ADRIANA CARDOSO DE MORAES CANSIAN

# ASPECTOS JURÍDICOS RELEVANTES DA INTERNET DAS COISAS (IoT): SEGURANÇA E PROTEÇÃO DE DADOS

TESE DE DOUTORADO

Orientador: Prof. Titular Dr. Newton De Lucca
Coorientador: Prof. Dr. Demi Getschko

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo - SP
2021

ADRIANA CARDOSO DE MORAES CANSIAN

# ASPECTOS JURÍDICOS RELEVANTES DA INTERNET DAS COISAS (IoT): SEGURANÇA E PROTEÇÃO DE DADOS

Tese de Doutorado apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de Doutor em Direito, na área de concentração de Direito Comercial n, sob a orientação do Prof. Titular Dr. Newton De Lucca e do Prof. Dr. Demi Getschko da Pontifícia Universidade Católica.

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo - SP
2021

Nome: CANSIAN, Adriana Cardoso de Moraes

Título: Aspectos jurídicos relevantes da internet das coisas (IoT): segurança e proteção de dados

Tese apresentada à apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de Doutor em Direito, na área de concentração de Direito Comercial.

Aprovado em:

BANCA EXAMINADORA

Prof. Dr: _____

Instituição: _____

Julgamento: _____

Prof. Dr: _____

Instituição: _____

Julgamento: _____

Prof. Dr: _____

Instituição: _____

Julgamento: _____

Prof. Dr: _____

Instituição: _____

Julgamento: _____

Prof. Dr: _____

Instituição: _____

Julgamento: _____

# AGRADECIMENTOS

À Espiritualidade Superior pela oportunidade de cumprir dignamente minha missão neste plano reencarnatório.

Às minhas filhas, Ana Luiza e Maria Alice, pela coragem de lutar por um mundo melhor e a inspiração para nunca desistir.

Ao meu marido, Adriano Cansian, pelo conhecimento compartilhado, pelo incondicional apoio acadêmico, a parceria de todos os dias e o amor de tantos anos.

Ao meu orientador, Newton De Lucca, pelas inestimáveis lições de direito e pela confiança em mim depositada.

Ao meu coorientador, Demi Gestschko, pelo forte laço de afeto que nos une e a honra de poder aprender com quem tudo viveu e tudo conhece sobre a internet brasileira.

À Resh Cyber Defense e à minha equipe do escritório, especialmente, ao Leon Campos, Eliazar Lino Jr, Caio de Moraes Cintra e Daniele Rodrigues pela parceria irretocável e a companhia de sempre.

Aos Professores Roberto Pfeiffer, Marcos Perez e Rodrigo Pagani, gratidão pelas muitas lições compartilhadas e a amizade que nos une.

Ao GEESIPDP - Grupo de Estudos Estratégicos em Segurança da Informação e Proteção de Dados Pessoais - especialmente ao amigo Roberto Taufick pela amizade e o conhecimento que estamos construindo juntos.

**SUMÁRIO**

**RESUMO** ..... **8**
**ABSTRACT** ..... **9**
**1 INTRODUÇÃO** ..... **10**
1.1 A tese aqui defendida ..... 10
1.2 Histórico e desenvolvimento da Internet: considerações que fundamentam a relevância do tema ..... 16
1.3 Internet e Direito no contexto brasileiro: apontamentos históricos ..... 20
**2 A INTERNET DAS COISAS: MATIZES CONCEITUAIS E VIESES DESENVOLVIMENTISTAS** ..... **23**
2.1 A Internet das Coisas ..... 24
2.1.1 O significado de coisas e o conceito formal de IoT ..... 24
2.1.2 A coleta de dados por IoT: um processo multifacetado ..... 31
2.1.3 A interoperabilidade como referência para usuários, fabricantes e desenvolvedores ..... 36
2.2 Os quatro pilares de inovação ..... 39
**3 DESAFIOS CIBERNÉTICOS E LEGAIS EM IOT** ..... **46**
3.1.1 Hexagrama Parkeriano ..... 49
3.1.1.1 Risco ..... 50
3.1.1.2 Ameaça ..... 50
3.1.1.3 Vulnerabilidade ..... 50
3.1.1.4 Exposição ..... 51
3.1.1.5 Contramedida ou salvaguarda ..... 51
3.2 Principais riscos de segurança em IoT ..... 51
3.2.1 Controle de acesso e identidade em IoT ..... 53
3.3 Boas práticas ..... 55
3.4 Respostas a Incidentes e Protocolo de *Data Breach* ..... 58
3.5 Da Política de Privacidade e de Segurança ..... 58
**4 PROTEÇÃO DE DADOS EM IOT: O GRANDE DESAFIO TÉCNICO-JURÍDICO** **59**
4.1 Aspecto histórico da proteção de Dados ..... 59
4.2 O contexto da governança: boas práticas e transparência ..... 61
4.3 A autodeterminação informativa e o consentimento válido ..... 62
4.4 Boas Práticas e medidas técnicas LGPD e menção a alguns padrões internacionais ..... 68
4.5 Direito à Portabilidade e IoT ..... 70
4.6 IoT e Dados Anonimizados ..... 73
**5 LEI, SOCIEDADE, MERCADO E INTERNET DAS COISAS** ..... **78**
5.1 O contexto legal: políticas para IoT, lacunas regulatórias e o papel dos contratos ..... 80
5.1.1 Internet das Coisas: um plano de ação para o Brasil ..... 81
5.1.2 IoT e Mercado ..... 88
5.1.3 Entraves à implementação da Política Nacional de IoT ..... 91
**6 UM MUNDO DE HUMANOS E MÁQUINAS** ..... **95**
**EPÍLOGO** ..... **105**
**BIBLIOGRAFIA** ..... **109**

## LISTA DE FIGURAS

Figura 1 - Reprodução da capa da revista "The Atlantic" de Julho de 1945. ..... 18
Figura 2 Relação proposta pela IoT ..... 27
Figura 3 Exemplo de IoT aplicada ao varejo ..... 30
Figura 4 Placa de um microcomputador tipo Arduino. ..... 31
Figura 5 Estrutura de Tráfego e Coleta de Dados na perspectiva da IoT ..... 33
Figura 6 Arquitetura de Referência de IoT ..... 38
Figura 7 Pilares de Inovação ..... 45
Figura 8 Strategic Research Agenda ..... 48
Figura 9 O funcionamento da Internet of Nano Things (IoNT) ..... 52
Figura 10 Ciclo de Vida de Desenvolvimento de Software simplificado ..... 56
Figura 11 Resultados direito a portabilidade GDPR Art. 20 (1) ..... 72
Figura 12 Resultados direito a portabilidade GDPR Art. 20 (2) ..... 73
Figura 13 Ecossistema dos dados ..... 75
Figura 14 Relatório do Plano de Ação ..... 83
Figura 15 Documentos do Plano de Ação 2 ..... 84

# LISTA DE SIGLAS

| | |
|---|---|
| 3GPP | *Third Generation Partnership Project* |
| AAA | *Authentication, Autthorization and Accounting* |
| ABINC | Associação Brasileira de Internet das Coisas |
| AGI | *Artificial General Intelligence* |
| AI | *Artificial Intelligence* |
| AMPS | *Advanced Mobile Phone System* |
| ANPD | Autoridade Nacional de Proteção de Dados |
| BCI | *Brain-Computer Interface* |
| BLE | *Bluetooth Low Energy* |
| BMI | *Brain-Machine Interface* |
| BNDES | Banco Nacional de Desenvolvimento Econômico e Social |
| BNDS | Banco Nacional Do Desenvolvimento |
| CASAGRAS | *Coordination and Support Action for Global RFID-Related Activies and Standardisation* |
| CERN | *Conseil Européen pour la Recherche Nucléaire* |
| CNIL | *Comission Nationale Informatique & Libertés* |
| CRM | *Customer Relationship Management* |
| CSA | *Cloud Security Alliance* |
| DAC | *Discretionary Access Control* |
| DDoS | *Distributed Denial of Service* |
| DRP | *Disaster Recovery Plan* |
| EDGE | *Enhanced Data rates for GSM Evolution* |
| ERP | *Enterprise Resource Planning* |
| ETSI | *European Telecommunications Standards Institute* |
| FDMA | *Frequency Division Multiple Access* |
| FISTEL | Fundo de Fiscalização das Telecomunicações |
| FTC | *Federal Trade Commision (USA)* |
| GDPR | *General Data Protection Regulation* |
| GPRS | *General Packet Radio Service* |
| GSM | *Global System for Mobile Communication* |
| HSPA | *High Speed Packet Access* |
| HTML | *HyperText Markup language* |
| HTTP | *HyperText Transport Protocol* |
| IDS | *Intrusion Detection Systems* |
| IEEE | *Institute of Electrical and Electronics Engineers*) |
| IERC | *European Research Cluster on the Internet of Things* |
| IETF | *Internet Engineering Task Force* |
| IIoT | *Industrial Internet of Things* |

| | |
|---|---|
| IoT | *Internet of Things* |
| IP | *Interner Protocol (Version 4)* |
| IPS | *Intrusion Prevention System* |
| IPv6 | *Internet Protocol Version 6* |
| ISO | *Internacional Organization for Standartization* |
| ITU | *International Telecommunications Union* |
| ITU-T | *ITU Telecommunication Standardization Sector* |
| LGPD | Lei Geral de Proteção de Dados |
| LTE | *Long-Term Evolution* |
| MCTI | Ministério da Ciência, Tecnologia e Inovação |
| NIST | *National Institute of Standards and Technology (USA)* |
| OASIS | *Organization for the Advancement of Structured Information Standards* |
| OTA | *Over The Air* |
| PIA | *Privacy Impact Assessment* |
| PMO | *Project Management Office* |
| PNIoT | Plano Nacional de IoT |
| SAE | *System Architecture* |
| SDLC | *Software Development Life Cycle* |
| SIEM | *Security Information And Event Management* |
| TCU | Tribunal de Contas da União |
| TDMA | *Time Division Multiple Access* |
| UMTS | *Universal Mobile Telecommunications System* |
| WWW | *World Wide Web* |

**RESUMO**

De natureza fundamentalmente multidisciplinar, esta tese envolve o estudo da Internet das Coisas (IoT) sob a perspectiva da segurança da informação e da proteção de dados pessoais. O trabalho analisa o desenvolvimento tecnológico com ênfase nos dispositivos interconectados por Internet das Coisas e todas as suas implicações sob o ponto de vista da coleta, guarda e tratamento de dados considerando, em particular, a importância do desenvolvimento seguro destes dispositivos com vistas a salvaguardar direitos e garantias fundamentais dos usuários. O recorte específico aqui apresentado propõe ainda uma profunda reflexão sobre o papel que as máquinas desempenham na sociedade contemporânea e como estas impactam institutos jurídicos seculares numa clara demonstração de que a outros vieses nortearão o direito num futuro cada vez mais próximo.

**ABSTRACT**

*Fundamentally multidisciplinary, this thesis involves the study of the Internet of Things (IoT) from the perspective of information security and personal data protection. The study analyzes the technological development with an emphasis on devices interconnected by IoT and all its implications from the point of view of data collection, storage, and processing. All this, considering the importance of the safe development of these devices to safeguard users' fundamental rights and guarantees. The specific outline of this research also proposes a deep reflection on the role that machines play in contemporary society and how they impact secular legal institutes in a clear demonstration that other biases will guide the law in an increasingly near future.*

# 1 INTRODUÇÃO

## 1.1 A tese aqui defendida

> Alguns dos meus amigos chegaram mesmo a afirmar que uma tese de doutoramento deveria ser o maior trabalho científico que um homem já fez ou jamais faria talvez, e que deveria esperar até que ele estivesse plenamente capacitado a expor o trabalho de sua vida. Não partilho essa opinião. Digo, apenas, que se a tese não é, de fato, uma tarefa tão capital, deve pelo menos ser, em intenção, o portão de acesso para um vigoroso trabalho criativo. Só Deus sabe quantos problemas existem a serem resolvidos, quantos livros a serem escritos, quanta música a ser composta! No entanto, com pouquíssimas exceções, para se chegar a tanto, é mister realizar tarefas maquinais que em nove entre dez casos, não se tem nenhuma razão imperiosa para realizar. Que o Céu nos livre dos primeiros romances que são escritos porque um jovem aspira ao prestígio de ser romancista e não porque tenha algo a dizer! Que o Céu nos livre, igualmente, dos ensaios matemáticos que sejam corretos e elegantes, mas destituídos de corpo e espírito. Que o Céu nos livre, sobretudo, do esnobismo que não somente admite a possibilidade desse trabalho apoucado e maquinal, mas deblatera, com espírito de arrogância depreciadora, contra a competição de vigor de ideias, onde quer que se possam encontrar." – Norbet Wiener. Cibernética e Sociedade.

A escolha pelo tema deste trabalho, indubitavelmente, merece registro. Não pela sua natureza pessoal, tampouco por quaisquer histórias *sui generis* que poderiam ter norteado a presente escolha, mas pelo viés inarredável da nova perspectiva da ciência jurídica.

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.

Mais do que a natureza multidisciplinar da atividade jurídica hodiernamente, a escolha do tema deste trabalho está intimamente relacionada ao que a engenharia e a ciência da computação pensaram, desenvolveram e implementaram para o futuro: a mudança de paradigma do usuário, uma vez que as máquinas podem relacionar-se sozinhas e, assim terem um protagonismo antes dedicado somente ao humano.

As frequentes e acentuadas mudanças pelas quais a sociedade tem passado, nos últimos cinquenta anos, fez com que a ciência jurídica paulatinamente também refinasse inúmeros

institutos, tais como, os contratos, os títulos de crédito e, até mesmo, a validade da assinatura hológrafa, que hoje, por meio de certificação digital, não precisa, necessariamente, ter como suporte o papel, podendo ser eletrônica.

É fato, também, que Direito e tecnologia caminham paralelamente, mas em velocidades muito distintas. Enquanto o primeiro necessita da materialização dos conflitos oriundos do uso deste ou daquele dispositivo ou sistema, os cientistas da computação e os engenheiros avançam a passos largos em busca de praticidade, rapidez e eficiência de todos os processos que permeiam a rotina das pessoas.

A Internet[1] que, embora tenha surgido com um viés político e, posteriormente, acadêmico, acabou por transportar-se para o uso civil, comercial, bancário, entre outros e à medida que avançou criou desafios, paradigmas e desejos.

A Internet das Coisas, tema central que norteia este trabalho, apesar de ter sido apresentada à comunidade acadêmica em 1999 por Kevin Ashton, está cada vez mais próxima do uso diário. É este o fenômeno sobre o qual o Direito precisará debruçar-se nos próximos anos, uma vez que a própria ordenação[2] jurídica existente hoje, cujo protagonista é um humano, necessitará revisitar suas bases, pela simples e boa razão de que a essência deste novo paradigma se concentra nas relações máquina a máquina.

---

[1] A palavra *Internet* será utilizada com a inicial maiúscula, a despeito das ponderáveis razões de nosso professor orientador, que apresentou suas razões para o uso do "i" minúsculo, da seguinte forma: "*Já tive a oportunidade de explicar o porquê de a minha utilização da palavra internet ser feita com a inicial minúscula e não em maiúscula, não obstante as respeitáveis razões apresentadas pelo professor Marcel Leonardi, em sua obra Tutela e Privacidade na Internet (São Paulo: Saraiva, 2002), que tive a honra e a satisfação de prefaciar, na qual o eminente professor apresenta ponderáveis argumentos para o emprego da palavra Internet, com a inicial maiúscula. Tenho me utilizado dela com "i" minúsculo — primeiramente em Aspectos jurídicos da contratação informática e telemática[1] e, posteriormente, no artigo inaugural da obra coletiva Direito & Internet – Aspectos Jurídicos Revelantes — fundado nas razões tão bem expostas pelo professor Le Tourneau, citado por Christiane Féral-Schuhl, na obra Cyber Droit – le droit à l'épreuve de l'internet, in verbis: " 'Faut-il rappeler, avant de commencer, que le mot 'internet' n'est pas une marque, mais un nom générique qui, comme tel, doit recevoir un article (l'internet) et point de majuscule, exactement comme le téléphone, le minitel, la radio, le telex ou la télévision'."* DE LUCCA, Newton, "Marco Civil da Internet – Uma Visão Panorâmica dos Principais Aspectos Relativos às suas Disposições Preliminares", in DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, C.R.P. de (Coords.). *Direito & Internet III*: Marco Civil da Internet (Lei 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, p. 26, nota de rodapé 11.

[2] Não obstante o uso correntio da expressão *ordenamento jurídico*, por parte da quase totalidade da doutrina brasileira − desavisada de que se trata de um evidente italianismo – preferimos o emprego de ordenação jurídica, seguindo, neste passo, a explicação de nosso professor orientador, que assim se pronunciou a respeito do vocábulo: "*Contra a quase unanimidade da doutrina nacional, venho me utilizando, invariavelmente, da palavra ordenação jurídica, de todo preferível, a meu ver, à palavra ordenamento jurídico. Com efeito, ela parece mais consentânea com o idioma português, não havendo razão para o emprego do italianismo, conforme já destacado pela autorizada voz do gramático Napoleão Mendes de Almeida. Afinal de contas, nós tivemos as ordenações afonsinas, manuelinas e filipinas e não ordenamentos afonsinos, manuelinos e filipinos...*", in DE LUCCA, Newton. *Da Ética Geral à Ética Empresarial* – São Paulo: Quartier Latin, 2009, p. 234, nota 1.

A partir destas considerações, funda-se o argumento preponderante deste trabalho, qual seja, a análise do novo contexto social no qual a Internet das Coisas está sendo cada vez mais inserida e, por conseguinte, alterando diversos protocolos de coleta de dados pessoais que incrementam as grandes bases de dados utilizadas para o desenvolvimento de máquinas que executem tarefas similares às humanas.

Impõe relevo a esta pesquisa o incontestável aumento da utilização de computadores e seus reflexos na vida em sociedade, sobretudo de softwares que utilizam inteligência artificial, conceito utilizado nesta justificativa nos termos formulados por John McCarthy em 1956 na primeira conferência sobre o assunto idealizada por ele e Marvin Minsky: *Darmouth Summer Research Project on Artificial Intelligence*[3]. Desde coisas prosaicas, rotineiras, até para tarefas muito elaboradas, sistemas computacionais são utilizados ao ponto de, muitas vezes, executarem tarefas humanas autonomamente. É esta uma realidade inexorável. Não haverá um mundo sem computadores, pelo contrário, eles estarão cada vez mais presentes e mais autônomos, tal como profetizou Pierre Teilhard de Chardin[4]: A evolução e o cristianismo, longe de estarem em conflito uns com os outros, são de fato parte do mesmo processo: a evolução de uma força espiritual benigna através de formas cada vez mais complexas de vida material na Terra.

Esta premissa envolve o conceito de noosfera em que seres humanos elevados a um novo plano evolutivo caracterizado pela coordenação global de energias intelectuais, sociais e espirituais que substituiria os reinos evolucionários prévios da geosfera e da biosfera.

Foram estas as ideias que orientaram John Arquilla e David Ronfeldt da Rand Corporation[5], nos anos 2000, a desenharem a espinha dorsal da estratégia de política de tecnologia e segurança da informação americana – a "*Noopolitik*"[6] – que representa um salto evolutivo no estado de poder, tornado possível pela revolução da informação.

---

[3] SILVA, N. C. Inteligência Artificial. In: Inteligência Artificial e Direito: ética, regulação e responsabilidade. São Paulo, SP: Thomson Reuters Brasil, 2019. p. 35.

[4] TEILHARD DE CHARDIN. *In*: WIKIPÉDIA: a enciclopédia livre. [São Francisco, CA: Fundação Wikimedia]. Disponível em https://pt.wikipedia.org/wiki/Teilhard_de_Chardin. Acesso em: 30 abril 2020.

[5] A RAND Corporation é uma instituição americana sem fins lucrativos que ajuda a melhorar as políticas e a tomada de decisões de governo por meio de pesquisas e análises. É formada grupo de especialistas de natureza investigativa e reflexiva cuja função é a reflexão intelectual sobre assuntos de política social, estratégia política, economia, assuntos militares, de tecnologia ou de cultura. Disponível em: https://www.rand.org. Acesso em: 13/01/2022.

[6] ARQUILA, John.; RONFELDT, David. (org.). *The Emergence of Noopolitk – Toward an American Information Strategy*. Disponível em: https://www.rand.org/pubs/monograph_reports/MR1033.html. Acesso em: 13/01/2022

No pensamento de Arquila e Ronfeldt A revolução da informação mudará não apenas o modo como as pessoas se comportam graças aos novos dispositivos tecnológicos, mas, mais essencialmente, a forma como as pessoas entendem e se organizam - social, cultural, política, econômica, governamental, militar e até mesmo espiritual.

Da mesma forma, a revolução da informação transformará a maneira como as nações se comportam e compreendem seus papéis no mundo.

Segundo a *Noopolitik,* as principais áreas em que o governo norte-americano deveria investir e concentrar-se, eram as seguintes:

- Fotônica;
- Conectividade universal;
- Computação ubíqua;
- Sensores pervasivos;
- Utilitários de informação global.

E estas diretrizes foram tão assertivas que, de fato, o mundo e não só os Estados Unidos, estão vivenciando cada uma dessas indicações, o que nos leva ao ponto fulcral deste trabalho: a utilização de sensores pervasivos na coleta de dados não estruturados, ou seja, que não guardam nenhuma relação entre si e nem uma estrutura definida.

Segundo Bruno Fábio de Farias (2016) [7]: "A computação pervasiva é um paradigma em que o computador se torna onipresente e invisível para o usuário, com capacidade de obter informações acerca do ambiente ao redor e utilizá-las para controlar, configurar e ajustar aplicações dinamicamente. Os sistemas pervasivos se caracterizam pelo uso de sensores disponíveis no ambiente, cujos dados são processados para prover serviços personalizados para os usuários". Atualmente, o principal gerador de dados de sensores é o dispositivo portátil pessoal, como *smartphone* e *tablet*, pois são dispositivos que possuem diversos sensores embutidos.

O conceito acima compõe o universo da Internet das Coisas ou *Internet of Things*, em inglês, cuja sigla é IoT[8] e quem vem cada vez mais mudando a vida das pessoas no mundo

[7] PAIVA, Bruno Fábio de Farias. Uma abordagem baseada em componentes para o desenvolvimento de aplicações pervasivas cientes de contexto de ambiente: foco em sensores**.** 2016. 109 f. Dissertação (Mestrado em Ciência da Computação) – Programa de Pós-Graduação em Ciência da Computação, Centro de Engenharia Elétrica e Informática, Universidade Federal de Campina Grande, Paraíba, Brasil, 2016.

[8] Neste trabalho convencionaremos a utilizar "IoT" como a sigla para Internet das Coisas, visto que ela é a padronização mais adotada, ainda que em textos e publicações de língua portuguesa. Assim "Internet das Coisas" e "IoT" serão usados de forma equivalente.

inteiro, tanto do ponto de vista de seus hábitos e costumes, como também do ponto de vista da quantidade de dados coletados por meio de cada dispositivo interligado à Internet.

Esse volume de dados alimenta o que conhecemos como *big datas*, grandes bancos de dados que são absorvidos para desenvolver as inteligências artificiais de modo a espelharem comportamentos e habilidades humanas, executarem tarefas e, até mesmo, tomarem decisões, o que tem suscitado por meio da comunidade acadêmica, grandes discussões sobre ética, regulação e a ciência do Direito diante de tão profunda inovação.

O estudo multidisciplinar entre direito e tecnologia é o objeto sobre o qual esta pesquisadora tem se debruçado nos últimos doze anos. As frequentes e irrefreáveis mudanças pelas quais a sociedade tem passado, inclusive nos processos que envolvem os poderes da República, a forma como as pessoas se comunicam, se relacionam e, até se desentendem, tem motivado não só a mim, como muitos outros estudiosos a desbravar as diversas possibilidades de adaptação dos velhos e arraigados institutos que herdamos do direito romano, bem como a modernização dos diplomas legislativos em vigor, mas passíveis de uma enormidade de melhorias.

Diante deste cenário inovador, pulsante e curioso repousa o interesse pela escolha do tema acima esmiuçado. Salienta-se, por óbvio, a natureza limitada desta pesquisa com vistas a responder algumas das muitas interrogações que povoam o imaginário dos operadores do direito, sobretudo aqueles que em sua rotina diária se deparam com as muitas dificuldades para encontrar soluções para problemas não contemplados na legislação vigente ou na jurisprudência pátria.

Neste ponto, cabe salientar a importância que teve a banca de qualificação desta tese, que contou com a participação dos Professores Roberto Augusto Castellanos Pfeiffer e Leonardo Parentoni Neto que contribuíram fundamentalmente para a especificação do objeto deste trabalho, apontando que os aspectos que englobavam o título do trabalho então proposto eram demasiadamente abrangentes para o tempo de que dispunha esta pesquisadora. Os ajustes e contornos que foram feitos a partir de tais considerações, por certo, tornaram este trabalho muito mais objetivo, pedagógico e relevante para a comunidade científica.

De outra banda, o afunilamento do escopo desta pesquisa, aproximou ainda mais a vida acadêmica da vida profissional desta autora, exatamente porque o trabalho como executiva numa empresa de segurança da informação e como advogada acompanhando par e passo o quanto as questões de proteção de dados estão relacionadas aos requisitos de segurança da

informação a que uma empresa precisa observar, tornou este trabalho um exercício não só teórico, mas também prático no que diz respeito às análises nele contidas.

A análise sobre o cenário multifacetado em que milhões de dados, em particular, dados pessoais, são coletados por dispositivos embarcados em sistemas utilizados para as mais diferentes tarefas cotidianas sem que os titulares dos dados, objeto da coleta, sejam sequer cientificados, expõe a fragilidade dos institutos jurídicos que protegem os direitos e garantias dos cidadãos e revela a ineficiência de leis, como a Lei Geral de Proteção de Dados – Lei 13.709/2018 que a despeito de objetivar a segurança jurídica necessária aos titulares dos dados nas mais diversas situações de coleta, guarda e tratamento, desconsidera o atual estágio de desenvolvimento tecnológico e a realidade ubíqua a que todas as pessoas estão expostas, sobretudo a partir da utilização de dispositivos que não foram desenvolvidos sob o conceito de privacidade e segurança das informações coletadas.

Para este estudo, entretanto, concentraremos esforços no que tange aos aspectos ligados à segurança da informação e à privacidade dos titulares dos dados coletados pelos dispositivos interconectados à Internet e não necessariamente controlados por um humano, não só do ponto de vista das possibilidades que existem no mercado, tais como os assistentes pessoais, entre outros que resolvem problemas a partir de comandos de voz ou mesmo de determinadas configurações devidamente ajustadas, mas, especialmente, aqueles que estão sendo desenvolvidos para tomarem decisões de forma autônoma, independentemente de um comando ou interferência do usuário ou desenvolvedor.

A partir das questões acima descritas e para fins metodológicos, o presente trabalho foi estruturado de forma a apresentar o conceito de Internet das Coisas, seus principais aspectos do ponto de vista técnico, especialmente no que diz respeito aos protocolos de segurança e privacidade, seu alcance em relação a um número cada vez maior de usuários e, por conseguinte, de dados coletados e como o tema vem sendo tratado enquanto agenda de desenvolvimento tecnológico em programas de pesquisa da União Europeia.

Adicionalmente, corrobora para esta análise o estudo da perspectiva do usuário, bem como o âmbito ético dos desenvolvimentos relacionados à Internet das Coisas e seus desdobramentos sociais com vistas a transformar hábitos, costumes e até mesmo as legislações.

A importância da interoperabilidade como mola propulsora para a coleta maciça de dados também é tema central deste estudo, uma vez que a partir dela é que se desenvolve o fenômeno do aumento exponencial de dados diuturnamente coletados.

A análise do contexto tecnológico suporta e subsidia o exercício ao qual nos propusemos inicialmente, qual seja, observar, apontar e sugerir em que medida tanto o mercado, quanto a sociedade podem se apropriar desta nova onda da computação, a computação ubíqua, nos exatos termos descritos por Mark Weiser[9].

Verá o leitor, assim como observou esta estudante ao longo da jornada cujo resultado é a tese que ora se apresenta que, a despeito do que o senso comum apregoa, nem só de benefícios usufrui a sociedade com o desenvolvimento tecnológico, há muitas outras questões que carecem de atenção e, talvez, o campo do saber que melhor auxilia nesta tarefa seja a filosofia corroborando nossa primeira menção neste apontamento introdutório de que o recorte factual sempre observado pelo operador do direito há de ser multidisciplinar, pois a ciência jurídica por ela mesma não dará conta de explicar, tampouco solucionar a complexidade das relações humanas atuais.

## 1.2 Histórico e desenvolvimento da Internet: considerações que fundamentam a relevância do tema

No final dos anos 60, do século XX, quando as bases da Internet foram lançadas, não haveria como imaginar a magnitude que ela alcançaria não só como mecanismo de comunicação, mas também como indispensável meio de negócios, lazer, aprendizagem e relacionamento. Criada como uma rede de computadores capaz de sobreviver a um ataque nuclear, pensada e desenvolvida para garantir conectividade e resiliência, passadas pouco mais de três décadas, a Internet revolucionou a maneira como pensamos, agimos, negociamos, nos relacionamos e nos divertimos.

Entretanto, em seus primórdios, a Internet era muito difícil de ser utilizada por pessoas que não fossem do meio científico ou que não fizessem parte de uma elite da subcultura de computadores e *hacking*, geralmente formada em torno de entusiastas libertários ou *hobistas* ligados às ciências exatas e à computação. O grande salto que arrancou a Internet dos grotões

[9] A computação ubíqua é a terceira onda da computação que está apenas começando. Primeiro tivemos os mainframes compartilhados por várias pessoas. Estamos na era da computação pessoal com pessoas e máquinas estranhando umas às outras. A seguir vem a computação ubíqua, a era da tecnologia 'calma', quando a tecnologia recua para o pano d efundo de nossas vidas. As tecnologias mais importantes são aquelas que desaparecem. Elas se integram à vida do dia a dia, ao nosso cotidiano, até serem indistinguíveis dele. In: WEISER, Mark. *The Computer for the 21 st Century*. Scientific American, v. 265, n. 3, p. 94-105, 1991.

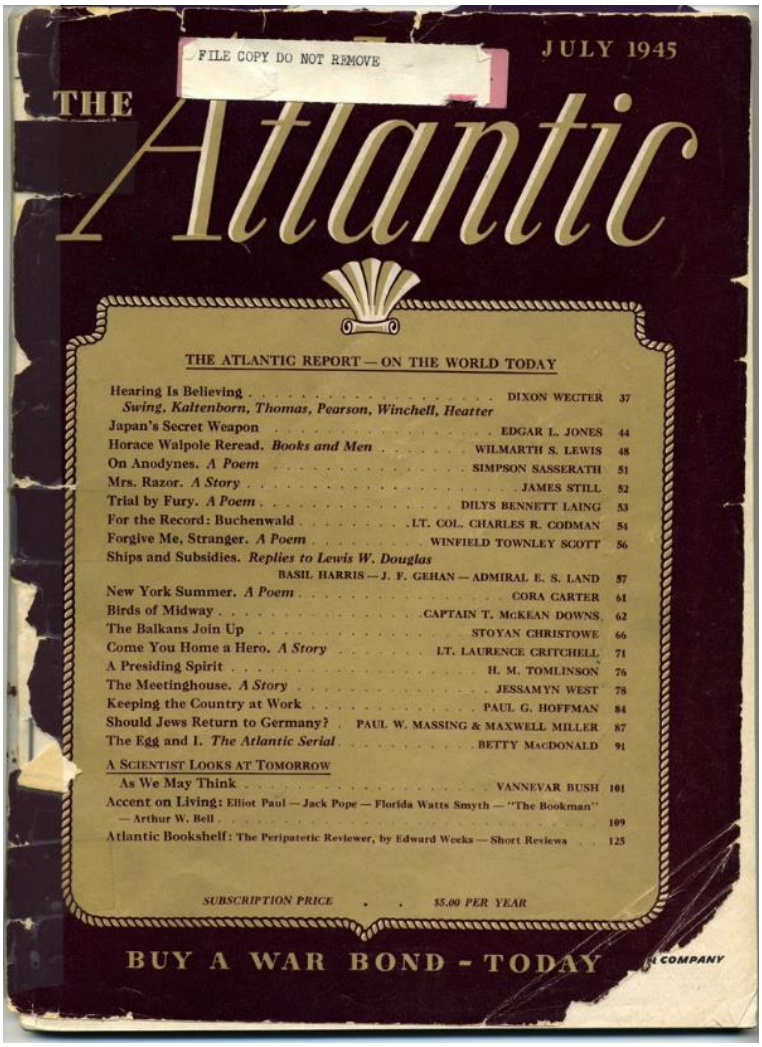
dos meios científicos e a trouxe ao mercado do mundo real deve-se à criação da *World Wide Web*.

Em março de 1989 o pesquisador Tim Berners-Lee do CERN (*Conseil Européen pour la Recherche Nucléaire*) propôs um método de hiperlinks para organizar e permitir o acesso de pesquisadores em física de altas energias a sistemas de bancos de dados usando a Internet. A ideia de hiperlink baseia-se numa proposta originalmente escrita em 1945 (Figura 1) pelo pesquisador Vannevar Bush para um trabalho de análises estratégicas desenvolvido, à época, para a já mencionada RAND Corporation. Bush escreve:

> Considere um futuro dispositivo… no qual um indivíduo armazena todos os seus livros, registros e comunicações, e que é mecanizado para que possa ser consultado com extrema rapidez e flexibilidade. É um suplemento íntimo ampliado para sua memória.[10]

[10] Tradução nossa do original em inglês "*Consider a future device … in which an individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility. It is an enlarged intimate supplement to his memory*". In: BUSH, Vannevar. *As We May Think*. The Atlantic. Issue July, 1945.)

*Figura 1 - Reprodução da capa da revista "The Atlantic" de Julho de 1945, onde Vannevar Bush publica seu artigo "As We Think", que criaria as bases do hipertexto, usado na Internet a partir de 1995.*




Fonte: *The Atlantic Magazine*, Julho de1945.[11]

Mais tarde, esta ideia acabaria revolucionando toda a humanidade. Com base em seus conceitos iniciais, cerca de um ano depois de apresentada a proposta, no final de 1990 Tim Berners-Lee, com o suporte de Robert Cailliau, havia produzido o conjunto de sistemas que permitiria o funcionamento da Internet de forma muito semelhante ao que conhecemos hoje. Foram desenvolvidos o Protocolo de Transferência de Hipertexto (HTTP – *HyperText Transport Protocol*), a Linguagem de Marcação de Hipertextos (HTML – *HyperText Markup language*), o primeiro navegador ou Browser, e o primeiro servidor de HTTP. Este conjunto de protocolos, linguagens, navegadores e servidores formou aqui que se convencionou a chamar

[11] Reprodução disponível em https://www.theatlantic.com/magazine/toc/1945/07/ (Acesso em 16/01/2022)

de *World Wide Web*, a *"*WWW*"* ou, simplesmente, *"Web".* A criação da Web é o tipo de ideia certa feita pelos motivos errados: permitir que algumas dezenas de físicos nucleares tivessem acesso fácil a dados de pesquisas. Isso acabaria por revolucionar a informação no século 20.

Logo depois, o segundo grande impulso que a Internet recebeu, e que complementaria a Web, foi a criação do software *Mosaic* em 1993. Até então, a Web de Berners-Lee era acessada somente em modo de textos, não muito diferente de se folhear um livro sem ilustrações e sem grandes atrativos para o grande público, com poucas funcionalidades. O *Mosaic* foi o primeiro navegador gráfico multiplataformas, criado por Marc Andreessen e Eric Bina, para ser usado no site da Universidade de Ilinois. Com o Mosaic, a Web ganhou a aparência de multimídia que possui hoje, permitindo a inserção não só de imagens, mas também de vídeos, áudio, jogos, softwares e toda uma ampla gama de aplicativos de interação.

Desde então, a Web não parou mais de evoluir, agregando novas funcionalidades, novas invenções, novos meios, mas também novos desafios e novos problemas. Um dos maiores problemas que afetam a Web desde seus primórdios é a questão de segurança das informações. Uma vez que tanto a Internet, como a Web, não foram criadas especificamente para negócios, em sua concepção original, elas não deveriam ser usadas para este fim.

Existe uma razão bem clara para que isso tenha ocorrido. No momento histórico em que a Internet e a Web floresciam havia grande preocupação em compartilhar as informações e em permitir o acesso à rede da forma mais universalizada possível, principalmente nos EUA.

Diferentemente do Brasil, na cultura americana existe um forte conceito de confiança mútua e comprometimento, em que as pessoas, por princípio, confiam umas nas outras de boa fé. Esta filosofia comportamental foi levada para o desenvolvimento tecnológico da rede, executado principalmente, como mencionado acima, por americanos. Isso fez com que as questões relativas à segurança das informações, à confidencialidade e à privacidade fossem deixadas de lado durante o desenvolvimento da maioria dos protocolos e aplicações que formam a Internet. Por exemplo, preocupava-se em enviar o e-mail rapidamente e sem falhas, de forma precisa, mas não havia preocupação em certificar-se que ele realmente partira de quem dizia partir, ou que ele tivesse algum tipo de confidencialidade. Assim, os servidores de e-mail confiavam uns nos outros sem preocupação com aspectos de segurança. Reflexos destas decisões tecnológicas do passado ressoam até hoje, visto ser bem sabido que muitas aplicações de massa na Internet, tais como *Facebook, Instagram* ou *Twitter*, ainda carregam arraigados problemas de segurança, privacidade e confiabilidade, que parecem não ter fim.

Atualmente, ressoa com muita evidência a preocupação com os aspectos de segurança, não só do ponto de vista dos sistemas computacionais, mas também dos processos. É fundamental que um analista possa responder o quão seguro um sistema é ou deveria ser e, consequentemente, o que pode ser feito para a melhoria da segurança, nos casos em que há a necessidade de alterações e atualizações.

Os analistas procuram respostas a estes questionamentos e a outros que forneçam medidas de quão eficientes são os esforços em segurança, de modo a reduzir os riscos ao qual um processo ou uma contratação está exposta, ou qual a redução nos riscos que deve ser esperada com a adição de novos mecanismos e controles sejam eles de segurança ou de elementos jurídicos, o que, normalmente, significa estimar valores passados e projetar valores futuros de cada uma das métricas dos processos ou contratos, tais como frequência de incidentes ou custos anuais destes incidentes. Para tomar decisões de segurança é necessário utilizar estas métricas para decidir quais escolhas devem ser realizadas, a fim de que estas influenciem efetivamente nas estratégias de segurança e na redução dos riscos.

Este breve recorte histórico-cultural nos dá a dimensão do quanto a Internet passou a influenciar a sociedade em seus mais diferentes níveis e segmentos. Desde o entretenimento, passando por negócios e transações bancárias, praticamente tudo hoje, transita pela Internet.

## 1.3 Internet e Direito no contexto brasileiro: apontamentos históricos

A influência na rotina e na vida das pessoas foi tão drasticamente alterada com o desenvolvimento e a utilização da Internet, sobretudo a partir dos anos dois mil, que o judiciário de diversos países foi chamado a resolver inúmeras demandas, inclusive diversas de natureza internacional, uma vez que a Internet possui a habilidade precípua de eliminar fronteiras, aproximar pessoas e transcender limitações geográficas também no que diz respeito aos problemas nos quais seus usuários podem se envolver. Feita esta ressalva, importa salientar que este trabalho enfoca a intersecção da Internet com o direito brasileiro.

Por aqui, a primeira decisão de que se tem notícia envolvendo a tecnologia é datada de 1998, no Habeas Corpus nº 76.689-0 da Paraíba em que se discute a publicação de cenas de sexo infanto-juvenil em rede BBS/ Internet de computadores, de acordo com a linguagem usada no próprio texto sob a relatoria do ministro Sepúlveda Pertence do Supremo Tribunal Federal. Sobre o Tema:

> EMENTA: "Crime de Computador: publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" -- ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial. (HC 76.689-0/PB, Relator: Min. Sepúlveda Pertence, publicado no Diário de Justiça número 213, Brasília, DF, do dia 06 nov 1998).

De lá para cá, as discussões e demandas avançaram muito. Em 2014, durante o evento conhecido como Net Mundial – encontro global multissetorial sobre o futuro da governança da Internet, a então presidente Dilma Rousseff sancionou a Lei 12.965 que ficou conhecida como Marco Civil da Internet. Cronologicamente, podemos destacar que a primeira iniciativa legislativa sobre o assunto partiu do, na época deputado, Eduardo Azeredo com o PL 24/1999.

Em 2012, entrou em vigor a Lei 12.737, mais conhecida como "Lei Carolina Dieckmann" que acrescentou o art. 154-a ao Código Penal para tratar da invasão de dispositivos informáticos.

Todas estas iniciativas legislativas e todo o tratamento realizado pelo judiciário brasileiro tem sido muito eficaz ao atendimento das diversas demandas originadas, sobretudo, no ambiente corporativo. Até porque, boa parte da conduta dos cidadãos na Internet é regulamentada por outras leis em vigor, tais como o Código de Defesa do Consumidor que, após o Decreto 7962/2013 passou a solucionar e a direcionar com mais efetividade o perfil dos consumidores que utilizam a Internet. Atualmente, a discussão mais relevante para os operadores do Direito que trabalham com questões que envolvem tecnologia recai sobre o tema da Privacidade. Dois projetos de lei tramitaram por alguns anos no congresso Nacional sobre o

tema, um deles, inclusive por iniciativa do Ministério da Justiça desde 2009. A saber: PL 4060/2012 e PL 5276/2016.

Finalmente, depois de longas discussões, debates e consultas públicas a Lei 13.709 foi sancionada pelo, então presidente, Michel Temer em 14 de agosto de 2018. Assim criou-se um forte movimento no mercado para que as empresas, sobretudo aquelas cujo principal ativo são dados, entrassem em conformidade com a nova legislação aplicável à matéria.

Para o escopo deste trabalho, porém, a atual legislação brasileira de proteção de dados e as outras legislações, tais como: a *General Data Protection Regulation e o California Consumer Privacy Act of 2018 (CCPA)*, respectivamente, legislações europeia e americana não suprirão a lacuna que será aberta a partir da popularização da Internet das Coisas. Isto porque, todas estas legislações e todo o tratamento dispensado aos processos judiciais envolvem apenas e tão somente, a pessoa natural, de acordo com o que dispõe o Código Civil, no Capítulo I do Livro de mesmo número.

O avanço a passos largos da Internet das Coisas pressupõe um novo arranjo jurídico-tecnológico, corporativo e procedimental no que respeita a coleta, guarda e tratamento de dados pessoais e para melhor ilustrar tais argumentos, segue um recorte teórico devidamente contextualizado com o escopo deste trabalho.

# 2 A INTERNET DAS COISAS: MATIZES CONCEITUAIS E VIESES DESENVOLVIMENTISTAS

Sim, é fato, o homem nunca descansa! Às vezes por necessidade, outras por ambição, mas movimentar-se em direção às conquistas faz parte da natureza humana. Foi assim, ao longo de toda história, porém tornou-se mais evidente no século XX com o surgimento da Internet e o aperfeiçoamento de sua arquitetura, seus protocolos e sua utilização.

De forma condensada, porém eficiente, podemos descrever o desenvolvimento da Internet em três grandes marcos:

- O primeiro: o seu nascimento oficial em 20 de outubro de 1969 na sala 3420 do Edifício Boelter Hall na UCLA – Universidade da Califórnia, Los Angeles - às 22:30h, sala do Prof. Leonard Kleinrock;
- O Segundo: a adoção do protocolo TCP/IP, em 1983, constante de duas camadas: a primeira, TCP - *Transmission Control Protocol* e a segunda IP - *Internet Protocol*, conceitos desenvolvidos por Bob Kahn e Vint Cerf. A criação e adoção destes protocolos formaram a base para permitir que a Internet suporte diversos aplicativos, tal como o faz hoje;
- O terceiro, e mais popular, desdobramento da Internet ocorreu nos anos 1990, conforme já mencionado, com a criação da *Word Wide Web*, que possibilitou a aproximação de todos os segmentos da sociedade à Internet tornando a rede mais agradável para navegação e mais abrangente em termos de conteúdo.

É óbvio que o desenvolvimento da Internet não se limita aos marcos acima transcritos e tampouco se restringem a tais eventos, posto que a partir dos anos noventa do século passado é que, de fato, a Internet impulsionou a economia e, sobretudo no Brasil, se desenvolveu e ganhou escala comercial.

O que importa efetivamente para este trabalho é o entendimento de que o objeto sobre o qual nos debruçaremos é uma evolução da Internet dentro da perspectiva de conexão não só entre máquinas, mas entre objetos e humanos, ou seja, entre tudo e todos, como preconizado

por KHAN[12]. Entendemos não se tratar de nenhum exagero dizer que estamos diante de uma mudança de paradigma e que essa mudança tem afetado profundamente a forma como vivem, pensam e interagem os seres humanos, da mesma forma que ocorreu quando do advento da Internet.

A ideia precípua ao conceito de IoT é a de que possamos controlar objetos remotamente e de podermos acessá-los como provedores de serviços, desde que com capacidade computacional e de comunicação para se conectarem à Internet. Por essa razão, o tema tem sido pesquisado e debatido não só na academia, mas também pelo setor produtivo e o poder público em busca de soluções viáveis para políticas de estado que melhor atendam aos cidadãos.

## 2.1 A Internet das Coisas

### 2.1.1 O significado de coisas e o conceito formal de IoT

O conceito de coisas remonta à caracterização proposta por Aristóteles (384 a. C. – 322 a.C), em sua obra As Categorias[13], como seres que apresentam substância (essência, qualidade, quantidade e relações).

Philophonus (490 d.C – 570 d.C), por sua vez, divide as coisas como possuidoras ou não de alma. Do que se conclui que, do ponto de vista filosófico, as coisas não são entes apenas materiais, mas também podem ter natureza virtual e podem se conectar por meio de eventos.

No contexto de Internet das Coisas, tais coisas podem ser:

a. Reais ou físicas;
b. Digitais ou virtuais;
c. Uma entidade que se move no tempo e no espaço;
d. Algo que pode ser identificado.

Este último requisito é absolutamente essencial, entendendo que as coisas no contexto de IoT podem ser identificadas por meio de números, nomes e endereços de localização. Mais do que isso, há uma questão fundamental no que diz respeito à identificação e o endereço de

[12] KHAN, R., KHAN, S. U., ZAHEER, R.; KHAN, S. Future Internet: the Internet of Things architecture, possible applications and key challenges. In: Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012. pp. 257-260.
[13] PECORARO, Rossano (org.). Os filósofos: clássicos da filosofia. V. I. De Sócrates a Rosseau. Vozes. Petrópolis: Puc-Rio de Janeiro. 2008.

localização das coisas em IoT, pois endereços IP[14], por exemplo, não podem ser considerados identificadores.

Mais do que os requisitos acima apontados, há a expectativa de que em IoT as coisas se tornem participantes ativos de todos os processos de que fizerem parte, tais como, transações comerciais, interações sociais, podendo se comunicar entre si e com o meio ambiente por meio da troca de dados e informações percebidas, reagindo de forma autônoma aos eventos do mundo real ou físico, influenciando-os por meio da execução de processos que acionam ações e criam serviços com ou sem intervenção humana direta de forma facilitada pelas interfaces que disponibilizam serviços e interações com essas coisas por meio da Internet, levando em conta requisitos atrelados à segurança e privacidade. Por óbvio, nem todas as coisas em IoT detêm todas estas características; se as tiverem, porém, isso as torna, certamente mais inteligentes[15] e, por conseguinte, ampliam sua capacidade de decisão autônoma sobre o ambiente.

Em termos de definições aceitas pela comunidade mundial, destacamos a definição proposta pelo ITU e IERC, Núcleo Europeu de Pesquisa sobre Internet das Coisas[16] que conceitua IoT como "uma infraestrutura de rede global dinâmica com recursos de autoconfiguração baseada em protocolos de comunicação padrão e interoperáveis onde "coisas"

---

[14] Endereço IP: número que identifica exclusivamente cada computador na Internet. O endereço IP de um computador pode ser atribuído ou fornecido permanentemente cada vez que ele se conecta à Internet por um provedor de serviços de Internet. Para acomodar o extraordinário crescimento do número de dispositivos conectados à Internet, um protocolo padrão de 32 bits, conhecido como IPv4 e que podia lidar com 232 (mais de 4 bilhões) de endereços, começou a ser substituído por um protocolo de 128 bits, IPv6, que poderia lidar com 2.128 (mais de 3.4 × 1.038) endereços, em 1999. Em inglês original: *IP address: number that uniquely identifies each computer on the Internet. A computer's IP address may be permanently assigned or supplied each time that it connects to the Internet by an Internet service provider. In order to accommodate the extraordinary growth in the number of devices connected to the Internet, a 32-bit protocol standard, known as IPv4 and which could handle 232 (over 4 billion) addresses, began to be replaced by a 128-bit protocol, IPv6, which could handle 2128 (over 3.4 × 1038) addresses, in 1999.* Disponível em: https://www.britannica.com/technology/IP-address (BRITANNICA, 2022) (Acesso em 13/01/2022)

[15] Ao entendermos que é a partir da significação, ou seja, da substância do significado, que podemos apreciar um termo, entendemos também, por consequência, que as outras palavras existentes no eixo sintagmático também são especializadas. Isso ocorre porque elas são empregadas junto a um significante cuja forma, sendo invariante, não autoriza uma significação que ocorra junto a uma palavra não terminológica. A significação por oposição requer que todas as palavras sejam especializadas ou não especializadas, pois não há uma definição positiva. De forma que sendo este um texto especializado, utilizaremos o vocábulo termo para apontamentos conceituais. ZILIO, Leonardo. Termo e valor linguístico: uma abordagem ensaística. Cadernos do IL, n. 42, p. 119-128, 2011, p.125. De forma que sendo este um texto especializado, utilizaremos o vocábulo termo para apontamentos conceituais. Assim, o termo inteligente, no presente trabalho deve ser entendido de acordo com a definição de Inteligência Artificial descrito por - FRAZÃO, Ana.; MULHOLAND, Caitlin. (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo, SP: Thomson Reuters Brasil, 2019, p. 5. Todo sistema computacional que simula a capacidade humana de raciocinar e resolver problemas, por meio de tomadas de decisão baseadas em análises probabilísticas.

[16] http://www.internet-of-things-research.eu/about_iot.htm (Acesso em 13/01/2022).

físicas e virtuais têm identidades, atributos físicos e personalidades virtuais e usam interfaces inteligentes e estão perfeitamente integrados à rede de informações"[17].

Uma infraestrutura de rede global, conectando objetos físicos e virtuais por meio da exploração de recursos de captura de dados e comunicação. Essa infraestrutura inclui desenvolvimentos de rede[18] e Internet existentes e em evolução. Ela oferecerá identificação de objetos específicos, sensores e capacidade de conexão como a base para o desenvolvimento de aplicativos e serviços federados independentes. Estes serão caracterizados por um alto grau de captura autônoma de dados, transferência de eventos, conectividade de rede e interoperabilidade. Também atuação e controle[19]. Esta é a definição compartilhada pelo CASAGRAS - *Coordination and Support Action for Global RFID-Related Activies and Standardisation*.

A definição formal utilizada pelo CASAGRAS no que diz respeito ao fato de que "a Internet das coisas existe sem necessariamente a utilização de Internet", redunda também no fato de que, possivelmente, este não seja o melhor nome para descrever a infraestrutura tecnológica que é objeto central deste trabalho. Internet das coisas não é um nome com aceitação universal, sendo bem recebido na Europa e no Brasil, mas nos Estados Unidos, por exemplo, há uma preferência por *pervasive computing* ou computação pervasiva, e no Japão escolheu-se a expressão *ubiquitous computing* ou computação ubíqua. Muito embora haja discussões acerca do melhor termo, fato é que exceto por algumas peculiaridades, em regra todos estes termos são utilizados como sinônimos[20]. O termo IoT é ainda utilizado a fim de designar a conectividade entre vários tipos de objetos do dia a dia, sensíveis à Internet, desde eletrodomésticos, carros, roupas, sapatos, remédios etc.[21]

---

[17] Em inglês original: *The Internet of Things (IoT) is defined by ITU and IERC as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network.*

[18] Desenvolvimentos de rede no sentido de que podem ser redes que não utilizem o protocolo IP o que, em última análise, significa dizer a Internet das coisas existe sem a Internet.

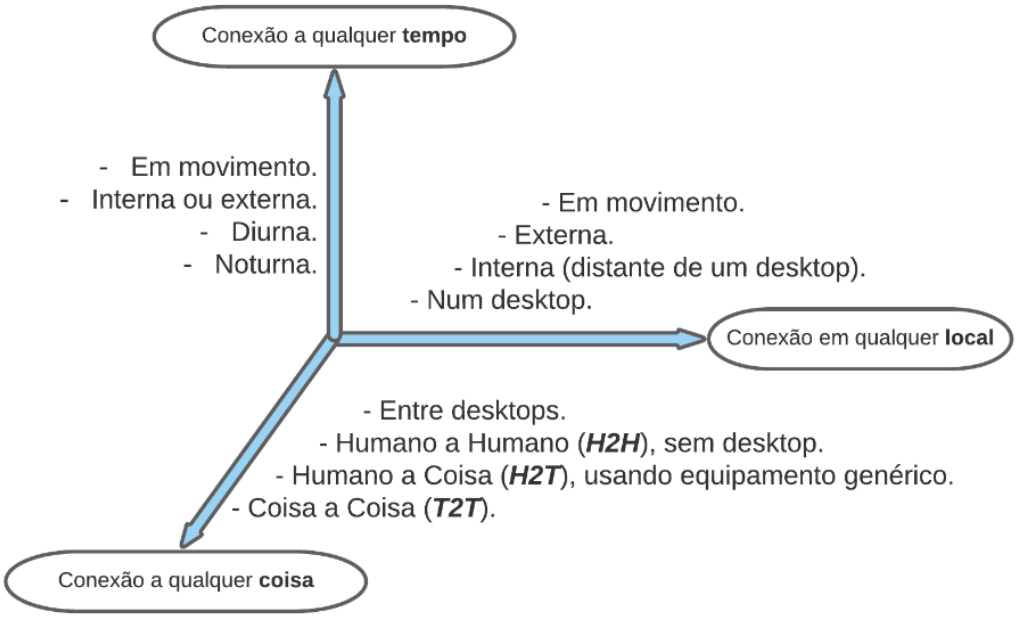
[19] Em inglês original: *A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent federated services and applications.These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability. - Also actuation and control* - (CASAGRAS, 2009).

[20] AMAZONAS, José Roberto de Almeida. Aula I: Iot Fundamentals. In: *IoT: Fundamentals and next generation IoT*. Curso online promovido pelo Fórum Brasileiro de IoT. 2020.

[21] SANTOS, Pedro Miguel Pereira. **Internet das Coisas: o desafio da privacidade.** Dissertação (Mestrado em Sistemas de Informação Organizacionais) – Instituo Politécnico de Setúbal, Setúbal, 2016.

Complementam esta definição também Magrani[22] e Nascimento[23], afirmando que "fazem parte desse conceito os dispositivos de nosso cotidiano que são equipados com "sensores capazes de captar aspectos do mundo real, como por exemplo temperatura, umidade e presença, e enviá-los a centrais que recebem estas informações e as utilizam de forma inteligente". A sigla refere-se a um mundo onde objetos e pessoas, assim como dados e ambientes virtuais, interagem uns com os outros no espaço e no tempo. A Figura 2 ilustra essas interações dos objetos de IoT com relação ao tempo e ao local ou ao espaço.

*Figura 2 Relação proposta pela IoT*




Fonte: ITU-SUDACAD (2017, tradução nossa).

Confrontando os conceitos aqui explanados e a partir do estudo em perspectiva sobre Internet das coisas, propomos uma definição que ultrapasse os conceitos técnicos e que seja compreensível para operadores do direito, entre outros profissionais que não tenham exatamente uma formação voltada para questões de engenharia e ciência da computação:

[22] MAGRANI, Eduardo. A Internet das Coisas**.** 1. ed. Rio de Janeiro: FGV Editora, 2018, p. 44
[23] NASCIMENTO, Rodrigo. O que, de fato, é internet das coisas e que revolução ela pode trazer? Computerworld, 12 mar 2015. Disponível em: https://computerworld.com.br/2015/03/12/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer/. (Acesso em 13/01/2022).

Internet das coisas é uma infraestrutura tecnológica que possibilita que objetos, tanto físicos quanto virtuais, se comuniquem de forma inteligente, seja pela Internet ou seja por outras redes de forma que possam ter identidades e até personalidades virtuais. Esta estrutura não existe por si mesma, mas intermedeia outras relações e congrega harmonicamente outras tecnologias possibilitando que sua utilização possa se dar em diferentes áreas do conhecimento e para as mais diversas aplicabilidades sempre com o objetivo de trazer benefícios sociais.

É fundamental, todavia, que entendamos em que medida esta infraestrutura influencia os institutos seculares do direito e até mesmo a ciência jurídica a ponto de ensejar este e outros trabalhos que, por certo, virão e que discutirão a convergência que existe entre IoT e direito. E este é o ponto fulcral deste estudo, visto que os dados compartilhados pelas tecnologias interoperáveis que compõem as infraestruturas de IoT pertencem a um indivíduo ou a uma pessoa natural, tal como preconiza a definição do Código Civil Brasileiro com seus direitos e obrigações, de forma que há preocupação quanto a dois pontos especificamente relevantes neste compartilhamento de dados no que diz respeito à segurança e à privacidade destas informações com vistas ao atendimento aos direitos dos titulares do dados nos termos do art. 18 da Lei 13.709/2018 – Lei Geral de Proteção de Dados.[24]

---

[24] 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 e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
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; (Redação dada pela Lei nº 13.853, de 2019);
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.
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Do ponto de vista técnico, a interconexão de objetos baseados em tecnologias interoperáveis não é recente e permeia o imaginário dos cientistas e engenheiros de computação desde os anos 1990, muito embora o conceito, tal como o conhecemos hoje tenha sido cunhado apenas em 1999 por Kevin Ashton do Instituto de Tecnologia de Massachussets nos Estados Unidos. A ideia subjacente à conexão de objetos repousa no pulsante desejo humano de transcender sua capacidade de superação e de praticidade da vida moderna, sobretudo no que diz respeito às atividades cotidianas e à melhoria de condições relacionadas à saúde, por exemplo.

> Se tivéssemos computadores que soubessem tudo sobre as coisas em geral - usando dados que coletassem sem a nossa ajuda - seríamos capazes de rastrear e contar tudo, e reduzir bastante o desperdício, a perda e os custos. Nós saberíamos quando é necessário substituir, reparar ou fazer um recall de um produto, e se estão novos ou ultrapassados. Precisamos capacitar os computadores com seus próprios meios de coletar informações, para que possam ver, ouvir e cheirar o mundo sozinhos, com toda a sua glória aleatória. O RFID e a tecnologia de sensores capacitam os computadores a observar, identificar e entender o mundo sem as limitações dos dados inseridos pelos humanos[25].

É certo, entretanto, que ao idealizar quaisquer tecnologias sobre as quais dissertamos aqui, os pesquisadores, pelo menos no estágio inicial, não consideraram os impactos que elas teriam sobre a privacidade e os direitos fundamentais salvaguardados pelos diplomas legais dos mais diferentes países onde elas fossem adotadas.

Ao supor qualquer avanço, melhoria ou desenvolvimento humano, há que se considerar a necessidade de dados que consubstanciem essas pesquisas e direcionem a tomada de decisão sobre as diretrizes que norteiam a adoção de qualquer tecnologia no ambiente pessoal, corporativo ou mesmo de natureza pública, quando pensamos em otimizar a vida dos cidadãos.

---

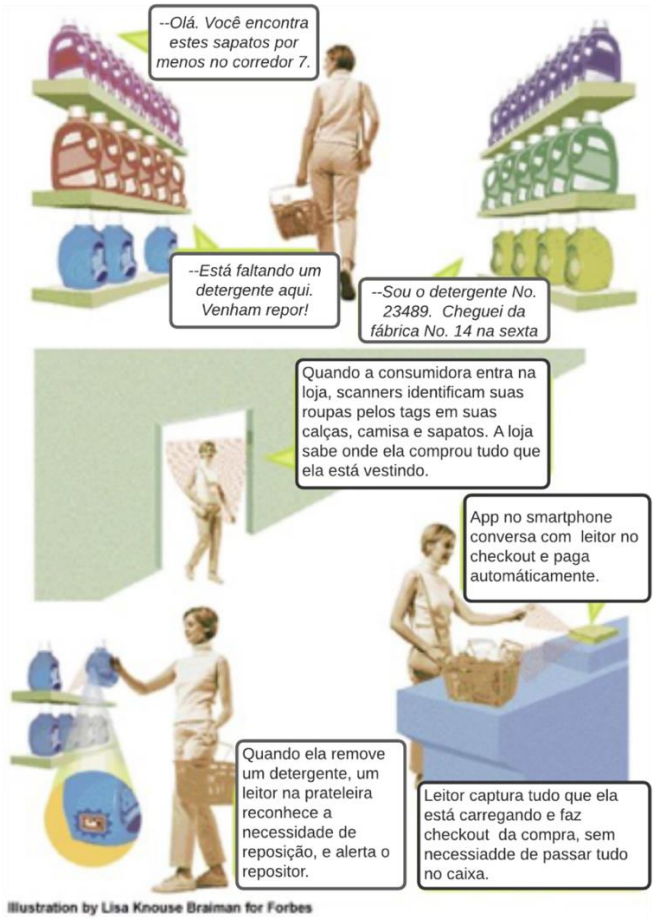
§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019)
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

[25] https://www.historyofinformation.com/detail.php?id=3411 (Acesso em 13/01/2022).

Há para tanto tecnologia disponível, como *wi-fi*, *bluetooth* e identificação por radiofrequência ou *RFID* que permitem que os objetos a elas conectados coletem, armazenem e compartilhem dados para tratamento de diferentes finalidades.

A extensão acurada da interconexão de coisas pode ser medida pela existência do que se denomina hoje "*wearebles*", que são peças do vestuário com tecnologias embarcadas a ponto de coletar e disponibilizar uma série de informações sobre aqueles que as vestem. Destacam-se nesta categoria, tênis, pulseiras, óculos, especialmente aqueles voltados à prática de atividade física[26].

*Figura 3 Exemplo de IoT aplicada ao varejo*

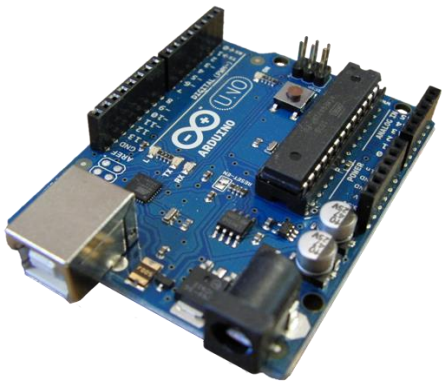



[26] Disponível em: https://www.consumidormoderno.com.br/2020/02/19/roupas-inteligentes-exercicios-fisicos/. (Acesso em 13/01/2022).

Fonte: ABBAS, M. (2014, tradução nossa)[27].

Seria negligente de nossa parte, ainda que de forma muito superficial não mencionarmos a importância da placa Arduíno na popularização da IoT, não só no Brasil, como no mundo. Isto porque o Arduíno é um dispositivo que permite que mesmo pessoas leigas possam utilizá-lo com o intuito de conectá-lo a LED's, *displays* de matriz de pontos, botões, interruptores, motores, sensores de temperatura, sensores de pressão de distância, receptores GPS, Wifi, entre outros. Do ponto de vista conceitual, um Arduíno é um computador minúsculo passível de programação para processar entradas e saídas entre o dispositivo e os componentes externos que se conectam a ele[28]. A Figura 4 apresenta uma placa de um micro computador tipo Arduino, cujas dimensões médias estão em torno de 70 mm x 50 mm, podendo chegar a minúsculos 33 mm x 17 mm.

*Figura 4 Placa de um microcomputador tipo Arduino.*



Fonte: https://pt.wikipedia.org/wiki/Arduino

### 2.1.2 A coleta de dados por IoT: um processo multifacetado

O primeiro ponto a ser discutido quando se pensa em coleta de dados por soluções de Internet das Coisas é a infraestrutura disponibilizada, uma vez que o requisito mínimo necessário é o suporte para a comunicação dos diversos dispositivos interconectados.

[27] ABBAS, M. Internet of Things (IOT) – *We Are At The Tip of An Iceberg*. In**:** MIMOS Berhad, 2014, Wismas IEM, Petaling Jaya. Disponível em: https://pt.slideshare.net/mazlan1/internet-of-things-iot-we-are-at-the-tip-of-an-iceberg/44-Crowdsensing . (Acesso em 13/01/2022).
[28] MCROBERTS, Michael. Arduino básico. Novatec Editora, 2018.

Sem estrutura de conectividade não há que se falar em Internet das Coisas ou mesmo em Internet, por se tratar do meio pelo qual os dados trafegam. Em última análise, podemos dizer que a IoT é uma extensão da Internet atual, uma vez que possibilita que todo e qualquer objeto com capacidade computacional e de comunicação se conecte tanto para que seja controlado remotamente, quanto para que seja provedor de serviços[29].

Neste contexto, é imperioso discutirmos, ainda que circunstancialmente no contexto desta pesquisa, o conceito de redes de computadores que vem passando por uma evolução em razão dos fenômenos aqui tratados. A clássica definição descreve as redes de computadores como um conjunto de computadores autônomos interconectados por uma única tecnologia (Tanembaum, 2002)[30], entretanto outros autores, tais como Kurose and Ross (2016)[31], tem observado que o próprio termo redes de computadores já pode ser considerado ultrapassado, haja vista a quantidade de equipamentos e tecnologias não tradicionais que são usadas na Internet.

Os objetos sobre os quais muito já falamos neste trabalho e que podem ser exemplificados a partir de televisores, *notebooks*, automóveis, *smarphones*, consoles de jogos, *webcams*, entre outros, compõem a lista de equipamentos citados na última definição de redes acima transcrita por terem sua capacidade de comunicação e processamento aliados a sensores.

Neste sentido, um dos fenômenos que mais tem chamado a atenção da comunidade acadêmica e do mercado é a quantidade de dispositivos interconectados. O Instituto Gartner prevê que o número de dispositivos conectados por meio de IoT em 2021 chegue a 25 bilhões, número que, segundo a *Juniper Research*, deve dobrar em 2022, quando possivelmente, teremos mais de 50 bilhões de dispositivos conectados à IoT[32].

Muito embora o caráter disruptivo da Internet das coisas seja bastante sedutor, é necessário apontarmos que os problemas são proporcionais aos números exponenciais acima apontados, uma vez que os dados coletados por todos estes dispositivos são passíveis de imperfeições, inconsistências e até mesmo de diferentes tipos, já que tanto podem ser gerados por pessoas, quanto por objetos. Isto sem falar na confiabilidade destes dados, relativamente às condições em que foram coletados.

---

[29] SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. 2016.
[30] TANEMBAUM, A. Computer Networks. Prentice Hall Professional Technical Reference, 4th edition. 2002.
[31] KUROSE, J. F. and ROSS, K. W. Computer Networking: A TopDown Approach (7th Edition). Pearson, 7th edition. 2016.
[32] https://inforchannel.com.br/2021/04/27/internet-das-coisas-e-protecao-de-dados/ (Acesso em 13/01/2022).

Especificamente sobre as condições de coleta, é importante mencionar que as diferentes possibilidades de aplicações em IoT se prestam aos mais diferentes setores da sociedade e da economia, tais como: aeroespacial, manufatura, automotivo, segurança de petróleo e gás, edifícios inteligentes, cuidados de saúde, transporte de mercadorias e pessoas, rastreamento de alimentos, farmacêutico, agricultura, mídia, entretenimento, logística, seguros, gestão da cadeia de abastecimento, entre outros. A Figura 5 ilustra uma estrutura de tráfego e coleta de dados numa estrutura de IoT.

Vale também ressaltar que a adoção do IPV6 (*Internet Protocol* versão 6) em 2012, permitindo um número muito maior de dispositivos de 128 bits de endereçamento no lugar do IPV4 (*Internet Protocol* versão 4) que dispunha de um espaço de endereçamento de 32 bits que permitia apenas 4,3 bilhões de dispositivos conectados, é também um fator preponderante no aumento exponencial de dispositivos interconectados e, consequentemente, no crescimento da Internet das Coisas.[33]

*Figura 5 Estrutura de Tráfego e Coleta de Dados na perspectiva da IoT*


Fonte: Autora

[33] MORAES, Alexandre de.; HAYASHI, Victor Takashi. Segurança em IoT. Entendendo os riscos e ameaças em Internet das Coisas. Alta Books. 2021. p. 06.

A ausência de padrões de interoperabilidade, a variedade de protocolos sem fio, os problemas de latência e as desafiadoras práticas de segurança integram, do ponto de vista técnico, o complexo cenário de coleta de dados realizada por Internet das coisas.

Uma questão fundamental a ser tratada é o fato de que dispositivos IoT podem se conectar utilizando diferentes tecnologias, tais como: 3G, 4G, 5G, Wi-fi, Bluetooth, Zigbee, entre outras. A título informativo, apresentaremos alguns destes conceitos para contribuir com a melhor compreensão do leitor acerca destas tecnologias utilizadas pelos dispositivos IoT:

- 1G (1981): todos os sistemas de comunicação sem fio são centrados em serviços de voz totalmente analógicos e utilizam a técnica de múltiplo acesso FDMA (*Frequency Division Multiple Access*). Tecnologia no Brasil: AMPS (*Advanced Mobile Phone System*).
- 2G (1992): no 2G, os sistemas de comunicação sem fio também são baseados em serviços de voz, porém utilizando sistemas digitais com técnica de múltiplo acesso TDMA (*Time Division Multiple Access*). Tecnologia no Brasil: GSM (*Global System for Mobile Communication*).
- 2.5G (1995): provia serviços de voz com alta capacidade e serviço limitado de dados. Tecnologias no Brasil: CDMA2000 (*Code Division MultipleAccess* 2000), CDMAOne, GPRS (*General Packet Radio Service*) e EDGE (*Enhanced Data rates for GSM Evolution*).
- 3G (2001): nessa geração, os sistemas de comunicação sem fio têm capacidade de prover serviços de voz e dados com boa qualidade. No Brasil, utiliza-se a tecnologia UMTS / HSPA (*Universal Mobile Telecommunications System / High Speed Packet Access*) em uma banda de 5 MHz.
- 4G (2011): é um sistema de voz e dados com alta taxa de transmissão de dados. O sistema LTE/SAE (*Long-Term Evolution / System Architecture Evolution*), padrão do 3GPP[34] (*Third Generation Partnership Project*), foi a tecnologia escolhida pela maioria dos países para ser usada como 4G.
- 5G (2018): propõe diversas características inovadoras para as redes sem fio, além de o seu desempenho ser abordado em termos de capacidade e taxa de dados, latência,

[34] O 3GPP é um projeto de parceria que reúne organizações nacionais de desenvolvimento de padrões de todo o mundo inicialmente para desenvolver especificações técnicas para a 3ª geração de telecomunicações móveis, celulares, UMTS. Site: https://www.3gpp.org/ (Acesso em 13/01/2022).

> eficiência espectral e sobretudo pela capacidade de conexão com dispositivos para IoT. O 5G, ainda em implantação no Brasil no momento de redação deste trabalho, terá um design que apresenta uma evolução das redes legadas, bem como uma revolução em seus paradigmas. Será necessário melhorar as tecnologias de acesso via rádio existentes e criar outras que sejam capazes de oferecer o alto desempenho que se espera da quinta geração de redes celulares.[35]

Além das tecnologias 3G, 4G e 5G, dispositivos IoT podem se conectar utilizando diversas outras tecnologias, tais como: Ethernet[36], Bluetooth[37], Wi-Fi[38] e Zigbee[39], entre outras.

Não bastasse esse emaranhado de dificuldades técnicas, somam-se a estes problemas, os requisitos de privacidade e a necessidade do atendimento às questões legais e regulatórias previstas nas diversas legislações sobre a matéria.

As evidências que compõem o conjunto necessário para a *accountability* ou prestação de contas, nos termos da legislação protetiva de dados pessoais, perpassam as questões de infraestrutura e as técnicas, inclusive no que diz respeito aos princípios de *privacy by deisgn e privacy by default.*

---

[35] P. Tracy. *Small cells: Backhaul difficulties and a 5G future*. Disponivel: https://www.rcrwireless.com/20160711/network-infrastructure/small-cells-tag31-tag99 (Acesso em 13/01/2022)

[36] O padrão Ethernet (IEEE 802.3) foi oficializado em 1983 pelo IEEE e está presente em grande parte das redes locais com fio existentes atualmente. Sua popularidade se deve à simplicidade, facilidade de adaptação, manutenção e custo.

[37] O Bluetooth é um protocolo de comunicação proposto pela Ericsson para substituir a comunicação serial RS-232. Atualmente, o *Bluetooth Special Interest* Group é responsável por criar, testar e manter essa tecnologia. Além disso, Bluetooth é uma das principais tecnologias de rede sem fio para PANs – *Personal Area Networks*, que é utilizada em *smartphones*, *headsets*, PCs e outros dispositivos. In: SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. 2016. p. 9.

[38] A tecnologia Wi-Fi é uma solução de comunicação sem fio bastante popular, pois está presente nos mais diversos lugares, fazendo parte do cotidiano de casas, escritórios, indústrias, lojas comerciais e até espaços públicos das cidades. O padrão IEEE 802.11(Wi-Fi1) define um conjunto de padrões de transmissão e codificação. In: SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. 2016. p. 8.

[39] O padrão ZigBee é baseado na especificação do protocolo IEEE 802.15.4 para a camada de enlace. As suas principais características são a baixa vazão, reduzido consumo energético e baixo custo. O ZigBee opera na frequência 2.4 GHz (faixa ISM), mas é capaz de operar em outras duas frequências, 868 MHz e 915 MHz. Essa tecnologia pode alcançar uma taxa máxima de 250 kbps, mas na prática temos taxas inferiores. In: SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. 2016. p. 8-9.

### 2.1.3 A interoperabilidade como referência para usuários, fabricantes e desenvolvedores

Com o objetivo de padronizar este segmento, a criação de uma arquitetura de referência ou um modelo de referência é muito importante para que no futuro os dispositivos que se denominam IoT possam estar realmente conectados uns com os outros, ou seja, que a interoperabilidade seja algo real e não apenas teórico. A importância de um modelo de referência diz respeito, sobretudo ao fato de que dispositivos IoT estão cada vez mais presentes em todos os setores da vida em sociedade, de forma que havendo uma referência a ser observada para o desenvolvimento destes dispositivos, alcança-se o mais importante no processo tecnológico em questão: a comunicação entre dispositivos de diferentes marcas e ou fabricantes e, consequentemente, a coleta de dados mais estruturados e em maior escala.

Embora existam diversas organizações que trabalhem no desenvolvimento e no processo de padronização de IoT, nem todas elas possuem uma arquitetura definida, ou seja, ainda estão em processo de aprendizagem ou aprimoramento do tema, como é o caso do IEEE (*Institute of Electrical and Electronics Engineers*), OASIS (*Organization for the Advancement of Structured Information Standards*), NIST (*National Institute of Standards and Technology*), IETF (*Internet Engineering Task Force*) e o ETSI (*European Telecommunications Standards Institute*), que possuem alguns artigos e documentos contendo seus estudos e contribuições para a temática. [40]

Para os cientistas da computação, 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. De acordo com Evanczuk (2018):

> Para trabalhar em conjunto, essas peças precisam de uma estrutura comum de protocolos e modelos de nível superior para se reconhecerem com segurança e trocar informações sobre dados, recursos e status. Embora o protocolo HTTP padrão da Web permita a interoperabilidade com alguns métodos de solicitação, campos de cabeçalho e códigos de resposta, a IoT precisa de muito mais informações, não apenas sobre a

[40] BORBA, Victor Ubiracy. Proposta de um modelo de referência para Internet das Coisas: aspectos de segurança e privacidade na coleta de dados. 2018.

> natureza da interação, mas também sobre estrutura e semântica da carga útil. (Tradução nossa)[41]

O IERC (*European Research Cluster on the Internet of Things*) é um dos programas que incentiva a pesquisa e o desenvolvimento tecnológico na União Europeia. Uma de suas linhas de investigação diz respeito à criação de uma visão comum para IoT juntamente com o ITU-T (2012), grupo de estudos sobre o tema na ITU (*International Telecommunications Union*), agência da ONU responsável pela normatização e regulação internacionais das tecnologias de informação e comunicação.

De acordo com Khan[42], existem diversos modelos e arquiteturas de referência para IoT, cada grupo ou empresa descreve o seu, o que muitas vezes causa conflitos de ideias e torna a tarefa de padronização mais complexa.

Neste trabalho, apresentaremos como arquitetura de referência, o modelo desenvolvido pelo ITU-T (*ITU Telecommunication Standardization Sector*) que, embora não seja o único e nem o mais importante, visto que este juízo de valor não é pertinente nesta discussão, é um dos mais conhecidos e considerados na comunidade desenvolvedora de dispositivos IoT.

Para os principais objetivos deste trabalho, o exemplo que segue é importante no sentido de que a segurança é dividida em um modelo genérico e outro específico, possibilitando que processos de autorização e autenticação sejam definidos para os dispositivos nas camadas de aplicação, rede e dispositivos. A camada de aplicação adiciona confidencialidade dos dados e proteção para integridade, controle de privacidade, auditoria de segurança e sistemas antivírus. A camada de rede, ainda, incorpora mecanismos de controle de integridade e confidencialidade, utilizando também protocolos seguros.

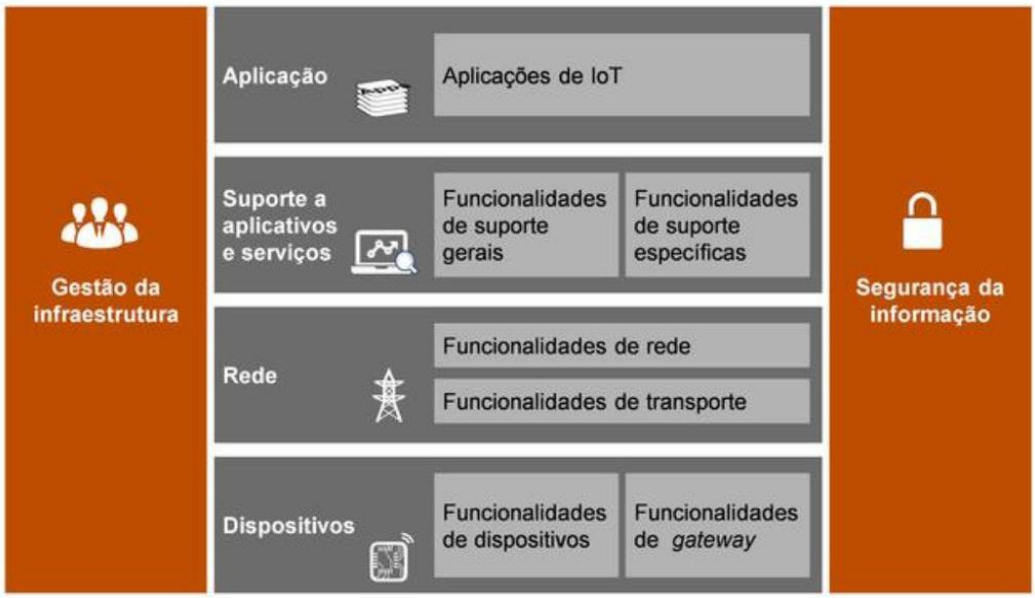
Importante mencionar que os conceitos de confidencialidade, integridade e privacidade serão mais bem detalhados nos capítulos subsequentes, tanto do ponto de vista técnico, quanto do ponto de vista jurídico.

---

[41] EVANCZUK, Stephen. *Why IoT Success Hangs on Interoperability***.** Mouser Electronics. Disponível em: https://www.mouser.com/blog/why-iot-success-hangs-on-interoperability (Acesso em 13/01/2022).

[42] KHAN, R., KHAN, S. U., ZAHEER, R.; KHAN, S. Future Internet: The Internet Of Things Architecture, Possible Applications And Key Challenges. In: Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012. P. 257-260. DOI: 10.1109/FIT.2012.53. Disponível em https://doi.org/10.1109/FIT.2012.53 (Acesso em 14/01/2022)

*Figura 6 Arquitetura de Referência de IoT*




Fonte: ITU-T (2012)

A primeira camada é a de dispositivos, ou objetos inteligentes que pode ser considerada uma camada de coleta, representando os objetos físicos, que através de sensores ou outro tipo de tecnologia coletam e em alguns casos processam dados. Já na camada de Rede, é onde estão concentradas as tecnologias utilizadas para comunicação, bem como toda a questão de gerenciamento e distribuição de mensagens, ou seja, é uma camada onde o tráfego de dados é abstraído.

Por fim, a camada de aplicação é responsável por tornar os recursos disponíveis para serem usados, seja por um outro dispositivo ou um sistema informacional, tal como os dispositivos que podem ser conectados aos carros disponibilizando dados.

Ressaltados todos os benefícios do que, comumente chamamos de objetos inteligentes, bem como dos processos que conectam estes objetos, propomos, neste estudo, um exercício de análise pautado em outra perspectiva, a da privacidade dos usuários destes objetos, tanto do ponto de vista de sua concepção, quanto do ponto de vista de seus termos de uso, políticas de privacidade e demais contratos que formalizem a relação desenvolvedor-consumidor.

Segundo Lemos e Marques[43], a "datatificação" ou transformação em dados digitais e processamento algorítmico de pessoas, hábitos e espaços numa rede espalhada é um grande desafio para a vida privada.

Para tanto, utilizaremo-nos dos conceitos abaixo descritos e da análise de como se interconectam na esteira de uma sociedade cada vez mais dependente das tecnologias e cada vez mais refém no que diz respeito à sua privacidade.

## 2.2 Os quatro pilares de inovação

Se as quatro primeiras décadas da Internet, todavia, foram fundamentais para o desenvolvimento de seus protocolos, sua robustez e sua consolidação como principal avanço científico do século XX, os anos 2000 fecharam este ciclo tecnológico sacramentando definitivamente a mudança paradigmática pela qual passou a humanidade desde que a Internet se tornou o farol das relações humanas.

Vivemos a era da inovação, do efêmero, das máquinas substituindo os humanos, tal como supúnhamos no século passado, e da pouca privacidade. A tecnologia fez com que o tempo fosse curto, que as notícias fossem rápidas, que a importância de alguns valores e princípios fosse discutível e que o mundo tivesse outras prioridades. Certamente numa proporção que os pioneiros da Internet nunca sonharam acontecer, mas como vanguardistas que eram, já enxergavam a dificuldade de harmonizar tantos interesses difusos sobre um mesmo tema.

> A questão mais relevante com relação ao futuro da Internet não é como a tecnologia se modificará, mas como o processo dessa mudança e evolução será gerenciado. Como descreve este artigo, a concepção da Internet sempre foi direcionada por um grupo principal de designers. No entanto, o formato desse grupo sofreu alterações quando as partes interessadas aumentaram. Como consequência do sucesso da Internet, surge uma proliferação de participantes (ou partes interessadas), que, agora,

[43] LEMOS, A., & MARQUES, D. (2019). Privacidade e Internet das Coisas: uma análise da rede *Nest* a partir da Sensibilidade Performativa. E-Compós, 22(1). Disponível em: https://doi.org/10.30962/ec.1611. P.01

> apresentam um investimento não só econômico como também intelectual na rede. (*Brief History of the Internet,* 1997, p.9. tradução nossa).[44]

Neste tópico, trataremos da Internet das coisas e sua correlação com os outros pilares de inovação, quais sejam: *big data*, inteligência artificial e proteção de dados sob o ponto de vista da implicação que cada um destes pilares interpõe ao outro, num movimento indissociável, de forma que a completa e irrestrita compreensão sobre os reais impactos destes pilares em sociedade, está atrelada ao estudo de todos eles, pelos menos no que tange à sua interação dentro dos processos tecnológicos a que se propõem, não há como separá-los ou analisá-los individualmente, sem que as características de um não resvalem no desenvolvimento dos outros.

O fluxo entrelaçado que os dados seguem hoje por meio da estrutura da Internet, começa maciçamente na coleta realizada por dispositivos que utilizam a tecnologia denominada Internet das coisas, compõem a formação dos grandes *big datas* que são utilizados para o treinamento das inteligências artificiais e todos estes processos e recursos desprezam em sua concepção o conceito de privacidade e a necessidade de o titular dos dados consentir, ou mesmo ser informado a respeito da frequência, a quantidade e a finalidade dos dados que são coletados, armazenados e tratados diuturnamente nas mais diferentes localidades.

Especificamente sobre *big datas*, chama a atenção a ausência de uma definição precisa e formal sobre o tema e parte, muitas vezes, de exemplos para esclarecer o conceito. Para Cravo[45], a capacidade de analisar gigantescas quantidades de informação, antes desconsideradas, com objetivo econômico redunda na principal característica para a definição de *Big Data*. Ressalta-se como complemento importante desta característica o fato de nunca termos tido tanta informação armazenada e, ao mesmo tempo, tanta tecnologia disponível para processá-la.

Reforça esta afirmação a descrição feita por Hilbert e López[46]:

---

[44] No original: *The most pressing question for the future of the Internet is not how the technology will change, but how the process of change and evolution itself will be managed. As this paper describes, the architecture of the Internet has always been driven by a core group of designers, but the form of that group has changed as the number of interested parties has grown. With the success of the Internet has come a proliferation of stakeholders – stakeholders now with an economic as well as an intellectual investment in the network.*

[45] CRAVO, Victor. O Big Data e os desafios da modernidade: uma regulação necessária? Revista de Direito Setorial e Regulatório, Brasília, v. 1, n. 2, p. 243-257, out. 2015.

[46] HILBERT, Martin. LÓPEZ Priscila. The World's Technological Capacity to Store, Communicate, and Compute Information. Science, abril de 2011, p. 60-65.

> A capacidade mundial de armazenar, comunicar e processar informação do quantitativo total de dados analógicos e digitais existente no mundo cresceu de 3 bilhões de gigabytes, em 1987, para 300 bilhões de gigabytes em 2007. Em 2013, o total de dados amealhados chegará a 1200 exabytes1, dos quais apenas 2% seriam analógicos. A capacidade de processamento de dados também aumentou de modo constante durante todo esse período, a quantidade de instruções que um computador pessoal conseguia processar em 1 segundo no ano 2007 – 6,4 x 1021 – equivalia ao máximo de impulsos nervosos executados por cérebro humano no mesmo tempo. Contudo, ao contrário das habilidades naturais de processamento de informações, a capacidade tecnológica mundial de processar dados vem crescendo a taxas visivelmente exponenciais. No futuro próximo, antevisto pela CISCO (2014), o tráfego anual total de dados pela Internet passará da casa dos zettabytes3 em fins de 2016, chegando a 1,6 zettabytes em 2018. (Tradução nossa)

Os números impressionam e os motivos que norteiam as análises dos grandes bancos de dados, embora sejam, prioritariamente econômicos, são de natureza nobre em sua essência, haja vista que uma das áreas do conhecimento mais beneficiadas pela análise a partir de *big datas* é a medicina. É certo, porém, que atrelado ao resultado obtido pela análise de grandes bancos de dados está a certeza de que a inexatidão e a extensão da informação ou descoberta apontada requerem profundidade o que não acontecia quando as amostras para análise eram menores, mas as metodologias mais rigorosas, por isso menos imprecisas.

Às diversas formas que a Internet já disponibilizava para a coleta de milhões de dados por minuto, juntou-se a Internet das Coisas com uma capacidade ainda maior de agregar informações a bases já robustas e, agora, ainda mais potentes. Isto porque a computação é onipresente, por meio dos dispositivos pervasivos, coletam informações de todas as pessoas em qualquer contexto.

Para um número tão grande de dados coletados há de existir uma finalidade nobre e porque não dizer inovadora, adjetivos que em forma e conteúdo se amoldam ao conceito de inteligência artificial cuja motivação foi a ambiciosa ideia de que as máquinas poderiam pensar e tomar decisões no lugar de humanos. Mote antigo, entretanto, formalizado apenas no século XX.

Segundo Silva[47], a ideia remonta a um guardião gigante e alado feito de bronze, o qual dava três voltas por dia na Ilha de Creta, com o objetivo de protegê-la de invasores data de 400 a. C. Da mesma forma que outras mitologias atribuíam a estátuas sagradas faculdades humanas dotadas de sabedoria e emoções.

No século XVII, as máquinas de calcular foram um grande marco do desenvolvimento e primordiais para o desenvolvimento dos computadores, bem como referências matemáticas, como a Álgebra Booleana, fundamental para o funcionamento de sistemas digitais.

Obviamente que, nestes primeiros anos do século XXI, tivemos notícias de sistemas baseados em redes neurais, tais como as que simulam a natureza cerebral humana, extremamente sofisticados e já adaptados para diversos segmentos da sociedade, bem como softwares pensados para questões morais, tais como a máquina moral que coloca o observador em diferentes contextos de julgamento[48] e de análise ética sobre o ponto em que estamos de interferência humana no universo.

Os dilemas éticos são os que mais têm chamado a atenção de pesquisadores de todo o mundo, pois agregam os muitos fatores envolvidos no desenvolvimento e aplicabilidade da inteligência artificial. E não seria para menos, observada a agressividade com que esta tecnologia tem se mostrado[49].

É necessário e salutar também pontuarmos que o "treinamento" de máquinas é realizado a partir de grandes bases de dados coletadas em diferentes cenários, pelos mais distintos dispositivos. E se existe um dilema ético sobre o quão profundamente o homem está intervindo em questões que, verdadeiramente, não se sabe se serão controláveis, a origem dos dados com quais as inteligências artificiais são treinadas também são discutíveis. Dados oriundos de dispositivos que desrespeitam a privacidade de seus usuários não só infringem leis, como também desviam eticamente o fluxo que estas informações percorrem.

Completa o fluxo aqui apresentado o vértice da privacidade e da proteção de dados. O conceito de privacidade remonta ao paradoxo de público e privado estabelecido na Antiguidade clássica e, posteriormente, incorporado à cultura romana. Óbvio está que tal contraposição à época guardava características relacionadas à posição dos indivíduos em sociedade e,

---

[47] SILVA, Nilton Correia da. Inteligência Artificial. In: FRAZÃO, Ana.; MULHOLAND, Caitlin. (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo, SP: Thomson Reuters Brasil, 2019. p. 37.

[48] Disponível em: https://www.moralmachine.net (Acesso em 13/01/2022).

[49] Algumas empresas produzem Robôs com alto grau de sofisticação. Disponível em: https://www.bostondynamics.com. (Acesso em 13/01/2022).

especialmente, com relação à sua condição de liberdade ou mesmo de sua atuação política. Como descreve Cancelier[50] a definição de privado, por exemplo, remonta às atividades concretas de sobrevivência em pequenas comunidades.

A ideia de isolamento como sinônimo daquilo que é privado, começou a se delinear na Idade Média, curiosamente a partir de necessidades fisiológicas e por natureza íntimas, porém apenas para os nobres e, apesar do largo lapso temporal que separa os dias de hoje do período histórico a que estamos nos referindo, Rodotà[51] assevera que a privacidade ainda é um privilégio de poucos.

É somente no alvorecer da sociedade burguesa que os contornos da privacidade ganham matizes que escalam entre o social e o particular ou privado, tal como assevera Doneda[52]. E é também na sociedade burguesa que expressões até hoje utilizadas em nossa Constituição, tais como intimidade e vida privada se solidificam[53], muito embora a privacidade como figura jurídica tenha se notabilizado no trabalho de Warren e Brandeis[54], é emblemático na consolidação do conceito de privacidade pelo fato de marcar a primeira vez que tal definição se torna objeto de uma discussão doutrinário-jurídica e por conseguinte um referencial de decisões judiciais.

A partir da segunda metade do século XX, curiosamente quando a Internet começa a se desenvolver, a relação entre o indivíduo, a sociedade e a informação também se modificam a ponto de rapidamente alguns perceberem que poderiam utilizar estas informações em proveito próprio, ferindo frontalmente direitos personalíssimos dos indivíduos, tal como leciona Doneda[55].

Especificamente a partir dos anos 1970, inicia-se um movimento legislativo sobre dados pessoais, em particular em alguns países europeus, por certo coerente com o desenvolvimento tecnológico da época, mas que guardava alguns princípios, como o da

---

[50] CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. Sequência (Florianópolis), p. 213-239, 2017.
[51] RODOTÀ, Stefano. A vida na sociedade da vigilância (coord. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, p. 23-232, 2008.
[52] DONEDA, Danilo. Da Privacidade à Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020.

[53] BRASIL. Constituição da República Federativa do Brasil.1988. Art 5º, inciso X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.
[54] BRANDEIS, Louis; WARREN, Samuel. The right to privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, dez. 1890.

[55] DONEDA, Danilo. Da Privacidade à Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020.

autodeterminação informativa que permeia as atuais legislações, tal como a Lei Geral de proteção de Dados Brasileira.

Embora o tema da proteção de dados seja hoje, talvez, aquele que mais vem sendo discutido no ambiente jurídico-acadêmico e corporativo, o interesse deste trabalho se restringe a dois princípios pouco debatidos, porém fundamentais para o entendimento do fluxo dos dados coletados por Internet das coisas, quais sejam: *Privacy by Design* e *Privacy by Default* ou privacidade desde a concepção e privacidade por padrão. Estes princípios, segundo o Regulamento Geral de proteção de Dados europeu (GDPR - *General Data Protection Regulation*) e a Lei Geral de Proteção de Dados Brasileira (LGPD) devem nortear o desenvolvimento de toda e qualquer aplicação que colete dados pessoais, não só como norteadores de conformidade com as citadas leis, mas como requisitos previstos em programação segura que mitiguem os riscos de vazamento de dados ou de acessos não autorizados a determinados sistemas ou bancos de dados. O *Privacy By Design* deve ser pautado a partir de sete princípios fundamentais, segundo Cavoukian[56] (tradução nossa):

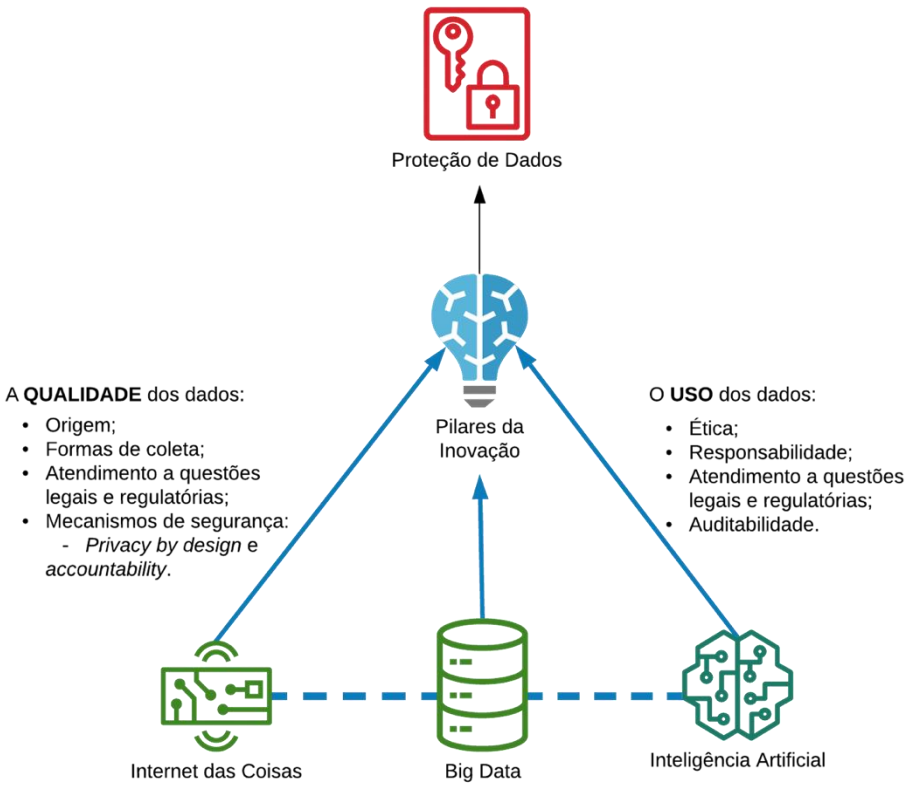
1. Proativo e não Reativo; Preventivo e não corretivo;
2. Privacidade como padrão;
3. Privacidade Inserida no Design;
4. Funcionalidade Completa – Soma positiva e não soma zero;
5. Segurança de Ponta a Ponta – Proteção do Ciclo de Vida;
6. Transparência e Visibilidade;
7. Respeito à Privacidade do Usuário.

Os princípios acima descritos são, claramente, os balizadores da qualidade dos dados coletados por dispositivos interconectados de forma ubíqua e são também a forma mais efetiva de respeito aos direitos personalíssimos dos titulares dos dados que são recolhidos e servem de insumo para a formação dos Big Datas que fomentam o aprendizado de máquinas dotadas de inteligência artificial.

A Figura 7 sintetiza e localiza cada uma destas questões no fluxograma dos pilares de inovação.

[56] CAVOUKIAN, Ann. Information & Privacy: 7 foundational principles. Internet Architecture Board. 2011. Disponível em: https://www.iab.org/wpcontent/IABuploads/2011/03/fred_carter.pdf. Acesso em: 26 ago. 2020.

*Figura 7 Pilares de Inovação*




Fonte: Autora

# 3 DESAFIOS CIBERNÉTICOS E LEGAIS EM IOT

Feitas as devidas, porém não exaustivas, explanações sobre os conceitos atinentes à Internet das Coisas, faz-se necessário também voltar nossos olhares para os dois aspectos sobre IoT que serão mais bem observados nesta tese, quais sejam: segurança e proteção de dados. Isto porque os conceitos tecnológicos que sustentam este trabalho têm o viés instrumental, uma vez que se trata de um estudo do direito e não de outra área. Servimo-nos dessas premissas conceituais para que possamos contextualizar as preocupações que ensejam o objeto desta pesquisa e para que tenhamos um conhecimento, ainda que raso, do processo de desenvolvimento tecnológico que nos rodeia e nos ampara na vida cotidiana, seja para fins pessoais, seja para atividades profissionais.

A Internet não foi idealizada com base em segurança, mas em conectividade, em outras palavras, a arquitetura descentralizada, porém resiliente da Internet atendia, em sua concepção, aos princípios que perpassavam as ideias de seus idealizadores nos anos 1960 durante o período que convencionou-se chamar de contracultura. Como elucida Bruce Schneier, renomado criptologista:

> A segurança de computadores existe há quase tanto tempo quanto os computadores. E embora seja verdade que a segurança não fazia parte do design da Internet original, é algo que tentamos alcançar desde o início. (tradução nossa).[57]

Obviamente, os seus desdobramentos demonstraram que protocolos de segurança eram necessários e compunham diversos serviços para os quais a Internet passou a ser utilizada.

Da mesma forma, ao incorporar o conceito de privacidade aos diversos diplomas legais europeus, os legisladores não supunham à época o quanto este conceito se tornaria fundamental nas relações sociais, sobretudo, no universo tecnológico no qual passamos a viver.

Pois bem, em um determinado momento histórico, estes dois conceitos passaram a ser complementares e norteados de boas práticas e programas de governança institucionais.

Não há, hoje em dia, possibilidade de se ter privacidade sem que os dispositivos que coletam dados pessoais por meio da Internet não atendam a determinados protocolos de

[57] No original: *Computer security has been around for almost as long as computers have been. And while it's true that security wasn't part of the design of the original internet, it's something we have been trying to achieve since its beginning.* In: SCHNEIER, Bruce. Security and the Internet of Things. Schneier on Security. 01 de Fevereiro, de 2017. Disponível em https://www.schneier.com/blog/archives/2017/02/security_and_th.html/ (verificado em 13/01/2022)

segurança estabelecidos pelos grupos que estudam e discutem o tema da segurança da informação.

É de importância capital para a fundamentação deste estudo que nos apoiemos em iniciativas de pesquisa já em andamento e que corroboram a nossa premissa de que os aspectos de segurança e de proteção de dados em desenvolvimentos de dispositivos conectados por meio de Internet das Coisas são não só necessários, como também norteadores dos novos paradigmas de privacidade e proteção em muitos países, especialmente naqueles que compõem a União Europeia e que pioneiramente inauguraram as discussões sobre o quão relevantes são os dados pessoais dos cidadãos nos mais diferentes contextos de tratamento, sobretudo quando içados por dispositivos eletrônicos por meio dos quais seus titulares desconhecem por completo tal ingerência.

No módulo apresentado na Figura 8, reproduzido da Agenda Estratégica de Pesquisa de Futuros Desenvolvimentos Tecnológicos[58], especialmente no item *Security and Privacy Technologies* – Segurança e Privacidade Tecnológicas – vemos claramente a preocupação com o desenvolvimento de protocolos que privilegiem a segurança e a privacidade do usuário em dispositivos de IoT numa evidente curva ascendente de inserção destes conceitos nos desenvolvimentos a partir do ano de 2020. Curiosamente, estes mesmos conceitos são privilegiados na agenda de pesquisa, bem antes da entrada em vigor do GDPR – Regulamentação Geral de Proteção de Dados – que ocorreu apenas em 25 de maio de 2018 do que se depreende que a cultura de proteção de dados e de privacidade em terras europeias antecede o regulamento acima citado, já que a Diretiva 95/46/CE, de 24 de outubro de 1995, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados[59] fomentou fortemente estes conceitos e os consagrou no regulamento de 2018 que tornou-se, inclusive, importante referência para a Lei Geral de Proteção de Dados Brasileira – Lei 13.709/2018.

[58] Vermesan, O.; Friess, P. (2013) *Internet of Things - Converging Technologies for Smart Environment and Integrated Ecosystems*. Denmark: River Publisher, 2013, p. 135.
[59] https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046 (Acesso em 13/01/2022)

*Figura 8 Strategic Research Agenda*

## Strategic Research Agenda

### Future Technological Developments

| Development | 2011–2015 | 2015–2020 | Beyond 2020 |
|---|---|---|---|
| **Power and Energy Storage Technologies** | • Energy harvesting (energy conversion, photovoltaic)<br>• Printed batteries<br>• Long range wireless power | • Energy harvesting (biological, chemical, induction)<br>• Power generation in harsh environments<br>• Energy recycling<br>• Wireless power | • Biodegradable batteries<br>• Nano-power processing unit |
| **Security and Privacy Technologies** | • User centric context-aware privacy and privacy policies<br>• Privacy aware data processing<br>• Virtualisation and anonymisation | • Security and privacy profiles selection based on security and privacy needs<br>• Privacy needs automatic evaluation<br>• Context centric security | • Self adaptive security mechanisms and protocols |
| **Material Technology** | • SiC, GaN<br>• Silicon<br>• Improved/new semiconductor manufacturing processes/technologies for higher temperature ranges | • Diamond | |
| **Standardisation** | • IoT standardisation<br>• M2M standardisation<br>• Interoperability profiles | • Standards for cross interoperability with heterogeneous networks | • Standards for automatic communication protocols |

Fonte: Vermesan, O.; Friess, P. (2013) *Internet of Things – Converging Technologies for Smart Environment and Integrated Ecosystems*, p. 135

Antecede o arrazoado puramente técnico, o entendimento do significado do vocábulo segurança que quando bem compreendido em muito auxilia o leitor a desnudar a essência do seu valor conceitual.

Segundo o dicionário Michaellis[60], a palavra segurança detém inúmeros significados, incluindo expressões de natureza profissional e até mesmo outras que se consolidaram ao longo do tempo consubstanciando a natureza sincrônica e diacrônica da língua nos termos de Ferdinand Saussure[61] para quem a língua poderia ser estudada durante um dado período (sincronia) e estudada ao longo do tempo (diacronia).

Para o escopo deste estudo, selecionamos alguns dos significados apresentados pelo dicionário que apontam para a direção que desejamos seguir. Inicialmente, segurança é o estado de quem ou do que se acha estável, sólido, firme, mas também pode ser o que protege de agentes exteriores, dando abrigo, proteção e resguardo. Pode, ainda, ser uma condição marcada por uma sensação de paz e de tranquilidade ou que está livre de danos ou riscos.

---

[60] https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/seguranca/ (Acesso em 13/01/2022)

[61] DE SAUSSURE, Ferdinand. Curso de linguística geral. Editora Cultrix, 2008.

Interessa-nos, particularmente, o sentido de proteção contra agentes exteriores que causem danos ou riscos. Entretanto, é importante salientar que a segurança sobre a qual dissertamos neste trabalho não se restringe ao ambiente computacional, mas se estende ao ambiente físico, visto que muitas das informações são compartilhadas indevidamente graças à ausência de mecanismos de ordem física que impeçam agentes maliciosos de terem acesso a informações que não deveriam ter.

A ISO (*Internacional Organization for Standartization*) é a maior organização de padronização no mundo e não se dedica apenas à segurança e tecnologia, além de ser um órgão não governamental e que tem a participação de mais de cento e sessenta países membros. Especificamente em relação à ISO 27001[62], vale destacar que seu escopo se consubstancia em implementar, operar, manter, revisar dentro de uma perspectiva de melhoria, sistemas de informação seguros, sejam eles físicos ou computacionais.

Vale também o registro de que os conceitos gerais sobre segurança citados anteriormente são os que aplicamos no estudo sobre a segurança da informação, área que se tornou fundamental a partir da popularização da Internet e de seus inúmeros recursos.

### 3.1.1 Hexagrama Parkeriano

O hexagrama Parkeriano, ou *Parkerian hexad*, é um conjunto de seis elementos da segurança da informação proposto por Donn B. Parker que acrescenta mais três propriedades às três outras constantes do triângulo CIA (*Confidentiality, Integrity, Availability* ou Confidencialidade, Integridade, disponibilidade).

Os atributos do hexagrama Parkeriano são os seguintes:

a. Confidencialidade.
b. Posse ou controle.
c. Integridade.
d. Autenticidade.
e. Disponibilidade.
f. Utilidade.

[62] A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação (ISO/IEC 27001:2013)

As propriedades acima descritas são consideradas aspectos únicos da informação e não se sobrepõem, de forma que em casos de violação de segurança uma ou mais dessas propriedades podem ser afetadas.

#### 3.1.1.1 Risco

O risco é a probabilidade que um atacante tem de se beneficiar de uma vulnerabilidade sistêmica e o seu correspondente impacto num determinado negócio ao qual aquele risco está atrelado. Por exemplo, se um *firewall*[63] tem diversas portas abertas, há maior probabilidade de um agente ameaçador usar uma delas para acessar a rede de forma não autorizada. Se um sistema de detecção de intrusão não for implementado na rede, haverá maior probabilidade de um ataque não ser percebido até que seja tarde demais.

#### 3.1.1.2 Ameaça

Uma ameaça é o indício da possibilidade de ocorrência de um incidente de segurança que pode ter como consequência prejuízos não só para o sistema, como também para a organização. Aquele que, normalmente, se utiliza da ameaça é chamado de atacante ou ameaçador.

As ameaças não se restringem ao ambiente digital, incluem também acessos físicos e processos que envolvem o comprometimento das pessoas com protocolos de segurança estabelecidos em políticas. Variam, além disso, de acordo com o nível de dependência de Estados e organizações aos sistemas interligados à Internet.

#### 3.1.1.3 Vulnerabilidade

O conceito de vulnerabilidade pressupõe a fraqueza ou ausência de proteção de um ativo que pode ser alvo de ameaças incluindo questões de natureza física, como a possiblidade de acesso de qualquer pessoa a uma sala com servidores, uma porta aberta no *firewall* ou a ausência de uma política de senhas.

---

[63] *Firewall:* "é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas". In: https://www.infowester.com/firewall.php. (Acesso em 13/01/2022).

#### 3.1.1.4 Exposição

A exposição se caracteriza a partir de um contexto de possíveis perdas provenientes de ataques a vulnerabilidades existentes no conjunto de sistemas e processos que envolvem a segurança da informação. É também o vetor que deve orientar as bases sobre as quais as políticas são implementadas, visto que o nível de exposição é o que aumenta ou diminui o risco de possíveis prejuízos.

#### 3.1.1.5 Contramedida ou salvaguarda

As contramedidas são um importante recurso para ser colocado em prática em situações de risco em potencial. Isto se dá na medida em que as políticas e procedimentos de segurança devem ser continuamente avaliados e testados para a observação da necessidade de mudança e/ou aprimoramento. E assim como as ameaças e as vulnerabilidades não se restringem aos riscos sistêmicos, mas a toda a cadeia de pessoas e processos.

## 3.2 Principais riscos de segurança em IoT

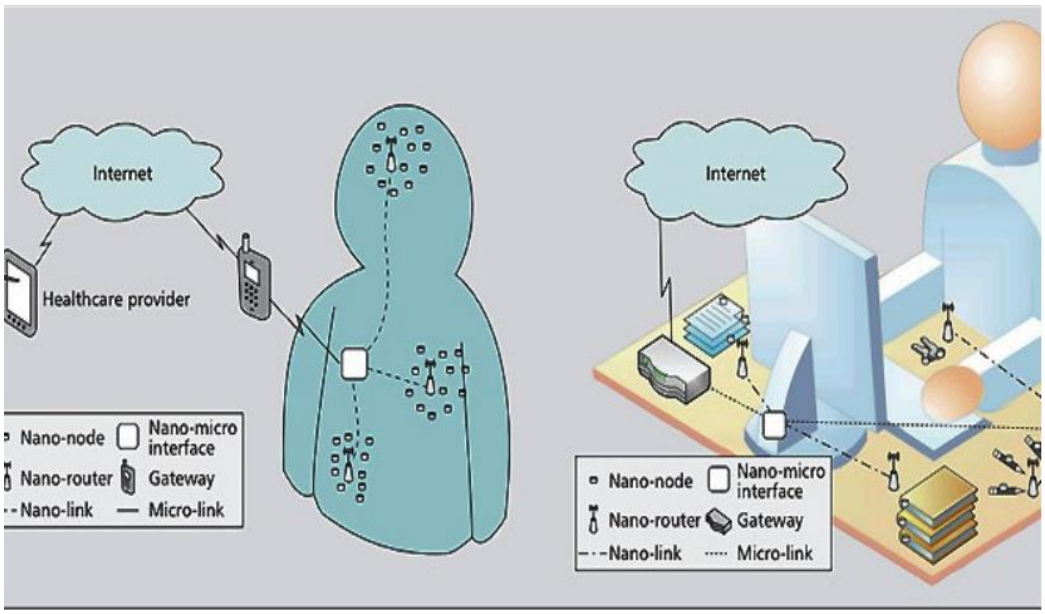
Não é difícil entender por que a segurança é um dos pontos mais críticos na adoção de dispositivos interconectados por meio de IoT. Todas os conceitos clássicos acima discutidos se aplicam ao contexto de IoT de forma ainda mais temerosa que em outros sistemas, arquiteturas e infraestruturas lógicas. Ou seja, quando os produtos, sistemas ou ambientes se descontrolam, os prejuízos e os danos podem ser irreparáveis pela simples e boa razão que ao fim e ao cabo, os dados que trafegam por esta tecnologia são dados, muitas vezes, pessoais e por essa razão, os incidentes de segurança ganham um contorno ainda mais aterrorizante.

Além disso, uma conhecida premissa de desenvolvimento também permeia os processos de desenvolvimento de dispositivos conectados por IoT, qual seja: segurança é inversamente proporcional à usabilidade. De fato, prioriza-se muito mais um sistema que seja fácil de ser usado ou até mesmo intuitivo, àqueles que necessitam de manuais de instrução, por exemplo. O produto para ser escalável precisa ser intuitivo, fácil de ser usado e prático e escalabilidade é uma característica fundamental no mercado de tecnologia.

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.

Outro ponto a ser considerado, quando se fala em segurança em IoT, diz respeito à mobilidade e ao tamanho dos dispositivos interconectados que podem chegar ao extremo das nano coisas criando o conceito de *Internet of Nano Things* – IoNT[64] que em muito tem sido utilizado para o desenvolvimento de dispositivos capazes de monitorar funções vitais do corpo humano, tal como apresentado na Figura 9.

*Figura 9 O funcionamento da Internet of Nano Things (IoNT)*




FONTE: SRINIVASAN (2019)

Há também uma outra questão bastante simples, mas extremamente importante a ser considerada quando tratamos dos riscos inerentes à segurança dos dispositivos interconectados por IoT: eles podem ser roubados ou perdidos o que compromete irremediavelmente a

[64] AKHTAR, Nikhat; PERWEJ, Yusuf. *The internet of nano things (IoNT) existing state and future Prospects*. GSC Advanced Research and Reviews, v. 5, n. 2, p. 131-150, 2020.

segurança dos dados que neles trafegam, inclusive porque podem expor a rede na qual estão conectados e a partir dessa informação, é possível se chegar a outras, como senhas de rede ou informações de endereçamento. Este é um tópico sobre o qual pouco se pensa ou mesmo se considera quando tratamos de segurança da informação, porque muitas vezes o leigo tende a pensar que grandes ataques cibernéticos pressupõem grandes esforços estratégicos e em muitos casos, a vulnerabilidade explorada é física, tanto com relação ao dispositivo em especial, quanto ao local onde dispositivos críticos estão instalados.

Segurança física complementa a segurança tecnológica, assim como o treinamento de pessoas sob o ponto de vista de protocolos seguros também corrobora com um cenário de maior segurança para as informações.

Para Moraes e Hayashi (2021)[65] há riscos também quanto aos dispositivos não acessíveis e conectados durante pouco espaço de tempo, sobretudo aqueles mais antigos cujo canal de comunicação não possibilita o uso de criptografia. Há também dificuldades em manter a segurança de dispositivos desconectados e é importante ressaltar que dispositivos IoT não são motores criptográficos, ou seja, sua comunicação com a Internet nem sempre ocorre em um canal seguro. Para os mesmos autores, também temos um problema quanto às chamadas senhas eternas que se referem às senhas que não podem ser trocadas, além dos dispositivos de vida curta que são aqueles alimentados por baterias, bem como os que usam *tags* ou RFID sem nenhum recurso de criptografia. Os autores destacam também a ausência de perímetro, visto que muitos dispositivos IoT são móveis e por isso podem se conectar tanto às redes 4G, quanto às redes Wi-Fi, além de alguns se conectarem diretamente à nuvem (*cloud)*. Quando existe perímetro, há a possiblidade pelo menos da instalação de um firewall, mas quando o perímetro não está demarcado, o controle é muito mais difícil. Por último, lembram que muitos dispositivos não são atualizados durante toda a sua vida útil e que muitos dispositivos por fazerem uso de senhas em texto claro podem facilmente sofrer ataques de negação de serviços distribuídos (DDoS – *Distributed Denial of Service*), além de outros tantos virem com portas de comunicação abertas facilitando a exploração de vulnerabilidades.

### 3.2.1 Controle de acesso e identidade em IoT

[65] MORAES, Alexandre de.; HAYASHI, Victor Takashi. Segurança em IoT. Entendendo os riscos e ameaças em Internet das Coisas. Alta Books. 2021. p. 39-43.

Falar em controle de acesso em sistemas IoT é uma tarefa que pressupõe a conjunção de inúmeros fatores em um ecossistema muito complexo que vai desde sensores, dispositivos de interação por linguagem natural, até os objetos inteligentes, tais como, máquinas, televisores, entre outros. De forma bastante simples, podemos dizer que o controle de acesso se refere a questões como por exemplo: como acender e apagar uma lâmpada em uma casa conectada. Como ter certeza de que o usuário é quem diz ser e que os diversos componentes do sistema também são confiáveis.

Para isso, é fundamental que combinemos dois aspectos que só funcionam suficientemente bem se estiverem intimamente relacionados, quais sejam, um bom controle de acesso e o gerenciamento robusto das credenciais dos usuários, de forma que sejam observadas as premissas básicas de segurança da informação relacionadas à confidencialidade, integridade e autenticidade das informações.

Do ponto de vista técnico[66], o tipo de controle de acesso mais utilizado em dispositivos IoT é o DAC – *Discretionary Access Control* que permite que para cada entidade, tenhamos uma lista de controle de acesso com pares do tipo: identificador-ação de maneira que todas as regras mapeiem usuário e ações permitidas em cada entidade-alvo. Este tipo de controle é comumente utilizado em dispositivos IoT, pela sua simplicidade. Outro conceito é o AAA – *Authentication, Autthorization and Accounting* que trata da possibilidade de aferir a identidade das entidades envolvidas no processo de comunicação entre dispositivo e plataforma, por exemplo. Diz respeito, ainda, à verificação das permissões do usuário para executar operações na plataforma IoT e por fim, referente à verificação da quantidade de recursos que o usuário consome durante seu acesso. Além disso, a *IoT Working Group* da *Cloud Security Alliance* (CSA)[67], recomenda a implementação de um servidor AAA que possibilite a definição de preferências e consentimento de uso e compartilhamento de seus dados.

Por fim, destacamos os principais métodos de autenticação em IoT: senha, token e biometria. Todos eles já conhecidos em função de serem utilizados para outros contextos tecnológicos, se resumem em aferir a identidade do usuário por meio de identificador e senha ou por meio de algum dispositivo como cartão ou chip, ou ainda por meio de um pré-cadastro em que baseados em características físicas, leitores de digitais ou câmeras identificam o usuário que está solicitando o acesso.

---

[66] Ibidem. p. 93-94.
[67] https://cloudsecurityalliance.org/research/working-groups/internet-of-things/ (Acesso em 13/01/2022)

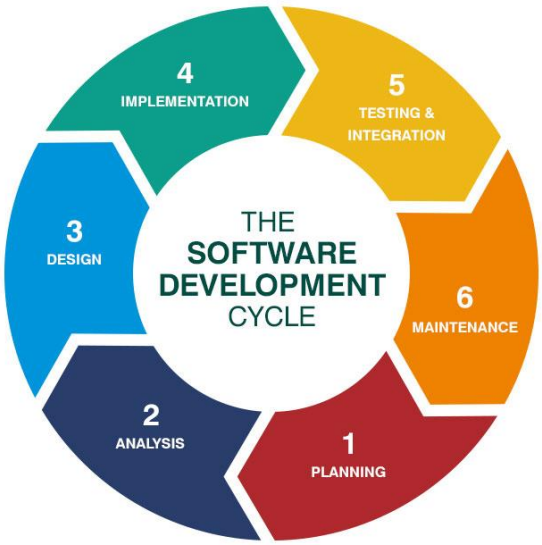
Idealmente, porém, a melhor alternativa é a combinação de múltiplos fatores, o que quer dizer que é possível que sejam utilizados dois ou mais dos recursos acima descritos num mesmo processo de autenticação para que, em caso de falha de um, o outro se sobreponha e consiga continuar garantindo a segurança do dispositivo. Neste ponto, voltamos à discussão já mencionada acima sobre a usabilidade e segurança, visto que a utilização de múltiplos fatores de autenticação ilustra à perfeição a opção de se utilizar apenas um desses métodos, visto que quanto mais camadas de segurança inserimos num processo de autenticação, menos prático, usável e acessível se torna o dispositivo. Não há, todavia, um meio termo para que se garanta a segurança sem que diversas camadas sejam sobrepostas, visto que um protocolo de segurança nunca é pensado a partir de um único mecanismo, pois este pode falhar por inúmeros motivos e um bom protocolo deve pressupor esta possibilidade.

## 3.3 Boas práticas

Uma boa escolha como prática de segurança em IoT é usar o método *Software Development Life Cycle* – SDLC (Ciclo de Vida de Desenvolvimento de Software), porque este método pressupõe a segurança em todas as fases do ciclo de desenvolvimento, desde a ideação, até os testes para o lançamento do software no mercado. Segundo SHYLESH[68], o "Ciclo de Vida de Desenvolvimento de Software é um processo usado pela indústria de software para projetar, desenvolver e testar softwares de alta qualidade". Uma visão simplificada do ciclo de desenvolvimento de software está ilustrado na Figura 10.

[68] SHYLESH, S. A Study of Software Development Life Cycle Process Models (June 10, 2017). Disponível em http://dx.doi.org/10.2139/ssrn.2988291 (Acesso em 13/01/2022)

*Figura 10 Ciclo de Vida de Desenvolvimento de Software simplificado*




Fonte: SHYLESH, 2017.

A definição de protocolos de segurança de um dispositivo IoT, assim como de qualquer outro produto de tecnologia deve estar presente desde a sua concepção em harmonia com outros requisitos de desenvolvimento de forma que na documentação do produto conste um módulo específico de segurança convergindo com outros módulos e complementando não só tecnicamente o produto, mas também atendendo a requisitos da legislação protetiva de dados pessoais e de privacidade vigente no Brasil.

A documentação do produto em desenvolvimento é tão importante que possibilita a tomada de decisões de forma mais assertiva e os ajustes que podem trazer grandes diferenciais para o produto no mercado. Atualmente, a inclusão de módulos de segurança e de requisitos de privacidade tornam o produto mais aderente, visto que a Lei 13.709/2018 – Lei Geral de Proteção de Dados brasileira privilegia a premissa do *privacy by design*, ou privacidade a partir da concepção, o que torna o produto não só legal como também mais robusto em termos de segurança, já que todos os protocolos seguros apresentam melhor performance quando são incluídos no projeto inicial. Segurança em sistemas legados ou em sistemas que foram desenvolvidos sem a perspectiva da segurança desde a sua concepção tornam o produto mais suscetível a ataques cibernéticos ou mesmo a falhas de autenticação ou de quaisquer outros protocolos inseridos posteriormente.

No processo de desenvolvimento, é importante a adoção de estruturas de segurança, a prática de segmentação de redes e a implementação de um sistema OTA (*Over The Air*) de entrega de atualizações sem fio, além de criptografia em tanto quanto possível e recomendável.[69]

Estruturas para segurança de redes, segurança da web, segurança de dispositivos móveis, criptografia, entre outros recursos estão disponíveis em larga escala para serem implementados aos processos de desenvolvimento, desde que respeitadas as suas configurações *by design* vez que o bom funcionamento dessas estruturas está intimamente relacionado ao seu padrão de desenvolvimento.

De todas as boas práticas listadas até aqui, consideramos que a implementação de um sistema OTA que se refere a vários métodos de distribuição de novas atualizações, muito provavelmente seja a mais importante, além é claro dos testes de vulnerabilidades (*pentests*) possíveis de serem realizados para a verificação de quão seguro é um sistema. Isto porque o contexto dos ataques cibernéticos é altamente dinâmico, de forma que um sistema considerado seguro hoje, pode não o ser amanhã em razão do fato de que vulnerabilidades antes não conhecidas podem ser exploradas, tornando o sistema crítico e passível de ataques de vários tipos de correção. Ocorre, porém, que um número significativo de ataques poderia ser evitado, caso estas vulnerabilidades, a maioria delas já conhecidas, fossem corrigidas. Fato que torna o processo de atualização e de testes fundamental para a garantia da segurança de produtos de IoT. Além disso, é importantíssimo que as metodologias utilizadas para realização dos *pentests* sejam pautadas em referências internacionais, tais como: OWASP Top 10[70] , SANS 25[71] e *Cyber Kill Chain*[72] .

Outro ponto já mencionado neste capítulo, mas de valor inestimável para a segurança dos produtos é o uso da criptografia de ponta a ponta, mas implementar criptografia apenas e tão somente não resolve o problema. Um sistema robusto e eficaz de gerenciamento de chaves é tão ou até mais importante do que o recurso criptográfico em si. Requisitos como: armazenamento seguro das chaves, identificação das chaves, autenticação de usuário e autorização de uso, ciclo de vida das chaves criptográficas, cópias de segurança das chaves criptográficas.

---

[69] SINCLAIR, Bruce. IoT: Como usar a Internet Das Coisas para alavancar seus negócios. Autêntica Business, 2018.
[70] https://owasp.org/ (Acesso em 13/01/2022)
[71] https://www.sans.org/ (Acesso em 13/01/2022)
[72] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Acesso em 13/01/2022)

## 3.4 Respostas a Incidentes e Protocolo de *Data Breach*

O mandamento disposto na Lei Geral de Proteção de Dados, em seu art. 48, prevê que o controlador deve comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança, quando esse pode provocar risco ou dano relevante aos titulares de dados[73]. Portanto, é notório que a segurança ultrapassa as medidas de segurança dispostas em organismos, tal como a já referenciada ISO. Embora padrões mundiais, tal como a padronização ISO 27001:2013 elenque a adoção de gestão e resposta a incidentes de segurança[74], a normatização brasileira, apesar de adotar o critério de risco ou dano relevante[75], há clara determinação de utilização de práticas de segurança a fim de evitar incidentes cibernéticos.

## 3.5 Da Política de Privacidade e de Segurança

Atine, portanto, que não há tão somente a necessidade de adoção de medidas e práticas de segurança, mas sim que, conforme previsto na legislação de dados nacional e outras regulamentações, tal como a Resolução nº 4.893 do Conselho Monetário Nacional[76], baixada pelo Banco Central, a qual em seu segundo artigo dispõe que as instituições que são contempladas nesta norma devem implementar e manter uma política de segurança cibernética.

Ademais, as políticas de segurança e políticas de privacidade preceituam e transparecem os parâmetros e objetivos pelos quais as organizações nortearam suas decisões e práticas quanto ao uso adequado das informações, bem como externalizam seu compromisso frente ao mercado.

---

[73] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

[74] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 27001:2013: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2013.

[75] A Autoridade Nacional de Proteção de Dados publicou em seu site a seguinte instrução: "Recomenda-se que os controladores adotem posição de cautela, de modo que a comunicação seja efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos. Ressalte-se, ainda, que eventual e comprovada subavaliação dos riscos e danos por parte dos controladores pode ser considerada descumprimento à legislação de proteção de dados pessoais." Disponível em https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca (Acesso em 13/01/2022).

[76] BANCO CENTRAL DO BRASIL. Resolução CMN Nº 4.893, de 26 de fevereiro de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Publicada no DOU de 1º/3/2021, Seção 1, p. 82/83.

# 4 PROTEÇÃO DE DADOS EM IOT: O GRANDE DESAFIO TÉCNICO-JURÍDICO

A proteção de dados, matéria que ganhou extrema relevância no Brasil nos últimos três anos em razão da sanção da Lei 13.709/2018, não é exatamente um tema recente, conforme veremos a seguir. Do ponto de vista internacional, remonta ao século XIX, muito embora tenha se desenvolvido com mais proeminência no século XX, especialmente a partir do advento da Internet.

Tendo sido objeto de profundos debates desde que se tornou pilar inarredável dos programas de governança das empresas dos mais diferentes portes e setores, o tema transcende os processos aos quais os tratamentos de dados estão sujeitos e, inevitavelmente, resvalam em discussões sobre coleta de dados automática e pelos mais diferentes dispositivos, sobretudo aqueles interconectados por Internet das Coisas.

Para além do compartilhamento dos dados humanos, há que se pensar sobre os dados compartilhados entre máquinas os quais, quase que em sua totalidade, não passam pelo consentimento de seus titulares.

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.

É tarefa inafastável do direito, em tempos de açodado desenvolvimento tecnológico, debruçar-se sobre os novos fenômenos sociais e alinhar seus institutos às novas condutas e aos novos desafios a que o homem tem se proposto não só como simplificação da vida cotidiana, mas também de desenvolvimento e superação dos limites humanos em tarefas até bem pouco tempo atrás impensadas para máquinas, robôs e inteligências artificiais.

## 4.1 Aspecto histórico da proteção de Dados

A tutela jurídica da proteção de dados é firmada de forma significativa dentro da sociedade burguesa, especialmente em razão ao direito à propriedade, pois, não é suficiente que

a proteção do bem – propriedade – não contemple o que ocorra dentro da mesma, ou seja, a proteção da privacidade. Tal premissa [77] é considerada, assim, o marco inicial do direito à privacidade conforme descrito no artigo "*The Right to Privacy"* de Louis Brandeis e Samuel Warren (1890)[78].

Brandeis, ao tornar-se juiz da Suprema Corte, proferiu um importante e icônico voto no caso *OLMSTEAD v. United States* de 1928, demonstrando que a privacidade não deveria restringir-se a grampos telefônicos e seu uso, mas sim considerando aspectos do futuro – até então, incertos – de novas tecnologias.

> Na aplicação da Constituição, nossa preocupação não deve ser somente sobre o que foi, porém o que será. O progresso da ciência, ao munir o governo de meios automatizados de espionagem, não irá parar com a escuta telefônica. Um dia, surgirão meios para que o governo, sem ter que remover papéis de uma gaveta, possa utilizá-los em juízo, tornando possível expor os fatos mais íntimos ocorridos dentro de uma casa. O progresso científico proporcionará meios para explorar crenças, pensamentos e emoções sequer expressas. [...]. Será possível que a Constituição não nos ofereça meios de proteção contra tais invasões da segurança individual?[79]

A privacidade e sua necessidade de contemplação expressa em forma de material ascendem de forma que a Declaração de Direitos Humanos de 1948, em seu artigo XII, as contemplam, tornando-se assim um direito fundamental, ultrapassando os limites e restrições anteriormente vinculadas a ela, quais sejam, privacidade na propriedade.

No território brasileiro, a proteção de dados marcou assento na ordenação jurídica a partir da Lei 7.232/84, a qual cuidou do tema da política nacional de informática, em específico em seu artigo 2º, VIII, que preceitua que as atividades de informática devem estabelecer mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados.

A proteção das informações ganha status de direito fundamental com a Carta Constitucional de 1988, especialmente por meio do instituto do *habeas data*, em seu artigo 5º, LXXII. Embora o remédio constitucional, segundo Alexandre de Moraes, seja um produto do período pós-ditadura militar e inspirada pelo *Freedom of Information Act*[80], segundo Frosini[81]

---

[77] ALVES, Alexandre Ferreira de Assumpção, et. Al. Problemas de direito constitucional. Rio de Janeiro: Renovar, 2001 p 113.
[78] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, dez. 1890.
[79] OLMSTEAD v. United States, 277 U.S. 438 (1928). Disponível no idioma original em inglês: https://supreme.justia.com/cases/federal/us/277/438/ (Acesso em 13/01/2022).
[80] MORAES, Alexandre de. Direito Constitucional. 13. ed. São Paulo: Atlas, 2003. p.116
[81] FROSINI, Tommaso Edoardo. *La Libertà Informatica: Brevi Note Sull'attualità Di Una Teoria Giuridica. Informatica E Diritto, XXXIV Annata,* Vol. XVII, 2008, n. 1-2, pp. 87-97

que aponta que direitos desta natureza são uma extensão da liberdade pessoal, ou seja, dispor de seus dados pessoais é um direito do cidadão, tal como dispor de seu corpo.

Segundo Doneda, a proteção de dados pessoais é associada ao direito à privacidade em diversas literaturas, o que marca o reconhecimento na tradição jurídica do direito à privacidade e posteriormente à proteção dos dados pessoais.[82]

Do ponto de vista formal, a Lei Geral de Proteção de Dados inicia sua tramitação na Câmara por meio do PL 4060/12, sendo o deputado Milton Monti (PR/SP) seu autor e no Senado Federal, por meio do PL 330/2013, de autoria do Senador Antônio Carlos Valadares.

Por fim, a Lei Geral de Proteção de Dados – Lei nº 13.709/2018 – é sancionada em 14 de agosto de 2018, alterada pela Lei nº 13.853/2019, bem como teve o prazo de entrada em vigor das suas sanções administrativas prorrogado pela Lei 14.010/2020.

## 4.2 O contexto da governança: boas práticas e transparência

Transparência é um conceito em foco no mercado de tecnologia e em inúmeros documentos e leis relativas à proteção de dados, tais como o GDPR[83] na União Europeia e a LGPD no Brasil.

É, por certo também, o conceito norteador das políticas de boas práticas fartamente utilizadas no meio corporativo, bem como fundamenta a relação de confiança e *accountability* entre o controlador de dados, nos termos do art. 6º, VI da LGPD e o titular das informações tratadas.

Com base na transparência, a utilização das informações pessoais coletadas, armazenadas e tratadas, nos mais diversos contextos, deve ser disponibilizada, tanto do ponto de vista do ciclo de vida do dado, como também em relação à sua finalidade, sob pena de direitos e garantias fundamentais não estarem sendo respeitados.

No caso específico deste estudo, a transparência deve nortear o desenvolvimento dos dispositivos de IoT que lançam mão das informações de seus usuários, sem que eles tenham conhecimento desta realidade e, dessa forma, não estabeleçam uma relação de confiança com os detentores ou controladores de dados.

---

[82] DONEDA, Danilo; et. al. Tratado de proteção de dados pessoais. 1 ed. Rio de Janeiro: Forense, 2021.

[83] Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (Acesso em 13/01/2022).

É imperativo, sob o viés da transparência, que toda e qualquer medida que vise à conformidade e à relação de observância dos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, não discriminação, responsabilização e prestação de contas, tal como disposto no art. 6º da LGPD, cumpram um ciclo que começa no organograma do software que será desenvolvido sob a premissa da IoT, integre os frameworks de privacidade das organizações e termine, fielmente documentados em políticas que estejam à disposição dos usuários para fins de atendimento administrativo, prestação de contas e fundamento de confiança das relações contratuais estabelecidas entre clientes e parceiros de negócios.

Os princípios aos quais as políticas de privacidade que dispositivos pervasivos precisam atender  perpassam a legislação protetiva de dados pessoais e todos os ajustes pelos quais as empresas e instituições públicas vem experimentando ao longo dos três últimos anos, a partir do GDPR, legislação que impulsionou a discussão sobre a necessária adequação dos padrões de privacidade, não só em países da União Europeia, como em todo o mundo, visto que este regulamento transcende os limites geográficos da sua jurisdição e contempla negociações comerciais com países cujo nível de proteção à privacidade seja inferior àquele proposto em sua legislação.

Ao discutir padrões de privacidade que envolvam dados humanos, é inafastável a análise sobre quais dispositivos realizam esta coleta, já que no mundo em que vivemos atualmente, dados estão muito mais próximos de máquinas que de humanos em razão da eficiência com a qual realizam operações de coleta, guarda e tratamento destes ativos.

## 4.3 A autodeterminação informativa e o consentimento válido

Para a efetiva aplicação de legislações protetivas de dados, especialmente quanto ao elemento da privacidade, a autodeterminação informativa torna-se conceito de observação imperiosa e dogmática, pois trata-se de elemento pelo qual, sem a devida consideração, o controle sobre os dados pessoais pode ruir.

Tal conceito é localizado no inciso II do Art. 2º da Lei Geral de Proteção de Dados, dispondo a autodeterminação informativa como fundamento do tratamento de dados no

Brasil. O referido conceito pode ser descrito como o direito de os indivíduos obterem poder para controlar e determinar o acesso e uso de seus próprios dados pessoais[84].

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'[85], a autodeterminação como medida abstrata é merecedora de atenção em suas aplicações, especialmente a partir de casos concretos.

Segundo SARLET[86], situa-se o direito à autodeterminação informativa a determinada decisão do Tribunal Constitucional Federal Alemão, de 15 de dezembro de 1983, dispondo que cada indivíduo possui a prerrogativa de decidir, de forma substancial, a divulgação e utilização de seus dados pessoais, contudo, não afirmando de forma prematura que o titular de seus dados possui o controle absoluto de suas informações, especialmente em razão da responsabilidade social.

No Brasil, o Supremo Tribunal Federal no acórdão publicado em 12 de novembro de 2020, na ADI 6387, a qual tratou sobre a Medida Provisória 954/2020, apresentou importante entendimento quanto à necessidade da clareza e precisão sobre o tratamento – neste caso, compartilhamento – de dados pessoais, e disponibilização de tais informações ao público, pois, não obstante a MP utilizar-se da pandemia causada pelo COVID-19, para justificar compartilhamento indevido, a corte superior entendeu que isso fere princípios basilares dos indivíduos, conforme se denota na ementa:

> EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. **1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na**

[84] DONEDA, Danilo; et. al. Tratado de proteção de dados pessoais. 1 ed. Rio de Janeiro: Forense, 2021, p. 64.
[85] REALE, Miguel. Lições preliminares de direito. 27 ed. São Paulo: Saraiva 2002, p. 18.
[86] Ibidem, p.69.

**medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.** 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não pode ser invocadas como pretextos para

> justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada. (ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO Dje-270 DIVULG 11-11-2020 PUBLIC 12-11-2020) (grifo nosso).

Em consonância com o princípio da autodeterminação informativa exposta nos casos, a Lei Geral de Proteção de Dados brasileira também estabelece o que seria o consentimento adequado e válido, relacionando-se assim com a ciência adequada do titular sobre o uso de seus dados.

O artigo 5º, inciso XII da referida legislação dispõe que o consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada[87]". Assim, o consentimento é enraizado de acordo com a possiblidade de o indivíduo determinar, de forma autônoma, o uso e processamento de seus dados pessoais.[88]

Ademais, Bioni em sua obra sobre os limites do consentimento[89] apresenta robusta pesquisa teórica sobre a dificuldade quanto à convergência do fluxo de informações e a informação e consentimento adequado, apresentando três estudos empíricos, concluindo que:

> O primeiro estudo empírico (subcapítulo 4.1.3.1) é clarividente sobre tal situação, evidenciando como funcionam tais modelos mentais vulneradores. Mais do que isso, ele denota o quão fundo é o buraco da assimetria informacional a ser escalado para que haja um efetivo controle das informações pessoais por seus titulares.
>
> O segundo estudo empírico (subcapítulo 4.1.3.2) expande esse déficit (informacional), coligando-o ao funcionamento e à inovação da tecnologia. A debilidade informacional do consumidor respinga na ausência de um conhecimento técnico que poderia tornar a tecnologia um instrumento de melhora do gerenciamento do fluxo informacional. No entanto, o que tais evidências empíricas assinalam é, justamente, o contrário. A tecnologia tem

[87] Art. 6º, inciso I da LGPD.
[88] DONEDA, Danilo. Da Privacidade à Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020. p. 287-296
[89] BIONI, Bruno Ricardo. Proteção de dados pessoais: funções e limites do consentimento. Rio de Janeiro: Forense, 2 ed. 2020, p. 221-222.

> sido utilizada para neutralizar essa possível habilidade, fragilizando, ainda mais, o elo mais fraco do mercado informacional.
>
> O terceiro estudo empírico (subcapítulo 4.1.3.1) sedimenta essas discrepâncias sob um olhar mais amplo: a assimetria é estrutural e é decorrente da própria dinâmica da economia dos dados pessoais. O diagnóstico de que os consumidores estão resignados com a perda do controle de suas informações é o efeito colateral – e por que não a própria ferida aberta – dessa nova vulnerabilidade, na qual o elo mais fraco rende-se (resigna-se) às forças do mercado informacional.

Denota-se assim que, existe no titular de dados uma vulnerabilidade, a qual é explorada, pois a ciência e informação sobre o tratamento de dados pessoais e suas respectivas finalidades não se faz de maneira clara ao usuário.

Se, a partir dos meios cotidianamente utilizados a informação adequada e o consentimento deixam as especificações da legislação protetiva de dados à deriva, contempla-se então que a IoT propõe desafios ainda mais específicos quanto à subsunção do fato à norma. Consoante ao desafio posto, Cunche, Morel & Métayer[90], discorrem sobre alguns requisitos para devida informação e consentimento, utilizando-se técnicas para executá-los.

Inicialmente, os autores são motivados pelas diretrizes dispostas no *Article* 29 *Data Protection Working Party*, o que propõe instruções para fiel adoção e cumprimento de práticas para exercício do consentimento válido[91], conforme estabelecido no Regulamento Geral Europeu de Proteção de Dados (GDPR), o qual possui grande similaridade ao consentimento disposto na LGPD.

Os autores[92] principiam seus argumentos a partir de requisitos gerais sobre a informação e consentimento adequado, sendo a IoT o pressuposto necessário, contempla-se a

---

[90] Cunche, M; Métayer, D; Morel, V. *A Generic Information and Consent Framework for the IoT*. 2019 18th IEEE *International Conference On Trust, Security And Privacy In Computing And Communications*.

[91] *Article 4(11) of the GDPR* define o consentimento como: "qualquer indicação dada livremente, específica, informada e inequívoca da vontade do titular dos dados, pela qual ele, por uma declaração ou por uma ação afirmativa clara, signifique concordar com o tratamento de dados pessoais que lhe digam respeito". Tradução nossa do original "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

[92] V. Morel, M. Cunche and D. Le Métayer, "*A Generic Information and Consent Framework for the IoT*". *18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering* (TrustCom/BigDataSE), 2019, pp. 366-373, doi: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00056 (Acesso em 13/01/2022).

figura dos titulares de dados "TD" (*Data Subject*) e controladores de dados "CD" (*Data Controllers*)[93]. Neste estudo, os autores assumem que os dispositivos dos controladores de dados (*Gatewey Devices*) são aptos a coletarem e comunicarem informações dos titulares de dados. Ainda, distinguem os autores entre política de privacidade dos titulares de dados como as determinações dadas pelos titulares em face de seus dados pessoais, e política de privacidade dos controladores, como as práticas de tratamento declaradas/documentadas pelo agente de tratamento[94].

Assim, é proposto um *framework* geral quanto ao respeito das referidas características, da seguinte forma: a política de privacidade dos controladores deve conter todas as informações necessárias, incluindo quais são os dados pessoais coletados e em qual momento as informações poderão ser tratadas; as informações dispostas na política devem ser notificadas ao titular, observando a distância do aparelho do controlador que permitirá o tratamento de dados; e deve-se apresentar as informações ao titular de forma e a tempo de que esse tenha não perca qualquer informação útil ou seja fadigado pela estrutura da apresentação das informações.

Quanto ao consentimento, os TD devem expressar sua manifestação de vontade a tempo suficiente de minimizar fadiga quanto à formatação, decidindo assim sobre seus próprios dados pessoais; o CD deve receber a notícia do consentimento que habilita a coleta dos dados, e garantir que não haverá coleta – ou os dados serão deletados imediatamente – caso o consentimento não seja consistente com sua política de privacidade; e armazenar o consentimento de forma adequada, a fim de demonstrar sua adequação ao GDPR, especialmente sobre quais dados dos titulares de dados são mantidos.

As interações entre os titulares de dados e os controladores, segundo os autores, devem ocorrer em duas partes: i.) interação do titular com o dispositivo e ii.) a comunicação entre o dispositivo do titular e os dispositivos do controlador[95].

Castellucia[96], também acompanhada de Métayer, um dos autores do estudo apresentado, objetivando alcançar a transparência e consentimento na IoT, raciocinaram de forma preliminar, associando as preposições expostas anteriormente, porém de forma mais tímida, assumindo a posição de que todas as informações sobre a coleta de dados e dispositivos que servirão de ferramentas para tal devem ser comunicadas eletronicamente aos titulares, os

[93] Optou-se aqui em adaptar a abreviação dos autores ao português (BR).
[94] Ibidem p.2
[95] Ibidem, p.2.
[96] CASTELLUCCIA, C. et al. Enhancing Transparency and Consent in the IoT. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2018, pp. 116-119, doi: 10.1109/EuroSPW.2018.00023.

quais devem ser capazes de expressar suas próprias escolhas, permitindo ainda o registro de tais decisões.

Outra possibilidade de *framework* para devida coleta de consentimento é apresentado por CHIKUKWA (2021), o qual segrega as etapas de seu framework da seguinte forma[97]: 1.) Coleta de Dados; 2.) Coleta de Consentimento; 3.) Gestão do Consentimento; 4.) Execução do Consentimento; e 5.) Auditoria de Consentimento.

Na primeira etapa, é detalhado que dispositivos conectados por IoT coletem dados pessoais por meio de sensores internos e transmitidos através de um *gateway*; em seguida, o consentimento deve ser coletado por meio de *logging in*, ou seja, por meio do *front-end* da aplicação, o usuário irá interagir com a base de dados do dispositivo IoT (*back-end*). Nesta etapa, o titular de dado deve ser informado sobre o tratamento de dados, por exemplo, com uma notificação (pop-up), a fim de que este tome sua decisão de maneira livre, informado e específica; quanto ao *Consent Manegement*, urge em razão da demanda de prestação de contas e comprovação de conformidade com as legislações, no caso, do GDPR; o *Consent Enforcement* aborda a etapa na qual o controlador monitora o acesso de terceiros aos dados pessoais coletados e tratados; por fim, o *Consent Auditing* se refere à auditoria e exames frequentes das etapas, processos de tratamentos e validação de *compliance*[98].

## 4.4 Boas Práticas e medidas técnicas LGPD e menção a alguns padrões internacionais

A proteção de dados regulada na Lei Geral de Proteção de Dados limita-se aos dados pessoais, os quais são tratados pelos agentes de tratamento (art. 5º, IX). Segundo mandamento legal, os referidos agentes devem adotar medidas de segurança técnicas e administrativas aptas a protegerem os dados pessoais (art. 46), observando a privacidade desde a concepção do produto ou do serviço até sua execução (art. 46, §2º).

Não obstante, a LGPD se aplica tanto aos dados pessoais tratados nos meios físicos, quanto digitais, o que, afeta dispositivos conectados por IoT de forma peremptória.

A interconectividade e a interoperabilidade, somadas à gama de possibilidades de fluxos e compartilhamentos de dados, especialmente dados pessoais, em tecnologias e serviços

[97] Do original*: 1.) Data Collection; 2.) Consent Collection; 3.) Consent Management; 4.) Consent Enforcement; e 5.) Consent Auditing.*

[98] Chikukwa, G. *A Consent Framework for the Internet of Things in the GDPR Era* (2021). *Masters Theses & Doctoral Dissertations. Dakota State University*. Disponível em https://scholar.dsu.edu/theses/362 (Acesso em 13/01/2022)

que utilizem a inteligência produzida a partir da IoT, devem cumprir os requisitos definidos pela legislação protetiva de dados pessoais.

Inicialmente, etapa imprescindível para devida aplicação da proteção de dados em IoT é a devida identificação dos atores, pois, é preciso que se saiba quem são os responsáveis pela adoção de medidas de boas práticas e segurança, bem como pela falta delas. Ao considerar os atores, a coexistência entre os diversos agentes envolvidos dentro de um ecossistema de IoT é variável, podendo assim alterar de cenário a cenário.

Em suas recomendações, o ITU – *International Telecommunication Union*, aponta que existem, ao menos, os seguintes atores: *device provider* (provedor de dispositivo); network *provider* (provedor de rede); *platform provider* (provedor de plataforma); *application provider* (provedor da aplicação); e *application customer* (cliente da aplicação)[99]. Ainda, é possível localizar a existência de outros atores, tais como os *Data Brokers (*agentes responsáveis pela venda de informações), *Gatekeepers* (agentes que servem como portões de acesso à determinados ambientes ou serviços e produtos), *Data Providers (*provedores de dados), *Service Consumer* (consumidor de serviços)[100].

As múltiplas conexões possíveis a partir do desenvolvimento da IoT demanda que todos os agentes, adotem medidas de boas práticas aptas a protegerem as informações.

Ocorre que, tal como à Lei Geral de Proteção de Dados criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável, entre outras funções, por promover e elaborar estudos sobre práticas nacionais e internacionais de proteção de dados (art. 55-J, VII), outras autoridades protetivas de dados já se manifestaram sobre alguns padrões para a proteção e o uso adequado dos dados pessoais.

A Agência Espanhola de Proteção de Dados (AEPD), trata sobre medidas seguranças de forma segmentada, buscando não a relação de todas as medidas, independente do contexto e dos dispositivos, mas sempre observando os cenários e suas respectivas particularidades. Alguns dos estudos elaborados pela agência hispânica sobre riscos e IoT são: IoT (I): *Qué Es Iot Y Techno Son Sus Riesgos*[101]; IoT (II): *Del Internet De Las Cosas Al Internet De Los*

---

[99] *Telecommunication Standardization Sector Of Itu. Itu-T*. Series Y: Global Information Infrastructure, Internet Protocol Aspects And Next-Generation Networks: Overview of the Internet of Things (*Recommendation ITU-T Y.2060*). Aprovado em 15 jul 2012. Disponível em: https://www.itu.int/rec/T-REC-Y.2060-201206-I/en. (Acesso em 13/01/2022).

[100] HADZOVIC, Suada; MRDOVIC, Sasa; RADONJIC, Milutin. *Identification of IoT Actors*. Sensors 2021. Disponível em https://doi.org/10.3390/s21062093. (Acesso em 13/01/2022).

[101] Disponível em https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-i-que-es-iot-y-cuales-son-sus-riesgos (Acesso em 13/01/2022).

*Cuerpos*[102]; e IoT (III) *Domótica*. *Internet De Las Cosas: Riesgos Y Recomendaciones* [103] – contemplando a identificação de alguns riscos para fins de mitigação de danos, tais como a possibilidade do sequestro dos dispositivos, bem como o controle destes dispositivos por terceiros, além de vazamento de dados.

O Governo do Reino Unido em 2018, publicou um guia denominado *Code of Practice for Consumer IoT Security*[104], recomendando medidas de fortalecimento de senhas, política de de análise de vulnerabilidades, comunicação segura, testes de integridade do software, repetição da validação dos dados inseridos, facilitação da eliminação de dados pessoais, monitoramento do sistema, entre outros.

Na França, a *Comission Nationale Informatique & Libertés* (CNIL), avançando na temática da proteção de dados em IoT, propõe, não apenas medidas de controle e segurança, como criptografia, anonimização dos dados, controle de acesso lógico e monitoramento da integridade, tal como exposto no artigo *Privacy Impact Assessment (PIA) – Aplication to IoT devices*[105], contemplando assim a análise de impacto e riscos específicos a dispositivos que usufruem da interconectividade proporcionada pela IoT.

Ainda, padrões de segurança no desenvolvimento de IoT *applications* são sugeridos pela FTC - *Federal Trade Commision*[106] *(USA)*, apontando a adoção de medidas de autenticação e controle de acesso, práticas de segurança já reconhecidas (melhores práticas), monitoramento de riscos e comunicações efetivas.

## 4.5 Direito à Portabilidade e IoT

O direito à portabilidade ampara o titular de dados na possibilidade de portar seus dados pessoais a outro fornecedor de serviço ou produto, conforme consta no art. 18, V, da LGPD, o qual, segundo Bergstein, afirma possuir duas dimensões, sendo uma delas assegurar ao titular de dados a possibilidade de obter cópia de suas informações em adequado formato, e

[102] Disponível em https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-ii-del-iot-al-iob (Acesso em 13/01/2022).
[103] Disponível em https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-iii-domotica (Acesso em 13/01/2022).
[104] Disponível em https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security (Acesso em 13/01/2022).
[105] Disponível em https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf (Acesso em 13/01/2022).
[106]Disponível em https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-keeping-internet-things-secure. (Acesso em 13/01/2022).

obrigando o controlador a disponibilizar os dados em formato que outro fornecedor de produtos ou serviços consiga utilizar[107]. Um exemplo do referido direito trata de prática adotada pelo Google, o qual permite que seus usuários realizem o *download* de arquivos que contenham suas atividades[108].

Neste passo, observamos novos desafios ao atendimento à portabilidade e IoT, pois ocorre aqui o chamamento da interoperabilidade para efetivação do direito posto pela LGPD.

Conforme mencionado neste trabalho, a ausência de padrões de interoperabilidade, a variedade de protocolos sem fio, os problemas de latência e as desafiadoras práticas de segurança integram, do ponto de vista técnico, complexificam o cenário de coleta de dados realizada por Internet das coisas – IoT.

Haja vista que, conforme preconiza a legislação, a portabilidade determina que o controlador disponibilize os dados em formado 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. Turner et al[109], realizaram um estudo prático quanto ao exercício da portabilidade de dados provenientes de um controlador a outro controlador, fundamentando-se no Art. 20 do GDPR para exercício de seus direitos.

O estudo foi divido em duas etapas, sendo que em sua primeira, os autores analisaram 160 políticas de privacidade de desenvolvedores/produtores de IoT, buscando entender qual o nível de informação sobre exercício de seus direitos preconizados no GDPR é informado aos titulares de dados[110]. Ato contínuo, os autores testaram a viabilidade ou disponibilidade dos sistemas IoT operacionalizam o direito de portabilidade[111].

Quanto à análise das políticas de privacidade, os autores identificaram que as informações sobre o direito à portabilidade são mínimas, sendo que a minoria habilita o exercício do referido direito[112].

---

[107] BERGSTEIN, L. Direito à Portabilidade na Lei Geral de Proteção de Dados. Revistas dos Tribunais, vol. 1003/2019, maio, 2019.
[108] JANAL, R. *Data Portability – A Tale of Two Concepts*, 8. JIPITEC 59, 2017, p.60.
[109] TURNER, S. et. al. *The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment.* New Media & Society, 2021, vol. 23(10) **p. 2861-2881**.
[110] Ibid, p.2861
[111] Ibid.
[112] Ibid, p.2875

Ademais, para realização do experimento prático, a fim de demonstrar a aplicação do exercício dos direitos preconizados no Art. 20 (1) [113] e (2)[114] do GDPR. O experimento foi realizado a partir da seleção de alguns dispositivos (*Device* 1), sendo que haveria a tentativa de transmitir os dados de um dispositivo a outro (*Device* 2). Os dispositivos escolhidos pelos autores foram (a) *Garmin Vivosmart 4* (*software version* 2.90.0.0), (b) *Fitbit Charge 3* (*firmware version* 28.20001.60.39), e dois assistentes domésticos (c) *Amazon Echo* (*software version* 641575220) e (d) *Google Home* (*firmware version* 156414)[115].

Os dispositivos foram utilizados pelo período de 3 (três) semanas, a fim de coletarem alguns dados pessoais. Ao final, os resultados estão apresentados na Figura 11.

*Figura 11 Resultados direito a portabilidade GDPR Art. 20 (1)*

**Table 2.** Article 20(1) result overview.

| Device 1 → Device 2 | (a) Received personal data | (b) Structured, commonly used, machine-readable | (c) Import possible | (d) Request method | (e) Timely | Issues encountered |
|---|---|---|---|---|---|---|
| Garmin → Fitbit | Yes | Yes | No | Button | Yes | File/folder structure; lack of explanation of files |
| Fitbit → Garmin | Yes | Yes | No | Button | Yes | Data within CSV files not structured to be machine-readable |
| Amazon Echo → Google Home | Yes | n/a | No | Form | Yes | Account exercise requested for not account used in the initial exercise |
| Google Home → Amazon Echo | Yes | Yes | No | Button | Yes | Home search activity amalgamated with general search activity |

CSV: Comma Separated Values.

Fonte: Turner, S. et. Al (2021).

Assim, compreende-se que os dispositivos receberam dados pessoais; os estruturaram de forma comum para a leitura computacional; não possibilitaram a importação de informações; possuíam métodos de requisição dos direitos; cumpriram o prazo disposto na legislação; sendo que os problemas encontrados vão desde ausência de explicação dos arquivos, ausência de

[113] GDPR: Artigo 20º, 1: O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: a) O tratamento se basear no consentimento dado nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a), ou num contrato referido no artigo 6.o, n.o 1, alínea b); e b) O tratamento for realizado por meios automatizados.

[114] GDPR. Artigo 20º, 2: Ao exercer o seu direito de portabilidade dos dados nos termos do n.o 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

[115] TURNER, S. et. al. *The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment*. New Media & Society, 2021, vol. 23(10), **p. 2869**.

estruturação no arquivo CSV, alteração da especificação de conta e confusão entre atividades gerais e “home”.

Ao analisar a possibilidade e exercer o direito preconizado no Art. 20 (2), os autores não conseguiram exercitá-lo, conforme se pode observar na Figura 12.

*Figura 12 Resultados direito a portabilidade GDPR Art. 20 (2)*

**Table 3.** Article 20(2) result overview.

| Device 1 → Device 2 | (a) Direct transmission follows same process with Device 1 as receipt of data in Art 20(1)? | (b) Direct transfer mentioned in privacy policy? | (c) Direct transfer technically feasible for Device 1? | (d) Direct transfer technically feasible for Device 2? |
|---|---|---|---|---|
| Garmin → Fitbit | No | No | No | No |
| Fitbit → Garmin | No | No | No | No |
| Amazon Echo → Google Home | No | No | No | No |
| Google Home → Amazon Echo | No | No | No | No |

Fonte: Turner, S. et al. (2021)

Assim, entre os dispositivos testados, nenhum deles possuía o mesmo processo de transmissão direta com o dispositivo 1; não mencionavam a transferência direta em sua política de privacidade; não possuíam viabilidade para transferência direta para o dispositivo 1; e não possuíam viabilidade para transferência direta ao dispositivo 2.

O direito à portabilidade de dados pessoais em tecnologias IoT poderia ser comparado à clássica régua de lesbos[116], uma vez que mesmo ciente da dificuldade ímpar para se estabelecer padrões e protocolos comuns entre as tecnologias de transmissão, que venham convergir para o efetivo cumprimento do direito, há a latente necessidade de que os dispositivos se adequem para evitar a inefetividade da norma.

Ademais, resta à ANPD, conforme estabelece o Art. 18, inciso V da LGPD, regulamentar o *modus operandi* do direito à portabilidade, devendo contemplar a gama de variáveis propostas pela IoT.

## 4.6 IoT e Dados Anonimizados

Os dados pessoais são informações que se relacionam a pessoas naturais identificadas ou identificáveis[117], distinguindo ainda a legislação os dados pessoais de dados pessoais

[116] A qual se adapta a todas as superfícies, sem perder sua utilidade e características.
[117] Art. 5º, I da LGPD.

sensíveis, que são informações de natureza mais intrínsecas, visto, pois, são mais aptos a provocar contextos de desigualdade e discriminação.[118]

A legislação nacional de proteção de dados define dados pessoais sensíveis como:

> dado pessoal sobre 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, quando vinculado a uma pessoa natural[119];

A compreensão sobre o que são dados e seus significados é um dos motores que potencializa o mercado e órgãos públicos o valor dos dados pessoais[120].

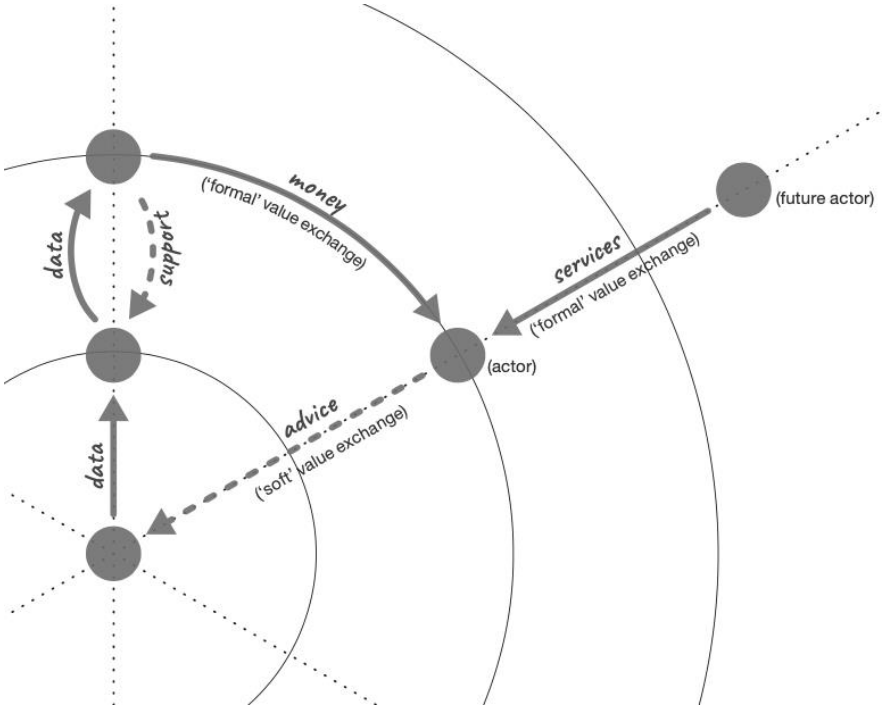
Conforme sustenta Korunovsca e Spiekermann (2017), a partir da ótica dos provedores de serviço, as pessoas compartilham seus dados pessoais em troca de serviços gratuitos, de livre vontade, entretanto, os serviços são gratuitos justamente por receberem dados pessoais[121].

Em 2019, o *Open Data Institute*[122] dispôs, de forma simplificada, uma breve exposição do ecossistema dos dados, conforme se verifica na Figura 13.

---

[118] NEGRI, S. M. C. A; KORMAZ, M. R. D. C. R. A Normatividade Dos Dados Sensíveis na Lei Geral de Proteção de Dados: Ampliação Conceitual e Proteção da Pessoa Humana. Revista de Direito, Governança e Novas Tecnologias, Goiânia, v. 5, n.1, p. 63-85, jan/jun de 2019.
[119] Art. 5º, II da LGPD.
[120] Meglena Kuneva, membra da *Consumer Comissioner,* proferiu a reconhecida frase: "*Data is the new oil"*, em seu discurso, disponível em https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156 (Acesso em 13/01/2022).
[121] Spiekermann, S.; Korunovska, J. *Towards a value theory for personal data*. Journal of Information Technology (2017).
[122] Disponível em: https://theodi.org/article/data-ecosystem-mapping-tool (Acesso em 13/01/2022).

*Figura 13 Ecossistema dos dados*




Fonte: ODI - *Open Data Institute* (2019)

Assim, denota-se que, no ecossistema destacado, os dados e os atores envolvidos colaboram, de forma estruturada, o uso, suporte, conversão das informações em serviços aos futuros atores da relação.

Tal ecossistema é construído a partir da perspectiva de *Big Data*, que, segundo Pfeiffer[123] em seu estudo sobre Economia Digital, *Big Data* e Legislação Antitruste, aponta que o *Big Data* possui como características os 5 "Vs", quais sejam: Volume, Velocidade, Variedade, Valor e Verificabilidade.

A estrutura e os dados produzidos e gerados, especialmente em razão da frequente interconectividade, somado a incentivos de mercados e estímulos de necessidades de inclusão, apontam que os dados pessoais permitem enxergar os titulares de dados de forma ainda mais singular, a partir de preferências individuais[124].

[123] PFEIFFER, Roberto Augusto Castellanos. "Digital Economy, Big Data and Competition Law" (February 27, 2019). In: Market and Competition Law Review, volume III, n. 1, April 2019, p. 53-89. Available at SSRN: https://ssrn.com/abstract=3440296

[124] MACHADO, F. I. S; RUARO, R. L. Publicidade Comportamental, Proteção de Dados Pessoais e o Direito do Consumidor. Conpedi Law Review, v.3, n. 2, p. 421-440, 2017.

A despeito da importância da personalização das informações, ou seja, do uso de dados pessoais propriamente ditos, a LGPD também contempla a possibilidade do uso de dados de titulares não identificados, denominados como dados anonimizados. No Art. 5º, inciso III, a lei dispõe que o dado anonimizado é um dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Outrossim, ocorre que a anonimização pode ser, na verdade, uma pseudoanonimização, que é quando o procedimento de anonimização seja possível de retorno ao status anterior.

Como se vê, Doneda dispõe sobre o entendimento de que tais técnicas podem minimizar riscos sobre o tratamento de dados:

> A chamada "anonimização" de dados pessoais – a retirada do vínculo da informação com a pessoa a qual se refere – é um recurso que algumas leis de proteção utilizam para diminuir os riscos presentes no seu tratamento. A mitigação de riscos é também obtida com técnicas como a da pseudonimização que, embora não torne o dado anônimo, pode dificultar a identificação do titular e é um recurso bastante utilizado.[125]

Enquanto a LGPD não conceitue a pseudoanonimização, da mesma maneira que dados anonimizados (Art. 5º, XI) ou anonimização (Art. 5º, III), o Regulamento Geral Europeu de Proteção de Dados o faz, em seu Art. 4º:

> Pseudonimização, o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável (GDPR).

Ainda, a já referenciada AEPD, em seu guia sobre *10 Maletendidos Relacionados con la Anonimización* reforçam o mesmo entendimento antes exposto, pois o uso de informações

[125] DONEDA, Danilo. Da Privacidade à Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020. p. 142.

adicionais pode colaborar para supor ou inferir indivíduos, sendo que os dados anônimos não permitem mais a associação[126].

Portanto, em que pese a relevância das informações personalizadas, o uso de técnicas de anonimização de dados converge com a diminuição do risco do tratamento de dados. Mas, seria viável que tecnologias IoT se utilizassem destas técnicas a fim de proteger a privacidade dos usuários?[127]

Inicialmente, Garcia e Neves (2021) em sua exposição no Congresso Brasileiro de Software, não localizaram soluções que conseguissem atingir a privacidade de dados baseando-se em anonimização, pois cada ambiente possui suas características[128]. Ademais, segundo Andrade (2019), é condição para maior aceitação dos titulares de dados a segurança e a confiabilidade quanto à estrutura e privacidade em ambientes de IoT[129], sendo que a anonimização serviria como mecanismo de segurança e preservação da privacidade dos titulares de dados[130].

Andrade (2019), como proposta, sugere que as tecnologias que utilizam IoT possuam um *Privacy-IoT-anonymize*, a fim de que os dados sejam anonimizados antes que seja enviado ao solicitante, sugerindo ainda como mecanismo de anonimização de dados em áudio a conversão do discurso em texto, com a posterior leitura com voz de máquina, despersonalizando assim o dado pessoal tratado[131].

Assim, em que pese o valor dos dados e o conhecimento dos indivíduos que podem ser gerados a partir de dispositivos IoT, a anonimização possui grande valor para mitigação de riscos no tratamento de dados, permitindo que a privacidade dos indivíduos seja um parâmetro imperativo no desenvolvimento de novos serviços e produtos, como a lei nacional de proteção de dados espera[132].

---

[126]Disponível em https://www.aepd.es/es/documento/10-malentendidos-anonimizacion.pdf (Acesso em 13/01/2022)

[127] "*Within this emerging IoT framework, a dizzying array of issues, questions, and challenges arise. One of the biggest questions revolves around living in a world where almost everything is monitored, recorded, andanalyzed. While this has huge privacy implications, it also influences politics, social structures, and laws*." In: GREENGARD, Samuel. *The Internet Of Things*. Cambridge: The MIT Press, 2015, p. 58

[128] NEVES, Flávio S.; GARCIA, Vinicius Cardoso; BONFIM, Michel Sales. Um Mecanismo Para Recomendação De Algoritmos De Anonimização De Dados Baseado No Perfil Dos Dados Para Ambientes Iot. In: Workshop De Teses E Dissertações (WTDSOFT) - Congresso Brasileiro De Software: Teoria E Prática (CBSOFT), 12. , 2021, Joinville. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 10-18.

[129] ANDRADE, Leandro Prado de. *Privacy Everywhere*: Mecanismo Para Tomada De Decisões E Garantia Da Privacidade Em Ambientes IoT. 2019. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de São Carlos, São Carlos, 2019.

[130] Idem, p.34.

[131] Idem, p.75.

[132] Art. 46, §2º da Lei Geral de Proteção de Dados.

# 5 LEI, SOCIEDADE, MERCADO E INTERNET DAS COISAS

Do ponto de vista temporal, poderíamos dizer que IoT é uma novidade, já que o termo surgiu em 1999, há exatos vinte e três anos. Todavia, quando se analisam os fenômenos de tecnologia, há que se ter um cuidado com o vocábulo novidade, uma vez que a alternância de novidades é muito veloz e a abrangência de cada uma delas, segue o mesmo padrão. Disso deduzimos que embora jovem, a IoT já está bastante incorporada ao universo acadêmico e ao mercado nacional e internacional.

A discussão sobre avanços tecnológicos ao longo da história, porém, é algo bastante controverso. A obra *Why the West Rules – For Now – The Patterns of History and What they Reveal About the Future*, em tradução livre, "Por Que O Ocidente Domina – Por Enquanto – Os Padrões Da História e o Que Eles Revelam Sobre O Futuro", de Ian Morris[133] considera o ano 14.000 a.C como o marco inicial do progresso da humanidade, uma vez que esta é a data que inaugura o período em que o planeta começa a esquentar, mas outros marcos temporais são citados frequentemente como importantes datas que apontam impulsos significativos do homem ao longo da história. De todos estes marcos e para o objetivo específico deste trabalho, visto que este estudo discute a confluência entre direito e tecnologia, especificamente IoT, concordamos com o autor que a invenção da máquina a vapor, na segunda metade do século XVIII, foi de longe, a maior e mais rápida transformação da história do mundo, inaugurando a primeira era das máquinas e, com certeza, a primeira inovação tecnológica. Se a primeira era das máquinas resolveu o problema da potencialização da força bruta, o computador que inaugurou a segunda era das máquinas resolveu a questão da força mental que, de igual forma, é fundamental para o progresso humano.[134]

A relevância destes dois feitos e a sua concomitância nos leva inevitavelmente a uma outra e ainda mais profícua discussão em nossos tempos no que diz respeito à divisão do trabalho, posto que se a máquina a vapor extinguiu diversas profissões, o computador o fez de igual maneira e os avanços percebidos nos últimos anos, nos faz pensar até onde vamos sobrepor máquinas a humanos em diferentes contextos. Realidades antes impensadas, tais como

---

[133] MORRIS, Ian. *Why the west rules-for now: The patterns of history and what they reveal about the future*. Profile books, 2010.

[134] BRYNJOLFSSON, Erik; MCAFEE, Andrew. A Segunda Era Das Máquinas: Trabalho, Progresso E Prosperidade Em Uma Época De Tecnologias Brilhantes. Rio de Janeiro, RJ: Alta Books, 2015.

um carro trafegar sozinho[135], um computador dominar a linguagem humana[136], ainda que com restrições e softwares realizarem de forma bastante eficaz processos de tradução em diferentes idiomas[137] já fazem parte das nossas vidas e a cada ano em versões cada vez mais avançadas, robustas e complexas.

De todas as inovações tecnológicas, sobretudo aquelas que mais se aproximam do domínio de habilidades humanas e, muitas vezes, até com a capacidade de superar os resultados percebidos por pessoas, nada se compara ao rendimento dos robôs humanoides que combinam reconhecimento de padrões à linguagem complexa e assim, surpreendem até os mais incrédulos sobre a potência computacional. Foi exatamente isso que aconteceu, quando o Watson[138] ganhou o famoso jogo americano *Jeopardy*![139] Em fevereiro de 2011 derrotando dois grandes competidores e respondendo, além de precisa, muito mais rapidamente que seus dois concorrentes[140]. O fato é célebre, entre outras razões de natureza científica, por caracterizar um marco para as máquinas pensantes, uma vez que o supercomputador da IBM conseguiu superar uma das principais barreiras até então enfrentadas pelos desenvolvedores, qual seja: a habilidade de transitar por diferentes áreas, de forma rápida e com domínio de competências linguísticas, antes dominados apenas por humanos, especialmente no que diz respeito a significados alternativos de palavras e expressões.

Para além do entretenimento, a robótica vem avançando a passos largos na automação industrial e em contextos relacionados às tarefas das Forças Armadas, bem como o aprendizado para tarefas imprecisas e com menos dependência da programação dos engenheiros, numa linha clara que indica que a inteligência artificial é atualmente o principal investimento desta área do conhecimento tornando a realidade dos filmes de ficção científica cada vez mais próxima das pessoas comuns que podem facilmente por meio de seus *smartphones*[141] ter acesso a câmeras, dispositivos de GPS[142], *media players*, plataformas de jogos, entre outras facilidades antes disponíveis apenas em laboratórios para o desenvolvimento de pesquisas de ponta,

---

[135] https://waymo.com/ (Acesso em 13/01/2022)
[136] https://www.inbot.com.br/blog/automatizar-tarefas-assistentes-pessoais/ (Acesso em 13/01/2022)
[137] https://rockcontent.com/br/talent-blog/o-que-e-traducao-automatica/ (Acesso em 13/01/2022)
[138] https://www.ibm.com/br-pt/products/watson-assistant (Acesso em 13/01/2022)
[139] https://www.jeopardy.com/ (Acesso em 13/01/2022)
[140] https://gizmodo.uol.com.br/computador-da-ibm-vence-de-lavada-dois-cerebros-humanos-em-jogo-de-conhecimentos-gerais/ (Acesso em 13/01/2022)
[141] COUTINHO, Gustavo Leuzinger. A Era Dos Smartphones: Um Estudo Exploratório Sobre O Uso Dos Smartphones No Brasil. 2014. 60 f., il. Monografia (Bacharelado em Comunicação Social) - Universidade de Brasília, Brasília, 2014.
[142] https://www.embrapa.br/satelites-de-monitoramento/missoes/gps

demonstrando nitidamente a mudança da sociedade em relação aos seus hábitos, costumes, formas de se comunicar e estabelecer negócios e colocando os seculares institutos do direito à prova de sua aplicabilidade em tempos tão desafiadores e ímpares se comparados a outros períodos históricos.

Essa nova realidade permeia uma das questões mais polêmicas para a ciência jurídica atual: os institutos jurídicos pensados para regular as interações humanas poderão ser utilizados também para as relações entre máquinas?

O que temos até agora em termos de políticas públicas brasileiras para suportar este cenário tão tecnológico e como o mercado vem se comportando diante dessas inovações?

Concentraremos nossa análise em território brasileiro em razão da contribuição que este trabalho pretende oferecer e para tanto, não poderíamos deixar de citar a iniciativa do Ministério de Ciência e Tecnologia em conjunto com o Banco Nacional de Desenvolvimento Social que desenvolveu no ano de 2017 um Plano Nacional de IoT cujo principal objetivo foi realizar um estudo para que o Brasil se beneficie da tecnologia IoT.

## 5.1 O contexto legal: políticas para IoT, lacunas regulatórias e o papel dos contratos

Se o debate para a aprovação de uma lei cujo espírito é o da privacidade dos dados pessoais e respeito à vida privada, custou intensos debates por, pelo menos oito anos no Brasil, o que dizer, então, dos aspectos regulatórios que envolvem IoT?

Atualmente, o debate tecnológico que passou pelo Congresso foi o Projeto de Lei (PL) nº 21/2020, que cria o marco legal do desenvolvimento e uso da Inteligência Artificial (IA) pelo poder público, empresas, entidades diversas e pessoas físicas. O texto – em tramitação – estabelece princípios, direitos, deveres e instrumentos de governança para a IA e tem suscitado acalorados debates, em vista do fato de que muitos especialistas consideram o tema ainda pouco discutido no Brasil para que se torne uma legislação.

O projeto de autoria do deputado Eduardo Bismarck (PDT-CE), foi aprovado na forma de substitutivo da relatora, deputada Luiza Canziani do PTB-PR e se aprovado no Senado, caberá apenas à União legislar sobre o tema, muito embora diversos aspectos, como ocorre em legislações dessa natureza, deverão ser regulamentados pelo Executivo Federal por intermédio de órgãos setoriais com competência técnica na área.

Segundo a relatora, a principal inspiração das modificações vem da proposta em tramitação no Parlamento Europeu e no Conselho da Europa para uma nova legislação europeia

a respeito de inteligência artificial. Ela ressaltou que não seguiu o modelo europeu quanto à proibição a priori de certos tipos de inteligência artificial ou de quais seriam de alto risco, deixando essas definições para a regulação ou autorregulação setorial posterior.[143]

Do ponto de vista da convergência entre este estudo e o projeto de lei sobre inteligência artificial que está em discussão nos interessa, particularmente, os princípios sobre segurança e privacidade, nos termos da Lei 13.709/2018 apontados no texto da relatora e que comprovam a pertinência de nossa preocupação com o tema.

Há, porém, um ponto extremamente importante no momento histórico em que este projeto de lei é apresentado que denota claramente o despreparo do legislador em tratar do contexto multidisciplinar entre direito e tecnologia, posto que é óbvio e este trabalho apontou esta questão em seu primeiro capítulo que antes de pensar em legislar sobre inteligência artificial, é fundamental legislar e, além disso, estabelecer políticas públicas para os dispositivos interconectados por meio de IoT, uma vez que são estes os responsáveis pela volumosa coleta de dados que se transformam em insumo para o treinamento de inteligências artificiais.

Essa inversão de regulações para tecnologias que permeiam o cotidiano das pessoas é a prova cabal da necessidade deste trabalho e da fulcral necessidade de atualização das grades curriculares dos cursos de direito com vistas a preparar os operadores da ciência jurídica do século XXI. 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.

### 5.1.1 Internet das Coisas: um plano de ação para o Brasil

Inicialmente, cabe registrar que todos os dados abaixo relacionados sobre políticas públicas referentes à IoT no Brasil foram extraídos dos estudos realizados pelo Tribunal de Contas da União (TCU) e do Banco Nacional de Desenvolvimento Econômico e Social (BNDES) devidamente referenciados nas notas de rodapé e na bibliografia disposta no final deste trabalho. Em nossas pesquisas, essas foram as fontes mais abundantes em termos de dados e análises sobre o que vem sendo feito no âmbito do governo federal no que diz respeito a iniciativas teóricas e práticas sobre IoT[144]. O governo tem investido em iniciativas de base,

[143] https://www.conjur.com.br/2021-set-30/camara-aprova-projeto-regula-uso-inteligencia-artificial
[144] Texto para discussão / Instituto Serzedello Corrêa. – Brasília: ISC/TCU, 2020.

como as voltadas à infraestrutura tecnológica, mas, para alcançar o próximo nível de desenvolvimento das cidades inteligentes, por exemplo, que é um dos eixos temáticos mais discutidos nos trabalhos de IoT precisará enfrentar desafios tais como os relacionados à capacitação de pessoal, contratação pública, tratamento de dados e cooperação entre municípios[145]. Para a Associação Brasileira de Internet das Coisas (ABINC), é fundamental:

> [...] adotar uma abordagem colaborativa e multissetorial para discussões sobre política de IoT. A IoT é uma área desafiadora para os formuladores de políticas, pois é um ambiente em rápido desenvolvimento e sua tecnologia abrange muitos setores e usos. Uma abordagem de governança colaborativa, que se baseie na experiência e no engajamento de uma ampla gama de partes interessadas, será necessária para desenvolver soluções eficazes e apropriadas. As políticas devem ter como objetivo promover a capacidade dos usuários de se conectarem, falarem, inovarem, compartilharem, escolherem e confiarem de uma maneira que promova a inovação e permita os direitos do usuário[146].

Como primeira iniciativa do Governo Federal para viabilizar a Internet das Coisas no Brasil registramos a edição da Lei 12.715/2012, que dispõe sobre uma redução nas alíquotas do Fundo de Fiscalização das Telecomunicações (Fistel) para estações móveis integrantes de sistemas de comunicação máquina a máquina.

A partir daí, alguns outros esforços foram identificados, entre os quais: a criação de uma Câmara temática para tratar do tema (Câmara de IoT); a coordenação de estudos com o objetivo de apresentar um diagnóstico e um plano de ação estratégico para o país na área; a constituição de Câmaras temáticas específicas para cada um dos ambientes a serem priorizados na implantação da IoT no Brasil; a articulação de instituições fundamentais para viabilizar assuntos transversais como financiamento, formação de capital humano, desenvolvimento de infraestrutura de conectividade para suportar as aplicações de IoT, além da criação de estruturas de governança no âmbito do Plano Nacional de IoT (PNIoT), apenas para citar os que consideramos mais relevantes a partir do critério de abrangência e importância tecnológica e econômica.

---

[145] https://www.bndes.gov.br/wps/portal/site/home/transparencia/consulta-operacoes-bndes (Acesso em 13/01/2022).

[146] https://abinc.org.br/politicas-para-iot/ (Acesso em 13/01/2022).

O estágio atual da PNIoT foi subsidiado em grande parte pelo vigoroso estudo coordenado pelo BNDES, em parceria com o MCTI, e conduzido pelo consórcio vencedor da Chamada Pública BNDES/FEP Prospecção 1/2016, constituído pelos entes McKinsey, Fundação CPqD e Escritório Pereira Neto Macedo.

O estudo[147] foi organizado, basicamente em quatro fases:

a. Diagnóstico geral e aspiração para o Brasil;
b. Seleção de verticais e horizontais;
c. Aprofundamento e elaboração do plano de ação (2018-2022) e;
d. Suporte a implementação.

Os objetivos de cada uma das fases, estão apresentados na Figura 14.

*Figura 14 Relatório do Plano de Ação*

| | Fase 1 (jan/17 - mar/17) | Fase 2 (abr/17 - mai/17) | Fase 3 (jun/17 - set/17) | Fase 4 (out/17 - mar/18) |
|---|---|---|---|---|
| | Diagnóstico e Aspiração Brasil | Seleção de verticais e horizontais | Investigação de verticais, elaboração da Visão e Plano | Suporte à implantação do Plano de Ação |
| Objetivos | • Obter visão geral do impacto de IoT no Brasil<br>• Entender competências de TIC do País<br>• Aspirações iniciais para IoT no Brasil | • Definir critérios chaves para seleção<br>• Priorizar verticais e horizontais | • Aprofundar-se nas verticais escolhidas<br>• Elaborar Visão para IoT para cada vertical<br>• Elaborar Plano de Ação 2018-22 | • Detalhamento dos 3 projetos mobilizadores do Plano de Ação<br>• Desenho de modelo de governança para o PNIoT<br>• Desenho da estrutura de monitoramento (PMO) |

Fonte: BNDS, 2017.

Para que se tenha a exata noção da extensão do estudo, segue a tabela de todos os documentos que o compõem, desde um relatório de aspiração do Brasil para IoT, até um desenho do modelo de governança para o Plano Nacional de IoT, conforme se observa na Figura 15.

[147] Disponível em https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil (Acesso em 13/01/2022).

*Figura 15 Documentos do Plano de Ação 2*


Fonte: BNDS, 2017

O estudo realizado pelo BNDS contribuiu em grande medida para a realização de um benchmark[148] internacional sobre projetos e políticas públicas de IoT em outros países do mundo, o que demonstrou que há países em estágios muito semelhantes ao nosso, muito embora haja outros muito avançados, como a Coreia do Sul. O Plano Nacional de Internet das Coisas é tão completo que chega até a propor uma governança[149] contendo a estrutura de uma câmara de IoT cuja função é de aconselhamento, além de um comitê gestor de natureza executiva, uma equipe de PMO (*Project Management Office* ou Escritório de Projetos), além de um observatório de IoT.

Outro vértice importante do estudo apontou para a necessidade de priorizar grandes áreas para a concentração de esforços de desenvolvimento de políticas públicas pautadas em IoT e neste ponto não podemos deixar de destacar que a exemplo de outros países do mundo,

[148]Disponível em https://rockcontent.com/br/blog/benchmarking/ (Acesso em 13/01/2022).
[149]Disponível em https://www.bndes.gov.br/wps/wcm/connect/site/05cd4ba1-042d-42b0-8b782409e85b7cca/relatorio-final (Acesso em 13/01/2022).

as áreas de saúde, indústria, cidades e ambiente rural. As três principais frentes desta priorização revelam-se nos itens abaixo:

> a) na possibilidade de direcionamento de esforços de atuação do governo, setor privado e academia;
>
> b) na canalização de tempo e recursos para ambientes onde a ação do governo seja realmente necessária; e
>
> c) na captura do maior benefício possível da IoT, considerando-se os recursos disponíveis.[150]

Outro apontamento fundamental identificado a partir do PNIoT foi a necessidade de ampliação da cobertura de redes e infraestrutura necessária para garantir a conectividade às soluções de IoT, além da onerosidade tributária dos dispositivos que se conectam por meio desta tecnologia. Sobre a última questão em relevo, é salutar mencionar que apesar de o PNIoT ter sido elaborado em 2017, somente em 2019 o governo federal editou o Decreto 9854 com base na livre concorrência e na livre circulação dos dados e em regras de segurança da informação e proteção de dados pessoais.

O referido decreto traz algumas definições indispensáveis, dentre as quais: Internet das Coisas (IoT), como sendo a infraestrutura que integra a prestação de serviços de valor adicionado e em seu art. 3º dispõe sobre os objetivos do PNIoT:

> a) melhorar a qualidade da vida das pessoas e promover ganhos de eficiência nos serviços, por meio da implementação de soluções de IoT;
>
> b) promover a capacitação profissional relacionada ao desenvolvimento de aplicações de IoT e a geração de empregos na economia digital;
>
> c) incrementar a produtividade e fomentar a competitividade das empresas brasileiras desenvolvedoras de IoT, por meio da promoção de um ecossistema de inovação neste setor;
>
> d) buscar parcerias com os setores público e privado para a implementação da IoT; e
>
> e) aumentar a integração do país no cenário internacional, por meio da participação em fóruns de padronização, de cooperação internacional em pesquisa, desenvolvimento e inovação e da internacionalização de soluções de IoT desenvolvidas no país[151].

---

[150] https://www.telesintese.com.br/wp-content/uploads/2021/06/028-109-2020-1-AN-Levantamento_Internet-das-coisas.pdf (Acesso em 13/01/2022).

[151] https://www.in.gov.br/en/web/dou/-/decreto-n-9854-de-25-de-junho-de-2019-173021041

O art. 4º do referido decreto, por sua vez, estabelece que ato do Ministro de Estado da Ciência, Tecnologia, Inovações e Comunicações (atual MCTI) indicará os ambientes a serem priorizados para aplicações de soluções de IoT, devendo incluir, no mínimo, os ambientes de saúde, cidades, de indústrias e rural. Complementarmente, o § 1º do art. 4º define que os ambientes de uso de IoT serão priorizados a partir de critérios de oferta, demanda e de capacidade de desenvolvimento local.

A partir das diretrizes estabelecidas no âmbito do artigo 4º, o MCTI procedeu com a criação das câmaras setoriais prioritárias por intermédio do estabelecimento de acordos de cooperação técnica com ministérios finalísticos, sendo estes: Ministério da Economia, Ministério da Agricultura, Pecuária e Abastecimento, Ministério da Saúde e o Ministério do Desenvolvimento Regional. Os acordos foram firmados para a implementação das Câmaras da Indústria 4.0, Agro 4.0, Saúde 4.0 e de Cidades Inteligentes respectivamente, tendo sido estabelecido um sistema de co-coordenação entre o MCTI e os referidos ministérios finalísticos em cada câmara[152].

O art. 5º do decreto define os temas (horizontais) que integrarão o plano de ação destinado a identificar soluções para viabilizar o PNIoT, como sendo:

> a) ciência, tecnologia e inovação;
> b) inserção internacional;
> c) educação e capacitação profissional;
> d) infraestrutura de conectividade e interoperabilidade;
> e) regulação, segurança e privacidade; e
> f) viabilidade econômica.

Neste ponto, frisa-se que o decreto repete os temas mencionados no estudo de 2017 sobre IoT e acrescenta a variável da viabilidade econômica como um facilitador da execução das políticas a serem implementadas.

O art. 6º do mesmo diploma legal dispõe sobre a implementação de projetos mobilizadores com o objetivo de facilitar a execução do PNIoT a partir de: plataformas de inovação em IoT; centros de competência para tecnologias habilitadoras em IoT; e o observatório nacional para o acompanhamento da transformação digital.

[152] Disponível em https://www.telesintese.com.br/wp-content/uploads/2021/06/028-109-2020-1-AN-Levantamento_Internet-das-coisas.pdf (Acesso em 13/01/2022).

Entre os projetos mobilizadores em andamento, destacamos o LABfaber[153] que integra o ecossistema de plataformas de inovação e encontra-se em fase final de estudo pelo Ministério da Ciência e Tecnologia e o Observatório Nacional para o Acompanhamento da Transformação Digital[154].

A Câmara de Gestão e Acompanhamento de Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e IoT, o decreto define em seu art. 7º que será constituída de órgão de assessoramento (de natureza não deliberativa) destinado à implementação do PNIoT, competindo-lhe:

> a) Monitorar e avaliar as iniciativas de implementação do PNIoT;
> b) Promover e fomentar parcerias entre entidades públicas e privadas para o alcance dos objetivos do PNIoT;
> c) Discutir com os órgãos e entidades públicas os temas do plano de ação de que trata o art. 5º do decreto;
> d) Apoiar e propor projetos mobilizadores; e
> e) Atuar conjuntamente com órgãos e entidades públicas para estimular o uso e desenvolvimento de soluções de IoT.

O decreto ainda trata dos membros da Câmara de IoT e da regularidade das reuniões que ordinariamente devem acontecer uma vez a cada semestre e extraordinariamente quando o presidente julgar necessário.

A definição do legislador sobre IoT no caso do presente decreto, como "a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade", importa porque impossibilita a cobrança de ICMS-Comunicação, nos termos da Súmula 334[155] do Superior Tribunal de Justiça, do que deduzimos que, embora outras iniciativas acerca da importância da privacidade nos processos de desenvolvimento dos dispositivos de IoT e de como o mercado pode, sem prejuízo de direitos e garantias dos titulares dos dados, beneficiar-se deste processo

[153] Laboratório-Fábrica de referência no desenvolvimento, domínio, prática e difusão de tecnologias digitais na manufatura competitiva de produtos tecnologicamente avançados, e à capacitação e disseminação de soluções em Indústria 4.0 - Fundação CERTI e FIESC, Estado de Santa Catarina https://labfaber.certi.org.br/ (Acesso em 13/01/2022).

[154] https://www.gov.br/mcti/pt-br/acompanhe-mcti/transformacaodigital/arquivosestrategiadigital/estrategiadigital.pdf (Acesso em 13/01/2022).

[155] A saber, o inteiro teor da Súmula 334 STJ: "O ICMS não incide no serviço dos provedores de acesso à Internet."

tecnológico, sejam muito incipientes ainda, o Estado brasileiro já lançou mão de como pode tributar esta tecnologia e absorver os dividendos que a sua utilização pode lhe trazer.

Curioso, ainda, analisar que sob o prisma discursivo haja uma preocupação acerca dos aspectos acima mencionados, mas nenhuma disposição que penalize, ou mesmo instrua empresas de desenvolvimento sobre a necessidade do respeito aos direitos dos titulares e sobre a forma como dados pessoais são utilizados como insumos às big datas e, posteriormente, ao treinamento de inteligências artificiais.

No nosso entendimento, este contexto se coaduna perfeitamente com a definição de lacuna regulatória, uma vez que, embora haja uma legislação a respeito, pouco se extrai acerca das especificidades que esta deveria abordar, tais como: princípios para o desenvolvimento de dispositivos que coletam dados respeitando a privacidade de seus usuários e penalidades, administrativas ou mesmo pecuniárias para o descumprimento destas disposições legais, bem como decretos que regulamentassem tais disposições, de forma a orientar o mercado de maneira assertiva sobre requisitos de programação segura e funcionalidades que coletam o consentimento claramente, expresso e inequívoco, tal como dispõe a LGPD.

De outra sorte, os contratos têm cumprido, eficientemente, as lacunas existentes na legislação e nas orientações do Poder Público, isto porque podem incorporar cláusulas que evidenciem as preocupações de privacidade e a necessidade de comprovação dos acordos firmados entre as partes. Cumpre também a função de contratos os denominados termos de uso e políticas de privacidade disponibilizados para a utilização de dispositivos pervasivos ou outros que coletem dados na medida de sua utilização.

Via de regra, esses documentos seguem a legislação do país de origem da empresa desenvolvedora, mas com adaptações à legislação do país em que são comercializados em razão da necessidade de atenderem autoridades ou mesmo direitos e garantias fundamentais estabelecidas por cada país dentro de sua jurisdição. Especificamente sobre regras protetivas de intimidade e privacidade, grandes ganhos houve a partir da entrada em vigor do GDPR em 25 de maio de 2018, sobretudo em razão das robustas multas aplicadas a grandes empresas que não estavam atentas a estes conceitos em seus produtos.

### 5.1.2 IoT e Mercado

Visto que este capítulo se destina à discussão sobre lei, sociedade, mercado e IoT e os dois primeiros já foram superados neste estudo, falaremos a partir de agora sobre os

desdobramentos do Plano Nacional de Internet das coisas, do ponto de vista mercadológico e social. Mais uma vez, os dados aqui transcritos foram retirados do Relatório do Tribunal de Contas da União e do BNDES aqui já referenciados acerca da implementação das políticas públicas que viabilizem o Plano Nacional de Internet das Coisas.

Os três setores priorizados no referido relatório como sendo básicos para a digitalização da economia são: agropecuária[156], indústria e serviço cujos métodos tradicionais de produção vêm sofrendo fortíssimo impacto das aplicações digitais e do uso intensivo de tecnologias de informação e comunicação, além da interconexão de dispositivos. Observa-se dentro do setor primário, por exemplo, que a digitalização de máquinas e implementos, bem como o sensoriamento e mapeamento remotos e dispositivos e sensores de IoT já são usados fartamente em atividades de agricultura[157], pecuária e silvicultura. Outra contribuição fundamental da tecnologia no campo, diz respeito ao uso de sensores para monitoramento, de luz, umidade, temperatura, umidade do solo, entre outros benefícios. Destaca-se, porém, a importância da automatização dos processos de irrigação, possibilitando que o acompanhamento das safras seja feito, inclusive remotamente, mas de forma muito mais assertiva, até mesmo para o meio ambiente, já que as técnicas de plantio podem ser aprimoradas[158].

O agronegócio é tão importante para o Brasil que em 2020, em meio à crise sanitária da Covid-19, alcançou a marca de 26,1% do PIB de acordo com dados do Centro de Estudos Avançados em Economia Aplicada (CEPEA) em parceria coma Confederação da Agricultura e Pecuária do Brasil (CNA)[159] e esta marca é o resultado, entre outras razões, do robusto investimento tecnológico que se tem feito para a melhoria das condições de plantio, bem como da flexibilização, inclusive tributária, para a aquisição de máquinas, dispositivos e sensores que auxiliem as atividades do setor.

No setor secundário, observamos o desenvolvimento da indústria 4.0 que conceitualmente diz respeito a máquinas e sistemas interconectados numa mesma cadeia produtiva o que possibilita que os processos possam, por meio de computadores, se autogerir,

---

[156] MONTOYA, Edwin Andrés Quiroga et al. *Propuesta De Una Arquitectura Para Agricultura De Precisión Soportada En* IoT. Revista Ibérica de Sistemas e Tecnologias de Informação, n. 24, p. 39-56, 2017.
[157] https://forbes.com.br/forbesagro/2021/09/o-que-saber-sobre-agricultura-inteligente-usando-iot/ (Acesso em 13/01/2022).
[158] https://blog.aegro.com.br/internet-das-coisas-na-agricultura/ (Acesso em 13/01/2022).
[159] https://www.cepea.esalq.usp.br/br/opiniao-cepea/agronegocio-brasileiro-importancia-e-complexidade-do-setor.aspx (Acesso em 13/01/2022).

dando a autonomia que permite que este modelo seja considerado um modelo inteligente e menos dependente da ação humana.

A IoT é um dos pilares deste contexto, inserindo por meio de robôs autônomos, sensores embarcados e captura de dados em tempo real mais assertividade nos processos, além de uma produtividade exponencialmente superior aos processos dominados por humanos. Outro importante benefício da IoT nos processos industriais está relacionado à maior segurança e eficiência energética dos processos integrados o que, por óbvio, resulta em maior lucratividade.

Os benefícios listados acima são mais do que inspiradores para que as políticas públicas voltadas para o desenvolvimento da Internet das Coisas no Brasil sejam impulsionadas a partir de iniciativas como o Plano Nacional de IoT acima descrito e comentado, bem como os incentivos fiscais previstos no Decreto 9854/2019, sobretudo nestes tempos em que a projeção industrial brasileira tem perdido espaço sobretudo para a indústria chinesa, mesmo dentro do mercado nacional. Especialmente no ano de 2021, a indústria brasileira tem enfrentado inúmeros entraves que a colocaram em uma situação periclitante e com possibilidades bastante desafiadoras para alavancar uma retomada digna de sua posição no PIB nacional.[160]

No setor de serviços, houve nos últimos anos um aumento exponencial de serviços que mesclam redes sociais, colaboração online e prestação de serviços, tal como vemos em plataformas como o Uber, no segmento de transportes e o *Airbnb* no setor hoteleiro, entre diversas outras que têm ganhado cada vez mais adeptos em virtude de sua praticidade e de seus preços atrativos em comparação aos mesmos serviços prestados de forma tradicional. Uma verdadeira revolução que, ao que tudo indica, é inevitável!

Por fim, listamos os números extraídos do Relatório do Tribunal de Contas da União relacionados às políticas públicas e programas do governo federal referentes à Internet das Coisas a respeito das aplicações de interoperabilidade de dispositivos relativos às cidades inteligentes, saúde, varejo, domicílios, escritórios e ambientes administrativos, logísticos:

> Nas cidades inteligentes, aplicações em transporte podem levar a impactos mensurados em mais de U$ 800 bilhões por ano em municípios ao redor do mundo, até 2025. Além desses, os efeitos resultantes do uso de medidores inteligentes voltados à eficiência energética e de distribuição de água podem ser superiores a U$ 69 bilhões por ano em todo o mundo. No segmento de saúde, dispositivos conectados

[160] https://g1.globo.com/economia/noticia/2021/09/01/dona-de-15-do-pib-industria-encolhe-02percent-e-enfrenta-dificuldades-na-retomada-veja-os-5-entraves-principais.ghtml (Acesso em 13/01/2022).

> e demais aplicações em IoT podem otimizar tratamentos médicos e a própria gestão dos hospitais com impactos econômicos previstos da ordem de U$ 1,6 trilhão em todo o mundo até 2025. O setor de logística também deve ser bastante beneficiado pelas aplicações de IoT. De fato, a interoperabilidade entre sistemas de IoT é a principal aposta para a base da cadeia logística da indústria do futuro, o que inclui aplicações em vias férreas, aéreas, fluviais e terrestres. Dentre elas, torna-se possível o rastreamento remoto de contêineres navais, trens e automóveis de carga; aplicações de navegação interconectada; o acompanhamento de rotas logísticas; e veículos de carga autônomos. Os impactos econômicos previstos para esse setor com tecnologias baseadas em IoT podem chegar a U$ 850 bilhões em todo o mundo até 2025. Sobre esse setor, observa-se uma representatividade do setor terciário de mais de dois terços do PIB brasileiro, além de um crescimento consistente no valor adicionado nacional com o tempo. De 2003 a 2016, a representatividade do setor terciário passou de 65,8% para 73% do valor adicionado ao PIB (peça 15, p. 94). Resumidamente, o impacto econômico que a IoT pode trazer para as economias mundiais encontra-se estimado entre U$ 3,9 trilhões e U$ 11,1 trilhões por ano até 2025. Somente para a economia brasileira, estima-se a captura de cerca de U$ 200 bilhões por ano desse valor total até 2025, representando cerca de 10% do PIB anual. (TCU, 2020, TC 028.109/2020-1, p. 6-7)[161]

### 5.1.3 Entraves à implementação da Política Nacional de IoT

De tudo o que discutimos neste capítulo acerca da Política Nacional de IoT, é importante asseverar que o primeiro grande desafio para que essa política seja colocada em prática é o aumento da conectividade em todo o território brasileiro, visto que há diferenças gritantes entre as várias regiões que compõe a federação e por isso a oferta de conectividade é tão rarefeita em alguns pontos, tais como as regiões norte e nordeste.

Além do aumento da infraestrutura de conectividade, segundo o relatório já referenciado do TCU:

> O desenvolvimento de um ecossistema de IoT depende da solução de desafios estruturais e específicos para financiamento no Brasil. Quanto aos desafios estruturais, observa-se que o país investe relativamente pouco em pesquisa e desenvolvimento (em torno de 1,2% do PIB brasileiro em PD&I), sendo o governo seu maior investidor de risco.

[161] BRASIL. Tribunal de Contas da União. Relatório de Levantamento, TC. 028.109/2020-1. Sessão 23 jun 2021, p.6-7.

Adicionalmente, observa-se ainda: uma participação limitada das TICs no montante de patentes depositadas (12,8% no período de 2009 – 2011); que somente 14,6% das empresas que mais usufruem das compras governamentais apresentavam um perfil inovador em 2008; uma grande pulverização de recursos no financiamento de projetos em PD&I (no período de 1997 – 2014, 25 mil projetos receberam um valor médio de 225 mil reais cada); um elevado nível de contingenciamento em fundos estatais (p.ex., no período de 2009 – 2014, o contingenciamento líquido FNDCT/Finep totalizou R$ 810,5 milhões); o baixo nível de cooperação entre ICTs-Empresas (apenas 11,4% dos recursos não-reembolsáveis são destinados a esta modalidade); entre outros (peça 18, p. 31). 227. Comparado com os seus pares regionais, o Brasil é líder em investimentos na América Latina. No entanto, ele ainda se encontra atrás de países líderes em inovação. Entre as questões centrais mapeadas pelo estudo de IoT, os principais desafios de investimento, financiamento e fomento podem ser sintetizados pelas perguntas: a) como criar um ambiente propício para inovação dadas as condições estruturais do país? B) como estimular o setor privado a aumentar seus investimentos em capital de risco e desenvolver processos de financiamento (de médio e longo prazo) para estimular a inovação? C) como aprimorar o uso dos instrumentos de incentivos fiscais? D) como aumentar a inserção global das empresas inovadoras brasileiras? E) como aumentar mais investidores internacionais? F) existe necessidade de desenvolver instrumentos de financiamento específicos para IoT ou apenas aperfeiçoar os existentes? 228. Essas são questões fundamentais a serem endereçadas para que se possa observar o desenvolvimento das tecnologias de IoT no país, considerado seu aspecto altamente tecnológico e inovativo. 229. Adicionalmente, deve-se destacar que, por mais de uma vez, *stakeholders* reportaram em suas entrevistas que expressiva parcela das empresas nacionais envolvidas com soluções de IoT consistem de PMEs, ainda que possam estar desenvolvendo soluções para empresas de grande porte. Isso torna-se relevante na medida em que constatou-se existir uma oferta reduzida de capital de risco disponível no mercado para as PMEs. 230. Buscando endereçar essas questões, o estudo de IoT que fundamentou a elaboração do PNIoT previu dentre suas iniciativas na horizontal de "inovação e inserção internacional": a) incentivar a adoção da IoT por meio de financiamento de projetos pilotos e estudos que comprovem benefícios da adoção de IoT; b) fortalecer centros de competência em tecnologias habilitadoras para IoT, com financiamento articulado por agências de fomento, para desenvolver pesquisa tecnológica de relevância internacional, com impacto comercial e/ou social relevante nos quatro ambientes priorizados, buscando interação com o setor empresarial e realizando transferências de tecnologia; c) viabilizar instrumentos de fomento para impulsionar a adoção e o lançamento no mercado de novas soluções desenvolvidas nas redes de

> inovação (p.ex.: isenções fiscais, subsídios diretos para compras de novas soluções etc.).
>
> Apesar dos referidos planos, na prática, observa-se um pequeno volume de recursos disponíveis atualmente para as referidas soluções, como: dispêndios de cerca de R$ 16 milhões em nove projetos pilotos selecionados pelo programa BNDES Pilotos IoT; investimentos de R$ 5 milhões por projeto a serem realizados pelo programa FINEP IoT (utilizando-se recursos do FNDCT). Por conseguinte, faz-se necessário acompanhar a implementação das iniciativas previstas no plano de ação do estudo de IoT, em particular aquelas relacionadas à questão das fontes de financiamento para o PNIoT, sendo esta uma barreira identificada em nossa realidade atual ao sucesso da política pública. (TCU, 2020, TC 028.109/2020-1, p. 31-32)[162]

Ademais, os dados e status apresentados a partir do relatório do TCU, ainda que apresentado diversos desafios à implementação, sucedem anteriormente a conclusão do Leilão de radiofrequência 5G, o que, necessariamente impactará o desenvolvimento da IoT no território brasileiro, conforme já se demonstrou no capítulo 1.

As ofertas somadas do leilão perfizeram o montante de R$47,2 bilhões, obrigando ainda as empresas vencedoras a levar a cobertura 5G a todas as capitais e cidades com mais de 30 mil habitantes; garantir internet 4G nas rodovias federais e localidades ainda sem conexão; e investir em projetos de conectividade em escolas[163].

Por fim, corroborando com os compromissos assumidos pelos vencedores do leilão[164], é necessário e inarredável destacar que o Brasil precisa investir na educação de seus cidadãos desde a educação básica, até os cursos profissionalizantes e superiores. Esta é uma lacuna que tem se tornado um gargalo na empregabilidade brasileira, visto que embora o desemprego esteja altíssimo, há segmentos em que sobram vagas por falta de profissionais qualificados[165]. Curiosamente, o setor em que mais sobram vagas é justamente o de tecnologia cujas

---

[162] Ibidem, p. 31-32.
[163] BRASIL. GOVERNO FEDERAL. Série Especial 5G. Leilão do 5G confirma expectativas e arrecada R$ 47,2 bilhões. Publicado em 05 nov 2021. Disponível em https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/11/leilao-do-5g-confirma-expectativas-e-arrecada-r-47-2-bilhoes. (Acesso em 13/01/2022).
[164] Conforme publicado em alguns meios de comunicação, Claro Vivo e Tim são responsáveis por arrematar faixa significativa do leilão. Disponível em: https://oglobo.globo.com/economia/tecnologia/leilao-do-5g-ao-vivo-claro-tim-vivo-sao-as-vencedoras-nos-lotes-mais-importantes-25263128 e https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/claro-vivo-e-tim-arrematam-faixa-de-35-ghz-do-leilao-do-5g (Acesso em 13/01/2022).
[165] https://abmes.org.br/linc/coluna/detalhe/1923/mercado-em-alta-sobram-vagas-na-area-de-tecnologia- (Acesso em 13/01/2022).

possiblidades, inclusive de trabalho remoto, abundam em redes sociais mais voltadas à área profissional como o Linkedin.

# 6 UM MUNDO DE HUMANOS E MÁQUINAS

Toda a construção deste trabalho teve como princípio norteador o viés cronológico e a interdisciplinaridade entre duas ciências, em tese, diametralmente opostas, quais sejam: o Direito e a Computação. Não só pela sua natureza conceitual, a primeira uma ciência humana e a segunda uma ciência exata, mas sobretudo por ambas terem como objetos de estudo questões muito distintas e com aplicabilidade muito diferentes.

Integram ainda este estudo outras disciplinas, tais como a sociologia, a filosofia e a política, por evidenciarem em diversos trechos a orientação do homem em seu tempo e suas respectivas escolhas no que tange ao desenvolvimento, preocupações e conquistas. O início da Internet, por exemplo, é marcado por uma escolha política, mas seu desenvolvimento está muito mais próximo do desejo pulsante do homem em evoluir e criar o novo, simplificando sua vida e melhorando a sociedade de que faz parte.

O momento político-filosófico e tecnológico em que vivemos é particularmente interessante por estreitar os laços entre a Computação e o Direito, embora em compassos de desenvolvimento diferentes, muitos pontos entre as duas ciências, necessariamente, já convergiram com o intuito de atender à sua razão social e o seu precípuo fundamento de harmonizar as relações humanas.

Se a palavra de ordem da Computação é subverter o atual estado de coisas, podemos dizer que a do Direito é reinventar, no sentido de repensar conceitos seculares e introduzir um novo agente aos seus institutos: a máquina.

Se as máquinas foram até agora coadjuvantes dos humanos, não o serão mais, protagonizarão as relações humanas e seus desdobramentos nos mais diferentes cenários, substituindo o poder de decisão humana e realizando tarefas complexas, até então impensadas para um computador.

A revolução das máquinas será feita por silício, energia e luz. O oceano de fibras ópticas que permeia toda a crosta terrestre está atingindo capilaridade suficiente para que a transmissão na velocidade da luz possa chegar aos lugares mais distantes, gerando larguras de banda sem precedentes. Onde existem obstáculos físicos que impedem a chegada das fibras, as tecnologias de transmissão de dados sem fio de 5ª geração se encarregam de suprir as necessidades. A abundância de poder de processamento do silício e da energia associada à largura de banda das tecnologias de transmissão permitirá que a Internet execute aplicações isócronas, nas quais os pacotes de dados serão transmitidos com intervalos de tempo iguais e

na velocidade da luz. Em outras palavras, os pacotes serão entregues ao receptor sem variações de atraso, em altíssima velocidade, o que permitirá uma nova sinergia entre máquinas, humanos e computadores, com possibilidades nunca imaginadas. Com aplicações e redes funcionando de maneira isócrona, na velocidade da luz, as questões legais também precisarão acompanhar este novo ambiente. Respostas de máquinas às ordens ou estímulos humanos irão acontecer de forma muito mais rápida e eficiente do que acontece hoje. Decisões que implicam a vida e as relações humanas e de negócios terão de ser tomadas em micro ou nanosegundos.

As interfaces cérebro-computador (*Brain-computer Interfaces – BCIs*) e interfaces cérebro-máquina (*Brain-Machine Interfaces – BMIs*) são dispositivos emergentes que, em breve, poderão auxiliar humanos com lesões cerebrais ou espinhais a se moverem ou se comunicarem. Os sistemas BCI/BMI dependem de sensores implantáveis que registram sinais elétricos do cérebro, e usam esses sinais para acionar dispositivos externos como computadores, próteses robóticas ou, claro, máquinas. A rápida evolução da aplicação das BCIs/BMIs permitirá que, num futuro breve e alcançável, os seres humanos se comuniquem diretamente com as máquinas[166]. Isso trará grandes desafios legais com relação à privacidade, autenticidade e integridade destas comunicações. Haverá implicações civis e criminais que envolvem máquinas e humanos. À medida em que esta simbiose – ou talvez dependência – da relação humano-máquina ou humano-coisas avance, os desafios legais aumentarão exponencialmente. Algoritmos que envolvem a aplicação de BCIs/BMIs precisam ser capazes de executar análises de dados muito sofisticadas, reconhecimento de padrões, aprendizado e tomada de decisão, e envolvem o uso massivo de inteligência artificial. Existem sérias preocupações sociais e éticas com relação a isso. Será necessária forte regulação a respeito do uso destas interfaces, e da relação entre os humanos e as máquinas, notadamente, mas não exclusivo, a sistemas de suporte à vida, atividades essenciais, ou mesmo econômicas.

Em janeiro de 2015, Stephen Hawking, Elon Musk e dezenas de cientistas alertaram sobre a necessidade de maiores análises sobre os impactos sociais da Inteligência Artificial e

[166] Uma equipe de pesquisadores deu um passo importante em direção a um novo conceito para um futuro sistema BCI - um que emprega uma rede coordenada de micro implantes de sensores neurais independentes, desenvolvidos em microescala e sem fio, cada um do tamanho de um grão de arroz, para registrar e estimular a atividade cerebral. Os sensores, chamados de "*neurograins*", gravam os pulsos elétricos feitos por neurônios e enviam os sinais sem fio para um concentrador central, que coordena e processa os sinais. Em um estudo publicado em 12 de agosto de 2021, na *Nature Electronics*, os pesquisadores demonstraram que o uso dos *neurograins* autônomos funciona para registrar a atividade neural em um roedor. Estudos avançam rapidamente para testes em humanos. In: LEE, Jihun et al. *Neural recording and stimulation using wireless networks of microimplants*. Nature Electronics, v. 4, n. 8, p. 604-614, 2021.

que tal tecnologia tem que ser controlada a fim de evitar que os pesquisadores criem algo que não pode ser controlado e, assim, salvaguardar o futuro da humanidade[167]. Conforme formulado por Russel e Norvig, esta hipótese é chamada de "Risco Existencial da Inteligência Artificial Geral" e alega que um progresso substancial na inteligência artificial geral (AGI - *Artificial General Intelligence*) poderia, um dia, resultar na extinção humana ou em alguma outra catástrofe global irrecuperável[168]. As vulnerabilidades de IoT criaram oportunidades por meio das quais os cibercriminosos e ciberterroristas podem lançar um ataque para comprometer pontos nevrálgicos da sociedade e da nação, ou até mesmo da existência humana.

Considerando-se o desenvolvimento industrial corrente em 2021, os sistemas de automação de manufatura têm utilizado dispositivos de IoT em abundância, criando uma categoria de aparelhos denominada de *Industrial Internet of Things* (IIoT), os quais executam diversos tipos de ações em plantas industriais, variando desde a indústria alimentícia até o controle de usinas nucleares.

Por outro lado, ainda em 2010, foi descoberto um novo tipo de ataque cibernético que logo se tornaria um divisor de águas na área da cibersegurança e da guerra cibernética. Um software malicioso que foi denominado de Stuxnet atacou usinas de enriquecimento de urânio do Irã. Por se tratar de um sistema industrial de alta centrifugação, extraordinariamente especializado, e cercado de diversos mecanismos de segurança física e tecnológica, houve impactos geopolíticos e repercussões internacionais sem precedentes[169]. Este foi o primeiro ataque cibernético utilizado como arma contra um sistema de controle industrial de um estado-nação. Antes do surgimento do Stuxnet, pensava-se que sistemas industriais, devido à sua obscuridade e isolamento, estariam fora do alcance dos ataques cibernéticos, e não seriam alvos de interesse. E assim foi criado um tipo de guerra assimétrica que passaria a ser utilizada por atores de estado-nação, alterando-se, para sempre, a visão sobre a segurança cibernética dos sistemas industriais. À época, o que poderia ter ocorrido caso o uso de *Industrial Internet of Things* estivesse mais difundido? Poderia a arma ter saído do controle? Um grave incidente

---

[167] HAWKING, Stephen at al. "*Research Priorities for Robust and Beneficial Artificial Intelligence: An Open Letter*". Disponível em https://futureoflife.org/2015/10/27/ai-open-letter/ (Acesso em 16/01/2022)

[168] RUSSEL, Stuart; NORVIG, Peter (2009). "*26.3: The Ethics and Risks of Developing Artificial Intelligence*". *Artificial Intelligence: A Modern Approach*. Prentice Hall. ISBN 978-0-13-604259-4.

[169] KARNOUSKOS, S. Stuxnet Worm Impact On Industrial Cyber-Physical System Security. IECON 2011 – 37th Annual Conference of the IEEE Industrial Electronics Society, 2011, pp. 4490-4494, doi: 10.1109/IECON.2011.6120048. Disponível em https://doi.org/10.1109/IECON.2011.6120048 (Acesso em 14/01/2022)

nuclear poderia ter sido iniciado, com repercussões catastróficas? O ataque poderia ter sido detectado mais rapidamente, ensejando uma resposta militar?

Em que pese o uso de IoT nas linhas de produção possibilitar melhor desempenho para a produção industrial, sua aplicação também traz consigo uma série de desafios tecnológicos, sociais, políticos e de segurança cibernética. Segundo Kandasamy[170] "o uso de dispositivos IoT para automatizar controles pode comprometer as plantas industriais e centros de informação". Estes dispositivos, em sua maioria, executam aplicações críticas, tais como controle e segurança de processos industriais complexos. Por exigirem protocolos técnicos rígidos, as implementações destes dispositivos de IIoT em tais ambientes são ainda mais desafiadoras e ainda não atingiram a maturidade. Ameaças que antes ficavam restritas às redes corporativas, institucionais e domésticas, hoje também apresentam capacidade de colocar em riscos os sistemas de automação industriais. Quais as implicações legais disso?

Como harmonizaremos esta convivência e como o Direito adaptar-se-á a desafios, como, a confiança necessária nesta nova modalidade de relacionamento? Como parametrizar estes novos contextos, de forma a extrairmos subsídios para os operadores do Direito lidarem com os institutos em vigor hoje e como adequar a ciência processual aos novos tempos?

Está no binômio – prestação de contas e auditabilidade – o ponto fulcral para iniciarmos esta jornada, isto porque a natureza dos dispositivos existentes no mercado não oferece esta possibilidade, de forma a obrigar o usuário a acreditar nas informações de documentos, como termos de uso e políticas de privacidade, escritos pelas próprias empresas desenvolvedoras e aderentes aos seus interesses comerciais e à sua segurança jurídica.

Além disso, há um grande hiato em relação ao nível informacional a que as pessoas estão expostas quando se trata de IoT, visto que muitas delas desconhecem o fato de, ao usarem um dispositivo dessa natureza, estarem expondo várias de suas informações, algumas delas sensíveis, para as empresas titulares da propriedade intelectual destes dispositivos. O único estudo abrangente sobre o uso de IoT no Brasil está focado em incentivar políticas públicas a respeito de sua adoção e em melhorar a questão da infraestrutura de telecomunicações, de forma a possibilitar o maior número possível de dispositivos conectados.

[170] KANDASAMY, K., Srinivas, S., Achuthan, K. et al. IoT Cyber Risk: A Holistic Analysis Of Cyber Risk Assessment Frameworks, Risk Vectors, And Risk Ranking Process. EURASIP J. on Info. Security 2020, 8 (2020). https://doi.org/10.1186/s13635-020-00111-0 (Acesso em 14/01/2022)

A vigência da LGPD – e a criação da ANPD[171] – fomentarão os esforços para a introdução de requisitos de privacidade e possibilitarão que, em alguma medida, tenhamos acesso aos critérios de coleta, guarda e tratamento de dados por IoT, entre todos os outros que realizam essas mesmas operações. Entretanto, o fato de ambas, tanto a lei, quanto a autoridade ainda serem muito jovens, visto que começaram a operar no segundo semestre de 2020, tendo entrado em vigor a legislação em 18 de setembro daquele ano e a Autoridade tendo iniciado seus trabalhos em 06 de novembro do mesmo ano, ainda não há evidências concretas de diretrizes para o desenvolvimento de dispositivos conectados por IoT, ou mesmo dispositivos de qualquer outra natureza tecnológica, cuja principal premissa de desenvolvimento esteja relacionada à privacidade por concepção ou mesmo por padrão, o que, em última análise, resulta em indicadores de segurança mais robustos e mais transparentes para o usuário.

Como a quantidade de artigos a serem regulamentados, discutidos ou mesmo orientados é enorme, a ANPD lançou uma agenda regulatória[172] para os anos de 2021-2022 que prevê consultas públicas e participação da sociedade no detalhamento da legislação, de forma a esclarecer controladores e operadores de dados em relação aos seus direitos e obrigações. Além disso, firmou parcerias com o cert.br[173] para a publicação de cartilhas sobre segurança na Internet e disponibilizou um guia de segurança para empresas de pequeno porte, visto que muitas delas possuem um quadro de colaboradores enxuto, mas lidam com grandes volumes de dados. Para além destes, esforços, nada há de efetivo no trato da segurança das aplicações, bem como da proteção quanto aos acessos indevidos e do compartilhamento não autorizado, do que se depreende que por esse lado, ainda há muito, para não dizer tudo por ser feito do ponto de vista da segurança cibernética no Brasil.

Chama a atenção, por outro lado, a quantidade de vazamentos de dados ocorridos ao longo do ano de 2021[174], sobretudo envolvendo órgãos da administração pública federal[175], o que, inclusive tem suscitado intervenções da própria ANPD[176] com relação aos pedidos de esclarecimentos sobre os aspectos de segurança dos programas de governança de dados

---

[171] https://www.gov.br/anpd/pt-br (Acesso em 14/01/22)
[172] https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313 (Acesso em 13/01/2022).
[173] https://www.cert.br/ (Acesso em 13/01/2022).
[174] https://tecnologia.ig.com.br/2021-03-28/ao-menos-oito-vazamentos-de-dados-aconteceram-no-brasil-em-2021--quem-e-punido-.html (Acesso em 13/01/2022).
[175] https://jus.com.br/artigos/94123/lgpd-e-a-administracao-publica (Acesso em 13/01/2022)
[176] https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas (Acesso em 13/01/2022)

implementados por controladores e operadores de dados em território nacional[177], o que claramente impõe uma urgência da discussão do tema e a tomada de decisões efetivas para a contenção destes danos.

Todo esse cenário ilustra uma realidade complexa e carente da união de esforços de diferentes segmentos, de distintas ciências e diversos órgãos de poder. A tecnologia não cessará seu desenvolvimento, tampouco se intimidará com os problemas aqui relatados, visto que seu mote não é esse, mas a sede de resolver os problemas da vida prática e mais do que isso, do desejo de cientistas se superarem na busca do perfeito, do belo e do impossível.

A julgar pelo que já vivenciamos quando a Internet passou a compor o rol de demandas do Judiciário e, durante muitos anos, a legislação em vigor se prestou à resolução dos inúmeros problemas trazidos à baila nos mais diversos casos concretos, possivelmente, pelo menos aqui no Brasil, conseguiremos harmonizar a conduta ativa das máquinas à legislação em vigor, mas, seguramente, isto não será suficiente a longo prazo. Haveremos de estudar outras formas de adequar o Direito à conduta proativa das máquinas, em especial, nas tomadas de decisões envolvendo questões morais, tais como as discutidas nos estudos do MIT denominados *Moral Machine*[178] em que, por meio de uma plataforma *online*, o internauta disponibiliza a perspectiva humana em relação às decisões tomadas por inteligências artificiais em carros autônomos.

Como já salientamos neste trabalho, a Computação caminha por si só, não esperando o Direito pensar sobre quais serão os possíveis reflexos jurídicos das inovações tecnológicas na vida das pessoas. Tem em mira, antes, a praticidade e as diversas maneiras de um computador tornar a vida humana mais simples, mais ágil e mais eficiente, de forma que humanos possam usar seu tempo com mais qualidade, desenvolvendo e realizando atividades mais prazerosas e menos repetitivas.

Este pensamento, de fato, é o ponto fulcral da IoT que numa visão menos tecnológica e mais humanista, não trata sobre tecnologias, mas sobre como tornar a vida em sociedade mais produtiva, mais rápida e mais eficiente. O caráter humanístico, indubitavelmente, é o que orienta todas as decisões de desenvolvimento das tecnologias, visto que por um prisma cronológico, a linha de raciocínio que se percorre é a de primeiramente pensar nas finalidades, em características circunstanciais e só depois destes pontos terem sido evidenciados é que se

[177] https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-audiencia-publica-da-comissao-de-ciencia-e-tecnologia-do-senado-federal (Acesso em 13/01/2022)
[178] Disponível em: https://www.moralmachine.net/hl/pt (Acesso em 13/01/2022).

discute sobre a tecnologia a ser utilizada e em que medida ela deve ser desenvolvida, considerando o estágio tecnológico de cada país.

Este ponto, possivelmente, arremata o objetivo deste trabalho, pois se à primeira vista, ele se assemelha a um estudo de Computação, a sua leitura e o viés de aplicabilidade que se extrai dos diversos pontos discutidos, bem como da interdisciplinaridade externada nas discussões aqui propostas, redundam em um estudo de natureza humanística e de valor jurídico na perspectiva relacional e mais atenta aos novos contornos do Direito na sociedade atual.

Resta claro, por todo o exposto, que não se trata de uma escolha, mas de um caminho de mão única, pois nos próximos anos experimentaremos avanços tão rápidos e tão disruptivos como sequer conseguimos imaginar hoje, de forma a possibilitar, inclusive, a destruição da humanidade, seja por atos maldosos, seja por acidente. Cabe, no entendimento desta pesquisadora, ao direito a prerrogativa de modular o desenvolvimento científico e estabelecer em que bases sucederão as intervenções de máquinas na vida em sociedade.

Muito embora isto pareça distópico e até ingênuo, há meios factíveis de se iniciar um processo de aculturação das boas práticas de segurança em desenvolvimentos de software e, por conseguinte, de respeito à privacidade dos usuários. A partir da regulamentação dos artigos 46, 47, 48, 49,50 e 51 da Lei Geral de Proteção de Dados que dizem respeito à segurança, ao sigilo dos dados e às boas práticas de governança, teremos um cenário profundamente inovador.

A obrigatoriedade da inserção de módulos de segurança nos fluxogramas de desenvolvimento, além de requisitos de programação segura, bem como políticas de pentests que mapeiem vulnerabilidades nas aplicações e as classifique com base em critérios previstos em metodologias reconhecidas, tais como *OWASP Top Ten*[179], *Sans Top 25*[180] e *Cyber Kill Chain*[181], e que dada a dinamicidade dos ataques cibernéticos, estes testes sejam recorrentes, em muito contribuiriam para a entrada no mercado de sistemas mais robustos e resilientes a ataques o que fatalmente diminuiria a quantidade de acessos indevidos ou vazamentos de dados, como popularmente se denominam estes eventos.

Mais do que a obrigatoriedade de camadas de segurança em softwares a partir de sua concepção e por padrão, cabe também à ANPD promover discussões, eventos e outros documentos sobre o entendimento do conceito de segurança, visto que nas palavras de Bruce

[179] https://owasp.org/www-project-top-ten/ (Acesso em 13/01/2022)
[180] https://www.sans.org/top25-software-errors/ (Acesso em 13/01/2022)
[181] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Acesso em 13/01/2022)

Schneier, importante criptógrafo americano, segurança é um processo e não um produto[182]. Nesta linha, os mapeamentos de processos de tratamento de dados devem incluir as diversas modalidades de conscientização, de acordo com o nível de maturidade da instituição sobre como a segurança pode ser melhorada, desde requisitos físicos, até os digitais que envolvem a guarda de informação em softwares largamente usados em ambientes corporativos, tais como, CRM'S – *Customer Relationship Management* ou Gestão de Relacionamento com o Cliente e ERP'S – *Enterprise Resource Planning* ou Sistema de Gestão Integrada. Cabe ainda salientar que um processo de auditoria sobre os contratos das licenças destes tipos de software pode ensejar a necessidade de aditivos com base na LGPD, bem como o versionamento, por parte do desenvolvedor, das aplicações que já operam no mercado no que diz respeito à segurança dos dados imputados nestes sistemas.

Para além de providências específicas no que diz respeito ao desenvolvimento de softwares, há diversas outras contramedidas e medidas mitigadoras, além de protocolos e políticas que, se não impossibilitam a ocorrência de um ataque cibernético e consequentemente o vazamento de dados, ao menos mitigam em grande medida os danos que estes podem causar.

A existência de uma política de segurança da informação é o primeiro passo para a introdução do conceito de segurança em uma instituição, seja ela pública, seja ela privada, pois não custa lembrar que a LGPD não se restringe a controladores e operadores apenas de natureza privada, mas também à administração pública em todas as suas instâncias. Hierarquicamente, é a política de segurança da informação que delimita as diretrizes, os princípios e até mesmo a metodologia por meio da qual a segurança será implementada, além de ser também um instrumento em constante atualização e que envolve requisitos de segurança física que observam a natureza do ramo de negócio a que ela se destina, bem como os riscos aos quais aquele controlador ou operador de dados está exposto.

Integram e complementam indissociavelmente os esforços preventivos na instituição de políticas de segurança os seguintes documentos:

- Política de restrição física e do ambiente;
- Política de acesso e política de BYOD[183];

[182] SCHNEIER, Bruce. Segurança.com: Segredos e mentiras sobre a proteção na vida digital. 2001.

[183] *Bring your own* device: traga seu próprio dispositivo.

- Política de backup, política de restauração de *backup* e política de gerenciamento de crise;
- Política de e-mail, política de evasão de dados;
- Conjunto de recomendações para contração de IDS (*Intrusion Detection Systems*) e IPS (*Intrusion Prevention System*) e SIEM (*Security Information And Event Management*) ou Sistema de Gerenciamento e Correlação de Eventos de Segurança;
- Política para contratação de software e hardware;
- Política de avaliação de risco cibernético;
- Documentação relacionada aos padrões de segurança recomendados, especialmente quanto às políticas de criptografia e gerenciamento de chaves;
- Termo de compromisso sobre SI e sigilo de dados voltado à alta direção;
- Documento descritivo de processos (PDCA)[184] produzido em parceria com a equipe técnica do cliente para manter atualizado o gerenciamento de segurança da informação;
- Matriz de *Due Diligence* de terceiros, específico de SI para comprovação de boas práticas;
- Análise de contratos de terceiros especificamente com relação aos aspectos de segurança da informação, bem como o apontamento de recomendações a respeito de boas práticas quando estas não estiverem expressas;
- Plano de Resposta a incidentes de segurança;
- Plano de Recuperação de desastre (*Disaster Recovery Plan – DRP*)[185]; e
- Plano de ação, definindo o conjunto de ações internas para dar efetividade à implementação de todas as políticas.

É de fundamental entendimento que estas proposições não são criações desta pesquisadora, mas propostas fartamente compartilhadas entre os profissionais que atuam na área de segurança cibernética e, reconhecidamente, tidas como boas práticas, o que ao fim e ao cabo se prestam aos fins mencionados na LGPD ao tratar do tema.

[184] PDCA: *Plan, Do, Check, Act*, ou Planejar, Fazer, Checar e Agir.
[185] O objetivo de um Plano de Recuperação de Desastre (DRP) é garantir que uma empresa organização possa reagir a um desastre ou outra emergência que afete os sistemas de informação e minimizar o seu efeito sobre as operações de negócios.

A produção de todos estes documentos, bem como sua efetiva implementação ensejam evidências de condutas proativas no enfrentamento às ameaças cibernéticas, mas não só. Reforçam cuidados simples no que diz respeito ao sigilo de documentos físicos e até sobre locais em que tais documentos estão guardados.

Por fim, simulam situações de crise e quais providências devem ser tomadas, tanto do ponto de vista técnico, quanto do ponto de vista jurídico e com isso melhoram a eficiência e a proteção dos dados dos titulares quando da ocorrência de incidentes cibernéticos ou mesmo de compartilhamento indevido de dados seja por quais meios forem.

A adoção de medidas, tais como as aqui descritas, denotam claramente um esforço técnico-jurídico no sentido de proteger controladores, operadores e titulares de dados de eventuais danos causados por incidentes de segurança e materializam a nova tendência a que os operadores do direito têm sido expostos, sobretudo no caso dos advogados afeitos a questões relativas ao ambiente corporativo, pois assumem um papel estratégico dentro da organização e contribuem para o sucesso do negócio na medida em que evitam danos reputacionais e prejuízos financeiros.

Há, desta forma, um horizonte já delineado e em franca expansão que espera do direito o entendimento e o apoio para melhorar o mundo, tornar a vida cotidiana mais prática e as pessoas mais felizes, visto que ao deixarem de fazer tarefas repetitivas e até mesmo mecânicas possam se dedicar àquilo que, de fato, lhes dá prazer e contentamento.

O exercício regulatório e o próprio ato judicante têm a missão de limitar os excessos, criar mecanismos de contenção, estabelecer diretrizes, apontar meios menos danosos para a disponibilização da informação, sobretudo em tempos de economia digital e de farto compartilhamento de dados e punir os atos que contrariem o justo progresso e a evolução saudável da humanidade o que somente será possível se o direito se atualizar, se acompanhar o desenvolvimento tecnológico, se estiver par e passo conexo com o tempo presente, com os ditames da sociedade contemporânea e os vieses tecnológicos que permeiam este momento histórico.

## EPÍLOGO

As conclusões, tão comuns ao final dos trabalhos acadêmicos não serão lidas aqui, visto que este estudo é datado, no sentido de que reflete os desdobramentos tecnológicos do momento em que foi escrito, mas também pelos ensinamentos do Prof. Fábio Konder Comparato em sua obra clássica O Poder de Controle na Sociedade Anônima a respeito das conclusões das dissertações científicas: "*Hodiernamente, porém, nem toda dissertação apresenta uma estrutura linear, mas radial ou sistemática*", concluindo, pouco mais adiante, que: "*Uma dissertação científica não deve, pois, literalmente falando, apresentar conclusões.*" Ao que, posteriormente foi complementado pelo Prof. Newton De Lucca quando apontou como verdadeiro exercício de humildade o momento de finalização de um estudo em razão de no momento do término sermos inundados fartamente pela sensação de desconhecimento e de limitação humana em face da complexidade do universo e das coisas e pessoas nele contidas. Será por tais evidências senão um erro, um "equívoco metodológico" a inserção de conclusões, visto não se poder concluir, mas apenas finalizar o registro de um momento histórico sobre determinado tema.

Ainda assim, é inimaginável que não arrematemos as discussões apresentadas neste estudo, consideradas, por óbvio, a limitação dos argumentos aqui debatidos e a estreita capacidade desta pesquisadora em contribuir com tema tão complexo e interdisciplinar.

É imperioso apontar, inicialmente, a dificuldade de se produzir uma tese jurídica com viés tão interdisciplinar quanto esta. Isto ocorre, sobremaneira, em razão de ser necessário um conhecimento, ainda que não aprofundado dos aspectos tecnológicos sobre os quais deverão as questões jurídicas ser discutidas. É, por certo, um conhecimento instrumental, mas que expõe a capacidade e o domínio do pesquisador sobre um tema diametralmente oposto àquele afeito à ciência jurídica o que requer um esforço e uma metodologia suficientemente didática para guiar o leitor pelos pontos que são, de fato, importantes.

Neste aspecto, vimos que algum conhecimento sobre o desenvolvimento da Internet, como ela funciona e seus principais impactos na sociedade foram primordiais para contextualizarmos o objeto deste estudo, visto que a Internet das Coisas é resultado da evolução da própria Internet.

No mesmo passo, seguiu o capítulo sobre segurança da informação, trazendo conceitos mais técnicos, porém fundamentais, para a discussão aqui proposta, pois se o nosso intuito era falar sobre proteção de dados em IoT, é impossível não tratar de segurança da informação, já

que é ela a responsável por orientar o processo de desenvolvimento seguro de dispositivos e, consequentemente, possibilitar que os dados neles armazenados estejam minimamente protegidos de ataques cibernéticos ou mesmo compartilhamentos indevidos. Ressalta-se, ainda, que a segurança da informação tem sido um dos principais temas relacionados a dados, não só no Brasil, como no mundo, em razão da quantidade exponencial de ataques cibernéticos que têm indisponibilizado sistemas corporativos e órgãos de governo numa onda vertiginosa de vazamentos de dados e prejuízos imensuráveis aos titulares.

Muito embora este estudo tenha compartimentado os assuntos, sobretudo por razões didático-pedagógicas, é indiscutível que eles se entrecruzam numa clara demonstração de que não será mais possível analisar temas eminentemente jurídicos, como a proteção de dados, sem que olhemos para questões técnicas, em especial pelo fato de que a coleta, o armazenamento e o compartilhamento de dados pessoais ocorre fundamentalmente por meio de dispositivos interconectados o que não é só uma tendência, mas um recurso com o qual toda a sociedade se movimenta.

Neste mesmo sentido, vimos a partir dos dados aqui referenciados como as máquinas têm se tornado cada vez mais protagonistas dos processos de tratamento de dados e até de atividades nunca realizadas automaticamente. É certo que a sociedade tem recebido estes avanços de forma muito diferente, até por questões econômicas e de desenvolvimento científico, mas é certo também que este é um processo inevitável e para o qual o direito precisa se atentar.

Ainda que vivamos em uma sociedade globalizada e recebamos notícias e insumos tecnológicos de outros países, é necessário registrar que do ponto de vista local, muito pouco avançamos no incentivo ao desenvolvimento de políticas públicas para implementação de IoT em diferentes contextos brasileiros e, mesmo com o robusto estudo realizado pelo Ministério da Ciência e Tecnologia em parceria com o BNDES em 2017, avançamos pouquíssimo na implementação da governança e das ações de facilitação para o desenvolvimento da Internet das Coisas no Brasil.

E este é um ponto, de fato, muito relevante, posto que anterior à discussão sobre a implementação e incentivos de políticas públicas voltadas à Internet das coisas, precisamos resolver problemas que antecedem esta tecnologia, tais como as questões de conectividade que são absolutamente díspares entre as diferentes regiões brasileiras. A pandemia da Covid-19 evidenciou este problema, na medida que com o isolamento social e a impossibilidade de as crianças e jovens frequentarem a escola fez com que as aulas fossem realizadas remotamente e

a falta de conectividade não permitiu o acesso de muitos alunos ao ensino remoto, além é claro, de outras questões, igualmente graves e relegadas a segundo plano pelos governos municipais, estaduais e federais.

É paradoxal que estejamos falando do desenvolvimento da Internet das Coisas e seus desdobramentos técnico-jurídicos num país que carece de conectividade em muitos espaços. É ainda importante registrar que a despeito da velocidade com que o desenvolvimento tecnológico se apresenta, o acesso a estes recursos é limitado, caro e inacessível para muitos brasileiros.

Na mesma linha do desrespeito aos direitos fundamentais, mas em outro sentido, observamos a voracidade com que o mercado tecnológico se organiza para escalar, independentemente da previsão legal de diversas normas gerais e setoriais. Era, até bem pouco tempo atrás, impensável questionar desenvolvedores sobre protocolos de segurança nos processos de desenvolvimento de software, isto porque a usabilidade sempre foi uma prioridade em detrimento da segurança. Não que não houvesse boas práticas, requisitos de programação segura, entre outras recomendações para se manter os dados coletados seguros e livres de acessos indevidos, além da mitigação de ataques cibernéticos.

A Lei 13.709/2018 – Lei Geral de Proteção de Dados, o GDPR – *General Data Protection Regulation*, entre outras legislações, compilaram as boas práticas de segurança da informação e os direitos inerentes aos titulares de dados pessoais num claro esforço de minimizar o compartilhamento indiscriminado de dados e a coleta desvinculada de uma finalidade específica.

A partir destas disposições legais, é possível estabelecer critérios claros baseados na segurança como padrão de desenvolvimento e, portanto, na observância dos preceitos relacionados aos direitos dos titulares nos mais diferentes contextos.

Seja em IoT, seja em qualquer outro contexto tecnológico, a segurança e a privacidade dos dados dos usuários devem ser reiteradamente consideradas, ainda que as máquinas estejam aptas a substituir humanos, há que se levar em conta princípios e valores que contemplem o bem, o justo e o coletivo, posto que nenhum desejo pessoal se sobreponha ao futuro da humanidade.

Do ponto de vista exclusivamente acadêmico, entendemos fundamental apontarmos as contribuições deste trabalho para a comunidade jurídica, mas não só para esta, como também para os engenheiros e cientistas da computação, em razão do fato de que este trabalho é um estudo interdisciplinar o que o faz consentâneo ao momento em que foi produzido, pois hoje profissionais do direito demonstram tanto interesse por tecnologia, quanto pela própria ciência

jurídica, haja vista a própria existência de segmentos, tais como o direito digital e a própria proteção de dados que vem se mostrando como um dos ramos mais profícuos para o exercício advocatício.

Na mesma linha, a produção de um trabalho acadêmico jurídico que considere, ainda que instrumentalmente, os vieses de desenvolvimento tecnológico contemporâneos, aproxima o exercício salutar da observância do cotidiano, de um conceito mais rigoroso do homem contemporâneo e seu comportamento em sociedade, o que inevitavelmente resvala na atividade judicante e na maneira como a ciência jurídica performa e evolui.

Tudo isso se dá, fundamentalmente, pela natureza ubíqua da tecnologia e de como ela vem transformando o mundo em todos os aspectos. O tempo em que vivemos não é só o que está mudando a perspectiva do usuário humano por máquinas, mas um lugar marcado historicamente pela fluidez, pela praticidade e pela celeridade, características que para o bem e para o mal refletem as muitas dúvidas que permeiam nosso imaginário.

Por fim, que este trabalho suscite muitas reflexões sobre o lugar para onde estamos indo e de que forma estamos caminhando. Mais do que isso, que entendamos o real papel da tecnologia em sociedade para que, ao fim e ao cabo, ela seja utilizada para o nosso progresso e não para o nosso aniquilamento, pois nas palavras de Arthur C. Clarke “Qualquer tecnologia suficientemente avançada é indistinguível de mágica”. Isto posto, que escolhamos as mágicas que nos façam sorrir, que tornem nossa vida mais prazerosa e o mundo mais justo.

**BIBLIOGRAFIA**


AAZAM, Mohammad; HARRAS, Khaled A.; ZEADALLY, Sherali. *Fog computing for 5G tactile industrial Internet of Things: QoE-aware resource allocation model*. IEEE Transactions on Industrial Informatics, v. 15, n. 5, p. 3085-3092, 2019.

ABBAS, M. Internet of Things (IOT) – *We Are At The Tip of An Iceberg*. In: MIMOS Berhad, 2014, Wismas IEM, Petaling Jaya. Disponível em: https://pt.slideshare.net/mazlan1/internet-of-things-iot-we-are-at-the-tip-of-an-iceberg/44-Crowdsensing (Acesso em 13/01/2022)

ACQUISTI, Alessandro. *The Economics of Personal Data and the Economics of Privacy*. Joint WPISP-WPIE Roundtable. Background paper #3. Disponível em: https://www.oecd.org/sti/ieconomy/46968784.pdf. (Acesso em 13/01/2022)

ADHATARAO, Sripriya Srikant et al. *ISI: Integrate sensor networks to Internet with ICN*. IEEE Internet of Things Journal, v. 5, n. 2, p. 491-499, 2017.

AKHTAR, Nikhat; PERWEJ, Yusuf. The internet of nano things (IoNT) existing state and future Prospects. GSC Advanced Research and Reviews, v. 5, n. 2, p. 131-150, 2020.

AL-FUQAHA, Ala et al. *Internet of things: A survey on enabling technologies, protocols, and applications*. IEEE communications surveys & tutorials, v. 17, n. 4, p. 2347-2376, 2015.

ALEISA, Noura; RENAUD, Karen. *Privacy of the Internet of Things: A Systematic Literature Review*. Proceedings of the 50th Hawaii International Conference on System Sciences, p. 5947-5956, 2017.

ALVES, Alexandre Ferreira de Assumpção, et. Al. Problemas de direito constitucional. Rio de Janeiro: Renovar, 2001. P. 113.

AMAZONAS, José Roberto de Almeida. Aula I: *Iot Fundamentals. In: IoT: Fundamentals and next generation IoT*. Curso online promovido pelo Fórum Brasileiro de IoT. 2020.

AMAZONAS, José Roberto et al. *Service level agreements for communication networks: A survey*. INFOCOMP Journal of Computer Science, v. 18, n. 1, p. 32-56, 2019.

ANDRADE, Leandro Prado de. *Privacy Everywhere*: mecanismo para tomada de decisões e garantia da privacidade em ambientes IoT. 2019. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de São Carlos, São Carlos, 2019.

ANJUM, Shaik Shabana et al. *Energy management in RFID-sensor networks: Taxonomy and challenges*. IEEE Internet of Things Journal, v. 6, n. 1, p. 250-266, 2017.

ARQUILLA, John; RONFELDT, D. *The emergence of noopolitik: Toward na american information strategy*. Disponível em: https://www.rand.org/search.html?query=noopolitik. (Acesso em 13/01/2022)

ARSHAD, Sobia et al. *Recent advances in information-centric networking-based Internet of Things (ICN-IoT).* IEEE Internet of Things Journal, v. 6, n. 2, p. 2128-2158, 2018.

ASLAM, Saleem; EJAZ, Waleed; IBNKAHLA, Mohamed. *Energy And Spectral Technology Cognitive Radio Sensor Networks For Internet Of Things*. IEEE Internet of Things Journal, v. 5, n. 4, p. 3220-3233, 2018.

ASSOCIAÇÃO BRASILEIRA DE INTERNET DAS COISAS. Políticas para IoT. Disponível em: https://abinc.org.br/politicas-para-iot/ (Acesso em 13/01/2022)

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 27001:2013: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2013.

ATZORI, L.; IERA, A.; MORABITO, G. *The internet of things: a survey*. Computer Networks, v. 54, n. 15, 2010. Disponível em: https://doi.org/10.1016/j.comnet.2010.05.010 (Acesso em 13/01/2022)

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. *From" smart objects" to" social objects": The next evolutionary step of the internet of things*. IEEE Communications Magazine, v. 52, n. 1, p. 97-105, 2014.

AUSTIN, John Langshaw. *How to Do Things with Words*. Clarendon Press, Oxford, 1962.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Disponível em: https://www.gov.br/anpd/pt-br (Acesso em 13/01/2022)

_____. ANPD está apurando no caso de vazamento de dados de mais de 220 milhões de pessoas. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas (Acesso em 13/01/2022)

_____. ANPD Participa de Audiência Pública da Comissão de Ciência e Tecnologia do Senado Federal. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-de-audiencia-publica-da-comissao-de-ciencia-e-tecnologia-do-senado-federal (Acesso em 13/01/2022)

AYRES, Marcel; RIBEIRO, José Carlos. A dimensão informacional na regulação do contexto de privacidade em interações sociais mediadas por dispositivos móveis celulares. Intercom: Revista Brasileira de Ciências da Comunicação, v. 41, n. 1, p. 81-97, 2018.

BALASUBRAMANIAM, Sasitharan; KANGASHARJU, Jussi. *Realizing the internet of nano things: challenges, solutions, and application*s. Computer, v. 46, n. 2, p. 62-68, 2012.

BARAD, Karen. *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Durham e London: Duke University Press, 2007.

BARTH, Susanne; DE JONG, Menno D. T. *The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior; A systematic literature review*. Telematics and Informatics, v. 34, n. 07, p. 1038-1058, 2017.

BECKER, Daniel; FERRARI, Isabela. Regulação 4.0: Novas tecnologias sob a perspectiva regulatória. São Paulo: Thomson Reuters-Revista dos Tribunais, 2019.

BECKER, Daniel; FERRARI, Isabela. Regulação 4.0: Novas tecnologias sob a perspectiva regulatória. Vol. II. São Paulo: Thomson Reuters-Revista dos Tribunais, 2020.

BELLI, Lucca. (2020). Uma perspectiva de Direitos Humanos para decriptar a ascensão da Internet das Coisas (IoT). Revista Brasileira De Direitos Fundamentais & Justiça, *13*(41), 157-181. https://doi.org/10.30899/dfj.v13i41.775. (Acesso em 13/01/2022)

BENÖHR, I. *The United Nations Guidelines for Consumer Protection: Legal Implications and New Frontiers*. In: Journal of Consumer Policy 43, 2020, pp. 105-124. Disponível em: ou https://doi.org/10.1007/s10603-019-09443-y . (Acesso em 14/01/2022)

BERGSTEIN, L. Direito à Portabilidade na Lei Geral de Proteção de Dados. Revistas dos Tribunais, Vol. 1003/2019, maio, 2019.

BEZERRA, Arthur Coelho. Vigilância e cultura algorítmica no novo regime global de mediação da informação. Perspectivas em Ciência da Informação, Belo Horizonte, v. 22, n. 4, p. 68-81, 2017.

BIONI, Bruno Ricardo. Proteção de dados pessoais: funções e limites do consentimento. Rio de Janeiro: Forense, 2ª ed. 2020.

BANCO NACIONAL DO DESENVOLVIMENTO. Relatório do plano de ação. Iniciativas e projetos mobilizadores. 2017. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil (Acesso em 14/01/2022)

_____. Consulta a operações do BNDES. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/transparencia/consulta-operacoes-bndes (Acesso em 13/01/2022)

BORBA, Victor Ubiracy. Proposta de um modelo de referência para Internet das Coisas: aspectos de segurança e privacidade na coleta de dados. 2018.

BÖSCH, Christoph. Et al. *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*. Proceedings on Privacy Enhancing Technologies, v. 2016, n. 4, jan. 2016. Disponível em: https://doi.org/10.1515/popets-2016-0038 (Acesso em 14/01/2022)

BRACHT, Fábio. Como Foi – e o Que Significa – A Vitória do Computador da IBM Sobre os Humanos em Jeopardy! Disponível em: https://gizmodo.uol.com.br/computador-da-ibm-vence-de-lavada-dois-cerebros-humanos-em-jogo-de-conhecimentos-gerais/ (Acesso em 13/01/2022)

BRANDEIS, Louis; WARREN, Samuel. *The Right to Privacy*. Harvard Law Review 4, v. IV, n. 5, p. 193-220, 1890.

BRASIL. CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). Processo Administrativo nº 08012.000172/1998-42. Representatne: Power-Tech Teleinformática Ltda. Representada: Damovo do Brasil S.A. (Matel Tecnologia de Informática Ltda. – MATEC). Relator: Conselheiro Celso Fernandes Campilongo. Brasília, 26 de março de 2003. Voto-vista do Conselheiro Ronaldo Porto Macedo Júnior, p. 17, nota de rodapé n. 20. Disponível em: https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_processo_exibir.php?0c62g277GvPsZDAxAO1tMiVcL9FcFMR5UuJ6rLqPEJuTUu08mg6wxLt0JzWxCor9mNcMYP8UAjTVP9dxRfPBcRhSHMvQSWaRvGPtitEodv1N7fx_BvMSYpr35EnbFPxV. (Acesso em 13/01/2022)

_____. Constituição da República Federativa do Brasil. 1988. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. (Acesso em 13/01/2022)

_____. Lei nº 12.965, de 23 de Abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (Acesso em 13/01/2022)

_____. Decreto nº 9854 de 25 de junho de 2019. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-9854-de-25-de-junho-de-2019-173021041 (Acesso em 13/01/2022)

_____. Ministério da Ciência e Tecnologia. Estratégia Digital Brasileira. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/inovacao/paginas/politicasDigitais/estrategia_digital/_brasileira/Estrategia_Digital_Brasileira.html Acesso em 03/12/2021 (Acesso em 13/01/2022)

_____. Portaria nº 11 de 27 de janeiro de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313 (Acesso em 13/01/2022)

_____. Senado Federal. Avulso Inicial da Matéria ou Proposição Original, de 12/03/2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1594003895291&disposition=inline (Acesso em 13/01/2022)

_____. Senado Federal, Comissão de Constituição, Justiça e Cidadania. Parecer da CCJ (resultante da aprovação do parecer da relatória Simone Tebet, em 22.05.2019). Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004 (Acesso em 14/01/2022)

_____. Senado Federal. Autógrafo da PEC (encaminhado à Câmara dos Deputados em 03/07/2019). Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7974467 (Acesso em 14/01/2022)

BREWSTER, Christopher et al. *IoT in agriculture: Designing a Europe-wide large-scale pilot*. IEEE communications magazine, v. 55, n. 9, p. 26-33, 2017.

BRITANNICA. *IP-adress*. In: Encyclopedia Britannica. Disponível em: https://www.britannica.com/technology/IP-address (Acesso em 13/01/2022)

BRYNJOLFSSON, Erik; MCAFEE, Andrew. A segunda era das máquinas: trabalho, progresso e prosperidade em uma época de tecnologias brilhantes. Rio de Janeiro, RJ: Alta Books, 2015.

BUCHENSCHEIT, Andreas et al. *Privacy implications of presence sharing in mobile messaging applications*. Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia–MUM '14, v. 1, n. 1, p. 20-29, Dec. 2014.

BUNZ, Mercedes. *The Internet Of Things: Tracing A New Field Of Enquiry*. Media, Culture & Society, v. 38, n. 8, p. 1278-1282, 2016.

BUSH, Vannevar. *As We May Think*. The Atlantic. Issue July, 1945. Disponível em https://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/ (Acesso em 16/01/2022)

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade Hoje: Perspectiva Histórica e o Cenário Brasileiro. Sequência (Florianópolis), p. 213-239, 2017.

CAO, Hung et al. *Analytics everywhere: generating insights from the internet of things*. IEEE Access, v. 7, p. 71749-71769, 2019.

CARBONI, Davide et al. *Scripting a smart city: the CityScripts experiment in Santander*. In: 2013 27th International Conference on Advanced Information Networking and Applications Workshops. IEEE, 2013. P. 1265-1270.

CASAGRAS. *RFID and the Inclusive Model for the Internet of Things*. CSA for Global RFID-related Activies and Standardization. 2009. https://docbox.etsi.org/zArchive/TISPAN/Open/IoT/low%20resolution/www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf (Acesso em 13/01/2022)

CASTELLUCCIA, C. et al. *Enhancing Transparency and Consent in the IoT*. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2018, pp. 116-119, doi: 10.1109/EuroSPW.2018.00023.

CASTRO, Bárbara Brito de. Direito Digital na era da internet das coisas – o direito à privacidade e a Lei Geral de Proteção de Dados Pessoais. Revista Fórum de Direito na Economia Digital – RFDED, Ano 3, N. 4, p. página inicial-página final, jan/jun. 2019. Disponível em: https://www.forumconhecimento.com.br/periodico/214/41795/89835 (Acesso em 13/01/2022)

CASTRO, Ivan Nunes. O que é benchmarking e qual a sua importância para o marketing digital. Disponível em: https://rockcontent.com/br/blog/benchmarking/ (Acesso em 13/01/2022)

CAVANILLAS, José Maria; CURRY, Edward; WAHLSTER, Wolfgang. *The Big Data Value Opportunity*. In: CAVANILLAS, José Maria; CURRY, Edward; WAHLSTER, Wolfgang (editors). *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe*. Springers Open. Disponível em: https://link.springer.com/book/10.1007%2F978-3-319-21569-3 (Acesso em 13/01/2022)

CAVOUKIAN, Ann. *Information & Privacy: 7 foundational principles*. Internet Architecture Board. 2011. Disponível em: https://www.iab.org/wpcontent/IABuploads/2011/03/fred_carter.pdf . (Acesso em 13/01/2022)

_____; JONAS, Jeff. *Privacy by Design in the Age of Big Data*. *Information and Privacy Commissioner of Ontario*, 2012. Disponível em: https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf (Acesso em 13/01/2022)

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Disponível em: https://www.cert.br/ (Acesso em 14/01/2022)

CHARDIN, T. Disponível em: https://pt.wikipedia.org/wiki/Teilhard_de_Chardin (Acesso em 13/01/2022)

CHAUDURI, Abhik. *Internet of things, for things and by things*. CRC Press. 2018.

CHENEY-LIPPOLD, John. *We Are Data*. New York: NYU Press, 2017.

CHIKUKWA, G. *A Consent Framework for the Internet of Things in the GDPR Era* (2021). Masters Theses & Doctoral Dissertations. Dakota State University. Disponível em https://scholar.dsu.edu/theses/362 (Acesso em 13/01/2022)

CHRIST, Oliver. *Martin Heidegger's Notions of World and Technology in the Internet of Things age*. Asian Journal of Computer and Information Systems, v. 3, n. 2, p. 58-64, 2015.

CISCO. *At a glance: Internet of Things. 2016*. Disponível em: https://www.cisco.com/c/dam/ en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf. (Acesso em 13/01/2022)

COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões. Uma abordagem global da protecção de dados pessoais na União Europeia. Bruxelas, 4 nov. 2010. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-7-2011-0323_PT.html (Acesso em 13/01/2022).

COMITÊ GESTOR DA INTERNET. Princípios para a governança e uso da Internet. Disponível em: https://principios.cgi.br (Acesso em 13/01/2022).

COMPARATO, Fábio Konder; SALOMÃO FILHO, Calixto. O poder de controle na sociedade anônima. Rio de Janeiro: Forense, 2014.

CONSULTOR JURÍDICO. Câmara aprova projeta que regulamenta uso da inteligência artificial. Disponível em https://www.conjur.com.br/2021-set-30/camara-aprova-projeto-regula-uso-inteligencia-artificial (Acesso em 13/01/2022)

CONSUMIDOR MODERNO. Roupas inteligentes prometem melhorar exercícios físicos em tempo real. Disponível em: https://www.consumidormoderno.com.br/2020/02/19/roupas-inteligentes-exercicios-fisicos/ (Acesso em 13/01/2022)

CORNO, Fulvio; DE RUSSIS, Luigi. *Training engineers for the ambient intelligence challenge*. IEEE Transactions on Education, v. 60, n. 1, p. 40-49, 2016.

COUTINHO, Dimítria. Ao menos oito vazamentos de dados aconteceram no Brasil em 2021: quem é punido? Disponível em: https://tecnologia.ig.com.br/2021-03-28/ao-menos-oito-vazamentos-de-dados-aconteceram-no-brasil-em-2021--quem-e-punido-.html (Acesso em 13/01/2022)

COUTINHO, Gustavo Leuzinger. A era dos smartphones: um estudo exploratório sobre o uso dos smartphones no Brasil. 2014. 60 f., il. Monografia (Bacharelado em Comunicação Social) – Universidade de Brasília, Brasília, 2014.

CRAVO, Victor. O Big Data e os desafios da modernidade: uma regulação necessária? Revista de Direito Setorial e Regulatório, Brasília, v. 1, n. 2, p. 243-257, out. 2015.

CUNCHE, M; MOREL, V; MÉTAYER, D. L. *A Generic Information and Consent Framework for the IoT*. 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 13th IEEE. International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2019, pp. 366-373, doi: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00056 (Acesso em 13/01/2022).

DAI, Lu et al. *A nature-inspired node deployment strategy for connected confident information coverage in industrial Internet of Things*. IEEE Internet of Things Journal, v. 6, n. 6, p. 9217-9225, 2019.

DANAHER, John. *The Threat of Algocracy: Reality, Resistance and Accommodation*. Philosophy and Technology, v. 29, n. 3, p. 245-268, 2016.

DE DONNO, Michelle; TANGE, K; DRAGONI, Nicola. *Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog*. IEEE Access, vol. 7, pp. 150936-150948, 2019, doi: 10.1109/ACCESS.2019.2947652.

DECEW, Judith Wagner. *In pursuit of privacy: law, ethics, and the rise of technology*. Ithaca: Cornell University Press, 1997.

DELEUZE, Gilles. Posdata sobre las sociedades de control.In: FERRER, Christian (Comp.). El linguaje libertario:Antología del pensamiento anarquista contemporáneo. Buenos Aires: Altamira, 1999.

DE LUCCA, Newton. A Cambial-Extrato, Revista dos Tribunais, São Paulo, 1985.

_____. A*spectos Jurídicos da Contratação Informática e Telemática.* São Paulo: Saraiva, 2003.

_____. Direito do Consumidor – Teoria Geral da Relação de Consumo, São Paulo: Quartier Latin, 2003.

_____. Títulos e contratos eletrônicos: o advento da Informática e suas consequências para a pesquisa jurídica. *In:* _____; SIMÃO Filho, Adalberto. (coords.) *Direito & Internet:* aspectos jurídicos relevantes. 2. Ed. São Paulo: Quartier Latin, 2005. P. 30 – 126.

_____. SIMÃO Filho, Adalberto. (coords.). *Direito & Internet: aspectos jurídicos relevantes*. 2. Ed. São Paulo: Quartier Latin, 2005.

_____. Da Ética Geral à Ética Empresarial – São Paulo: Quartier Latin, 2009, p. 234.

_____. SIMÃO Filho, Adalberto. LIMA, C.R.P de. (coords). *Direito & Internet III: Marco Civil da Internet. Lei 12.965/2014*. São Paulo: Quartier Latin, 2015. Tomos I e II.

_____. Yuval Noah Harari e sua Visão dos Dados de Cada um de Nós. Coluna Migalhas de Proteção de Dados, 02 de Junho de 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/346519/yuval-noah-harari-e-sua-visao-dos-dados-pessoais-de-cada-um-de-nos (Acesso em 13/01/2022)

_____. Entrevista ao site Migalhas. Disponível em https://www.migalhas.com.br/coluna/german-report/330304/entrevista-prof-dr-newton-de-lucca. (Acesso em 13/01/2022).

DE SAUSSURE, Ferdinand. Curso de linguística geral. Editora Cultrix, 2008.

DEMENTSHUK, Márcia; HENRIQUES, Percival. Pássaros voam em bando: A história da Internet do século XVIII ao século XXI. João Pessoa: Editora ANID, 2019.

DIETER, Michael. *Dark Patterns: Interface Design, Augmentation and Crisis*. In: BERRY, David M.; DIETER, Michael. Org.). Postdigital Aesthetics. London: Palgrave Macmillan UK, 2015. P. 163-178. Disponível em: http://link.springer.com/10.1057/9781137437204_13 (Acesso em 13/01/2022)

DIJCK, Jose van; POELL, Thomas; WAAL, Martijn de. *The Platform Society*. New York: Oxford University Press, 2018.

DIRKZWAGER, Aimee; CORNELISSE, Jimi; BROK, Tom; CORCORAN, Liam. *Where does your data go? Mapping the data flow of Nest*. Masters of Media. 2017.

DOHR, Angelika et al. *The internet of things for ambient assisted living*. In: 2010 seventh international conference on information technology: new generations. Ieee, 2010. P. 804-809.

DONEDA, Danilo; et al. Tratado de proteção de dados pessoais. 1 ed. Rio de Janeiro: Forense, 2021.

_____. Da Privacidade à Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020.

_____. Princípios de proteção e dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; de LIMA, C.R.P. (Coords.). Direito e Internet III: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo, Quartier Latin, 2015, pp. 369-384.

DOTY, Nick; GUPTA, Mohit. *Privacy Design Patterns and Anti-Patterns Patterns Misapplied and Unintended Consequences*. Proceedings of the Ninth Symposium on Usable Privacy and Security, v.1, n.1, p. 1-5, 2013.

DOURISH, Paul; GÓMEZ CRUZ, Edgar. *Datafication and Data Fiction: Narrating Data and Narrating with Data*. Big Data & Society, v. 5, n. 2, p. 1-10, jul. 2018.

DOURISH, Paul. *The Stuff of Bits*. Cambridge: MIT Press, 2017.

EHRHARDT JÚNIOR, M; PEIXOTO, E. L. C. Breves notas sobre a ressignificação da privacidade. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 16, p.35-56, abr./jun.2018. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/230/212 (Acesso em 13/01/2022)

EL-MOUGY, Amr; AL-SHIAB, Ismael; IBNKAHLA, Mohamed. *Scalable personalized iot networks*. Proceedings of the IEEE, v. 107, n. 4, p. 695-710, 2019.

ELVY, Stacy-Ann. *Commodifying Consumer Data In The Era Of The Internet Of Things*. Boston College Law Review, v. 59, n. 2, fev. 2018, p. 423-522.

EMBRAPA. *GPS – Global Positioning System*. Disponível em: https://www.embrapa.br/satelites-de-monitoramento/missoes/gps (Acesso em 13/01/2022)

EUROPEAN COMISSION. *Guidelines On Transparencyunder Regulation* 2016/679 (wp.260rev.01). Disponível em: https://ec.europa.eu/newsroom/article29/items/622227 (Acesso em 13/01/2022)

EUROPEAN COMMISSION. *Towards a thriving data-driven economy*. Disponível em: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy (Acesso em 13/01/2022)

EVANCZUK, Stephen. *Why IoT Success Hangs on Interoperability*. Mouser Electronics. Disponível em: https://www.mouser.com/blog/why-iot-success-hangs-on-interoperability . (Acesso em 13/01/2022)

FATHY, Yasmin; BARNAGHI, Payam. *Quality-Based And Energy-Efficient Data Communication For The Internet Of Things Networks*. IEEE Internet of Things Journal, v. 6, n. 6, p. 10318-10331, 2019.

FELDSTEIN, Steven. *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace, 2019. Disponível em: https://carnegieendowment.org/2019/09/17/global- expansion-of-ai-surveillance-pub-79847 (Acesso em 13/01/2022).

FINN, Ed. *What Algorithms Want: Imagination in the Age of Computing*. Cambridge: MIT Press, 2017.

FOUCAULT, Michel. Microfísica Do Poder. 2. Ed. Rio de Janeiro: Paz e Terra, 2015.

FOX, Nick J.; ALLDRED, Pam. *Sociology and the New Materialism: Theory, Research, Action*. London: SAGE Publications, 2016.

FRAZÃO, Ana.; MULHOLAND, Caitlin. (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo, SP: Thomson Reuters Brasil, 2019.

FROSINI, Tommaso Edoardo. *La libertà informatica: brevi note sull'attualità di una teoria giuridica*. Informatica e diritto, XXXIV annata, Vol. XVII, 2008, n. 1-2, pp. 87-97

FTC STAFF REPORT. *Internet of things: privacy & security in a connected world*. 2015. [S.l.: s.n.]. Disponível em https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (Acesso em 13/01/2022).

GAILLARD, Guillaume et al. *Kausa: KPI-aware scheduling algorithm for multi-flow in multi-hop IoT networks*. In: International Conference on Ad-Hoc Networks and Wireless. Springer, Cham, 2016. P. 47-61.

GAILLARD, Guillaume et al. *Service Level Agreements for Wireless Sensor Networks: A WSN operator's point of view*. In: 2014 IEEE Network Operations and Management Symposium (NOMS). IEEE, 2014. P. 1-8.

GALLEGO, B. C. & DREXL, J. *IoT Connectivity Standards: How Adaptive is the Current SEP Regulatory Framework?*. IIC 50, 135–156 (2019). Disponível em https://doi.org/10.1007/s40319-018-00774-w (Acesso em 13/01/2022).

GARCÍA, Nieves Buisán. "*Procedimientos por vulneración de la normativa de protección de datos: tramitación de denuncias*". In: LOMBARTE, Artemi Rallo (org.). Tratado de Protección de Datos. Actualizado Con la Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Valencia: Tirant lo Blanch, 2019, pp. 548-581.

GIRAU, Roberto; MARTIS, Salvatore; ATZORI, Luigi. *Lysis: A platform for IoT distributed applications over socially connected objects*. IEEE Internet of Things Journal, v. 4, n. 1, p. 40-51, 2016.

GONZÁLEZ, Mariana. Tradução Automática: O Que É, Quando Usar E Por Que Devemos Ter Cuidado Com Ela. Disponível em: https://rockcontent.com/br/talent-blog/o-que-e-traducao-automatica/ (Acesso em 13/01/2022).

GRAEF, Inge; HUSOVEC, Martin; PURTOVA, Nadezhda. *Data portability and data control: Lessons for an emerging concept in EU law*. In: German Law Journal, v. 19, n. 6, 2018, pp. 1359-1398. Disponível em: https://www.cambridge.org/core/journals/german-law-journal/article/data-portability-and-data-control-lessons-for-an-emerging-concept-in-eu-law/5904FB88DDC1B9E6EC651A7F89058433. (Acesso em 13/01/2022).

GREENGARD, Samuel. *The Internet Of Things*. Cambridge: The MIT Press, 2015, p. 58

GRUNES, Allen P.; STUCKE, Maurice E. *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*. In: University of Tennessee Legal Studies Research, Paper n° 269, 2015. Disponível em: https://ssrn.com/abstract=2600051. (Acesso em 13/01/2022).

HADZOVIC, Suada; MRDOVIC, Sasa; RADONJIC, Milutin. *Identification of IoT Actors. Sensors*. 2021; 21(6):2093. Disponível em https://doi.org/10.3390/s21062093 (Acesso em 13/01/2022).

HARARI, Yuval Noah. 21 lições para o século 21. Editora Companhia das Letras, 2018.

HASSAN, Najm; CHOU, Chun Tung; HASSAN, Mahbub. *eNEUTRAL IoNT: Energy-neutral event monitoring for Internet of nano things*. IEEE Internet of Things Journal, v. 6, n. 2, p. 2379-2389, 2019.

HAWKING, Stephen at al. "*Research Priorities for Robust and Beneficial Artificial Intelligence: An Open Letter*". Disponível em https://futureoflife.org/2015/10/27/ai-open-letter/ (Acesso em 16/01/2022)

HIGH, Peter. *Carnegie Mellon Dean of Computer Science on the Future of AI*. 30 out. 2017. Disponível em: https://www.forbes.com/sites/peterhigh/2017/10/30/carnegie-mellon- dean-of-computer-science-on-the-future-of-ai/#4a8a2df32197 (Acesso em 13/01/2022).

HILBERT, Martin. LÓPEZ Priscila. *The World's Technological Capacity to Store, Communicate, and Compute Information*. Science, abril de 2011, p. 60-65.

HINTZBERGEN, Jule et al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Brasport, 2018.

HOFFMANN-RIEM, Wolfgang. Teoria geral do direito digital: transformação digital, desafios para o Direito. Rio de Janeiro: Forense, 2021.

HOWER, Mike. *As "Internet Of Things" Grows, So Do E-Waste Concerns.* Sustainable Brands, 29 dez. 2014. Disponível em: www.sustainablebrands.com/news_and_views/waste_not/mike_hower/internet_things%E2%80%99_grows_so_do_e-waste_concerns . (Acesso em 13/01/2022).

IBM. Watson Assistant: Agente Virtual Inteligente. Disponível em: https://www.ibm.com/br-pt/products/watson-assistant (Acesso em 13/01/2022).

INBOT. Automatizar Tarefas: Vantagens De Contar Com Assistentes Pessoais Virtuais No Dia A Dia. Disponível em: https://www.inbot.com.br/blog/automatizar-tarefas-assistentes-pessoais/ (Acesso em 13/01/2022).

INFORWESTER. O Que É Firewall? – Conceito, Tipos E Arquiteturas. In. https://www.infowester.com/firewall.php (Acesso em 13/01/2022).

INTERNET DAS COISAS E PROTECÃO DE DADOS. Inforchanel. 2021. Disponível em: https://inforchannel.com.br/2021/04/27/internet-das-coisas-e-protecao-de-dados/ (Acesso em 13/01/2022).

INTERNET DAS COISAS. In: WIKIPÉDIA: A Enciclopédia Livre. [São Francisco, CA: Fundação Wikimedia]. Disponível em: https://pt.wikipedia.org/wiki/Internet_das_coisas (Acesso em 13/01/2022).

IoT-A – *Internet Of Things Architecture*. *Project website*: https://cordis.europa.eu/project/id/257521 (Acesso em 13/01/2022).

ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements. ISO - Internacional Organization for Standartization, 2013*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:en (Acesso em 13/01/2022)

ITU – *INTERNATIONAL TELECOMMUNICATION UNION*. *Next Generation Networks – Frameworks and Functional Architecture Models: Overview of the Internet of Things. Series Y: global information infrastructure, internet protocol aspects and next-generation networks*. Recommendation ITU-T Y.2060 (06/2012) renumbered as ITU-T Y.4000 on 2016-02-05. 2012.

JANAL, R. *Data Portability – A Tale of Two Concepts*, 8. JIPITEC 59, 2017, p.60.

JONES, Meg Leta. *Privacy Without Screens & The Internet of Other People's Things*. Idaho Law Review, v. 51, p. 639-660, 2015. Disponível em https://digitalcommons.law.uidaho.edu/idaho-law-review/vol51/iss3/3 (Acesso em 14/01/2022)

JUNG, J.; Chun, S. ; Jin, X. & Lee, K. *Quantitative Computation of Social Strength in Social Internet of Things*. In IEEE Internet of Things Journal, vol. 5, no. 5, pp. 4066-4075, Oct. 2018, doi: 10.1109/JIOT.2018.2869933. Disponível em https://doi.org/10.1109/JIOT.2018.2869933 (Acesso em 14/01/2022)

KAIWARTYA, Omprakash et al. *Virtualization In Wireless Sensor Networks: Fault Tolerant Embedding For Internet Of Thing*s. IEEE Internet of Things Journal, v. 5, n. 2, p. 571-580, 2017.

KANDASAMY, K., Srinivas, S., Achuthan, K. et al. *IoT Cyber Risk: A Holistic Analysis Of Cyber Risk Assessment Frameworks, Risk Vectors, And Risk Ranking Process*. EURASIP J. on Info. Security 2020, 8 (2020). https://doi.org/10.1186/s13635-020-00111-0 (Acesso em 14/01/2022)

KARIMOVA, Gulnara Z.; SHIRKHANBEIK, Amir. *Society of things: An alternative vision of Internet of things*. Cogent Social Sciences, v. 1, n. 1, p. 1-7, 2015. Disponível em https://www.tandfonline.com/doi/full/10.1080/23311886.2015.1115654 (Acesso em 14/01/2022)

KARNOUSKOS, S. *Stuxnet Worm Impact On Industrial Cyber-Physical System Security*. IECON 2011 – 37th Annual Conference of the IEEE Industrial Electronics Society, 2011, pp. 4490-4494, doi: 10.1109/IECON.2011.6120048. Disponível em https://doi.org/10.1109/IECON.2011.6120048 (Acesso em 14/01/2022)

KERBER, Wolfgang; SCHWEITZER, Heike. *Interoperability in the Digital Economy. Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. MAGKS Joint Discussion Paper Series in Economics, n. 12, 2017. Disponível em: https://ssrn.com/abstract=2922515 . (Acesso em 14/01/2022)

KERBER, Wolfgang. *Data-sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars*, 2019. Disponível em: https://ssrn.com/abstract=3445422 . (Acesso em 14/01/2022)

KHAN, R., KHAN, S. U., ZAHEER, R.; KHAN, S. *Future Internet: The Internet Of Things Architecture, Possible Applications And Key Challenges*. In: Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012. P. 257-260. DOI: 10.1109/FIT.2012.53. Disponível em https://doi.org/10.1109/FIT.2012.53 (Acesso em 14/01/2022)

KOKOLAKIS, Spyros. *Privacy Attitudes And Privacy Behavior: A Review Of Current Research On The Privacy Paradox Phenomenon*. Computers and Security, v. 64, p. 122-134, 2017. Disponível em https://www.sciencedirect.com/science/article/pii/S0167404815001017 (Acesso em 14/01/2022)

KUROSE, J. F. and ROSS, K. W. *Computer Networking: A Top-Down Approach*. Pearson; 7ª edição. 26 de abril de 2016. 864p. ISBN-10: 9780133594140

KYNDRIL. Recuperação De Plataformas Híbridas. Disponível em: https://www.kyndryl.com/br/pt/services/business-continuity/draas (Acesso em 14/01/2022)..

Labfaber. Disponível em: https://labfaber.certi.org.br/ (Acesso em 14/01/2022)

LAN, Lina et al. *An IoT Unified Access Platform For Heterogeneity Sensing Devices Based On Edge Computing*. IEEE access, v. 7, p. 44199-44211, 2019. DOI: 10.1109/ACCESS.2019.2908684. Disponível em https://doi.org/10.1109/ACCESS.2019.2908684 (Acesso em 14/01/2022)

LEE, J., Leung, V., Lee, AH. et al. *Neural Recording And Stimulation Using Wireless Networks Of Microimplants*. Nature Electron 4, 604–614 (2021). https://doi.org/10.1038/s41928-021-00631-8 (Acesso em 14/01/2022)

LEINER, Barry M. *et al*. *Brief History of the Internet*. 1997. Disponível em: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf. (Acesso em 14/01/2022)

LEITE, Eduardo de Oliveira. Monografia Jurídica. 10ª Ed. São Paulo: Revista dos Tribunais, 2014.

LEMIC, F. et al. *Survey on Terahertz Nanocommunication and Networking: A Top-Down Perspective*. In IEEE Journal on Selected Areas in Communications, vol. 39, no. 6, pp. 1506-1543, June 2021, doi: 10.1109/JSAC.2021.3071837. Disponível em https://doi.org/10.1109/JSAC.2021.3071837 (Acesso em 14/01/2022)

LEMOS, A. & MARQUES, D. Privacidade e Internet das Coisas: uma análise da rede Nest a partir da Sensibilidade Performativa. *E-Compós*, *22*(1). 2019. Disponível em: https://doi.org/10.30962/ec.1611. (Acesso em 14/01/2022)

LEMOS, André; BITENCOURT, Elias. Sensibilidade Performativa E Comunicação Das Coisas: Explorando As Narrativas Algorítmicas Na Fitbit Charge HR2. In: ENCONTRO ANUAL DA COMPÓS, 26., 2017, São Paulo. São Paulo: Faculdade Casper Líbero, 2017.

LENTZSCH, Christopher et al. *Integrating a Practice Perspective to Privacy by Design.* In: TRYFONAS, Theo. (Ed.). Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. P. 691-702.

LÉVY, Pierre. Cibercultura. Trad. de Carlos Irineu da Costa, São Paulo: Editora 34, 1999.

_____. O que é virtual? Trad. De Paulo Neves, 5ª reimpressão, São Paulo: Editora 34, 2001.

LI, C.; Mo. L. and Zhang, D. *Review on UHF RFID Localization Methods*. In IEEE Journal of Radio Frequency Identification, vol. 3, no. 4, pp. 205-215, Dec. 2019, doi: 10.1109/JRFID.2019.2924346. Disponível em https://doi.org/10.1109/JRFID.2019.2924346 (Acesso em 14/01/2022)

LI, J.; Li, J.; Yuan, R.; Zhang, R. and Fang, B. *Fog Computing-Assisted Trustworthy Forwarding Scheme in Mobile Internet of Things*. In IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2778-2796, April 2019, doi: 10.1109/JIOT.2018.2874808. Disponível em https://doi.org/10.1109/JIOT.2018.2874808 (Acesso em 14/01/2022)

LIMBERGER, Têmis. Da Evolução Do Direito A Ser Deixado Em Paz À Proteção Dos Dados Pessoais. Revista do Direito, Santa Cruz do Sul, p. 138-160, jul. 2008. ISSN 1982-9957. Disponível em: https://online.unisc.br/seer/index.php/direito/article/view/580/472 . (Acesso em 14/01/2022)

LIN, Yi-Bing et al. *NB-IoT talk: A Service Platform For Fast Development of NB-IoT Applications*. IEEE Internet of Things Journal, v. 6, n. 1, p. 928-939, 2018.

LIU, Mingliu et al. *Combinatorial-Oriented Feedback For Sensor Data Search In Internet Of Things*. IEEE Internet of Things Journal, v. 7, n. 1, p. 284-297, 2019.

LIU, Xuyang et al. *Overview Of Spintronic Sensors With Internet Of Things For Smart Living*. IEEE Transactions on Magnetics, v. 55, n. 11, p. 1-22, 2019.

LIU, Yinqiu et al. Tornado: *Enabling Blockchain In Heterogeneous Internet Of Things Through A Space-Structured Approach*. IEEE Internet of Things Journal, v. 7, n. 2, p. 1273-1286, 2019.

LOCKEED MARTIN. *The Cyber Kill Chain*. Disponível em: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Acesso em 14/01/2022)

LOMBARTE, Artemi Rallo. *Del Derecho A La Protección De Datos A La Garantia De Nuevos Derechos Digitales*. In: LOMBARTE, ARTEMI Rallo (org.). *Tratado de Protección de Datos. Actualizado Con la Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales*. Valencia, Tirant lo Blanch, 2019, capítulo 1, p. 23-52.

LORENZETTI, Ricardo Luis. *Informática, Cyberlaw, E-Commerce in Tratado de los Contratos*, Tomo III, Capítulo LXVII, Santa Fé, Argentina: Rubinzal-Culzoni Editores, abril de 2000 e *In* Direito & Internet - Aspectos Jurídicos Relevantes, obra coletiva, São Paulo: Edipro, 2000.

_____. *Comercio Electrónico*, Buenos Aires: Abeledo-Perrot, 2001.

MA, Zheng et al. *High-Reliability And Low-Latency Wireless Communication For Internet Of Things: Challenges, Fundamentals, And Enabling Tchnologies*. IEEE Internet of Things Journal, v. 6, n. 5, p. 7946-7970, 2019.

MACCROY, Frank; KATSAMAKAS, Evangelos. *Competition of Multi-Platform Ecosystems in the IoT*. Disponível em: https://ssrn.com/abstract=3737414. (Acesso em 14/01/2022)

MACHADO, Charles M. LGPD e a Administração Pública: Qual o Nível de Segurança dos Seus Dados na Administração Pública? 2021. Disponível em: https://jus.com.br/artigos/94123/lgpd-e-a-administracao-publica (Acesso em 14/01/2022)

MACHADO, F. I. S; RUARO, R. L. Publicidade Comportamental, Proteção de Dados Pessoais e o Direito do Consumidor. Conpedi Law Review, v.3, n. 2, p. 421-440, 2017. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/11550/2/PUBLICIDADE_COMPORTAMENTAL_PROTECAO_DE_DADOS_PESSOAIS_E_O_DIREITO_DO_CONSUMIDOR.pdf. (Acesso em 14/01/2022)

MACHADO, Gabriel C. Agronegócio Brasileiro: Importância E Complexidade Do Setor. Disponível em: https://www.cepea.esalq.usp.br/br/opiniao-cepea/agronegocio-brasileiro-importancia-e-complexidade-do-setor.aspx (Acesso em 14/01/2022)

MADDOX, T. Cisco: *The Internet Of Everything Is At Tipping Point*. TechRepublic, 18 fev. 2018. Disponível em: https://www.techrepublic.com/article/cisco-the-internet-of-everything-is-at-tipping-point/ (Acesso em 14/01/2022)

MAGRANI, Eduardo. A Internet Das Coisas. Rio de Janeiro: FGV Editora, 2018.

MATTERN, F. e Floerkemeier, C. *From the Internet of Computers to the Internet of Things*. In: Sachs K., Petrov I., Guerrero P. (eds) From *Active Data Management to Event-Based Systems and More*. Lecture Notes in Computer Science, vol 6462. 2010. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-17226-7_15 (Acesso em 14/01/2022)

MCROBERTS, Michael. Arduino básico. Novatec Editora, 2018.

MEIRA, Silvio. Sinais Do Futuro Imediato, #1: Internet Das Coisas. Ikewai, Recife, Dez. 2016. Disponível em https://silvio.meira.com/silvio/sinais-do-futuro-imediato-1-internet-das-coisas/ https://doi.org/10.1007/978-3-642-17226-7_15 (Acesso em 14/01/2022)

MENDES, Laura Schertel. A Tutela Da Privacidade Do Consumidor Na Internet: Uma Análise À Luz Do Marco Civil Da Internet E Do Código De Defesa Do Consumidor. In: DE LUCCA, N.; SIMÃO FILHO, A. ; LIMA, C.R.P de. Direito e internet III: Marco Civil da Internet (Lei n. 12.965/2014). Tomo I. São Paulo: Quartier Latin, 2015, pp. 471-502.

MENDES, Luis Gustavo. 5 Formas De Aproveitar A Internet Das Coisas Na Agricultura E Tornar Sua Fazenda Mais Rentável. O Blog da Aegro. 22 de dezembro de 2020. Disponível em: https://blog.aegro.com.br/internet-das-coisas-na-agricultura/ (Acesso em 14/01/2022)

MEOLA, Andrew. *How The Internet Of Things Will Affect Security & Privacy*. Business Insider, 24 Ago. 2016. Disponível em https://www.insider.com/internet-of-things-security-privacy-2016-8 (Acesso em 14/01/2022)

MONTOYA, Edwin Andrés Quiroga et al. *Propuesta De Una Arquitectura Para Agricultura De Precisión Soportada en IoT*. Revista Ibérica de Sistemas e Tecnologias de Informação, n. 24, p. 39-56, 2017.

MORAES, Alexandre de. Direito Constitucional. 13. Ed. São Paulo: Atlas, 2003. P.116

MORAES, Alexandre de.; HAYASHI, Victor Takashi. Segurança em Iot: Entendendo Os Riscos E Ameaças Em Internet Das Coisas. Alta Books. 2021.

MORAL MACHINE. Disponível em: https://www.moralmachine.net/ (Acesso em 14/01/2022)

MOROZOV, Evgeny. Big Tech: A Ascensão Dos Dados e a Morte Política. Tradução de Claudio Marcondes. Ubu Editora LTDA-ME, 2018.

MORRIS, Ian. *Why the west rules-for now: The Patterns Of History And What They Reveal About The Future*. Profile books, 2010.

NAIME, Laura; GERBELLI, Luiz Guilherme; BASÍLIO, Patrícia. Dona De 1/5 Do PIB, Indústria Encolhe 0,2% E Enfrenta Dificuldades Na Retomada; Veja Os 5 Entraves Principais. Disponível em: https://g1.globo.com/economia/noticia/2021/09/01/dona-de-15-do-pib-industria-encolhe-02percent-e-enfrenta-dificuldades-na-retomada-veja-os-5-entraves-principais.ghtml (Acesso em 14/01/2022)

NASCIMENTO, Rodrigo. O Que, De Fato, É Internet Das Coisas E Que Revolução Ela Pode Trazer? Computerworld, 12 de março de 2015. Disponível em: https://computerworld.com.br/2015/03/12/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer (Acesso em 13/01/2022).

NEGRI, S. M. C. A; KORMAZ, M. R. D. C. R. A Normatividade Dos Dados Sensíveis Na Lei Geral De Proteção De Dados: Ampliação Conceitual E Proteção Da Pessoa Humana. Revista de Direito, Governança e Novas Tecnologias, Goiânia, v. 5, n.1, p. 63-85, jan/jun de 2019.

NEVES, Flávio S.; GARCIA, Vinicius Cardoso; BONFIM, Michel Sales. Um Mecanismo Para Recomendação De Algoritmos De Anonimização De Dados Baseado No Perfil Dos Dados Para Ambientes Iot. In: Workshop de Teses e Dissertações (WTDSOFT) – Congresso

Brasileiro De Software: Teoria e Prática (CBSOFT), 12. 2021, Joinville. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2021 . p. 10-18.

NORMAN, Jeremy M. *Kevin Ashton Invents The Term "The Internet Of Things*". Disponível em: https://www.historyofinformation.com/detail.php?id=3411 (Acesso em 14/01/2022)

NOURA, Mahda.; ATIQUZZAMAN, Mohammed.; GAEDKE, Marting. *Interoperability in Internet of Things: Taxonomies and Open Challenges.* Mobile Networks and Applications, v. 24, issue 3, p. 796-809, jun. 2019. Disponível em: https://doi.org/10.1007/s11036-018-1089-9 . (Acesso em 14/01/2022)

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO .BR. Estatísticas. Disponível em: https://registro.br/dominio/estatisticas/ (Acesso em 14/01/2022)

_____. Pesquisa Sobre O Uso Das Tecnologias De Informação e Comunicação Nos Domicílios Brasileiros – TIC Domicílios 2018. Disponível em: https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2018/ (Acesso em 14/01/2022)

O'REILLY (2005). *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*. 2005. Disponível em: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (Acesso em 13/01/2022).

OJHA, Tamoghna et al. *DVSP: Dynamic Virtual Sensor Provisioning In Sensor–Cloud-Based Internet Of Things*. IEEE Internet of Things Journal, v. 6, n. 3, p. 5265-5272, 2019.

OLMSTEAD v. United States, 277 U.S. 438 (1928). Nos. 493, 532 and 533. U.S. Supreme Court. Disponível no idioma original em inglês: https://supreme.justia.com/cases/federal/us/277/438/ (Acesso em 13/01/2022).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT – OECD. *The Internet of Things: Seizing the Benefits and Addressing the Challenges. Ministerial Meeting on the Digital Economy, Background Report, 2016*. OECD Digital Economy Papers. 2016. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/the-internet-of-things_5jlwvzz8td0n-en (Acesso em 14/01/2022).

ORTIGOSA, Adrián Palma. *Contexto Normativo de la Protección de Datos Personales*. In: FERNÁNDEZ, Juan Pablo Murga; SCAGLIUSI, María de los Ángeles Fernández; TEJADA, Manuel Espejo Lerdo de; CABRERA, Sara Lorenzo; ORTIGOSA, Adrián Palma (orgs.). Protección de Datos, Responsabilidad Activa y Técnicas de Garantia. Adaptado a la nueva Ley Orgánica 3/2018, de 5 deciembre, de Protección de Datos Personales y garantia de los derechos digitales. Saragoça: Reus, 2018, pp. 9-23 (capítulo 1).

OSAMY, Walid; KHEDR, Ahmed M.; SALIM, Ahmed. *ADSDA: Adaptive Distributed Service Discovery Algorithm for Internet of Things Based Mobile Wireless Sensor Networks.In IEEE Sensors Journal, vol. 19, no. 22, pp. 10869-10880, 15 Nov.15, 2019, doi: 10.1109/JSEN.2019.2930589.* Disponível em https://doi.org/10.1109/JSEN.2019.2930589 (Acesso em 14/01/2022).

OWASP Top Ten. Disponível em : https://owasp.org/www-project-top-ten/ (Acesso em 14/01/2022).

PAIVA, Bruno Fábio de Farias. Uma abordagem baseada em componentes para o desenvolvimento de aplicações pervasivas cientes de contexto de ambiente: foco em sensores. 2016. 109 f. Dissertação (Mestrado em Ciência da Computação) – Programa de Pós-Graduação em Ciência da Computação, Centro de Engenharia Elétrica e Informática, Universidade Federal de Campina Grande, Paraíba, Brasil, 2016.

PAN, Xin-yu, MA, Jing-zhong, WU, Cheng-xia. *Product Pricing Considering The Consumer Preference Based On Internet Of Things*. Cluster Computing (2019) 22:S15379–S15385. Disponível em https://doi.org/10.1007/s10586-018-2601-5 (Acesso em 14/01/2022).

PASQUALE Frank. *The Black Box Society – The Secret Algorithms That Control Money and Information*. Cambridge and London: Harvard University Press, 2015.

PAUL, Biswajit. *A Novel Mathematical Model to Evaluate the Impact of Packet Retransmissions in LoRaWAN*. In IEEE Sensors Letters, vol. 4, no. 5, pp. 1-4, May 2020, Art no. 7500204, doi: 10.1109/LSENS.2020.2986794. Disponível em https://doi.org/10.1109/LSENS.2020.2986794 (Acesso em 14/01/2022).

PECORARO, Rossano (org.). Os Filósofos: Clássicos Da Filosofia. V. I. De Sócrates a Rosseau. Vozes. Petrópolis: Puc-Rio de Janeiro. 2008.

PEPPET, Scott R. *Regulation The Internet Of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*. Forthcoming Texas Law Review, 2014, p. 1-78. Disponível em https://ssrn.com/abstract=2409074 (Acesso em 14/01/2022).

PÉREZ LUÑO, Antonio Henrique. *Cibernetica, Informatica y Derecho (Un análisis metodológico),* Bologna: Publicaciones del Real Colegio de España, 1976.

PFEIFFER, Roberto Augusto Castellanos. "A Saga da Autoridade Nacional de Proteção de Dados: do veto à Lei nº 13.853/2019". In: DE LUCCA, N.; SIMÃO FILHO, A.; de LIMA, C.R.P (coords.). Direito e Internet IV: Lei Geral de Proteção de Dados. São Paulo, Quartier Latin, 2019.

_____. *Digital Economy, Big Data and Competition Law*. (February 27, 2019). In: Market and Competition Law Review, volume III, n. 1, April 2019, p. 53-89. Available at SSRN: https://ssrn.com/abstract=3440296

_____. *Internet of things and competition law: main challenges*. Extended abstract, provisional version to be presented at the 15th annual ASCOLA Conference. Disponível em: https://law.haifa.ac.il/images/ASCOLA/Pfeiffer_paper.pdf . (Acesso em 14/01/2022).

PIERLEONI, Paola et al. *The Scrovegni Chapel Moves Into The Future: An Innovative Internet Of Things Solution Brings New Light To Giotto's Masterpiece*. IEEE Sensors Journal, v. 18, n. 18, p. 7681-7696, 2018.

PIZARRO, Ramón Daniel. *El Deber De Información En Los Contratos Informáticos*. *In* Revista de Derecho Privado y Comunitario, vol 3, *Contratos modernos*, Santa Fé: Rubinzal-Culzoni, 1994.

PLOUFFE, James. *The Ghost Of Iot Yet To Come: The Internet Of (Insecure) Things In 2017*. Mobile Iron, 23 dez. 2016. Disponível em: https://www.mobileiron.com/en/blog/ghost-iot-yet-come-internet-insecure-things-2017 (Acesso em 14/01/2022).

PONCIANO, Lesandro et al. *Designing for Pragmatists and Fundamentalists: Privacy Concerns and Attitudes on the Internet of Things.* Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems, v.1, n.1. 2017.

PÖTTNER, Wolf-Bastian et al. *Constructing Schedules For Time-Critical Data Delivery In Wireless Sensor Networks*. ACM Transactions on Sensor Networks (TOSN), v. 10, n. 3, p. 1-31, 2014.

RADOMIROVIC, Saša. *Towards A Model For Security And Privacy In The Internet Of Things*. In: international workshop on the security of the internet of things, I., 2010, Tóquio. Anais… Tóquio: Keyo University, 2010.

RAFIQUE, Wajid et al. *An Application Development Framework For Internet-Of-Things Service Orchestration*. IEEE Internet of Things Journal, v. 7, n. 5, p. 4543-4556, 2020.

RAND CORPORATION. Disponível em: https://www.rand.org. (Acesso em 14/01/2022).

RANI, Rinki; KUMAR, Sushil; DO HARE, Upasana. *Trust Evaluation For Light Weight Security In Sensor Enabled Internet Of Things: Game Theory Oriented Approach*. IEEE Internet of Things Journal, v. 6, n. 5, p. 8421-8432, 2019.

RASHID, Md Mamunur et al. *A Survey On Behavioral Pattern Mining From Sensor Data In Internet Of Things*. IEEE Access, v. 8, p. 33318-33341, 2020.

REALE, Miguel. Lições Preliminares De Direito. 27 ed. São Paulo: Saraiva 2002, p. 18.

RIAÑO RIAÑO, Diana Patricia. Integração de Dados Estatísticos Sociais no Desenvolvimento de uma Possível Arquitetura para a Internet das Coisas. Tese de Doutorado. Universidade de São Paulo. Disponível em https://www.teses.usp.br/teses/disponiveis/3/3142/tde-20122016-081503/publico/DianaPatriciaRianoRianoCorr16.pdf (Acesso em 14/01/2022).

RICOLFI, Marco. *IoT and the Ages of Antitrust*. Working Paper n. 4, 2017. Disponível em: https://nexacenter.org/nexacenterfiles/4.%20ricolfi.pdf. (Acesso em 14/01/2022).

RODOTÀ, Stefano. A Vida Na Sociedade Da Vigilância (coord. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, p. 23-232, 2008.

ROMAN, Rodrigo; ZHOU, Jianyng; LOPEZ, J. *On The Features And Challenges Of Security And Privacy In Distributed Internet Of Things.* Computer Networks, n. 57, p. 2266-2279, 2013.

_____; NAGERA, Pablo; LOPEZ, J. *Securing The Internet Of Things*. IEEE Computer, v. 44, p. 51-58, 2011. doi: 10.1109/MC.2011.291. Disponível em https://doi.org/10.1109/MC.2011.291 (Acesso em 14/01/2022).

ROSE, Karen.; ELDRIDGE, Scott.; CHAPIN, Lyman. *The Internet Of Things: An Overview — Understanding The Issues And Challenges Of A More Connected World*. The Internet Society, p. 1, 4, out. 2015. Disponível em: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf.

RUSSEL, Stuart; NORVIG, Peter (2009). "*26.3: The Ethics and Risks of Developing Artificial Intelligence". Artificial Intelligence: A Modern Approach*. Prentice Hall. ISBN 978-0-13-604259-4.

SANS. CWE/SANS. *Top 25 Most Dangerous Software Errors*. Disponível em: https://www.sans.org/top25-software-errors/ (Acesso em 14/01/2022).

SANCHO LÓPEZ, Marina. *La Protección de Datos en el Reino Unido: Evolución del Right to Privacy y escenarios Post-Brexit*. Pamplona: Aranzadi, 2019, pp. 133-162 (capítulo 4, "Reflexiones en torno a conceptos clave").

SANTOS, Carlos Cesar.; SALES, Jefferson David de Araújo. O Desafio Da Privacidade Na Internet Das Coisas. Revista Gestão. Org, v. 13, Edição Especial, 2015, p.282-290. Disponível em: https://periodicos.ufpe.br/revistas/gestaoorg/article/view/22115 (Acesso em 15/01/2022)

SANTOS, Pedro Miguel Pereira. Internet Das Coisas: O Desafio Da Privacidade. Dissertação (mestrado em sistemas de informação organizacionais) — Escola Superior de Ciências Empresariais, Instituto Politécnico de Setúbal, 2016.

SANTOS, Manoel Joaquim Pereira dos. Considerações Iniciais Sobre A Proteção Jurídica Das Bases De Dados, Artigo Publicado Na Obra Coletiva Direito & Internet - Aspectos Jurídicos Relevantes, São Paulo: Edipro, 2000.

_____. A Nova Lei do Software: Aspectos Controvertidos da Proteção Autoral. In: Revista da Associação Brasileira da Propriedade Intelectual nº 29, julho/agosto de 1997.

_____. e ROSSI, Mariza Delapieve. Aspectos Legais do Comércio Eletrônico - Contratos de Adesão. In: Revista de Direito do Consumidor n.º 36.

SANTOS, Maria Cecília de Andrade. Contratos Informáticos - Breve Estudo. Revista dos Tribunais n.º 762, abril de 1999.

SCHNEIER, Bruce. Segurança .Com: Segredos E Mentiras Sobre a Proteção na Vida Digital. Campus, 2001.

_____. *Security and the Internet of Things*. Schneier on Security. 01 de Fevereiro, de 2017. Disponível em https://www.schneier.com/blog/archives/2017/02/security_and_th.html/ (Acesso em 13/01/2022)

SHAMSZAMAN, Zia Ush; ALI, Muhammad Intizar. *Toward A Smart Society Through Semantic Virtual-Object Enabled Real-Time Management Framework In The Social Internet Of Things*. EEE Internet of Things Journal, vol. 5, no. 4, pp. 2572-2579, Aug. 2018, doi: 10.1109/JIOT.2017.2779106. Disponível em https://doi.org/10.1109/JIOT.2017.2779106 (Acesso em 14/01/2022)

SHYLESH, S. *A Study of Software Development Life Cycle Process Models* (June 10, 2017). Disponível em http://dx.doi.org/10.2139/ssrn.2988291 (Acesso em 13/01/2022)

SICARI, Sabrina.; RIZZARDI, Alessandra.; GRIECO, Luigi Alfredo.; COEN-PORISINI, Alberto. *Security, Privacy And Trust In Internet Of Things: The Road Ahead*. Computer Networks, Volume 76, 15 January 2015, Pages 146-164. Disponível em https://doi.org/10.1016/j.comnet.2014.11.008 (Acesso em 15/01/2022)

SILVA, N. C. Inteligência Artificial. In: Inteligência Artificial e Direito: ética, regulação e responsabilidade. São Paulo, SP: Thomson Reuters Brasil, 2019. p. 35.

SINCLAIR, Bruce. IoT: Como usar a Internet Das Coisas para lavancar seus negócios. Autêntica Business, 2018.

SINGH, Vivek K.; MANI, Ankur; PENTLAND, Alex. *Social Persuasion In Online And Physical Networks*. Proceedings of the IEEE, v. 102, n. 12, p. 1903-1910, 2014. doi: 10.1109/JPROC.2014.2363986. Disponível em https://doi.org/10.1109/JPROC.2014.2363986 (Acesso em 14/01/2022)

SKARMETA, Antonio F.; RAMOS, José L. Hernández-Ramos.; MORENO, Victoria M. *A Decentralized Approach For Security And Privacy Challenges In The Internet Of Things*. In: 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 67-72, doi: 10.1109/WF-IoT.2014.6803122. Disponível em https://doi.org/10.1109/WF-IoT.2014.6803122 (Acesso em 14/01/2022)

SOKOLOVA, Lara. O que saber sobre agricultura inteligente usando IoT: Como a tecnologia está transformando a produção de alimentos e os desafios de sua implementação e segurança dos sistemas. Disponível em: https://forbes.com.br/forbesagro/2021/09/o-que-saber-sobre-agricultura-inteligente-usando-iot/ (Acesso em 14/01/2022)

SONY PICTURES. *Jeopardy! América favorite quiz show*. Disponível em: https://www.jeopardy.com/ (Acesso em 14/01/2022)

SPIEKERMANN S, Korunovska J. *Towards A Value Theory For Personal Dat*a. Journal of Information Technology. 2017;32(1):62-84. doi:10.1057/jit.2016.4 Disponível em https://doi.org/10.1057/jit.2016.4 (Acesso em 14/01/2022)

SRINIVASAN, C.R. Rajesh, B. Saikalyan, P. Premsagar, K. and Yadav, E.S. *A Review on the Different Types of Internet of Things (IoT)*. Jour of Adv Research in Dynamical & Control Systems, Vol. 11, No. 1, 2019.

TANEJA, Mohit; JALODIA, Nikita; DAVY, Alan. *Distributed Decomposed Data Analytics In Fog Enabled IoT Deployments*. IEEE Access, v. 7, p. 40969-40981, 2019. doi: 10.1109/ACCESS.2019.2907808 . Disponível em https://doi.org/10.1109/ACCESS.2019.2907808 (Acesso em 14/01/2022)

TANEMBAUM, A. *Computer Networks*. Prentice Hall Professional Technical Reference, 4th edition. 2002.

TEILHARD DE CHARDIN. In: WIKIPÉDIA: a enciclopédia livre. [São Francisco, CA: Fundação Wikimedia]. Disponível em https://pt.wikipedia.org/wiki/Teilhard_de_Chardin . (Acesso em 14/01/2022)

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU. ITU-T. Series Y: *Global Information Infrastructure, Internet Protocol Aspects And Next-Generation*

*Networks: Overview of the Internet of Things (Recommendation ITU-T Y.2060).* Aprovado em 15 jul 2012. Disponível em: https://www.itu.int/rec/T-REC-Y.2060-201206-I/en . (Acesso em 14/01/2022)

THEODOROU, Tryfon; MAMATAS, Lefteris. *A Versatile Out-Of-Band Software-Defined Networking Solution For The Internet Of Things*. IEEE Access, v. 8, p. 103710-103733, 2020.

TIMBERG, Craig. *Net Of Insecurity - A Flaw In The Design*. The Washington Post. 30 de maio, 2015. https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/ (Acesso em 14/01/2022)

TOKARNIA, Mariana. Um Em Cada 4 Brasileiros Não Tem Acesso À Internet, Mostra Pesquisa. Agência Brasil. Rio de Janeiro. 29 de abril de 2020. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/um-em-cada-quatro-brasileiros-nao-tem-acesso-internet (Acesso em 14/01/2022)

TRACY, Phillip. *Small Cells: Backhaul Difficulties And A 5G Future*. Disponivel em: https://www.rcrwireless.com/20160711/network-infrastructure/small-cells-tag31-tag99 (Acesso em 14/01/2022)

TRIBUNAL DE CONTAS DA UNIÃO. Relatório de Levantamento sobre Internet das Coisas. Disponível em: https://www.telesintese.com.br/wp-content/uploads/2021/06/028-109-2020-1-AN-Levantamento_Internet-das-coisas.pdf (Acesso em 14/01/2022)

TSCHIDER, Charlotte. *Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age* (February 24, 2018). 96 DENV. U. L. REV. 87 (2018), Disponível em http://dx.doi.org/10.2139/ssrn.3129557 (Acesso em 15/01/2022)

TURNER, S. et. al. *The Exercisability Of The Right To Data Portability In The Emerging Internet Of Things (IoT) Environment*. New Media & Society, 2021, vol. 23(10) 2861-2881.

UCL. *New Peer-Reviewed Article Highlights The Need To Improve Data Portablity*, 13 jul. 2020. Disponível em: https://www.ucl.ac.uk/steapp/news/2020/jul/new-peer-reviewed-article-highlights-need-improve-data-portability . (Acesso em 14/01/2022)

UNIÃO EUROPEIA. Exposição de Motivos (e inteiro teor) do Regulamento Europeu de Proteção de Dados Pessoais (Regulamento UE 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. (Acesso em 14/01/2022)

_____. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* Official Journal of the European Union, 04 May 2016. Disponível em: https://eur-

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. (Acesso em 14/01/2022)

VALTER, Per; LINDGREN, Peter; PRASAD, Ramjee. *The Consequences Of Artificial Intelligence And Deep Learning In A World Of Persuasive Business Models*. IEEE Aerospace and Electronic Systems Magazine, v. 33, n. 5-6, p. 80-88, 2018.

VANBERG, Aysem Diker; ÜNVER, Mehmet Bilal. *The Right To Data Portability In The GDPR And EU Competition Law: Odd Couple Or Dynamic Duo?*. In: European Journal of Law and Technology, v. 8, n. 1, 2017. Disponível em: https://arro.anglia.ac.uk/id/eprint/701565/1/Diker%20Vanberg_2017.pdf (Acesso em 14/01/2022)

VEGA-BARBAS, Mario et al. *Interaction Patterns For Smart Spaces: A Confident Interaction Design Solution For Pervasive Sensitive Iot Services.* IEEE Access, vol. 6, pp. 1126-1136, 2018, doi: 10.1109/ACCESS.2017.2777999. Disponível https://doi.org/10.1109/ACCESS.2017.2777999 (Acesso em 14/01/2022)

VERMESAN, Ovidiu; BACQUET, Joël (Ed.). *Next Generation Internet Of Things: Distributed Intelligence At The Edge And Human Machine-To-Machine Cooperation*. River Publishers, 2019. 300 pp. ISBN-10: 8770220085

_____; FRIESS, P. *Internet of Things - Converging Technologies for Smart Environment and Integrated Ecosystems*. Denmark: River Publisher, 2013, p. 135.

_____. *Internet Of Things – The Call Of The Edge. Everything Intelligent Everywhere.* River Publicshers, 2020, 392pp. ISBN-10: 8770221960

WANG, Mu et al. *Design Of Multipath Transmission Control For Information-Centric Internet Of Things: A Distributed Stochastic Optimization Framework*. IEEE Internet of Things Journal, v. 6, n. 6, p. 9475-9488, 2019. doi: 10.1109/JIOT.2019.2929263. Disponível em https://doi.org/10.1109/JIOT.2019.2929263 (Acesso em 14/01/2022)

WANG, Xiaofan et al. *Privacy-Aware Efficient Fine-Grained Data Access Control In Internet Of Medical Things Based Fog Computing*. IEEE Access, v. 6, p. 47657-47665, 2018.

WEBER, Rolf H. *Internet Of Things: Privacy Issues Revisited*. Computer Law & Security review, v. 31, Elsevier, 2015. Pp 618–627. DOI: 10.1016/j.clsr.2015.07.002. Disponível em https://doi.org/10.1016/j.clsr.2015.07.002 (Acesso em 14/01/2022)

_____. *Internet Of Things - Governance Quo Vadis?* Computer Law & Security Review, v. 29, p. 341-347, 2019. DOI 10.1016/j.clsr.2013.05.010: Disponível em: https://doi.org/10.1016/j.clsr.2013.05.010. (Acesso em 14/01/2022)

WEI, Jiannan et al. *A Privacy-Preserving Fog Computing Framework For Vehicular Crowdsensing Networks*. IEEE Access, v. 6, p. 43776-43784, 2018, doi: 10.1109/ACCESS.2018.2861430. Disponível em https://doi.org/10.1109/ACCESS.2018.2861430 (Acesso em 14/01/2022)

WEISER, Mark. *The Computer for the 21st Century*. Scientific american, v. 265, n. 3, p. 94-105, 1991.

WHITEHOUSE. *Presidents - Dwight D. Eisenhower*. Disponível em: https://www.whitehouse.gov/about-the-white-house/presidents/dwight-d-eisenhower/ (Acesso em 14/01/2022)

_____. *Presidents - John F. Kennedy*. Disponível em: Disponível em: https://www.whitehouse.gov/about-the-white-house/presidents/john-f-kennedy (Acesso em 14/01/2022)

WILLIAMS, Meredydd; NURSE, Jason R. C.; CREESE, Sadie. *The Perfect Storm: The Privacy Paradox and the Internet-of-Things*. In Proceedings of 2016 11Th International Conference on Availability, Reliability and Security (ARES), v. 1, n. 1, p. 644-652, 2016. DOI: 10.1109/ARES.2016.25 Disponível em https://doi.org/10.1109/ARES.2016.25 (Acesso em 14/01/2022)

WRIGHT, Joshua D. *How to Regulate the Internet of Things Without Harming its Future: Some Do's and Don'ts*. Remarks of Commissioner, Federal Trade Commission at the U.S. Chamber of Commerce. Washington, D.C. May 21, 2015. Disponível em: https://www.ftc.gov/system/files/documents/public_statements/644381/150521iotchamber.pdf . (Acesso em 14/01/2022)

WROBEL, Gregory G. *Connecting Antitrust Standards to the Internet of Things*. Antitrust, v. 29, n. 1, p. 62-70, 2014. Disponível em: https://www.vedderprice.com/-/media/files/vedder-thinking/publications/2014/09/connecting-antitrust-standards-to-the-internet-of/files/aba-antitrustconnecting-antitrust-standards-to-the/fileattachment/aba-antitrustconnecting-antitrust-standards-to-the.pdf . (Acesso em 14/01/2022)

WU, Na; LIANG, Qilian. *Sparse Nested Cylindrical Sensor Networks For Internet Of Mission Critical Things*. IEEE Internet of Things Journal, v. 5, n. 5, p. 3353-3360, 2017. doi: 10.1109/JIOT.2017.2736645. Disponível em https://doi.org/10.1109/JIOT.2017.2736645 (Acesso em 14/01/2022)

WU, Qiong et al. *Delay-Sensitive Task Offloading In The 802.11p-Based Vehicular Fog Computing Systems.* IEEE Internet of Things Journal, v. 7, n. 1, p. 773-785, Jan. 2020, doi: 10.1109/JIOT.2019.2953047. Disponível em https://doi.org/10.1109/JIOT.2019.2953047 (Acesso em 14/01/2022)

ZHANG, Ruizhi. *The Application of Fog Computing and Internet of Things Technology in Music Resource Management Model*. IEEE Access, v. 8, p. 11840-11847, 2020, doi: 10.1109/ACCESS.2019.2963199. Disponível em https://doi.org/10.1109/ACCESS.2019.2963199 (Acesso em 14/01/2022)

ZIEGELDORF, Jan Henrik.; MORCHON, Oscar Garcia.; WEHRLE, Klaus. *Privacy In The Internet Of Things: Threats And Challenges.* Security Comm. Networks 2014; 7:2728-2742. Volume 7. DOI 10.1992/sec.795 Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1002/sec.795 (Acesso em 14/01/2022)

ZILIO, Leonardo. Termo E Valor Linguístico: Uma Abordagem Ensaística. Cadernos do IL, n. 42, p. 119-128, 2011.

ZINGALES, Nicolo. *Of Coffee Pods, Videogames, And Missed Interoperability: Reflections For EU Governance Of The Internet Of Things*. TILEC Discussion Paper No. 2015-026, v. 26, 2015. https://dx.doi.org/10.2139/ssrn.2707570 . (Acesso em 14/01/2022)

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Public Affairs, 2019. 704 pp. ISBN-10:1610395697