de forma adequada, mas sim porque não houve a devida governança e prestação de contas que preconiza a legislação.

3.2.2. Investimento em segurança e prevenção de danos na utilização de produtos inteligentes

Em 2017, o Instituto Brasileiro de Defesa do Consumidor (IDEC) manifestou certa preocupação quanto a Internet das Coisas, no sentido de que pode trazer riscos aos usuários, como vazamento de dados, atuação de hackers e aplicação de golpes[253]. Afinal, ao mesmo tempo em que rápido desenvolvimento da IoT aumenta o número de conexões, os sistemas se tornam mais vulneráveis[254]. Como explica Renato Opice Blum:

> Muita interação = muita facilidade; muitos dados = muitos interesses = muito dinheiro. Esta sequência, obrigatoriamente reconhecida quando objetos são associados à internet, foi fácil e rapidamente percebida pelos indivíduos mal-intencionados que atuam na Web. Logicamente, a partir do momento em que coisas (relógios, fogões, TVs) precisam de dados reais e atualizados de seus usuários para funcionar de forma personalizada, esses objetos passaram a atrair a atenção de infratores.[255]

Lembra-se que além de pessoas físicas, as próprias empresas também podem ser usuárias de produtos IoT e, portanto, precisam manter suas informações de negócios protegidas de ataques maliciosos[256]. Vale ressaltar que a informação por si só não tem grande valor, mas sim o que o que se faz a partir dela.[257]

---

[253] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Para Idec, Internet das Coisas pode trazer riscos aos usuários. Disponível em: https://idec.org.br/em-acao/em-foco/para-idec-internet-das-coisas-pode-trazer-riscos-aos-usuarios. Acesso em: 16 ago. 2023.

[254] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. *Data protection regulations and international data flows: Implications for trade and development*. Genebra: United Nations Publications, 2016. P. 74. Disponível em: https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. Acesso em: 05 out. 2023.

[255] BLUM, 2021, p. 266.

[256] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2016, p. 74.

[257] MARTINS, 2021, p. 214.

Nesse sentido, é legítimo dizer que privacidade e segurança deve ser o cerne do desenvolvimento de produtos inteligentes, sobretudo quando se lida com informações pessoais. Trata-se de um binômio que causa preocupação também no contexto doméstico, como apontado pelo estudo da Conferência das Nações Unidas sobre Comércio e Desenvolvimento.[258]

Dado que o tratamento das informações coletadas por dispositivos inteligentes implica em riscos, o aprimoramento de técnicas de segurança serve justamente para prevenir ou minimizar o impacto de possíveis danos. Por isso, Blum diz que: "[...] toda forma de acesso à Rede Mundial, inclusive realizadas através de objetos inteligentes, precisa resguardar a segurança das informações de seus clientes e a proteção à privacidade, evitando vazamentos, obtenções indevidas de dados e seu respectivo desvio de finalidade"[259].

Quanto à segurança, as palavras de Adriana Cansian vão no sentido de que:

> O conceito de segurança pressupõe um processo em que muitas variáveis precisam ser combinadas para que se chegue a um nível razoável de proteção, quando se fala da guarda e armazenamento de dados, visto que a manutenção de requisitos como a confidencialidade, depende muitas vezes do respeito às políticas de controle de acesso e às políticas de senhas. No caso específico dos dispositivos interconectados por IoT, o conceito de segurança pressupõe a observação de mecanismos projetados desde a ideação do produto, ou seja, concebidos a partir do seu desenvolvimento, considerando todas as fragilidades do usuário final.[260]

Assim, o investimento em infraestrutura e pesquisa por parte dos fabricantes de produtos inteligentes seria a direção para melhorar os aspectos de segurança e privacidade, o que pode ser alcançado com técnicas de anonimização, implementação das PETs e internalização da cultura do *privacy by design* no desenvolvimento de fabricação de produtos inteligentes. Por outro lado, existem obstáculos que dificultam o processo, como o tamanho

---

[258] Uma vez que a maior parte dos itens domésticos são atualmente operados através da Internet/WIFI, consumidores estão preocupados com a proteção dos seus dados e da sua rede doméstica de ataques maliciosos, como o hacker de um dispositivo de entrada sem chave, um abridor de portas de garagem ou qualquer outro sistema doméstico conectado ao WIFI. (Tradução nossa). No original: *"Since most household items are today being operated through the Internet/WIFI, consumers are concerned about the protection of their data and home network from malicious attacks such as hacking a keyless entry device, a garage door opener, or any other home system connected to WIFI". In:* UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. *Data protection regulations and international data flows: Implications for trade and development*. Genebra: United Nations Publications, 2016. P. 74. Disponível em: https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. Acesso em: 05 out. 2023.

[259] BLUM, 2021, p. 268.

[260] CANSIAN, 2022, p. 55.

dos dispositivos que, podem ser tão pequenos que já se fala até em uma “internet das coisas pequenas” (IoNT).[261]

Por fim, um relatório do Comitê Consultivo de Segurança e Estabilidade da ICANN encontrou soluções para transparência e segurança na IoT através do DNS, como técnicas de autenticidade dos serviços e criptografia, além da necessidade de treinamento de profissionais do área, de forma que os fabricantes saibam interagir com o DNS.[262]

[261] CANSIAN, 2022, p. 55.

[262] ICANN SECURITY AND STABILITY ADVISORY COMMITTEE. *The DNS and the Internet of Things: Opportunities, Risks, and Challenges*. SAC 105. Relatório, 28 maio 2019. P. 10-20. Disponível em: https://www.icann.org/en/system/files/files/sac-105-en.pdf. Acesso em: 03 out. 2023.

CONSIDERAÇÕES FINAIS

Os espaços domésticos não fogem da transformação tecnológica viabilizada pela Internet das Coisas. A reflexão sobre os impactos que uma casa inteligentes pode causar no contexto jurídico, encontra justamente o paradoxo da casa como sendo o lugar onde o indivíduo exerce seu direito de estar só, sua intimidade e privacidade, ao mesmo tempo em que se torna ambiente de possíveis violações de direitos pelo fato de ser fonte de produção de informações pessoais.

Sendo o consentimento aquilo que, *a priori*, legitimaria o tratamento de dados pessoais coletados pelos dispositivos inteligentes, foi possível observar certa fragilidade quanto a sua aplicação diante do cenário de casas inteligentes. Tal fragilidade decorre da inevitável assimetria de poder e de informação que incide sobre as duas facetas da autodeterminação informativa (controle dos dados pessoais e acesso à informação), entendida como sendo o plano de fundo do consentimento.

Tendo em vista a datificação da economia mundial, é impossível garantir um efetivo controle e poder de escolha aos usuários, consumidores e titulares. Além disso, a aplicação do consentimento em um sistema de IoT encontra obstáculos na própria estrutura dos dispositivos, na multiplicidade de dispositivos interconectados e na pluralidade de titulares de dados.

Em suma, apesar da racionalidade por trás das legislações de proteção de dados ser a autodeterminação informativa exercida através do consentimento, esse estudo discutiu que o instituto, da forma pela qual é concebido e aplicado hoje, não está adequado às peculiariedades da IoT. Alternativamente, valorizar normas de responsabilização e prestação de contas poderia ser uma saída para garantir maior transparência e aos usuários dos produtos inteligentes. Nesse ponto, as PETs, a cultura corporativa do ESG e a implementação da privacidade nos processos de desenho e fabricação dos produtos (*privacy by design*) podem ser aliados dos fabricantes. Em paralelo, investimentos em sistemas cada vez mais seguros é prevenir e mitigar os danos que um incidente de segurança pode causar aos consumidores-titulares.

A IoT já é uma realidade carregada de mudanças na sociedade e com implicações sociojurídicas relevantes, de forma que urge pensar sobre os desafios que esta nova etapa tecnológica carrega. Por mais difícil que possa parecer, é preciso que o direito caminhe junto com as essas transformações, preparando o mercado para que atividades sejam exercidas de forma ética, regulada e fiscalizada

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Tecnologia 5G: Saiba mais sobre a tecnologia que vai revolucionar a conectividade. Gov.br: Ministério das Comunicações, 22 fev. 2021. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/5G/tecnologia-5g. Acesso em: 08 jul. 2022.

ALVI, Atif; NABI, Zubair. *Clome: The Practical Implications of a Cloud-based Smart Home*. IBM Research Report. 2014. Disponível em: <https://dominoweb.draco.res.ibm.com/fea5c1645d95c27285257d02005c4ec1.html>. Acesso em: 25 ago. 2023.

ANSCOMBE, Tony. *IoT and privacy by design in the smart home*. Bratislava: Eset - enjoy safer technology**,** fev. 2018. Disponível em: https://iapp.org/resources/article/iot-and-privacy-by-design-in-the-smart-home/#:~:text=IoT%20and%20privacy%20by%20design%20in%20the%20smart,to%20the%20creation%20of%20a%20basic%20smart%20home. Acesso em: 13 set. 2023.

ARGENTINA. Proteccion de Los Datos Personales. Lei 25.326. Buenos Aires, 2000. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790. Acesso em: 21 set. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Publicações da ANPD**.** Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em 28 set. 2023.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento.* 2. ed. Rio de Janeiro: Forense, 2020. 328 p.

BLUM, Renato Opice M. S. Internet das Coisas: A Inauguração do novo mundo e suas intercorrências jurídicas. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital, Direito Privado e Internet.* 4 ed. São Paulo: Editora Foco, 2021, p. 265 - 279.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF, 5 out. 1998.

_____. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF, 11 set. 1990.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Brasília, DF, 10 jan. 2002.

_____. Lei nº 10.741, de 1º de outubro de 2003. Estatuto da Pessoa Idosa. Brasília, DF, 1 out. 2003.

_____. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, DF, 23 abr. 2014.

_____. Lei 13.105, de 16 de março de 2015. Código de Processo Civil. Brasília, DF, 16 mar. 2015.

_____. Lei nº 13.146, de 6 de julho de 1015. Estatuto da Pessoa com Deficiência. Brasília, DF, 6 jul. 2015.

BRASIL. Lei nº 13.709, de 14 de outubro de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 14 out. 2018.

_____. Lei nº 14.533, de 11 de janeiro de 2023. Política Nacional de Educação Digital. Brasília, DF, 11 jan. 2023.

_____. Decreto nº 9.854, de 25 de junho de 2019. Plano Nacional de Internet das Coisas. Brasília, 25 jun. 2019.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro, RJ, 7 dez. 1940.

BRANCHER, Paulo Marcos Rodrigues. Proteção internacional de dados pessoais. *Enciclopédia jurídica da PUC-SP.* Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Internacional. Cláudio Finkelstein, Clarisse Laupman Ferraz Lima (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/496/edicao-1/protecao-internacional-de-dados-pessoais. Acesso em: 23 ago. 2023.

CANSIAN, Adriana Cardoso de Moraes. *Aspectos relevantes da internet das coisas (IoT): segurança e protenção de dados*. 2022. 142 p. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2022.

CASA Inteligente com Alexa. Amazon. Disponível em: https://www.amazon.com.br/b?ie=UTF8&node=20000328011. Acesso em: 31 ago. 2023.

COELHO, Alexandre Zavaglia; HOLTZ, Ana Paula Ulandowski. Legal Design | Visual Law: comunicação entre o universo do Direito e os demais setores da sociedade. *Thomson Reuters*. Ed eletrônica. 2020. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/legal-one/biblioteca-de-conteudo-juridico/legal-design-visual-law.html. Acesso em: 11 set. 2023.

COGLIATTI, Rafaella S. *Coding For Lawyers*. Github. Disponível em: https://github.com/rafacogliatti/Coding_for_LawyersUNIBO-96363-. Acesso em: 03 out 2023.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. *Data protection around the world*. Disponível em: https://www.cnil.fr/en/data-protection-around-the-world. Acesso em: 09 out. 2023.

CONSEIL EUROPÉEN POUR LA RECHERCHE NUCLÉAIRE. *A short history of the Web: the Web has grown to revolutionise communications worldwide*. Homepage. Genebra. Disponível em: https://home.cern/science/computing/birth-web/short-history-web. Acesso em: 07 jul. 2022.

CONSENTIMENTO. *In:* DICIO, Dicionário Online de Português. Porto: 7Graus, 2023. Disponível em: https://www.dicio.com.br. Acesso em: 24 jul. 2023.

CONSENTIR. *In:* DICIO, Dicionário Online de Português. Porto: 7Graus, 2023. Disponível em: https://www.dicio.com.br. Acesso em: 24 jul. 2023.

DOMINGO ESPETACULAR. Crise das Big Techs coloca futuro do setor em xeque. Youtube, 20 de nov. de 2022. Disponível em: https://www.youtube.com/watch?v=5yJRCI6RcuM&t=0s. Acesso em: 14 ago. 2023.

DONEDA, Danilo Cesar Maganhoto. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. 364 p.

ELEVANT, Ina. *Consent as a basis of processing personal data in the Internet of Things*. 2021. 85 p. Dissertação (Mestrado em *International Business Law*) - Faculdade de Direito, Universidade de Helsinki, Finlândia, 2021. Disponível em: https://ethesis.helsinki.fi/repository/handle/123456789/38817. Acesso em: 02 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. *California Consumer Privacy Act of 2018*. Califórnia, CA, 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 21 set. 2023.

EUROPEAN DATA PROTECTION BOARD. *Guidelines 05/2020 on consent under Regulation 2016/679*. Versão 1.1, maio de 2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt#:~:text=Diretrizes%2005%2F2020%20relativas%20ao%20consentimento%20na%20ace%C3%A7%C3%A3o%20do,2016%2F679%204%20May%202020%20Guidelines%2005%2F2020%20321.3%20KB. Acesso em: 29 set. 2023.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Ed. Thomson Reuters, 2019, p. 99-129.

GARCIA, Milena. Apple Watch: veja 7 vezes em que o relógio salvou a vida das pessoas. *TechTudo*, 28 de ago. de 2021. Disponível em: https://www.techtudo.com.br/listas/2021/08/apple-watch-veja-7-vezes-em-que-o-relogio-salvou-a-vida-das-pessoas.ghtml. Acesso em: 08 jul. 2022.

GRATÃO, Paulo. Supermercado de SP adota carrinho inteligente, que soma e recebe o pagamento das compras. *Pequenas Empresas & Grandes Negócios*, 3 de maio de 2022. Disponível em: https://revistapegn.globo.com/Banco-de-ideias/Varejo/noticia/2022/05/supermercado-de-sp-adota-carrinho-inteligente-que-pesa-soma-e-recebe-o-pagamento-das-compras.html. Acesso em: 31 out. 2023.

HUDIG, Anna I.; NORVAL, Chris; SINGH, Jatinder. *Transparency in the consumer Internet of Things: data flows and data rights*. Reino Unido: University of Cambridge, Imperial College London, 2023. Disponível em: http://www.iot-transparency.org/. Acesso em: 29 ago. 2023.

ICANN SECURITY AND STABILITY ADVISORY COMMITTEE. *The DNS and the Internet of Things: Opportunities, Risks, and Challenges*. SAC 105. Relatório, 28 maio 2019. 28 p. Disponível em: https://www.icann.org/en/system/files/files/sac-105-en.pdf. Acesso em: 03 out. 2023.

ÍNDIA. *The Digital Personal Data Protection Act.* PRS - Legislative Research**.** Nova Deli, 2023. Disponível em: https://prsindia.org/acts/parliament. Acesso em: 23 set. 2023.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Para Idec, Internet das Coisas pode trazer riscos aos usuários. Disponível em: https://idec.org.br/em-acao/em-foco/para-idec-internet-das-coisas-pode-trazer-riscos-aos-usuarios. Acesso em: 16 ago. 2023.

INSTITUTO CIDADES SUSTENTÁVEIS. Pesquisa Cidades Sustentáveis: desigualdades. São Paulo, 2022. Disponível em: https://www.cidadessustentaveis.org.br/paginas/pesquisas. Acesso em: 18 out. 2023.

INTERNATIONAL TELECOMMUNICATION UNION. *Global Digital Regulatory Outlook 2023: Policy and regulation to spur digital transformation*. ITU Publications, 2023. 116 p. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2023-PDF-E.pdf. Acesso em: 31 ago. 2023.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. *ICANN Acronyms and Terms.* Disponível em: https://www.icann.org/en/icann-acronyms-and-terms. Acesso em: 29 ago 2023.

_____. *ICANN for Beginners.* Disponível em: https://www.icann.org/en/beginners. Acesso em: 29 ago 2023.

JIMENE, Camilla do Vale. Capítulo VII - Da Segurança e das Boas Práticas: Seção I - Da segurança e do sigilo de dados. *In:* MALDONADO, Viviane Nóbrega; BLUM, Opice Renato (Coord.). LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019. P. 329-354.

KETTERMANN, Matthias C. *Law and Governance of the Internet. In: _____. The Normative Order of the Internet: A Theory of Rule and Regulation Online.* Estados Unidos da América: Oxford University Press, 2020. P. 59-130. Disponível em: https://academic.oup.com/book/39694. Acesso em: 05 jul. 2023.

LEITE, JR Emiliano; MARTINS, Paulo S.; URSINI, Edson L. A Internet das Coisas (IoT): Tecnologias e Aplicações. *In*: *Brazilian Technology Symposium*. 1., Campinas, dezembro de 2017. Disponível em: https://lcv.fee.unicamp.br/images/BTSym-17/Papers/76926.pdf. Acesso em: 30 ago. 2023.

LINS, Theo. Indústria 4.0 E IoT – Internet Das Coisas E Automação. Laboratório iMobilis, 22 set. 2015. Disponível em: http://www2.decom.ufop.br/imobilis/industria-4-0-e-iot/. Acesso em: 30 ago. 2023.

MAGRANI, Eduardo. *A Internet das Coisas.* Rio de Janeiro: FGV Editora, 2018. 192 p. Disponível em: http://eduardomagrani.com/livro-internet-da-coisas-2018/; Acesso em: 13 dez. 2022.

MARTINS. Guilherme Magalhães. A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e a sua principiologia. *Revista dos Tribunais*, São Paulo, v. 1027, p. 203 - 243, maio 2021.

MIRAGEM, Bruno; MARQUES, Claudia Lima. O necessário diálogo entre a LGPD e o Código de Defesa do Consumidor e os novos direitos do consumidor-titular dos dados. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR, Otávio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. P. 795-817. Disponível em: https://brunomiragem.com.br/artigos/026-o-necessario-dialogo-entre-a-lgpd-e-o-codigo-de-defesa-do-consumidor.pdf. Acesso em: 18 out. 2023.

NEMOTO, Miriam Christi Midori Oishi. *Inovação tecnológica: um estudo exploratório de adoção do RFID (Identificação por Radiofrequência) e redes de inovação internacional.* 2009. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2009. Disponível em: http://www.teses.usp.br/teses/disponiveis/12/12139/tde-18122009-105036/. Acesso em: 24 ago. 2023.

O que é a IoT?. Amazon. Disponível em: https://aws.amazon.com/pt/what-is/iot. Acesso em: 24 ago. 2023.

O que é IoT?. Oracle. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/#industries-iot. Acesso em: 24 ago. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 1948. Disponível em: https://brasil.un.org/pt-br/91601-declara%C3%A7%C3%A3o-universal-dos-direitos-humano. Acesso em: 1 set. 2023.

_____.*The 17 Goals*. Disponível em: https://sdgs.un.org/goals. Acesso em: 5 out. 2023.

PACETE. Luiz Gustavo. IoT amplia vendas de eletrônicos e expõe o desafio da sustentabilidade. *Forbes* [online], 30 set. 2022. Disponível em: https://forbes.com.br/forbesesg/2022/09/iot-amplia-vendas-de-eletronicos-e-expoe-o-desafio-da-sustentabilidade/. Acesso em: 09 out. 2023.

POOL PARTY (temporada 11, ep. 4). *Modern Family* [Seriado]. Direção: Abraham Higginbotham. Produção: Steven Levitan. Estados Unidos: Picador Productions, 2019. (25 min.), son., color.

RAPOPORT, Izabel Duva. A Curiosa Origem do Ditado “Quem cala consente”. Aventuras na História, *UOL* [online], São Paulo, 24 jul. 2023. Disponível em: https://aventurasnahistoria.uol.com.br/noticias/almanaque/de-onde-vem-expressao-quem-cala-consente.phtml . Acesso em: 24 jul. 2023.

REPÚBLICA POPULAR DA CHINA. Lei de Proteção de Informações Pessoais. China, 2021. Disponível em: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm. Acesso em: 21 set. 2023.

RODRIGUES, Sandra Souza.; FORTES, Renata Pontin de Mattos. Uma revisão sobre acessibilidade no desenvolvimento de internet das coisas: oportunidades e tendências. *Revista de Sistemas e Computação*, Salvador, v. 9, n. 1, p. 19-40, jan./jun. 2019. Disponível em: https://revistas.unifacs.br/index.php/rsc/article/view/5708#:~:text=UMA%20REVIS%C3%83O%20SOBRE%20ACESSIBILIDADE%20NO%20DESENVOLVIMENTO%20DE%20INTERNET,um%20t%C3%B3pico%20de%20significativo%20interesse%20nos%20%C3%BAltimos%20anos. Acesso em: 22 set. 2023.

SALUTES, Bruno. O que é IP. *CanalTech*, 21 out. 2023. Disponível em: https://canaltech.com.br/software/o-que-e-ip/. Acesso em: 29 ago. 2023.

SANTOS, Bruno P.; *et al*. Internet das Coisas: da Teoria à Prática. *In:* AUGUSTO, F. S.; LUNG, L. C.; GREVE, F. G. P.; FREITAS, A. E. S. F. (Org.). Livro de Minicursos. *XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*; Porto Alegre: SBC, 2016, 315 p. Disponível em: https://bps90.github.io/assets/files/MinicursosSBRC2016.pdf. Acesso em: 28 set. 2023.

SOUZA, Erick. São Paulo instala semáforos inteligentes; entenda como funcionam. *Estadão* [online], São Paulo, 23 ago. 2023. Disponível em: https://mobilidade.estadao.com.br/mobilidade-com-seguranca/transito/semaforos-inteligentes-sao-paulo/. Acesso em: 28 ago. 2023.

SPACCAQUERCHE, Paulo. Aplicações de IoT que se tornaram viáveis com o 5G. *ABINC: Associação Brasileira de Internet das Coisas*, São Paulo, 29 de maio de 2023. Disponível em: https://abinc.org.br/aplicacoes-de-iot-que-se-tornaram-viaveis-com-o-5g/. Acesso em: 16 ago. 2023.

STATISTA RESEARCH DEPARTMENT. *Number of households with smart home products and services in use worldwide from 2017 to 2025.* Disponível em: https://www.statista.com/statistics/1252975/smart-home-households-worldwide/#:~:text=The%20number%20of%20households%20worldwide%20using%20smart%20home,increase%20even%20further%20to%20more%20than%20530%20million. Acesso em: 25 ago. 2023.

TANZI, ATTILA. *A Concise Introduction to International Law.* 2. ed. Turim: Eleven international publishing, 2022. 285 p.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. (Regulamento Geral sobre a Proteção de Dados). Eur-Lex. Disponível em: Acesso em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. 11 set. 2023.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. *Data protection regulations and international data flows: Implications for trade and development*. Genebra: United Nations Publications, 2016. 154 p. Disponível em: https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf. Acesso em: 05 out. 2023.

UNIVERSITÀ DI BOLOGNA. *Unibo.it,* Itália, 2023. Disponível em: https://www.unibo.it/it/homepage. Acesso em: 10 ago. 2023.

WEBER, Rolf H.; WEBER, Romana. *Internet of Things: Legal Perspectives*. Springer Berlin, Heidelberg, 2010. 135 p. Disponível em: https://www.dhi.ac.uk/san/waysofbeing/data/governance-crone-weber-2010.pdf. Acesso em: 26 jul. 2023.

👍: EMOJI DE 'joinha' firma acordo contratual, diz tribunal canadense: decisão leva em consideração "nova realidade na sociedade canadense", em que sentimentos são traduzidos nas pequenas figuras disponíveis nos smartphones. *Veja* [online], 7 jul. 2023. Mundo. Disponível em: <https://veja.abril.com.br/mundo/%f0%9f%91%8d-emoji-de-joinha-firma-acordo-contratual-diz-tribunal-canadense/>. Acesso em: 14 ago. 2023.